Harokopio University

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Σχολή: Πληροφορικής &Τηλεματικής
Τμήμα: Πληροφορικής & Τηλεματικής
Πρόγραμμα Μεταπτυχιακών Σπουδών: Πληροφορική και Τηλεματική
Κατεύθυνση: Τηλεπικοινωνιακά δίκτυα και υπηρεσίες τηλεματικής

Τίτλος Εργασίας: Cyber Crime: Using Technology against itself.

Διπλωματική Εργασία

Όνομα φοιτητή: Σιβένας Τρύφων

Αθήνα, [2017]

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Σχολή: Πληροφορικής &Τηλεματικής
Τμήμα: Πληροφορικής & Τηλεματικής
Πρόγραμμα Μεταπτυχιακών Σπουδών: Πληροφορική και Τηλεματική
Κατεύθυνση: Τηλεπικοινωνιακά δίκτυα και υπηρεσίες τηλεματικής

Τριμελής Εξεταστική Επιτροπή

Δρ. Ριζομυλιώτης Παναγιώτης, Επιβλέπων Καθηγητής
Μόνιμος Επίκουρος Καθηγητής, Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου.

Δρ. Καμαλάκης Θωμάς
Επίκουρος Καθηγητής, Τμήμα Πληροφορικής & Τηλεματικής, Χαροκόπειο Πανεπιστήμιο.

Δρ. Αναγνωστόπουλος Δημοσθένης
Καθηγητής, Τμήμα Πληροφορικής & Τηλεματικής, Χαροκόπειο Πανεπιστήμιο.

Ο Σιβένας Τρύφων,

δηλώνω υπεύθυνα ότι:

1) Είμαι ο κάτοχος των πνευματικών δικαιωμάτων της πρωτότυπης αυτής εργασίας και από όσο γνωρίζω η εργασία μου δε συκοφαντεί πρόσωπα, ούτε προσβάλει τα πνευματικά δικαιώματα τρίτων.

2) Αποδέχομαι ότι η ΒΚΠ μπορεί, χωρίς να αλλάξει το περιεχόμενο της εργασίας μου, να τη διαθέσει σε ηλεκτρονική μορφή μέσα από τη ψηφιακή Βιβλιοθήκη της, να την αντιγράψει σε οποιοδήποτε μέσο ή/και σε οποιοδήποτε μορφότυπο καθώς και να κρατά περισσότερα από ένα αντίγραφα για λόγους συντήρησης και ασφάλειας.

Περίληψη στα Ελληνικά

Στόχος της παρούσας διπλωματικής εργασίας είναι η μελέτη του σύγχρονου ηλεκτρονικού εγκλήματος και της μεθοδολογίας που ακολουθείται. Συγκεκριμένα, γίνεται μια ανάλυση στο νομικό πλαίσιο και τα αρχικά βήματα της νομοθεσίας για την αντιμετώπιση του ηλεκτρονικού εγκλήματος. Εν συνεχεία πραγματοποιείται σύγκριση των ποινών για τα ηλεκτρονικά εγκλήματα σε χώρες όπου έχει θεσπιστεί αντίστοιχο νομικό πλαίσιο. Σε δεύτερο επίπεδο γίνεται μια μελέτη στη ζημία που έχει προκαλέσει το ηλεκτρονικό έγκλημα τα τελευταία έτη. Ακολούθως πραγματοποιείται ανάλυση στη λογική, συμπεριφορά και σκεπτικό του σύγχρονου ηλεκτρονικού εγκληματία. Πραγματοποιείται λεπτομερής αναφορά στη μεθοδολογία που ακολουθούν για να αποσπάσουν πληροφορίες και δεδομένα τα οποία μπορούν είτε να χρησιμοποιήσουν είτε να μεταπωλήσουν. Επίσης γίνεται αναφορά στο παράνομο διαδίκτυο και στα κρυπτο κανάλια επικοινωνίας. Εκτενής ανάλυση γίνεται στην ανωνυμοποιησή τους αλλά και στη λογική της αποφυγής έκθεσης προσωπικών τους δεδομένων που μπορεί να οδηγήσουν στη σύλληψη τους. Ανάλυση πραγματοποιείται σε επιχειρησιακή λογική, μεθόδους προστασίας, μεθόδους επιθέσεων και μεθοδολογίες που αξιοποιούν τα κλεμμένα δεδομένα. Επιπροσθέτως μελέτη γίνεται στα εργαλεία που χρησιμοποιούν οι ηλεκτρονικοί εγκληματίες για να πραγματοποιούν τις δραστηριότητες τους. Τέλος πραγματοποιείται αναφορά για τους μηχανισμούς που υπάρχουν σήμερα για την αντιμετώπιση του ηλεκτρονικού εγκλήματος αλλά και για την λογική αποζημίωσης των θυμάτων του ηλεκτρονικού εγκλήματος.

Λέξεις κλειδιά: Ηλεκτρονικό έγκλημα, ηλεκτρονική απάτη, ανωνυμοποίηση, μεθοδολογία εγκλήματος, νομοθεσία εγκλήματος.

Harokopio University of Athens
Department of Informatics and Telematics

Master thesis in:

Cyber Crime: Using Technology against itself.

Name: Sivenas Tryfon

Semester: 3rd

ID number: 15210

e-mail: tryfon@sivenas.eu

Abstract

This thesis is focused in analyzing a new form of crime that has developed over the years and is inseparably linked with the technological evolution of the 21st century. Described in detail are the aspects of how cyber criminals operate, their motives, techniques and methods of bypassing various security systems. In depth analysis of deploying and maintaining cybercriminal operation security, methodologies, solutions and issues. This thesis contains the most up to date methods used by cybercriminals in order to illegally acquire valuable data such as, credit card numbers, login details to e-banking, email accounts. Written in detail is the way cybercriminals use stolen data and how they are sold at underground marketplaces and the deep web. Also included is an extensive research of the legal legislation regarding cybercrime worldwide and the global organizations created to protect and inform citizens. Finally, an analysis on the way cybercriminal departments handle cybercriminal cases around the globe.

Keywords: Cyber Crime, Crackers, Operation Security, computer crime legislation, online fraud.

Acknowledgements

I would like to thank my Supervisor Dr. Rizomiliotis Panagiotis for his tremendous help and support on completing this master thesis in the very interesting and challenging field of cybercrime.

On a second note I would also like to thank, Mr. Richard Boscovich head of Microsoft's Digital Crime Unit and Miss Angie Lyndon security analyst at Microsoft for sharing their valuable time and assisting me in completing this thesis.

Also Mr. Tomaseto Gianelli, cybersecurity expert at Symantec for his insights, guidance and his input in writing this thesis from a different point of view.

Mr. Lorenzo Quatrini head of the antifraud department in Amazon, thank you for your help, guidelines, assistance and tips. Thanks also for that complementary enrollment on the Amazon prime student book rental project and for your recommendations.

My warmest regards for your help in assisting me to carry out this master thesis and for sharing your valuable time and resources with me in both emails and in Skype.

Finally, I would like to thank the US team of Maxmind that did let me study the source code of the algorithm and for the compliment trial.

Contents

Picture Database

Statement of Original authorship

The work included in this thesis, hasn't been published or used by any other University. To the best of my insight and conviction, the proposal contains no material already distributed or composed by someone else aside from where due reference is made.

On a second note, this thesis is here by available for digital distribution for academic, scientific and backup purposes of any form to Harokopio's University Library and repository.

Introduction

Based on the initial concept of computer networking, an idea conceived by Joseph Carl Robnet Licklinder professor of Massachusetts Institute of Technology, until this vary day, a lot of things have evolved and changed. Since Gordon Moore's law in the early beginnings of 1980's a new era begun of the modern technological - digital revolution.

This information and telecommunications revolution has contributed to great advancements over the last 20 years, whereas personal computers, smartphones, tablets, hybrid devices, wearables are embedded to modern everyday life. As far as networking goes, huge advancements where made as well on the telecommunication front where the internet took its place in modern society. In short term the internet is a network of networks consisting private, academic, business, corporate and public networks linking them globally via networking technologies, topologies and protocols. The internet contains tremendous amount of information, resources and services as well. The internet has revolutionized the way people get educated, work and communicate. Moving forward from web 1.0 to web 2.0 information sharing came to a new level.

This combination of technological and networking advancement has resulted into an information explosion that is actually changing the modern social construction economy, health, governments, warfare and even education. That is why this modern society is rightfully called as "information" society. It is calculated than in an average day internet users create over 2,5 quintillion bytes of data based on IBM's calculations. Furthermore, IBM calculates that by 2020 the amount of everyday information will increase up to 44 zettabytes of data. It is well worth mentioning that in 2016 over 46 per cent of the world population was connected to the internet daily, this means 3.424.971.237 individuals logged online every day. (internet live stats, 2016)

It is stunning that the issue of the IPv4 exhaustion came along and IPv6 came to assist and actually fix some security flaws IPv4 had by default. In the past two decades internet and cyberspace in general played a major role in everyday modern life. Countries, companies, corporations and individuals rely on the internet as their day to day partner in their activities.

Utilizing web 2.0 social media brought the world to new means of communication thus virtually eliminating issues and disturbances of the past. Countries and corporations have changed the way their economies work. Relying on security and availability the aforementioned entities created digital economies.

Pairing digital economies with the ease of high tech products embedded in day to day life, ecommerce has grown in a rapid way the last years.

Not only that but one is able to understand that users have switched from the ecommerce and computer usage and went to more compact solutions; mobile smartphones, thus starting the age of mobile commerce. Mobile commerce inside the protective bubble of e commerce grew rapidly as well.

Today individuals are able to make purchases, view newspaper and chat with their friends using a mobile smartphone or a tablet.

However even though the internet has revolutionized the way societies used to work and many individuals rely on it, it isn't safe by default. Major security flaws are to be found in almost every form available. Either it is a bad implementation or a software related issue, the security flaw remains.

Since these flaws are public, anyone with basic logic can see them or reverse engineer them. Today there are individuals browsing and surfing with the main purpose of locating security "flaws". These individuals may have good or bad intentions. In most reported cases, it is the other way around. Purpose of this thesis is to describe those individuals that have bad intentions regarding online security, widely known as cybercriminals. Cybercrime is a tremendous issue regarding online security that can damage countries, governments, companies and individuals as well.

1. Semantic approach of Cybercrime.

It is a fact that the information society described above isn't only a society of knowledge and development. The internet could be described as a copy of the regular society that contains every type and category of individual. This indeed means that criminals are using the internet and its services as well for illegal activities. A huge plus is the general feeling that the internet provides to its users; anonymity, thus allowing certain individuals to commit actions they wouldn't commit in real life. (Viano, 2016)

Furthermore, this feeling is cultivated due to the fact that criminals can't be exposed by showing their face thus revealing their identity. Criminals feel safer on the internet since they can easily pose as a different individual online by using several applications that actually assist in concealing their true identity and data. It goes without saying that using these applications and practices online does in fact pose as an issue in law enforces trying to locate the aforementioned criminal.

Opposed to regular real life crime, cybercrime can occur in seconds without the need of the criminal actually leaving his home. Today in order to commit a cybercrime no special equipment is need apart from a computer and internet access. Cybercriminals could have extended knowledge or basic knowledge. However, cybercriminals that aren't in fact knowledgeable often buy services from knowledgeable ones and do a form of outsourcing. (Wild, MacEwan & Weinstein, 2011)

Comparing to regular crime, cybercrime is considered to be easier for individuals that have resources and basic knowledge. This is why lately cybercrime has become a major issue posing as a threat to every individual using the internet.

As a conclusion one would say that cybercrime can be performed by everyone and can hurt anyone. Truth of the matter is that the internet wasn't created in a well-structured manner it is classless and it does carry ambiguous ethics. Based on the aforementioned reasons this is why cybercrime has become a major target for both cybercriminals and organized crime migrating to online offences. (Wall, 2007)

The term cybercrime arose in order to put under one "umbrella" every new form of crime that resulted from the rapid technological advancements and the wide usage of the internet. (Yar, 2013) In Greek legal legislation, the word cybercrime describes a vast amount of online crimes. However, abroad it seems that cybercrime is also known as digital crime, ecrime, electronic crime, cyberspace crime, economic cybercrime, identity theft crime and has indeed many categorizations. (Marion, 2016)

Truth of the matter is that a clear definition of cybercrime doesn't exist yet since legal legislation and frameworks around the globe are still taking small steps. In order to successfully articulate the cybercrime term one should reach out companies and agencies responsible of handling such cases.

According to Symantec, cybercrime is every illegal activity carried away with the usage of computer or computer network. It is understandable that is a very broad definition however Symantec points out that cybercrime is at higher risk now based on the fact that there is a sheer number of connected people and devices online.

On top of that Symantec shares two facts on their 2016 cybersecurity assessment; cybercrime has actually surpassed illegal drug trafficking and it is the top "moneymaker" and secondly every three seconds an individual's identity is stolen as a part of cybercriminal activities. (Symantec, 2016)

Europe, and specifically Europol's department responsible of Cybercrime, known as EC3 defines cybercrime as the criminal activity carried out by using a computer that has the purpose of illegally making profit of exploited data. It seems Europol's and Interpol's approach regarding cybercrime is purely focused on online economic theft. (EC3, 2015)

Looking at the Greek agency responsible of handling cybercriminal activities, cybercrime is considered to be the criminal actions committed with the use of computers and data processing systems and are in fact punishable by specific penalties according to Greek Legislation. Furthermore, Greek Legislation, based on the European Legal Framework regarding cybercrime, categorizes online crimes into two types; crimes with the usage of computer and crimes carried out on the internet by using a computer. (Greek Cyber Crime Centre, 2016)

On the other side of the globe, in the United States, the Federal Bureau of Investigations classifies cybercrime as the second largest threat the last five years. FBI defines cybercrime as the issue that is created or occurs in a computer network when a perpetrator violates the integrity, availability and confidentiality of computer systems physical or virtual with aim of abusing data. Clearly the Federal Bureaus definition includes distributed online crimes as well. (FBI, 2016)

According to reports and statistics of agencies, companies and corporations responsible of cybercrime prevention the most common forms of cybercrime are:

- Cracking (may be referred to as hacking), it's one of the most used methods cybercriminals use to illegally attain data, illegally access information systems and computers with the target of acquiring sensitive information. By manipulating or exploiting vulnerabilities crackers are able to gain unauthorized access to protected systems and resources in general. (Erickson, 2015)

Cracking has many classifications and methodologies that will be studied extensively in the next chapter. Recent example of cracking is the yahoo attack that took place in December of 2016 where 1 billion email accounts where compromised.

- Second in line comes the act of identity theft, it is widely used by every form of cybercriminal, seasoned or new. Identity theft is quite easy to implement and it actually is the criminal pretending to be a different individual. Identity theft is used in conjunction with other criminal activities and is considered to be a very profitable one. Examples of identity theft can lead to a cybercriminal getting a credit card issued in a victim's information without his knowledge. (Jewkes & Yar, 2009)
- Spreading malware, is one widely used online crime as well although considered to be an offshoot of cracking. There are several types of malware with different capabilities. Malwares are extensively studied in the next chapter. Malwares can assist a cybercriminal gathering vast amounts of data. They are malicious software with many abilities such as, monitoring keystrokes, getting remote access to the victim's workstation, requesting ransom to unlock the hard drive, getting root access or even escalating privileges are some examples of malware. (Elisan, 2012)
- Money Laundering, although this term is a bit old and didn't have a direct relation with cybercrime, money laundering has become easier with the internet. Since it is considered by FBI a "white collar" crime many criminals offer these types of services. Using different methodologies and channeling money through different channels, authorities are unable to locate the original source. The money laundering scheme is a quite profitable one amongst online fraudsters due to the vast amount of payment processors and gateways available online and due to the fact of the recent growth of cryptocurrencies. (Goodman, 2016)
- Online economic fraud, or scams, these are activities that cybercriminals carry out in order to monetize. Using stolen credit cards, or accessing stolen information on bank accounts cybercriminals are able to steal online. There are many variations and strategies carried out by cybercriminals today that are written in detail in the chapter bellow as well.
- Child pornography.
- Pirated software and general copyright infringement issues. (Mitrou, 2016)

Bottom line, based on the legal framework and the organizations that study and protect individuals of cybercrime there are two major categories regarding cybercrime:

- Crimes that are made online and have multiple targets and victims including information systems as well

- Crimes where the computer is aiding the crimes, thus used as a tool in completing a crime. (Mitrou, 2016)

An attempt to analyze and articulate the term cybercrime including every aspect of it would be, every criminal activity carried out with a computer or online using electronic communications that seeks to obtain unlawful access and data in order illegally acquire economic prosperity.

1.2 Internet and Legal Legislation

Legal Legislation and law in general seems to have issues approaching and safeguarding the internet of cybercrime. This is due to legal advisors having difficulty understanding the complexity of online crimes, since their lack of technical knowledge. It goes without saying that in order to be successful in creating a solid legal framework regarding cybercrime both legal and IT experts are needed. Having a closer look in the matter the lack of evidence and the few cases that reached court and received a penalty for online crimes is making things even more difficult. As far as legal experts, lawyers and solicitors go, facing cybercrime and legislating is a new form of crime. (Holt, Bossler & Seigfried-Spellar, 2015)

Globally there where some attempts to create the basics of online and criminal legislation that can be classified in four stages:

1. The decade of 1970- 1980, where the legal legislation started to create framework regarding privacy, personal data and very personal (sensitive) data.
2. 1980 and afterwards, where there where the first unsuccessful attempts to combat online economic theft.
3. The same decade the basic framework regarding copyright infringement was created
4. Finally, 1990's was the start date of declaring content either illegal or unwanted. (Mitrou,2016)

1.2.1 Greek Legal Legislation

Following the same European regulatory regarding cybercrimes, Greece embedded in its legal legislation some add- ons in form of Presidential Decrees in order to be on the same page as the rest of the Europe.

However, legislation regarding online crime isn't in any way completed. Greek regulatory authorities didn't create a new framework regarding online crime, they however added some articles on top of the above legislation. The same workaround logic was followed by a lot of Countries inside and outside Europe as well. (EC3, 2015)

In fact, the Presidential Decree 45 of 2005 has 5 basic articles:

- Article 370A, that tries in a way to protect the privacy of electronic communications. As an example, one can imagine the privacy of his phone calls. Based on that article the criminal will be punished with one year sentence
- Article 370B, an attempt to punish unlawful access specifically if they are protected by any means of security such as passwords. This is an attempt to punish online criminals that is however punished with 3 months sentence.
- Article 370C, that is the Greek attempt with one article to punish both crackers and copyright infringements. It clearly states that if someone breaks in security measures and gains access to a computer or information systems will be punished with 3 months sentence and a penalty of 29 euro.
- As far as online fraud, article 386A is an attempt to target economic online crime that states that if someone unlawfully changes information, adds or deletes data with the purpose of financial gain will be sentenced with 3 to five months' sentence. The penalty fee is defined based on the size of the damaged the criminal did.
- Lastly article 348A is about child pornography that forbids anyone to view, offer or sell children pornography. The penalties are a 2-year minimum sentence and penalty fees of 50.000 up to 300.000 euro.

It's worth mentioning that on articles 370A and 370C the victims need to file a report in order for criminal to be prosecuted whilst on article 386A and 348A the procedure is automated. (Mitrou,2016)

Overall the same principle applies in most of the European countries. Considering the above, one understands that the legal legislation wasn't ready to handle the extra work that cybercrime needed. So far law is rushing to legislate but on this confusion a lot of basic information gets left away.

In regards to the penalties and sentences it seems so far, the law is somehow friendlier to online crimes with the exception of online child pornography. Average penalties for cracking in Europe are from 1 month up to 10 months of sentence. Legislation seems a bit generic and there are a lot of factors to take into consideration as will be studied in the above chapters.

1.3 Cybercrime in numbers

Cybercrime started gaining attention as early as 2002, however there where cases prior to that date. It is unclear when the first cybercrime incident was reported and there are many different variations to calculate. In fact, the nature of the first cybercrime is unknown.

Nevertheless, in 2004 numbers started growing. It is worth mentioning that in 2004 cybercrime brought damages to US companies up to 280 million dollars. (FBI,2016)

Cybercrime is evolving in a fast manner and its always changing character and approach. This is why there is also difficulty upon tracking down cybercriminals. (Marion, 2016)

Today cybercrime has reached an amount where in 2016 there was a loss of over 550 Billion dollars globally. A shocking report comes from IBM that predicts that by 2019 the global cost of cybercrime will increase up to 2 trillion dollars. (IBM, 2016)

However, as the 2016 Global Risks report mentions, a large part of cybercrime goes undetected so not even experts can put an exact number, these are estimates and no one really knows the damage cybercrime has caused. One thing is certain; every year the number of cybercrime losses is increasing upwards rapidly. (Goodman, 2016)

Looking closely to the matter of identity theft it is worth mentioning that Theft Resources Center in their annually report mentions over 29 million records were exposed in the US.

Lastly, Ponemon's 2016 review and IDG mention in their report a 42% rise in cybersecurity incidents in general. (Ponemon,2016)

2. Cyber Criminals

It has come to an understanding that individuals that abuse services and commit a crime online using a computer either as tool, as a target or both is known as a cybercriminal. (Alisdair, 2015)

Based on arrests made from various departments regarding fighting cybercrime around the globe there is no apparent "textbook" cybercriminal. The factors that lead to cybercrime vary. Overall cyber criminals seem to have few common grounds, since their age group is not related neither is their work status. It is obvious that there are cyber criminals across the globe and they aren't country specific although cybercrime seems to flourish in specific countries with laid back legal legislation or high level tolerance to online crimes.

However cyber criminals in comparison to regular old fashioned criminals and thieves have one major difference, basic financial stability. As previously stated cyber criminals need a computer in order to operate and a broadband connection to have the slightest working setup. This actually means that cyber criminals will operate in order to make larger financial gain since their fundamental needs are covered instead to the old fashioned criminal type that mostly steals to cover these fundamental needs such as food or shelter. (Senker,2016)

Cyber criminals may operate on their own, or scale their business to a larger cybercriminal group or team. These teams could consist of either known real life cyber criminals or cyber criminals that they've never met and only talk to on encrypted channels online. On top of that there are many regular old fashioned criminal groups that hire cyber criminals in order to get a piece of the online crime market share.(Clough, 2015)

Cyber criminals and cybercrime in general caught the media's attention as well and in fact many documentaries, series and even movies regarding cybercrime have come across the last five years. This occurred due to the classic "good guy" "bad guy" scenario. Although, this thesis will prove that the way media presents cyber criminals, online crime and authorities responsible in general has nothing to do with the way it gets presented in public.

Picture 1: How Cyber Criminals are posed in Media.

In order to get a comprehensive understanding of the cybercriminal mindset one would have to approach the issue from multifarious aspects.

2.1 Cyber Criminal Profiling

Criminal profiling is a solution available to scientific investigators in order to narrow down the number of suspects and actually do an evaluation of the possibility of a suspect committing a crime. By analyzing the scene of the crime scientists can acquire behavioral characteristics of the suspect that committed the crime. (Attrill, 2015)

Although psychological profiling is mainly used in crimes related to murder, many scientists and security analysts try to understand the means and motive of cybercrime. There are difficulties in understanding the sociological, psychological and criminological aspects of cyber criminals due to the small amount of information the global law enforcement gathers and shares with the scientific community. (Lickiewicz, 2011)

Apart from the actual forensic investigation that occurs when an arrest is made, scientists try to identify patterns by comparing recorded cybercrimes that may lead to a conclusion.

However profiling cyber criminals is still at an early stage, scientists and investigators in this field have come across some similarities that most cyber criminals have in common. (Attrill, 2015)

This is also due to the fact that every cybercriminal actually uses a unique way of carrying out an attack with the majority of times using custom made software and self-developed techniques. (Lickiewicz, 2011) Lickiewicz suggests that one database of criminal offences should be created. If the database is properly created it should assist security specialists to accumulate information on perpetrators on crimes of the same nature. Regardless of Lickiewicz study in 2011 no further measures were taken regarding the aforementioned database up to date.

An interesting approach in profiling cyber criminals was from the University of New Delhi where the department of psychology tried to create four major heads which most cybercriminal seem to have in common. (Rashmi, 2014)

TECHNICAL KNOW-HOW	PERSONAL TRAITS	SOCIAL CHARACTERISTICS	Motivating Factors
Sharp (intelligent)	Impatient	Anti-establishment	Monetary Gain
Focussed	Determined	Lack Social skills	Greed (easy, quick money)
Well-trained	Insensitive	Inferiority complex	Political beliefs
Strategic planners	Secretive	Low self-worth	Emotions
Bully	Aggressive	Marginalised	Disregard for law
Resourceful	Strong-willed	Radical	Intolerance
Goal oriented	Passionate	Mass-destruction	Thrill-seeking

Picture 2: Screenshot from Rashmi's 2014 publication regarding Cyber Criminal profiling.

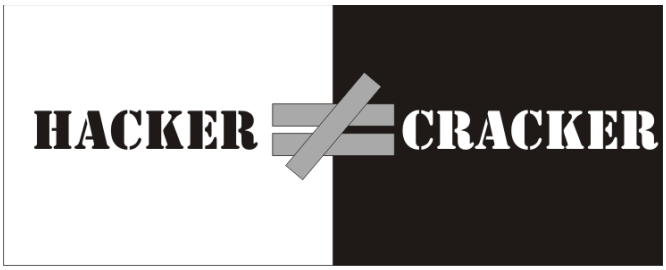
Cross referencing these results with the largest agency in the globe regarding fighting cybercrime it seems most cyber criminals have four basic charachetirists: (https://www.fbi.gov/wanted/cyber 2015)

- Some point of technical skill
- They are very disciplined and have strong motivation
- They are highly organized
- They have out of the box thinking

2.2 Categorization of Perpetrators

Individuals with extensive knowledge in computers, networking and IT infrastructure that are able to breach or bypass any type of online security protocol are commonly known as crackers. Although press and media promotes these individuals as “hackers”, the correct term is cracker. Various misunderstandings also come to the cracker theory as some claim that crackers are only responsible for reverse engineering and not the actual breach of security systems. (Senker,2016)

RFC 1392 defines hacker as a person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. On the other hand, based on RFC 1392 again cracker is a person who attempts to access computer systems without authorization. (RFC,1993)



Picture 3: Difference between terms hacker and cracker.

As stated above it is quite difficult to try and categorize cyber criminals based on their sociological and psychological factor. (Kirwan & Power, 2013) Although there isn’t any official categorization regarding crackers they are mostly divided into five large groups:

- **Amateurs**, they are the less- skilled type of cracker common known as “script kiddies”. By utilizing existing instructions and basic tools found in the internet they are trying to build up their skills and gain experience. Usually tools posted online might already be patched by their developers, it seems that the majority of amateurs by trial and error can actually cause damage.
- **White hat crackers**: they mostly work in large companies and their responsibilities involve using white hat methods to pen test and maintain the security level of a company. These types of crackers utilize a form of ethical hacking and even though they are doing penetration testing that by default is a form of an attack it’s an offensive strategy to protect the company’s assets and not to cause harm. Main objective of their work is to expose and fix vulnerabilities prior to malicious attackers exploiting them. It goes without saying that white hat crackers have a complete understanding of their actions and the legal legislation. This is why white hat crackers may be also referred to as ethical hackers. (Engerretson, 2013)

- **Gray hat crackers**: This type of cracker works and uses custom techniques that may or may not be legal. They consist of a combination between white hat and black hat (explanation bellow) crackers. They do have an understanding of the actions they are carrying out but mostly they are trying to locate exploits and vulnerabilities in a system without the owners, company's permission or knowledge. Their purpose is to let the company, owner or administrator know about the issues and the crackers offer to fix the issue for a nominal fee. Gray hat crackers are also known for working closely with government projects to test and assess the security levels of several projects. (Regalando, Harris & Harper, 2015)
- **Black hat crackers**: These individuals are wrongfully referred by media as "hackers". The Black Hat cracker uses custom made tools, has no work ethics and usually his target is monetizing from every bit of information he can get his hands in. Black hat crackers work either alone or in large criminal groups. Their teams are constructed from their real-life circle or from other crackers they meet and talk with in encrypted channels. This type of cracker is the most wanted and usually these are the ones that come up with the zero day hacks. Due the nature and the zero tolerance regarding the law black hat crackers are usually known as cyber criminals. (Stryker, 2012)
- **Hacktivists**: It is in fact a combination of words hack and activism. Some crackers feel that by hacktivism they show anti systemic behavior and political protest. Hacktivists lately were known for doing DDOS attacks. There are many communities online and crypto IRC channels where hacktivists coordinate their attacks. (Shukla& Mehra, 2015)

Most of these terms used to describe the crackers were coined in defcon, a conference about hacking, an event that is held annually in Las Vegas since 1993. On top of that many security experts claim that the terms white hat and black hat arose from old westerns where the "good" cowboys wore a white cowboy hat rather than the "bad" guys that wore a black cowboy hat.

Picture 4: from Defcon Convention in 2015, Old western where supposedly the terms Black hat and White hat where coined.

A different categorization occurs on whether the cracker is attacking from the inside or the outside of a target.

- If a cracker acts within the target organization as an employee, thief or even by accident, it is considered an insider attack.
- On the other hand, if the cracker attempts to penetrate from the outside, it is considered as an outsider attack. (Shukla & Mehra, 2015)

2.3 Motives of Cyber Criminals

As previously mentioned the first motive of any cybercriminal is financial gain. However, it is not the only one. Cyber criminals have a serious of motives as well and they may belong to more than one category. (Clough, 2015)

Based on research that concluded in March of 2016 carried out by IBM Security department known as IBM X-Force there are five motives for cyber criminals:

- Financial gain, cyber criminals will create new tools, techniques and always look for vulnerabilities they can exploit in order to make profit. It goes without saying that cyber criminals that know how to utilize the exploits are able to make a large income with minimal effort and time. These profits driven attacks and their methodology differs widely between cyber criminals.
- Ego or vanity, the concept of getting known, a lot of cyber criminals love to leave their signature on the attacks they carry out or the exploits they locate. As a moto, cyber criminals always use some special nickname or a signature that corresponds to them. Sometimes they even post on social media regarding the attacks they have carried out.
- Entertainment or simply put just for the thrill of it, in fact there are a lot of gray hat crackers that are trying to find exploits just to test their potential. (Erickson, 2015)
- Political, religious or ideological motives, there are always crackers that manage to carry out attacks to make known of their political or religious views and aspects.
- Personal emotions. Sometimes former employees of a company or dissatisfied customers of a brand might carry over attacks. Clearly, they are based on revenge and some might even lead to extortion. (Kirwan & Power, 2013)

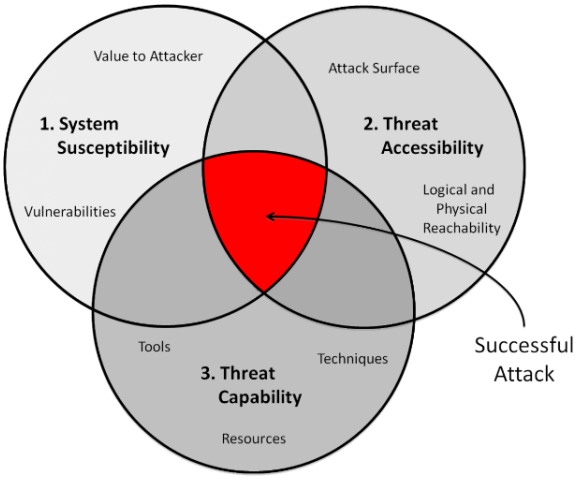
Picture 5: Crackers leaving their signature in a php webpage.

2.4 Methodology

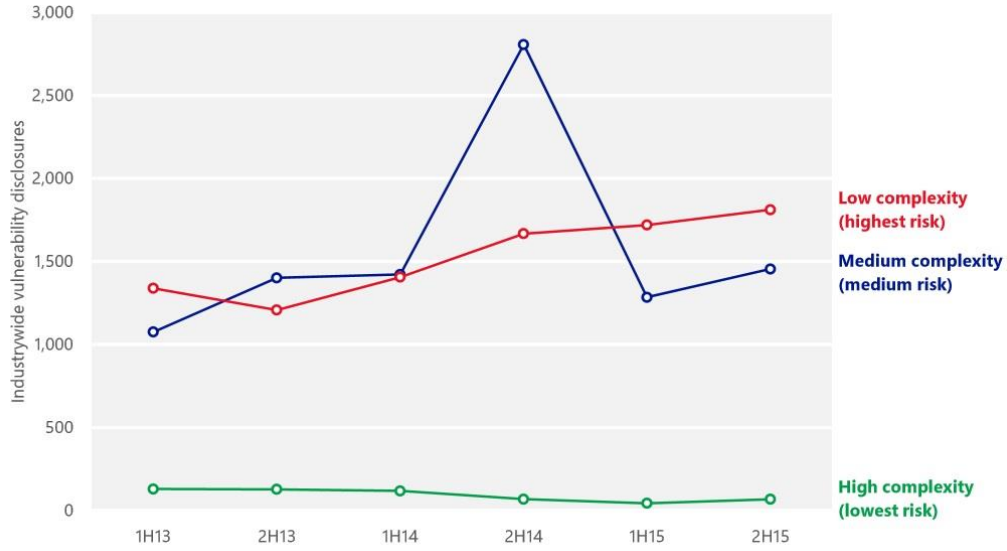
Various methods have been used by cyber criminals in order to carry out their attacks. First thing needed from cyber criminals is gathering resources. It is obvious that the methodology depends on the actual target. (Clough,2015) This chapters is focused on analyzing the most recent and successful methods used by cyber criminals in order to get resources and steal personal information up to date. It will not however focus on outdated or patched methods of the past.

Cyber criminals try to locate and abuse vulnerabilities in software. In Computer security terms vulnerabilities are issues and weaknesses inside software that could possibly allow cyber criminals to compromise the Confidentiality, Integrity and Availability of software.

Vulnerabilities are mostly divided in three categories based on their complexity, of low, medium or high. As it seems low complexity vulnerabilities are the easiest to exploit and higher risk, whereas high complexity vulnerabilities are actually lower risk in general. (Donaldson, Siegel & Williams, 2015)



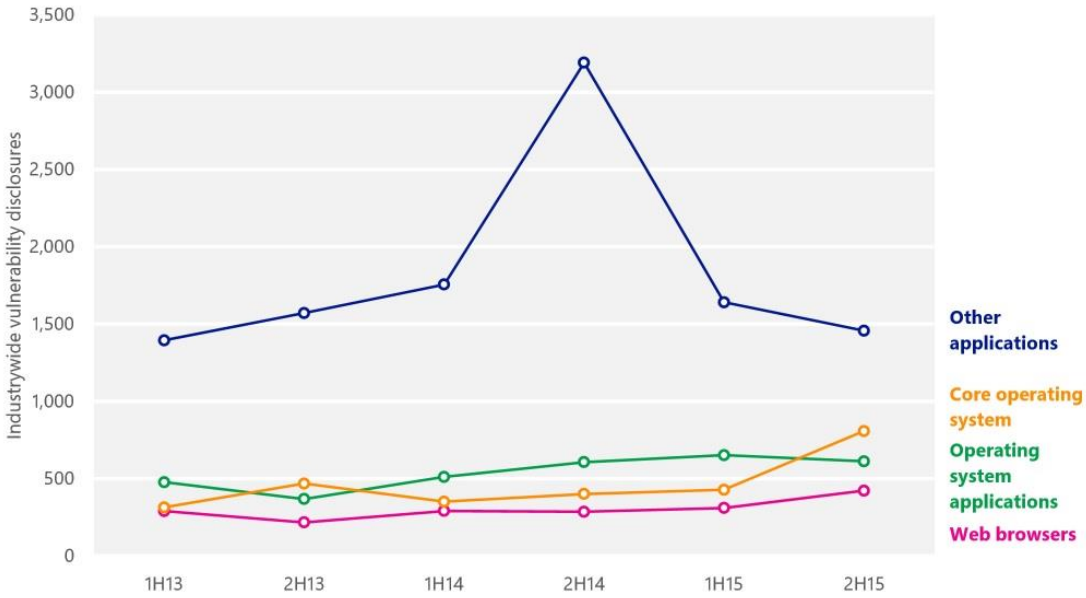
Picture 6: Analysis on Vulnerability logic abuse.



Picture 7: Statistics from 2015 Microsoft's report regarding vulnerabilities.

Based in Microsoft's Security Intelligence report of 2015 vulnerabilities that are abused can be divided into four major categories:

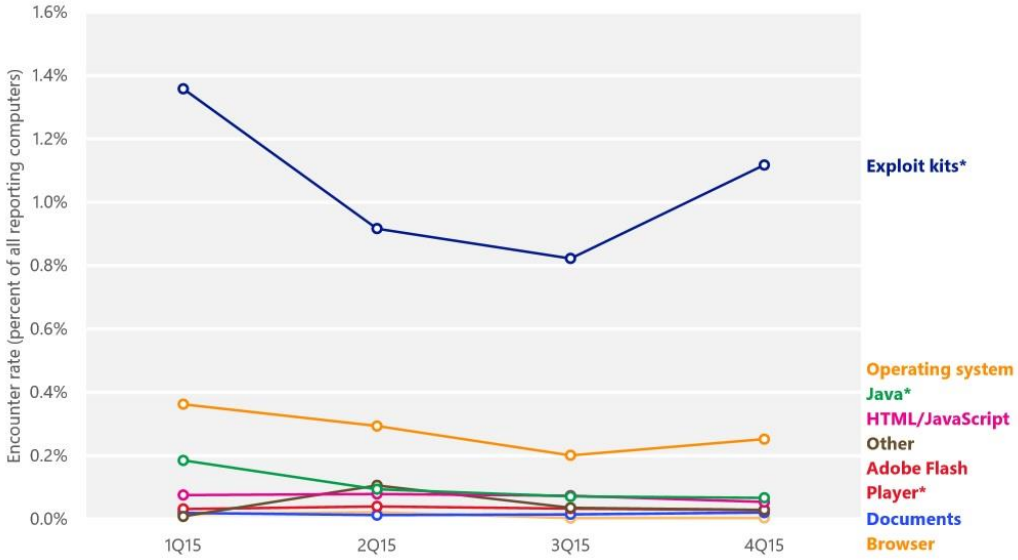
- Core Operating system vulnerabilities
- Operating system application vulnerabilities
- Browser vulnerabilities
- Other application vulnerabilities (Microsoft,2015)



Picture 8: Statistics from 2015 Microsoft's report regarding software with most vulnerabilities.

In these Vulnerabilities, cyber criminals create a code that utilizes the software vulnerabilities in order to get private information of the victim or even install malware.

This code is commonly referred to as an exploit. Several exploits and exploit kits are available in marketplaces being either sold or free for use. Exploit kits are quite easy to buy, use and operate, thus making things easier for criminals with less programming knowledge. (Senker, 2015)



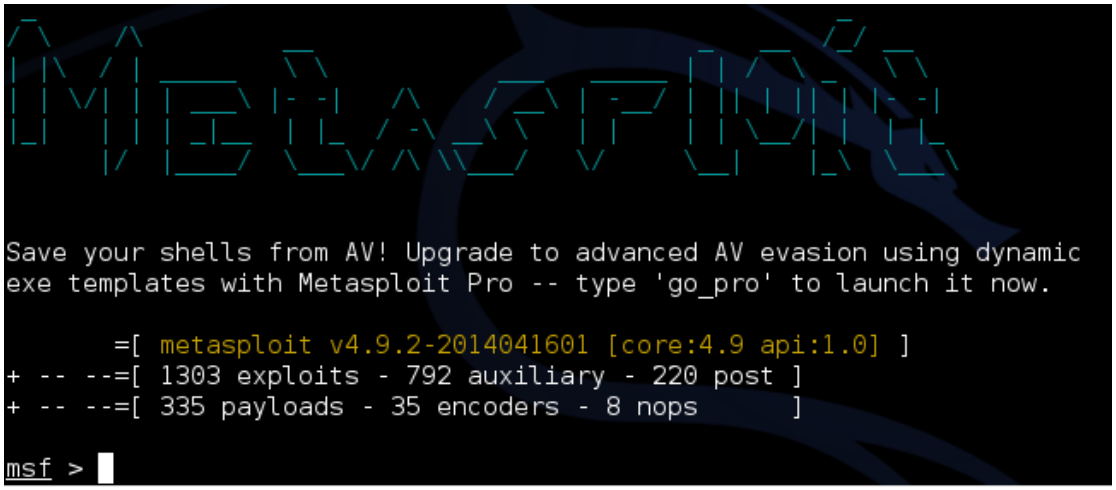
Picture 9: Statistics from 2015 Microsoft's report regarding exploits.

Exploits can be purchased or downloaded on the internet or on black markets where cyber criminals operate. Although a vast amount of knowledge can be acquired from free exploit databases and the white papers they may contain such as the exploit db from Offensive Security. This exploits database intention was to upload security issues on specific software in order to get patched, but as it seems the majority of those exploits aren't actually patched by their developers. This leads to those exploits being used for illegal purposes.

Picture 10: Screenshot originally from www.exploitdb.com.

A very useful open source tool that was created for Penetration Testing is the Metasploit framework which is actually where most exploits are created, tested and configured. The metasploit framework already has over 1300 different exploits for Microsoft Windows Operating systems.

Various versions and different user graphic interface with almost the same exploits can be found in the Armitage and Cobalt Strike that seem user friendlier due to the GUI they provide. (Kennedy, O'Gorman & Kearns, 2011)



Picture 11: Screenshot from Metasploit framework running in Kali Linux 2.0.

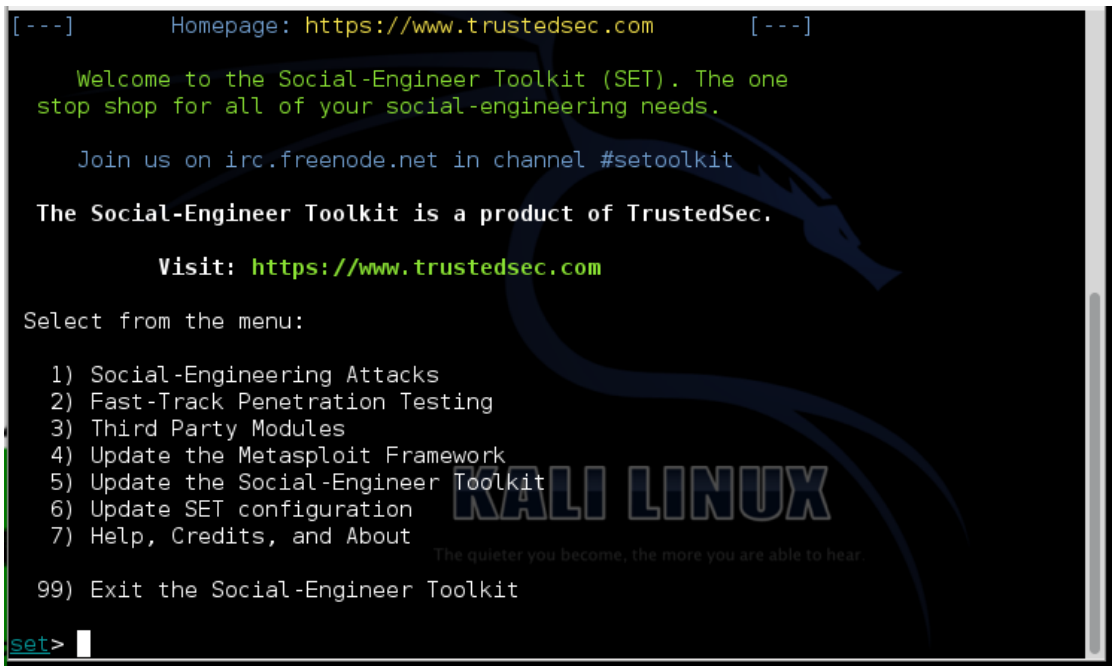
Metasploit is an amazing tool for White Hat penetration testing although it can be used by cyber criminals that abuse those exploits in order to reach with ease their victims.

In cyber criminal's terms king of all the exploits is an unknown newly discovered exploited vulnerability that goes by the name of a zero-day attack/vulnerability. It is in fact a vulnerability that was discovered by a cybercriminal that later on created an exploit code and either used it, sold it, or published it. By the time the original developer figures the vulnerability and patches it, it is no longer a zero-day attack although the cybercriminal would have already monetized from this exploit.(Shackelford, 2016)

2.4.1 Social Engineering

One of the most basic methods that criminals use to monetize is relatively easy. It comes by the name of Social Engineering and aims to get information from other users. Attackers can impersonate and spoof in order to appear to be from a bank, a money institution or even a company in order to get information that they will later on utilize to their needs.

With the use of social engineering attackers can acquire passwords as well and sensitive information. Social Engineering is a very basic attack and there is also a toolkit developed by trustedsec that is embedded in almost all Linux penetration testing distributions. (Engerretson, 2013)



Picture 12: Example of SET embedded in Kali Linux.

Social Engineering attacks are quite old but never outdated since attackers always change their approach in order get closer to their victims. (Senker,2016)

Social Engineering attacks do not occur only to individuals. Many attackers try to target major retailers in order to get information regarding company's infrastructure and even pose as employers using a believable story in order to acquire some login information. When targeting companies their major target is getting the email of an employee. It goes without saying that on attacks described below, criminals tend to try to get access to the SMTP server of a corporation because it holds tremendous amount of information that can be exploited in various ways. Cyber criminals also spoof emails trying to pose as an executive or even the CEO of a corporation in order to give orders to make transfer of funds to bank accounts controlled by them. (Goodman,2016)

Recently arose the social engineering method of false claim- non-receipt - false representation, where criminals make a purchase from an online retailer and then make a falsified claim regarding the status of the parcel. They then contact the retailer by using smart social engineering techniques try to get a replacement or a refund of the face value of the item purchased. In United Kingdom and the United States of America this issue has gone through the roof the last 3 years. It is actually a combination of social engineering and terms and on conditions abuse. Various departments fighting cybercrime across the globe have made arrests regarding this troublesome issue of false representation online.

Picture 13: Headline from Social Engineering attack.

Cyber criminals use this method because it is quite easy to implement and it doesn't require a lot of resources that aren't embedded in a Linux distribution or isn't free to use. Social engineering is also used in order to deceive victims in order to click, download or install malicious files containing malwares.

2.4.2 Spamming

Spam is the method of sending unsolicited messages online. It was commonly used to send mass emails and the recipients could either be an individual or a company. Spam is so common that almost any individual that uses the internet will come a across spam email at some point of their lives. Webmail providers and third party companies have created algorithms in order to block and filter incoming spam and forward these emails to a specific named "spam" folder. However, this method isn't foolproof since sometimes (based on filter) Spam email will arrive at the individual's emails inbox. (Krebs, 2015)

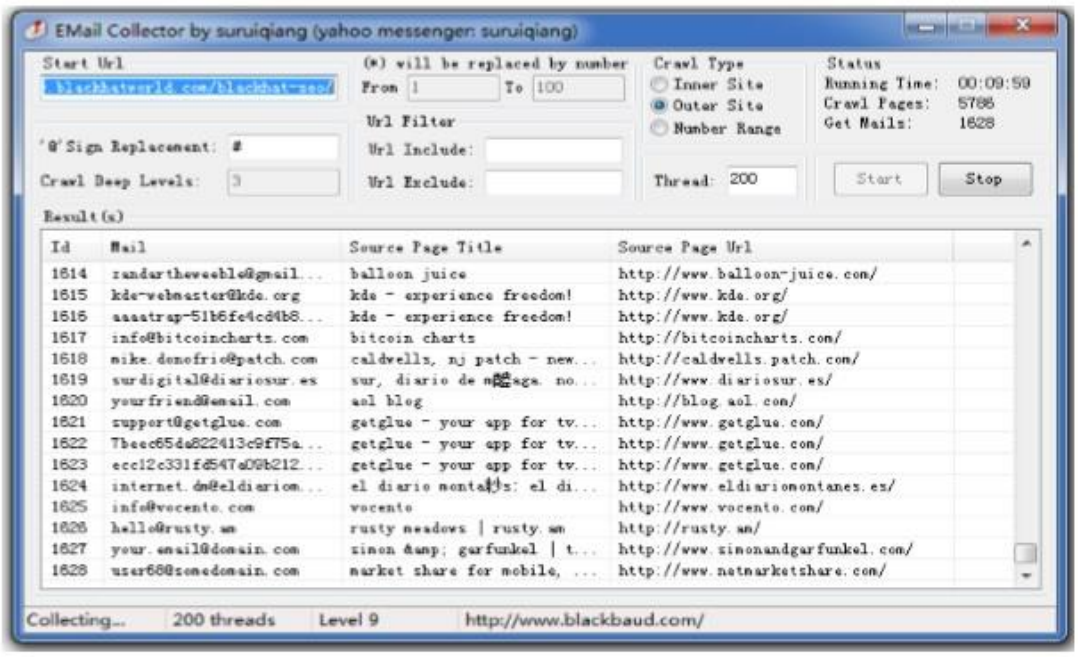
Spam isn't just there to clog users email inbox, it serves multiple purposes. Based on Radicati Research Group case study, most spam emails are regarding commercial advertising sales on dubious products, pyramid schemes, get rich quick and telemarking scams. Spam is also used by cyber criminals in order to send phishing links to a victim in order to get their personal information and commit in general identity theft. Spam messages are also known to contain viruses, Trojan horses and malware.

Spam has flourished over the past years and moved from spam emails to online spam in social networking – media, in online messaging, online gaming, blogs and wikis, mobile phone text messaging (SMS), spam indexing. The reason behind spam success is mostly because of pour information on how to avoid suspicious emails and secondly on the fact that it is actually very cheap attack to carry out. (Krebs, 2015)

Attackers carry out something that is called spam campaign and is used to send mass emails from cracked email accounts to multiple emails containing phishing pages. Spam campaign also occurs when attackers wish to hide some information from the victim's personal email account so they email bomb it in order to lose track of important emails. (Krebs, 2015)

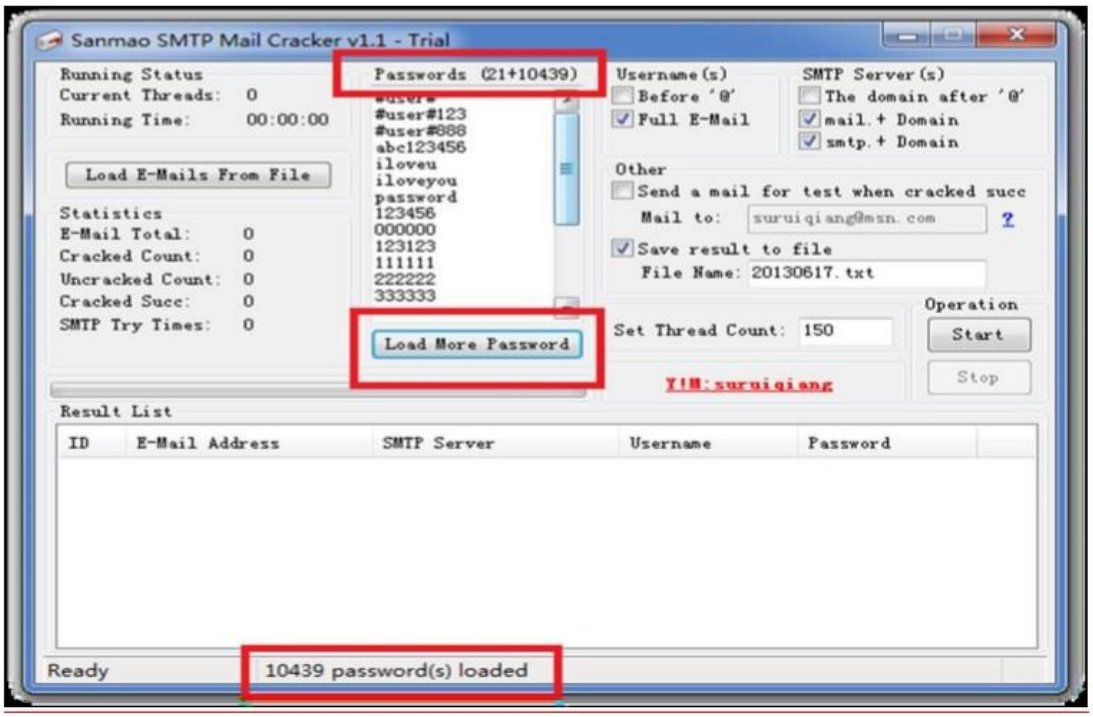
Cyber criminals that wish to start a spam campaign in order to get information or simply send a phishing page have one major opponent as previously stated and that is spam filters. A couple of years ago, criminals used to create fresh, newly made email accounts and started mass mailing possible victims. Today due the spam phenomenon receiving tremendous attention spam filters and companies are able to look and trace the age of email accounts, the IP of the sender the SMTP server and its blacklists.

The first thing attackers do in order to start a spam campaign is to create a spam database. Virtual Private Servers with Microsoft Window's Server software is preferred since it does allow by default access to port 25. However, many companies and corporations that offer Virtual Private Server solutions have embedded a block on the SMTP port 25 a feature that is easily bypassed by whitelisting the VPS in the firewall. By selecting specific domains, they extract email accounts using various tools. Virtual private servers are available to purchase with anonymous online currency in low prices to 20 USD per month. Pricing depends on where the actual datacenter is located and the features it offers.



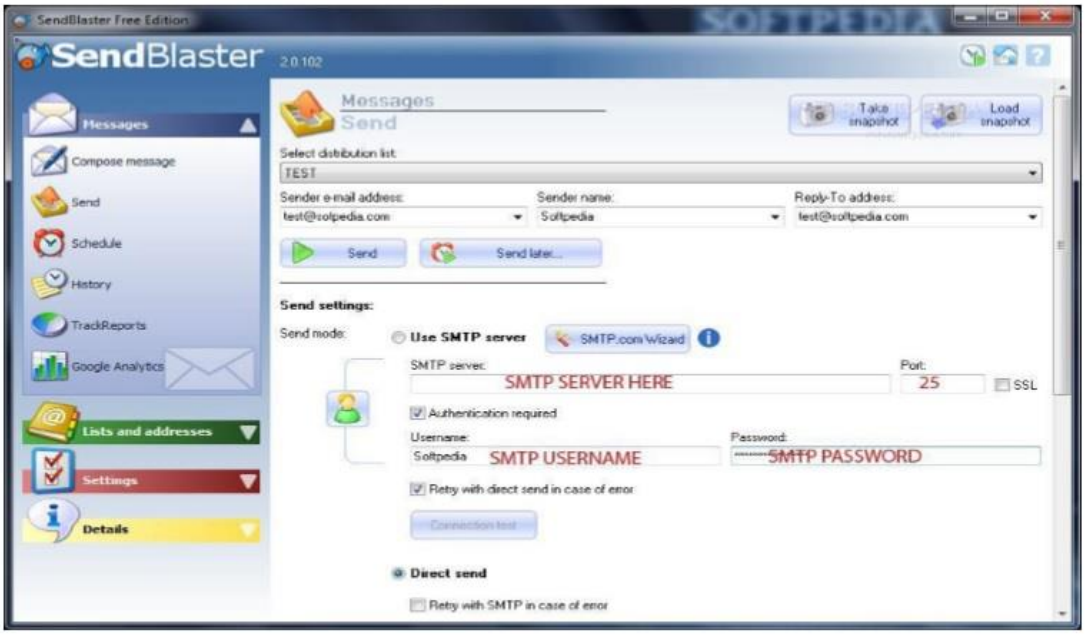
Picture 14: Screenshot from custom made application regarding collecting email leads.

Then with the help of other tools and a large wordlist of common password combinations they try to crack (brute force) the SMTP email accounts. Most of the times all these tools run in a 24/7 basis in the Virtual Private Server in order to create a better database and higher chances of the email hitting the inbox of a user and not going into the spam folder.



Picture 15: Screenshot from custom made application regarding cracking SMTP servers..

After creating a big enough database criminals then use legitimate mass emailing applications in order to send their spam emails.



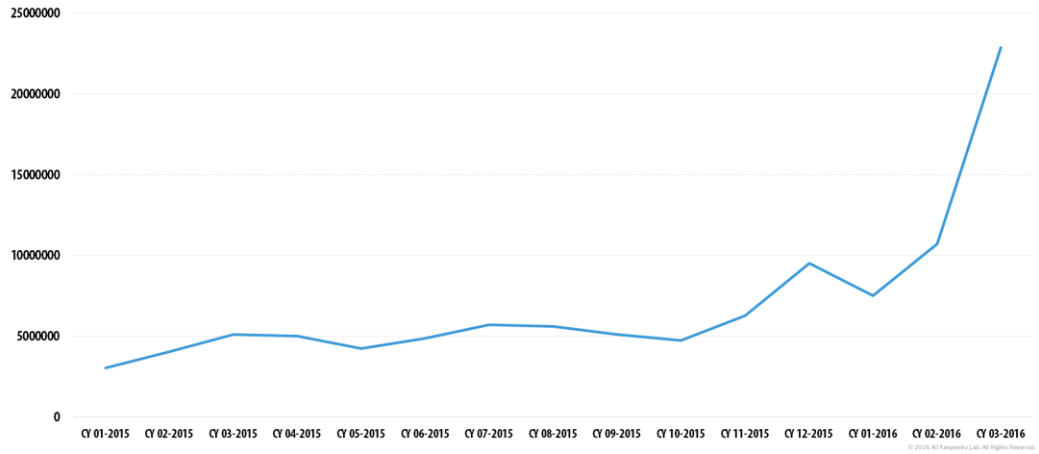
Picture 16: Screenshot from SendBlaster application for mass emailing.

As indicated above spam is quite easy attack to carry out and criminals tend to use it and combine it with many different features. An interesting factor comes from a recent study from Internet Crime Complaint Center (IC3) in 2015 where Business email compromise had reached losses of 263.000.000 USD while individual email compromise reached loses of 11.000.000 USD in the United States. (FBI,2015)

To sum up, criminals accessing email accounts empowers them to know about:

- Privacy, such as messages, calendars, google or skype chats, photos, work related papers or even the location of individual
- Harvest, data of the individual such as email contacts, file hosting accounts, google documents, drobox files or even software license keys
- Finance such as bank accounts, payment processors or payment gateways
- Accounts, subscriptions and payments, an individual has and makes, such as Facebook, twitter, amazon, iTunes, skype, Netflix, Hulu+, origin, steam, etc. (Krebs,2015)

These are the results of the first quarter of 2016 based on Kaspersky's labs regarding volume of malicious spam.



Picture 17: Screenshot from 2016 Kaspersky's report regarding amount of Spam for the first Quarter.

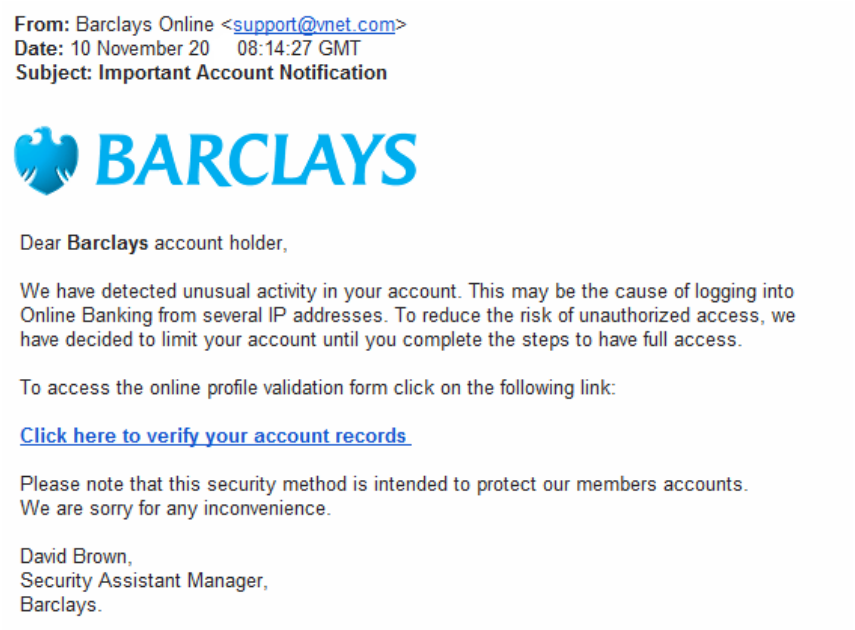
2.4.3 Phishing

Phishing is a form of evolved social engineering attack since attackers impersonate a trusted source in order to get private and sensitive information from their victims. Attackers usually try to pose as a legitimate company or representative in order to ask some personal details of the victim. This information sometimes may include usernames and passwords and financial information such as e-banking log in details or even all the victims credit card credentials.

The logic behind phishing is quite simple, attackers usually send an email that is created to either hit the emotional state, scare or confuse the individual in order to make a speedy decision and actually fall on the attackers' trap by filling the information or clicking the hyperlink inside the email. These hyperlinks appear to the victim legitimate as attackers are either cloning a legitimate and copyrighted site or using one that has the same legitimate images. (Shackelford, 2016)

In the past phishing attacks where generic and used vague terms. They weren't at all personalized because attackers didn't actually know any information regarding the victim apart from their email

address. This lead to the phishing email stating generic titles such as “Dear Sir/Madam”. On top of that phishing emails may have poor grammar, capitals in strange places and misspelled words.



From: Barclays Online <support@vnet.com>
Date: 10 November 20 08:14:27 GMT
Subject: Important Account Notification

BARCLAYS

Dear **Barclays** account holder,

We have detected unusual activity in your account. This may be the cause of logging into Online Banking from several IP addresses. To reduce the risk of unauthorized access, we have decided to limit your account until you complete the steps to have full access.

To access the online profile validation form click on the following link:

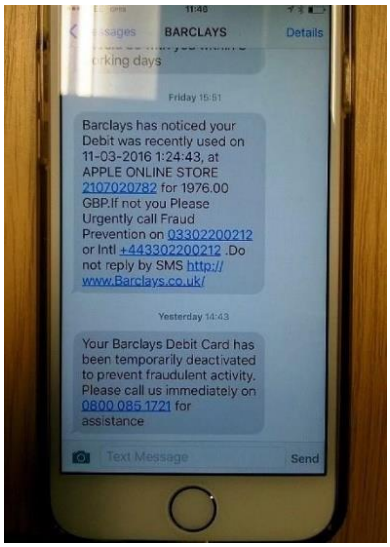
Click here to verify your account records

Please note that this security method is intended to protect our members accounts. We are sorry for any inconvenience.

David Brown,
Security Assistant Manager,
Barclays.

Picture 18: Screenshot from Generic phishing email claiming to be from Barclays Bank LLC in UK.

Today phishing attacks have evolved and attackers are getting smarter to a point where they are now sending personalized phishing campaigns. Reverse email searching and social media has helped criminals to acquire information they couldn’t get in the past. Personalized emails containing the victim’s name or even address and phone number are in fact very realistic so more individuals fall on the phishing trap. On the other hand, phishing isn’t executed via emails only, it is conducted via sms, via fake sites of legitimate company’s offering products at a very discounted prices.



Picture 19: Photo of a personalized phishing campaign where the victim gave information to cybercriminals.

In order to create a phishing website, cyber criminals buy domain names with untraceable digital currency such as bitcoin from various companies that are accepting them as payment methods. By default, these companies don't have high security and do not require verification upon the individual buying a domain name. The cost of a a domain name is as low as 1 USD per year. Cybercriminals do not target specific country based domains, such as .com or .co.uk or .au but go for the newly made .xyz, .io or .biz domains. After owning the main domain, they can create as many subdomains they wish in order to look similarly to the real site.

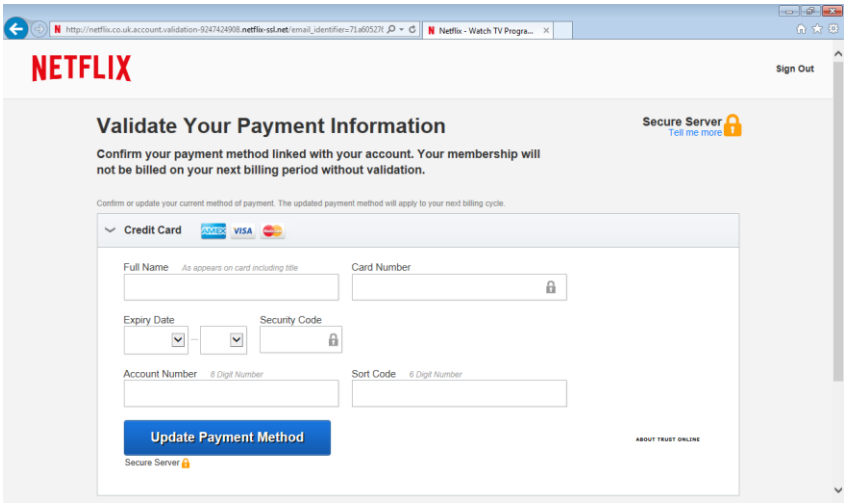
Picture 20: Example of a company accepting Bitcoin payments.

The main purpose is to misspell the legitimate site a bit or slightly change the domain name in order to fool the victim that this is the legitimate site. A google search will reveal an enormous amount of companies that are actually accepting payments via online virtual currencies. As a matter of fact, both Amazon and Microsoft will implement bitcoin payments by the end of 2016. (Microsoft 2015)

Second in the list of successfully owning a phishing page is uploading it to a hosting server. Since phishing pages are small in size free hosting will do, but there also companies that offer this service via anonymous online currency payments (bitcoin).

Truth of the matter is free hosting services will cancel the free hosting subscription upon receiving the first complaint whilst paid for hosting may leave the phishing site live up to one month. These anonymous hosting companies once more require non-to very little information regarding owner and content of the aforementioned phishing site. One month hosting costs on average 5 USD on anonymous hosting providers so cost effective it has huge potential for cyber criminals.

Cyber criminals clone, create or buy phishing webpages of major retailers offering products or services at very discounted prices. These phishing websites may be about tv subscriptions such as Netflix, offers regarding apple devices at very discounted prices, payment processors and gateways such as PayPal or even actual banks. (Shackelford, 2016)



Picture 21: Netflix phishing Page hosted free in www.boxhosting.cl

After the victim falls to the phishing page trap and enters his/her personal details, cyber criminals based on the setup receive an email or view via cPanel every bit of information there is on the form. Cyber criminals also get the IP of the victim, the user agent used and the time zone. Cyber criminals can use this information or sell it to black markets to others criminals that will then utilize them to the best way possible. Some phishing pages are so well built that they will redirect the user to another phishing webpage of his bank to enter extra credentials and verify the purchase with additional information. (Luttgens, Matthew & Mandia, 2014)

Based on the Global Phishing survey of 2015 by Anti-phishing Working Group (APWG) 569 companies where targeted and there where more than 123.000 attack last year.

	2H2014	1H2014	2H2013	1H2013	2H2012	1H2012
Phishing domain names	95,321	87,901	82,163	53,685	89,748	64,204
Attacks	123,972	123,741	115,565	72,758	123,476	93,462
TLDs used	272	227	210	194	207	202
IP-based phish (unique IPs)	3,095	2,317	837	1,626	1,981	1,864
Maliciously registered domains	27,253	22,679	22,831	12,173	5,833	7,712
IDN domains	103	112	82	78	147	58
Number of targets	569	756	681	720	611	486

Picture 22: Screenshot from 2015 Global Phishing Survey of 2015.

As it turns out phishing is cyber criminals best bet so far in order to harvest personal information and data.

2.4.5 Malware

Malware is a generic term that is often used for malicious software that spreads in computers and it interferes with their operations.

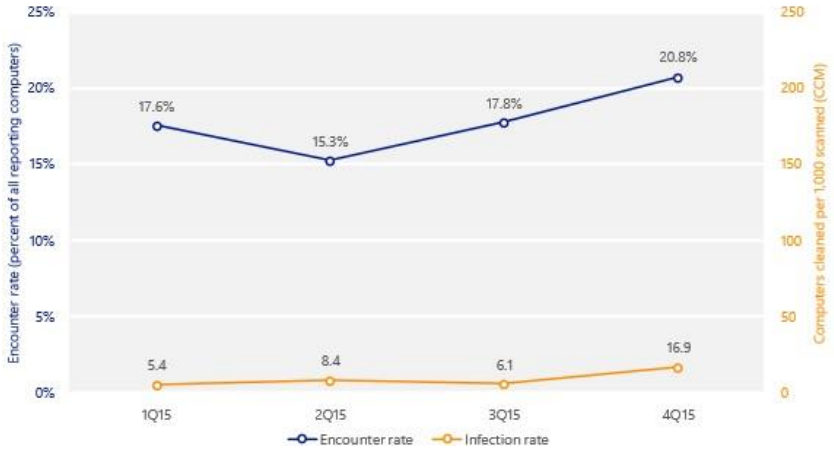
Malware may be dangerous, for instance, erasing documents or creating framework crashes, however may likewise be used to harvest personal information and data. There are multiple forms of malware that a user can come across to such as:

- Viruses, which is the most common type of malware, it can actually cause a medium level dysfunction and it can damage mostly software, files and sometimes cause hardware damage. Most viruses are self-replicating and spread from computer to computer. Viruses are mostly carried within other types of files (a host file) where they can later on spread and infect the target computer/ file system. Viruses can't spread on their own, they require some type of human interaction in order to start spreading. This may be the user installing or opening a suspicious file. This is why virus coders use social engineering methods and exploits in order to deceive the victim to open the file that contains the virus. As far as virus coding goes, most newly created viruses can take up to 6 months to get detected and patched by antivirus companies. By this time the virus would have already spread and sometimes evolved to a new virus developed from the same or a different virus developer. Another fact in computer virus coding is that their major Operation System target is Microsoft's Windows because it does in fact has 85% of Computer operating system usage. Viruses are able to cause damages up to billions of dollars every year due to wasted computer resources, corrupted data, system failures and overall an increased maintenance cost. (Elisan, 2012)
- Worms, they have a lot of similarities as viruses with their basic difference being that they can spread autonomously without the need of the victim's interaction. Worms are notorious for spreading to computer networks and their creation is based on security failures, exploits and vulnerabilities of a target computer. As a matter of fact, worms are more severe than viruses and can be used to drop Trojan horses to victims. (Eilam, 2015)
- Trojans, or Trojan horses, most of them appear like a legitimate software or program but it actually isn't. Its purpose is to help criminals gain access to a computer. There are lots of Trojans and most of them have different features but their main purpose is to steal data without the individual's knowledge. The majority of Trojans unlike viruses don't need to be carried in a host file. Spreading Trojans, just like viruses require social engineering from the developer's part.

Based on the privileges the Trojan gets it can crash a computer or the device they affect, they can delete or even modify files, they can cause data corruption, they can spy victim's data, key inputs, personal information and they can be a part of a bigger entity a lot of cyber criminals use such as a botnet.

- Spyware, is actually a form of software that intrudes the victim's privacy and gathers personal information and data without their knowledge and approval. It can monitor and record the victim's online presence such as the websites visited by the victim, it can also record the victim's keystrokes and transmit them to a third party. Spyware is usually found in free software that requires from the victim to watch or click an advertisement in order to use it, commonly known as adware. Spyware can also be used to capture screenshots of the victim's computer, record sound, even take a snapshot if the victim's setup involves a web camera. As a matter of fact, spyware is considered to be the most dangerous form of malware as it's only objective is purely to invade victim's privacy . There are various versions of spyware with different functions, most of them have the ability to install on their own on a system by either using a social engineering method to deceive the user or by using a software vulnerability. (Elisan, 2012)
- Ransomware, is a form of malware, that gets installed into the victim's computer and actually encrypts major files or the file system of a computer. The key point behind ransomware is that cyber criminals demand a ransom payment in order to provide the victim a key to decrypt the data. As with every type of malwares there are different versions of ransomwares. Some of them are based on social engineering and in fact scare tactics to make the victim pay the ransom. Simpler ransomwares are easy to reverse with basic computer knowledge without the need to pay the cyber criminals. However, sophisticated ransomwares are able to encrypt the entire hard drive or the Master File Table making decrypting without a key near impossible. There are several cases where companies that didn't have a foolproof backup and disaster recovery solution paid cybercriminals their outrageous demands in cryptocurrency in order to have their hard drivers decrypted.

  As technology, operating systems and software in general seem to evolve, the same law applies to malware and their coders. Sophisticated malware and ease of use is a combination cybercriminals go for. Since this form of malware could be a part of a bundle sold to inexperienced criminals, they target for, all in one tool with high level potential. Bottom line, software security shouldn't be taken in vain, because the results of bad security is what helps cyber criminals prosper. (Jewkes & Yar, 2009)



Picture 23: Microsoft's report on malwares shows that in 2015 over 20% of computers encountered malware threats in 2015.

2.4.6 Botnets

Even though it belongs in the malware category, botnets have dealt a tremendous amount of damage lately and will be studied as a different entity. Botnets are the biggest threat to the internet and the activities it has to offer. The word botnet derives from the combination of the word ro-**bot** and **net**-work. A bot, as previously stated is a form of malware that allows cyber criminals to take control over an infected computer that has broadband connection.

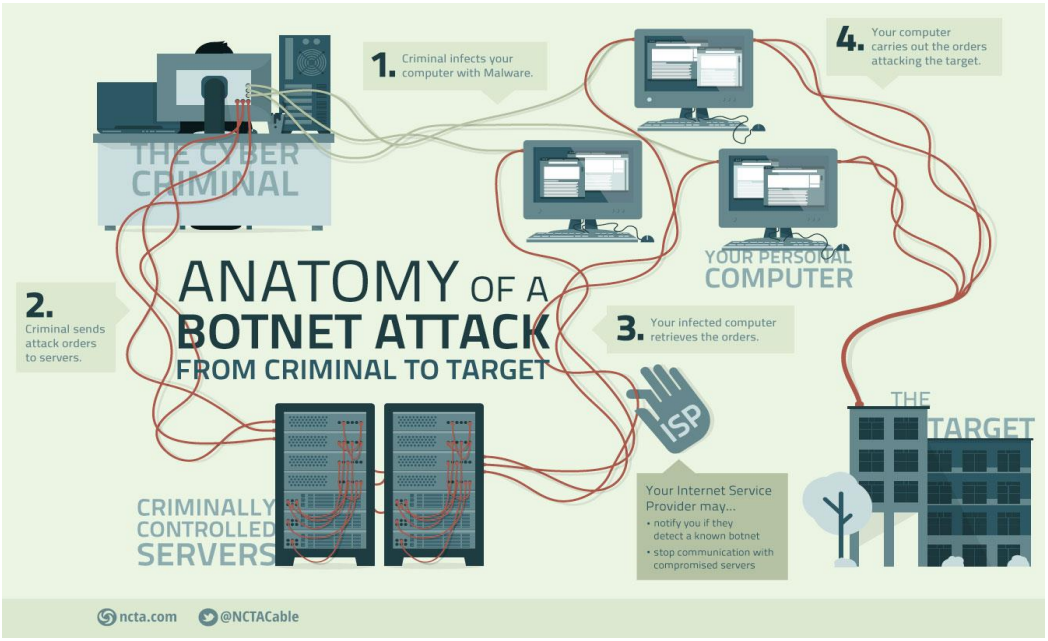
A botnet is an uncertain number of compromised computers (usually thousands) connected to the internet that communicate with each other and receive their basic commands from a unique computer controlled by cyber criminals/botmaster named Command and Control Center. A botnet may spread around the globe with hundreds – thousands victim computers (bots/zombies) regardless of their location. A botnet can spread via spam email that contains attachments, instant messaging, peer to peer, file sharing technologies, etc. Botnets are able to recruit new vulnerable computers by using infection methods from several classes of malware including of course self-replicating worms and email viruses. (Eilam, 2015)

Botnets are cyber criminals best tool so far because they are typically easy to implement, they come in a large variety of forms and it is rather difficult to get traced back to the criminals.

Cyber criminals have endless possibilities of usage of bots but they are mostly used for:

- Using resources without the victim's knowledge, cyber criminals can use the bot computer resources to crack passwords, solve captchas or use victim's bandwidth and distribute projects across the botnet.
- Make distributed denial of service attacks
- Running spam campaigns

- Sent false traffic that appears legitimate and click fraud
- Collecting information and data
- Conducting other illegal projects.
- Install other types of malware.



Picture 24: In the picture above its described in a nutshell the anatomy of a botnet.

Having a closer look in the botnets anatomy, cyber criminals create a malicious software that contains the bot binary which runs without the need of being compiled. The next step is spreading the malware using methods described above. The victim by installing the bot binary gets infected and the it tries to communicate with the command and control center. Depending on the method used to code the bot binary, the infected computer (bot) needs to communicate with the command and control center in order to be able to send and receive messages and commands. This is possible with rallying mechanisms such as an IP hardcoded in the bot binary, seed IP addresses of other hosts that will lead to the command and control center, also with domain names. As botnets evolve, rallying mechanism evolve as well. After victim computer contacts the command and control center it is officially part of the botnet. Cyber criminals access the command and control center without revealing their identity thus sending commands completely anonymous. On the other hand, several botnets work via peer to peer and no command and control center is needed. (Bleaken, 2010)

An infamous example of a botnet toolkit is ZeuS which created botnets that were able to remotely steal personal information belonging to the victim's computer. This bot was able to run regardless of user access privileges. ZeuS has an embedded key logger and a screenshot capturing ability that was able to capture keystrokes on virtual keyboards as well.

As mentioned above, cyber criminals can utilize their bots to make Distributed Denial of Service Attacks (DDoS). DDoS is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. DDoS attacks are able to create such conditions that a legitimate user isn't able to access the system resource. Main purpose of DDoS attack isn't to actually steal data; it is to paralyze websites or computers. By sending that massive number of requests from a large number of computers worldwide criminals are able to flood the victim's server. The victim tries to serve those requests that later on becomes unavailable to legitimate users. (Bleaken,2010)

DDoS attacks can be divided into five categories:

- UDP flood attack, that used to work by sending a large amount of UDP packets to a target computer. This method is quite outdated and it isn't used anymore because it is easily detected.
- TCP flood attack, that works by sending a large number of packets to victim server that uses lots of bandwidth resources.
- TCP SYN flood attack, that works by sending a tremendous number of requests to initialize a TCP connection with the victim that is forced to keep track of partially open connections made.
- Smurf attack, that involves sending ICMP ping requests to victim broadcast address with a fake source address by spoofing the IP address.
- ICMP flood, which is partially the same as smurf attack with the main difference being that it doesn't broadcast address. (Bleaken, 2010)

2.5 Exchange of information online.

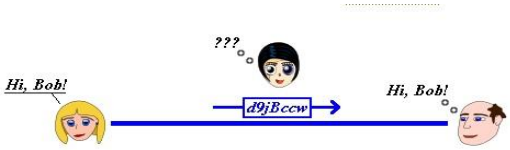
Cyber criminals do have in fact online communities where they talk and exchange information, tips or post mostly old patched and outdated exploits for newcomers to test. In order to categorize these forms of communication, one would have to approach the issue by its security protocol.

In normal hypertext (http) indexed internet there are forums with 4 being the most significant where there is shared information.

1) Hack forums
2) Mpgh forums
3) Cracking king
4) Nulled forums

In terms of chatting, Cyber criminals still use IRC channels that are a bit outdated. Their most used form of instant message communication is via XMPP protocol widely known as "jabber".

The XMPP protocol, is a decentralized, near real time instant messaging protocol based on XML language. Several applications / messengers where created regarding XMPP protocol. Paired with the add-on Off -the-record Messaging that uses a combination of AES symmetric key algorithm, Diffie Hellman key exchange and SHA-1 hash function cybercriminals are able to communicate with perfect forward secrecy. (Smith, 2016)



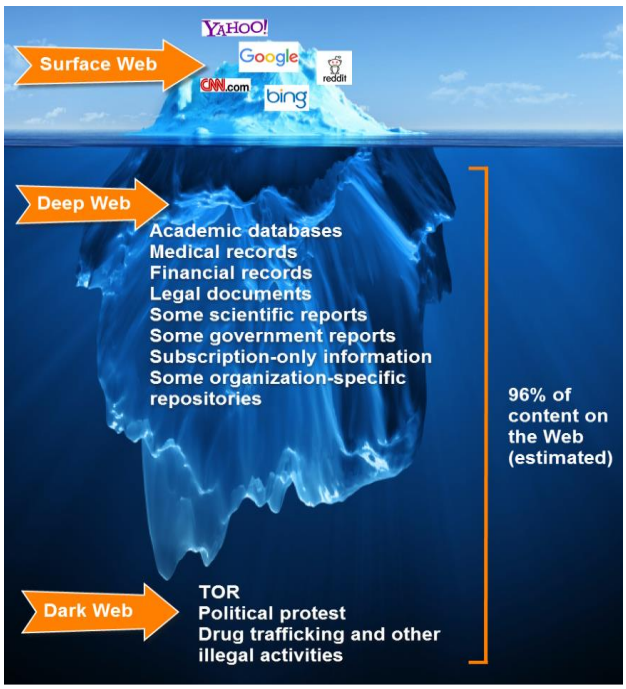
Picture 25: Screenshot from www.cypherpunks.com explaining the usage of Off-the-record.

As far as sending asynchronous messages cybercriminals favorite method is via PGP encryption. PGP derives from Pretty Good Privacy and is an encryption software that offers cryptographic privacy and authentication. With the usage of PGP one can sign, encrypt, decrypt, emails, texts, files even directories. PGP uses symmetric-key cryptography and public-key cryptography as well. PGP is the best option for encrypting asynchronous messages since the only thing needed in the public key of received. After sending the encrypted message the received can decipher the key by using his own private key and no one else can read the contents. (Smith, 2016)

Apart from communicating, cybercriminals that wish to sell, create online stores and sell their sniffed and illegally acquired data. However, these types of illegal online stores also work in the form of a brokerage where a team of cybercriminals creates a community and other cybercriminals list and sell their data. The team of cybercriminals that created the illegal community gets a percentage of every sale. There are three major online stores that sell these types of data such as:

1. slilpp.biz, a Russian created website that sells stolen information on e-banking details, email leads and cracked accounts from various merchants' stores.
2. xdedic.biz, a Russian website that offers log in details to compromised computers and servers. This type of website works in a form of a brokerage and recently got much attention from law enforcements and moved its services from the regular internet.
3. ccard.ru, a Russian website that offers stolen credit cards information from around the world.

However, being on the indexed side of the internet, or Clearnet as cyber criminals like to call it, isn't safe at all. Cybercriminals base their communication and operation in a different part of the internet named Deep web or Darknet. (Osborne, 2014)



Picture 26: Screenshot explaining the actual content of the internet and the size of the "uncharted" Deep Web.

Deep Web is based on onion routing, an anonymous communication method over a computer network. Onion routing works by encapsulating messages in various layers of encryption analogous to layers of an onion. Transmitting data occurs through a large series of network nodes called onion routers that each one sort of peels a layer, revealing that data's next destination. The message throughout its journey gets encrypted at every "stop". By revealing the last destination, the message arrives to its receiver and gets decrypted.

In order to access the deep web criminals, download a modified version of a popular web browser by Mozilla, in order to relay and actually be able to visit onion links. Its name is TOR and it is a browser that has every security feature patched. Tor is a product for anonymity but cybercriminals use it to protect their identity and visit illegal marketplaces and conduct illegal business in general.

Tor has by default JavaScript disabled and it doesn't accept any type of cookies. Tor has been configured in order to hide every bit of information that regular browsers show and it has webRTC leaks patched. Opposed to regular www, onion links have a completely different layout. In www, in order to use the search engine "google" one would have to type "www.google.com" in his browser whilst in deep web in order to use the search engine "grams" would have to type in TOR browser "grams7enufi7jmdl.onion". Onion is pseudo top level domain host suffix designating an anonymous hidden service reachable via the TOR network. These addresses aren't actually DNS names, and onion TLD isn't in the internet DNS root but with TOR browser onion addresses can be viewed. Main purpose of onion addressing system is to make tracing back very difficult. (Smith, 2016)

Picture 27: At left: Tor browser logo and on the right: Logo of the equivalent of Google in Deep web.

Several illegal marketplaces have flourished over the past years and several others where closed by local enforces. Today there are five marketplaces in deep web that offer illegally acquired physical items, drugs, counterfeit items, stolen information, guides and how to's:

1. AlphaBay market
2. Dream market
3. Valhalla market
4. Outlaw market
5. Hansa market

Cybercriminals either sell or buy resources needed in order to utilize them based on their purposes. Cybercriminals can also rent their resources for a fee such as Virtual Private servers, Remote Desktops, or botnet network in order for other cybercriminals to carry on attacks. At this point cybercriminals, have maintained an entry level of anonymity. One major issue that came across was how to make payments completely anonymous. Cryptocurrencies and especially Bitcoin was the answer to that question.

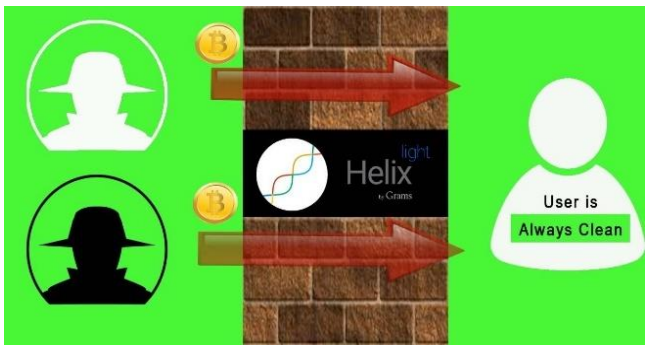
Bitcoin by default is a cryptocurrency and a payment system, their developer claims to be Satoshi Nakamoto which is still uncertain if it's one person or a dedicated team. Bitcoin was publicly realized in 2008 and is widely used today.

Bitcoin isn't the first cryptocurrency but it is the largest one when comparing it with other types of online cryptocurrencies. Bitcoin gained attention as it was the first decentralized digital currency. In order to buy bitcoins one would have to open up a bitcoin wallet. This is the user's virtual wallet. Countless companies today offer both offline and online wallets for bitcoin and even offer mobile application for faster transactions. In order to make a bitcoin payment one would have to know the recipient's bitcoin address. This could be considered as the receiver's public key. Bitcoin addresses get generated instantly and they are an outcome of several mathematical operations. Bitcoin addresses are alphanumeric and sometimes they can be presented as a QR code. (Frisby, 2014)

Picture 28: Screenshot taken from a major VPN company that accepts Bitcoin payments.

Bitcoin is stable by using blockchain technology a peer to peer software technology that protects the integrity of a digital piece of information. Blockchain is a distributed database that maintains a list of growing records named blocks. Each block can't be altered or edited and it does contain a timestamp and a link to its previous block. By using computers across the network bitcoins and without implementing centralized points bitcoin has no risk of failure and no one can attack the bitcoin network. One major thing about bitcoin is that transaction is public and transparent but the identity of the people behind payments are always private by default. (Frisby, 2014)

Apart from the security and anonymity blockchain and bitcoin provide, cybercriminals often use tumbling services in order to clean bitcoins earned by doing online fraud. There are several brokerage companies offering to mix bitcoins with new ones from the blockchain for a nominal percentage. By mixing or tumbling the bitcoins every possibility of locating the transaction via the blockchain is lost and cybercriminals can cash out these funds without fear of being targeted or located from local enforcements. (Stryker, 2012)



Picture 29: Screenshot from Helix, a Bitcoin Tumbling service that explains how tumbling works.

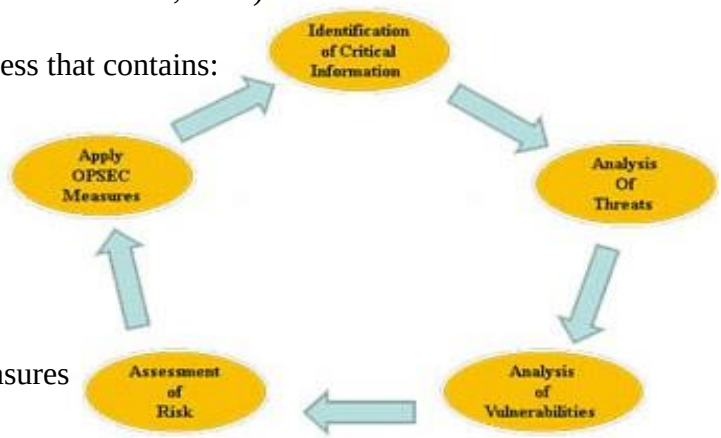
Encrypted messaging email, TOR browser, onion routing, bitcoins and blockchain is the top of the iceberg and do not actually offer total anonymity for cyber criminals to operate. The next chapter is focused in how cybercriminals reach total anonymity to conduct illegal operations.

3. Operation Security

It is a well-known fact that security analysts like to use military language (slang) and idioms in order to describe situations and conduct strategic analysis. Same feature applies to crackers regardless of hat color. Operation Security or OpSec is a term that originated from the U.S military slang and it is the process of identifying critical information, analyzing received data and taking measures regarding critical information. (Tipton & Nozaki, 2016)

In fact, Operation Security is a five-step process that contains:

- Identification of critical information
- Analysis of possible threats
- Vulnerabilities analysis
- Risk assessment
- Application of appropriate OpSec measures



Operation security has evolved from U.S military and has been used by private sector as well in many fields including Information Technology. Today operation security is an established methodology used by military, federal entities as well by businesses. As far as Information Technology goes, there are five different sub-categories where operation security is implemented such as:

- Information Security (InfoSec)
- Communications Security (ComSec)
- Transmission Security (TranSec)
- Cybersecurity
- Counter Intelligence

As a matter of fact, operation security grew so much that today there are professionals able assist companies and organizations in order to implement the basics of operation security. In order to implement operational security there are three key questions every security expert has to answer:

- “If you don’t know the threat, how can you know what to protect?” This question is in order to specify the possible threats that every professional security expert should know of.
- “If you don’t know what to protect, how do you know you are protecting it?” The second question is regarding selecting sensitive information to protect.

- “If you are not protecting it, the opponent wins?” The last question is about an operation security assessment in order to determine if critical information is vulnerable to exploitation by adversaries.

As the industry involves, larger amount of companies and organizations implement operation security on their businesses tactics in order to protect sensitive information from accidental disclosure, corporate espionage or even internal espionage. Operation security doesn’t assist businesses themselves but it also gives confidence to businesses clientele that their sensitive information is protected. (Hubbard, Seiersen & Geer, 2016)

As far as cybercriminals go, operation security is their most important component in their criminal operations. It is the stepping stone that allows them to conduct illegal business without getting arrested. Bottom line, having a solid operation security is what keeps cybercriminals safe from law enforcements agencies around the globe. In the cybercriminal world there are known three types of operation security:

- Good operation security
- Somewhat safe operation security
- Bad operation security

Having good operation security means, having:

- Encryption, it is the first and most important feature of having a reliable operation security
- Authentication, having always enabled two factor authentication in services
- Isolation, this means contacting other cybercriminals via encrypted channels and only share necessary information
- Compartmentalization, always keeping separate work setup and personal setup
- Multiple identities (Identity theft), cybercriminals must use different identities in order to remain safe
- Keep everything anonymous
- Never share information in real life
- Be somewhat paranoid, most cybercriminals have the fear that law enforcement is looking for them so they are always vigilant
- Act regularly, cybercriminals mustn’t overdo it and purchase items they couldn’t normally afford to
- Never share information on social media

- Always change base setup, guest machine, IP's, mac addresses user agents never keep the same for long time
- Using bulletproof hosting

On the other hand, having a bad operation security mostly means:

- Having difficulty keeping up fake identities, this means using real and fake information as well, or using their own home IP address
- Using the same IP or credentials, this is a common mistake that cybercriminals do
- Using weak or easy to remember passwords
- Leaving trails and mixing their work setup to their personal setup
- Posting on social media about it, or letting close friends know

3.1 Hardware gear

Cybercrime can't happen without the usage of either a computer or a broadband connection. It goes without saying that cybercriminals need to have a hardware setup in order to use it in their activities.

Operation Security wise most cybercriminals buy their equipment with cash. The logic behind this move is not having traced back any information regarding purchased items. That explains why cybercriminals never buy online both legitimately or through illegal sources their equipment. The most preferable choice on computer is an easy to carry, lightweight, with an average battery life but powerhouse laptop or Ultrabook. This occurs due to the fact that cybercriminals can conduct their business both outdoors and indoors. Also, this laptop – Ultrabook, is considered to be disposable if some part of the operation security goes wrong.

As far as connectivity goes, a wireless 2,4 Ghz USB adapter is needed, because most of wireless cards embedded in laptops aren't able to actually inject code. The best option would be a wireless USB adapter that doesn't need drivers both in windows or Linux operating systems and that has an RP-SMA adaptor in order to change the antenna based on the situation.

Picture 30: Examples of the best used wireless lan cards from Alfa Network and TP-Link. Covered in copper is the RP- SMA adaptor.

Another handy tool used as well by cybercriminals is a mobile broadband modem that usually comes to a form of a USB dongle and accepts SIM cards. This is a popular way to utilize the 3G or even the 4G networks by local cellular providers. Cybercriminals can purchase anonymous preactived SIM cards with data plans and are able to use them without being traced back. The only downside on using a USB mobile broadband modem is that only one device can be online at a time. Lately cybercriminals use as well Mi-fi which is actually a wireless broadband router which accepts SIM cards that is able to act as a wi-fi hotspot, so cyber criminals can connect more than one devices if needed at a time. Even though, cellular companies can locate the signal based on the base station it was registered to no arrests have been made so far with criminals using 3g or 4g data plans. (Holt, Bossler & Seigfried-Spellar, 2015)

Picture 31: At left: 4G usb data stick. At Right: Mifi Hotspot.

Cybercriminals are known to purchase disposable smartphones in order to use wireless tethering and other features. After a while, they dispose the smartphone and buy a new one. This is often called as an “android burner phone” because android Operating System is easily customizable compared to different mobile operating systems available in market today. (Stryker, 2012)

There is a form of cybercriminals that doesn’t like to be mobile and operates from their homes. These types of cybercriminals mostly use configurable routers that run Linux in order to connect to Virtual Private Network service providers and then connect their device online. There are two options when going for configurable - flashable routers:

- Tomato firmware routers, based on Hyper WRT that is Linux core firmware distribution, which offers some form of extra customization and is able to unlock the routers potential.
- DDWRT firmware routers, that is a Linux based alternative open source firmware that provides a tremendous amount of customization and extra features, detailed menus and easy to manage user interface.

Both router firmware’s are able to connect to OPENVPN, which is an SLL VPN solution and Point to Point Tunneling Protocol (PPTP) that is a feature for implementing virtual private networks. One would say that openvpn is broadly used due to its security features. Point to point tunneling isn’t used anymore due to latest discovered vulnerabilities.

Having a VPN service in a flashable router, means every time the user restarts the router, clients that connect to that router receive an address from a specific location where the VPN provider operates and not the ISP of the user. There are various companies that manufacture high quality flashable routers such as Asus, Netgear, Cisco- Linksys. (Smith, 2016)

Several cybercriminals have a card reader-writer in their basic operation security hardware. Today card readers are able to both read and write on magnetic stripe, clone cards and even HID cards as well.

Hardware equipment is a major component in cybercriminal activities but the most important in having a great operation security is securing software and data.

3.2 Operating systems

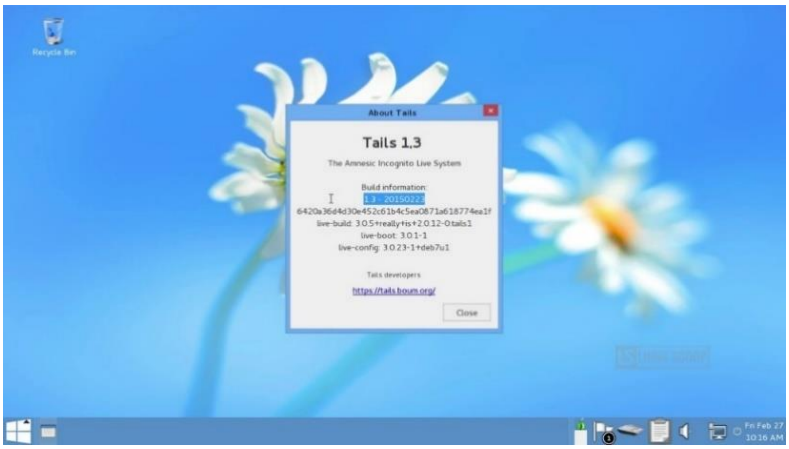
The first layer of security in a successful cybercriminal OpSec is using different equipment for criminal operations and different for personal usage. However as previously stated cybercriminals adopting the onion peel logic try to create as many layers of security they can. The most important part that actually secures the setup is selecting the correct operating system. There are two key features every cybercriminal has to take in mind: Encryption, and selecting the correct operating system for each project.

Cyber criminals are known to use operating systems with two methods:

1. Running a Live CD/DVD or live USB with the operating system. By creating a bootable drive containing a bootable operating system, they are able to conduct criminal activities on top of their personal setup. This OpSec is solid due to the nature of this setup since when taking out the usb stick or the dvd there aren't any data saved. On top of that it is quite easy to hide and destroy the usb stick by either breaking it in extreme scenarios or throwing it in water. This setup offers good amount of operation security but overall it is rather slow since the media loads from a dvd drive or a usb stick. (Luttgens, Matthew & Mandia, 2014)

One operating system that offers security features and can run on live usb is TAILS. Tails is an Amnesic Incognito live Debian based Linux distribution and its main feature is providing both privacy and anonymity. Tails can establish these features by forcing all traffic through TOR network and blocking every non-anonymous connection. By being amnesic, tails, doesn't leaves any digital fingerprints. Tails also has PGP encryption, XMPP messenger, and TOR bundle preinstalled. Tails is quite easy to use and the graphic user interface will look like windows 8 -8.1.

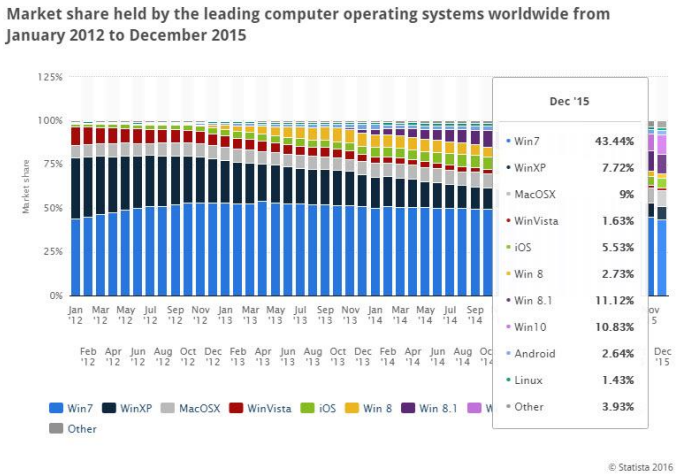
It is worth mentioning that the National Security Agency of the United States of America has marked this distribution as “catastrophic”. (FBI,2015)



Picture 32: Screenshot showing Tails Bundle running from a live USB.

2. Installing a secure operating system. This is a major key component that has to be studied extensively.

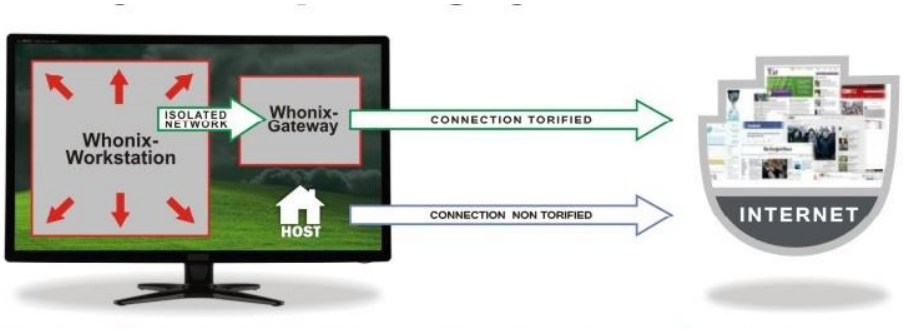
Based on large amount of Common Vulnerabilities and Exposures (CVE’s) it seems that Microsoft’s windows is not a “secure” operating system, what seems extraordinary is that it holds close to 55% of desktop operating systems market share. (Microsoft, 2015)



Picture 33: Microsoft statistics in operating systems.

Cyber criminals tend to use Linux based operating systems due to being free, stable, not requiring drivers, being easily customizable and they don’t have issues as much with malware or backdoors in software. It seems that cybercriminals favorite Linux distributions are security oriented ones that offer encryption and features they use on regular basis such as hard drive encryption, PGP encryption, XMPP messaging and ability to connect to a virtual private network.

A great example is Whonix, that is an operating system that is designed for advanced security and privacy. Whonix main advantage is its ability to channel all information through Tor network. On top of that whonix has an embedded failsafe in order to protect users from IP and DNS leaks. This isolated environment that whonix offers is also by default modded to have anti malware and anti-exploit features in order to lower threats in general. Whonix is divided into two separate versions, the whonix workstation and whonix gateway, although only Whonix gateway is needed in order to torify the network. Whonix gateway doesn't need to be combined with whonix workstation. Several users use whonix gateway as a "tor router" in order to send their traffic of their primary operating system that could be a different Linux distribution or even Microsoft windows operating system. (Goodman, 2016)



Picture 34: Analysis of how Whonix workstation and Gateway Torify the network.

There are various options when it comes to selecting a Linux distribution as a primary - host operating system. It seems, apart from the standard and generic Linux distributions such as Ubuntu, kubuntu, xubuntu, mint, open suse, arch Linux, and others, cyber criminals use distributions that where created in order to analyze and evaluate systems and network security. These distributions are known as Penetration Testing distributions (Pen testing) and are broadly used by white hat hackers and security analysts. Penetration testing distributions have evolved recently and they now offer a user-friendly design and interface as opposed to the past.

The most used penetration testing distribution comes from offensive security and it is known as Kali Linux, although it may be referred as well by its previous name, backtrack. Kali Linux is a Debian derived Linux distribution that has embedded almost all of the available penetration testing programs. Kali was designed to do penetration testing, digital forensics, security assessment, reverse engineering, cracking and supports cryptography. It also supports socks proxies by default but unlike its competition it doesn't support openVPN protocol, that needs slight modification to run correctly. (Dieterle, 2015)

Picture 35: Screenshot from the latest version of Kali Linux light.

Following the same logic there are more penetration testing widely used such as:

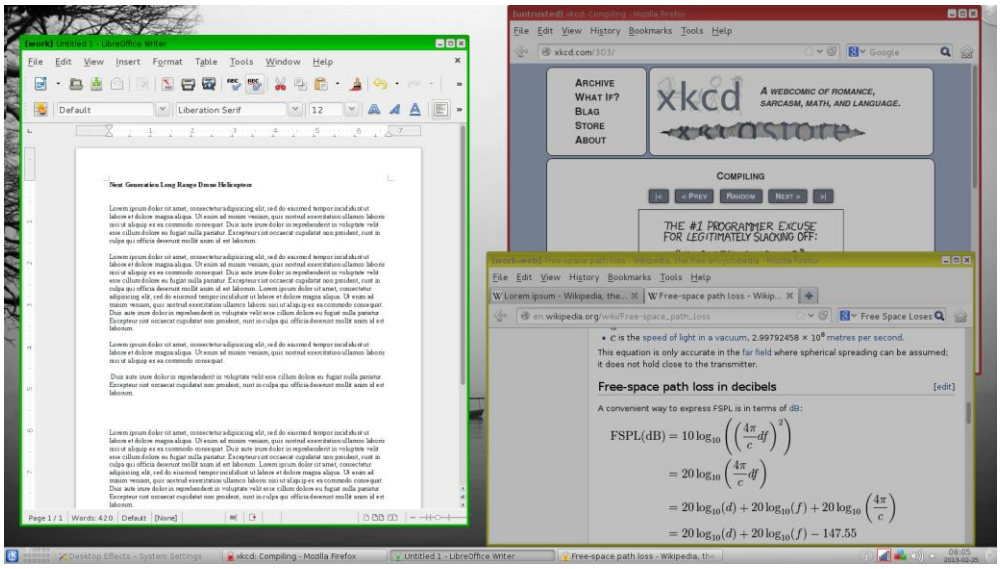
- KNOPPIX, that is an old penetration distribution
- Parrot Security OS, that is Debian based considered to be the most lightweight penetration testing suite that is more oriented in cloud penetration testing and future Internet of Things Security issues.
- Backbox Linux, that is based in Ubuntu desktop and offers a wide range of anonymity tools
- Pentoo, based in Gentoo Linux, is quite popular although there are several stability issues
- Black Arch Linux, it's an Arch Linux expansion that assists in penetration testing with 1082 embedded tools.
- Fedora security spin, is a distribution for security auditing and testing that offers a wide range of tools as well.

There are also specific distributions that are used such as:

- Deft that contains that Digital Advanced Response Toolkit that has a wide range of Microsoft Windows Forensics tools
- CAINE that derives from Computer Aided Investigative Environment, that is an Italian distribution focused purely in digital forensics with automated tools
- Wifislax a Spanish distribution based on Slackware that is focused in wireless network cracking. It features all the latest wireless cracking tools, included evil twin and WPS cracking apart from the usual air crack suite.
- Hirens Boot CD and System rescue CD, both are Linux distributions used to assist in Microsoft windows issues and vulnerabilities.

A great example of security by compartmentalization is Qubes, which is a free open source operating system that offers specific compartments (called qubes, thus naming the operating system) that are completely isolated from each other. This provides user with advanced security as they are able to use each qube for different operations without worrying about malicious software or being tracked.

If one qube gets compromised all other qubes are unharmed. On top of that qubes operating system offers disposable qubes in order for users to view suspicious email and attachments or test software or simply view downloaded files without having to worry regarding containing a malware. The major advantage of having qubes operating system is that even if an attack occurs to an isolated operating system inside a qube, user can keep going using other qubes without having to worry about the compromised operating system. Another great feature that security by compartmentalization offers is that every application that runs in each operating system installed is sandboxed and in no way will create issues to the other operating systems inside qubes. Qubes has been named as “a digital fortress” and as “the most secure than almost any other operating system available today” from the economist.



Picture 36: Qubes OS with three virtual Operating systems running colored as green, red and yellow.

Cyber criminals use Qubes as a host computer because it is easy to torify their network with it’s input of whonix gateway, thus creating as many qubes they can use in the torified network. Below is described the simple procedure of how a large number of cybercriminals behave online with Qubes OS.

Qubes OS	Whonix Gateway	Kali Linux
Qubes OS	Whonix Gateway	Microsoft Windows

In the chapter above has been studied the aspect of having a safe host operating system, however cybercriminals don't tend to just install the operating system in a hard drive. In order to maintain a high level operation security complete hard drive encryption is required. Encryption is a key component and adds an extra layer of security by protecting the information the hard drive contains so only the individual that knows the password can access it. There are several tools available with the most popular being True Crypt a free encryption software that was discontinued in 2014 due to speculation of security issues. Although based on the same source code new encryption software became publicly available with Vera Crypt being the most popular one. (Schneier, 2016)

Vera Crypt, just like its predecessor True Crypt offers full hard drive encryption, partition encryption and it offers the ability of creating encrypted compartments named volumes.

VerCrypt offers a vast amount of individual ciphers such as:

- AES
- Serpent
- Two fish
- Camellia
- Kuznyenchik

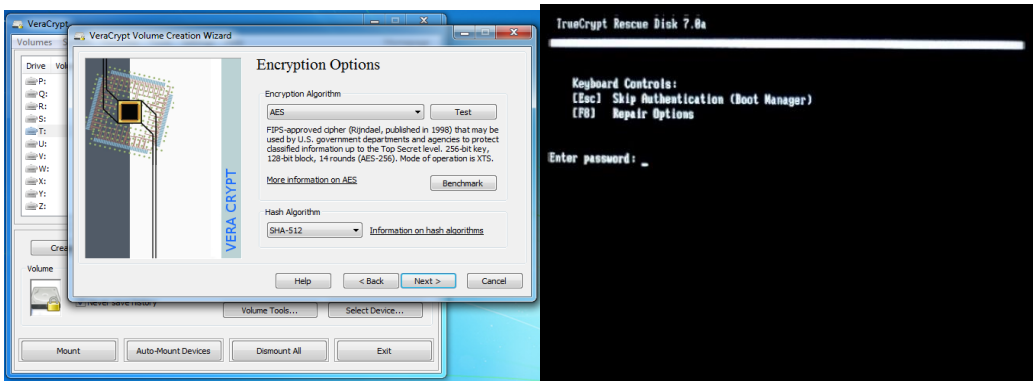
It also offers combinations of cascaded algorithms such as:

- AES-twofish
- AES-twofish-Serpent
- Serpent-AES
- Serpent-Twofish-AES
- Twofish-Serpent.

On a final note VeraCrypt offers SHA-256 and SHA 512, Whirlpool RIPEMD-160 and Streetbog cryptographic algorithms.

What makes VeraCrypt one of the best options in encryption is being available in both windows and Linux, it's support by their developers and being open source meaning that users can find out that there is no backdoor implemented in the application and just like its predecessor its ability to create both hidden volumes and public ones. This is a major key component as users create a visible encrypted compartment that inside contains files and a hidden compartment that only the user is aware of. This ability is currently known as plausible deniability, since the user can always deny the existence of the hidden compartment and its components due to lack of evidence.

Even if a user is forced to reveal a password, revealing the visible compartments encryption key couldn't harm the individual as the hidden compartment will still remain hidden with a different password. (Holt, Bossler & Seigfried-Spellar, 2015)



Picture 37: At left: Screen shot of Veracrypt menu in Microsoft windows, at right: Starting up an OS Veracrypt encrypted drive.

3.2.1 Virtualization

Due to the high growth of the 1990's and 2000's in the information technology field, new datacenters where created by corporations. This lead to an increased cost of creating and maintaining the physical datacenter infrastructure. There are more than one issues apart from the actual cost of hardware such as, cooling, management and maintenance. The actual issue was the underutilization of servers in the datacenter. A research from International Data corporation suggested that the average usage of a server was close to 15%. Virtualization came to address this issue.

Virtualization is the act of creating virtual versions of both physical hardware and software and has actually revolutionized the way information technology sector used to work. By transforming hardware into software virtualization allows multiple operating systems to run as virtual machines on top of the host server – computer. Virtualization assists both corporations and individuals. (Portnoy, 2016)

Virtualization tools for home computers are software based applications that allow users to create and deploy more than one virtual environment – operating system. This virtual operating system is known as Virtual Machine (VM). Focusing on individual usage, today there is a vast amount of virtualization software available both free and paid for such as KVM, VMware, parallels and virtual box. The virtual machine running in the host computer is usually known as guest and it is completely isolated from the host computer. As far as hardware resources go the user deploying the virtual machine is responsible in customizing and allocating physical to virtual resources.

3.2.2 Importance of virtualization in cybercriminal operation security

Virtual machines are broadly used by cyber criminals in order to cover their online tracks and avoid getting hardware fingerprinted. Having a closer look in the virtual machine implementation in a cybercriminal operation security, cyber criminals install one of the aforementioned virtualization applications on their host machine and on top of that create a virtual machine with a different operating system. One of the most used examples is cyber criminals using Linux distributions in their host computer, installing a bundle application of a virtualization tool create an encrypted compartment and on top of that install in the guest virtual machine a Microsoft windows operating system. Some virtualization applications offer virtual machine encrypting and password protection for an extra layer of security. It goes without saying that their operation security isn't secure enough or complete at this point since more layers of security need to be added.

In 2016 various online websites and online stores apart from regular browser fingerprinting, IP recording and DNS querying, save information regarding each user that visits the website. This extra piece of information regarding visitors is known as HardwareID, Hardware fingerprint or Device fingerprint. (Smith, 2016)

These are information about:

- OSType
- OSVersion
- Language
- ComputerName
- UserName
- Windir
- HDDnumber (Mostly on payment processors such as PayPal)
- Serial/IMEI (on mobile devices)

Using a virtual machine means being quite difficult to get fingerprinted since the host OS will have real hardware devices with their true id's whilst the guest OS will have virtual hardware devices with different id's. At this point virtualization actually assists cybercriminals in spoofing completely their hardware information. The above statement can be verified with various ways, such as checking the users MAC address in both host and guest from a terminal using on windows "getmac" or in linux "ifconfig" or even checking the hard disk serial number via terminal by typing in windows Vol C: assuming that the hard drive is "C" and in linux by typing "inxi -Dxxd".

Cybercriminals know that having different hardware ID than the one used in criminal activities is essential this is why it is preferred to use virtual machines.

3.3 Network related Operation security

So far it has been described how cybercriminals approach their operation security regarding creating and maintaining both physical and virtual applications in order to protect their identity focused on the hardware part. It is understandable at this point with the above analysis that there is no security regarding their online presence.

Each person that connects online receives a unique address commonly known as an Internet Protocol (IP) address. This numerical address is based on TCP/IP and serves two purposes, the first is providing identification to host or network interface and the second is the ability to locate an address. IP comes in two versions, IPV4 that is 32bit and IPv6 that is 128bit address.

IP address is assigned from Internet Service Provider of each user and could be static or dynamic.

With the setup described in the previous chapter, if a cybercriminal tries to do criminal activities online his IP address, his browsing history and more information will be known both to his ISP and to the victim's server, this is why it is important to hide their IP regardless of activity. If illegal activity occurs Law enforcements are able to trace the IP address of a user and find his physical address with co- operation of the user's ISP. (Viano, 2016)

Cyber criminals and online perpetrators in general need to use IP address hiding mechanisms in order maintain a high-level operation security and protect their identity. In the IP hiding subject, there isn't a specific pattern used by cybercriminals since most of them try to use IP hiding services on top of other IP hiding services thus creating more layers of security.

3.3.1 Virtual Private Network

One would say that the frontline of cybercriminals hiding their IP address is a Virtual Private Network (VPN). Virtual Private Networks allow users to connect from their IP address in a private and encrypted tunnel and channel their online traffic through this channel. VPN assists by providing a different IP address and DNS server based on the location of the VPN provider. This actually means if a user connects to a VPN from the USA and the VPN provider has datacenters in the Netherlands, the user's external IP will be from the Netherlands. However, the VPN provider will know the users primary IP and Internet Service Provider and might keep logs of the user's activity, logon / logoff times and bandwidth usage.

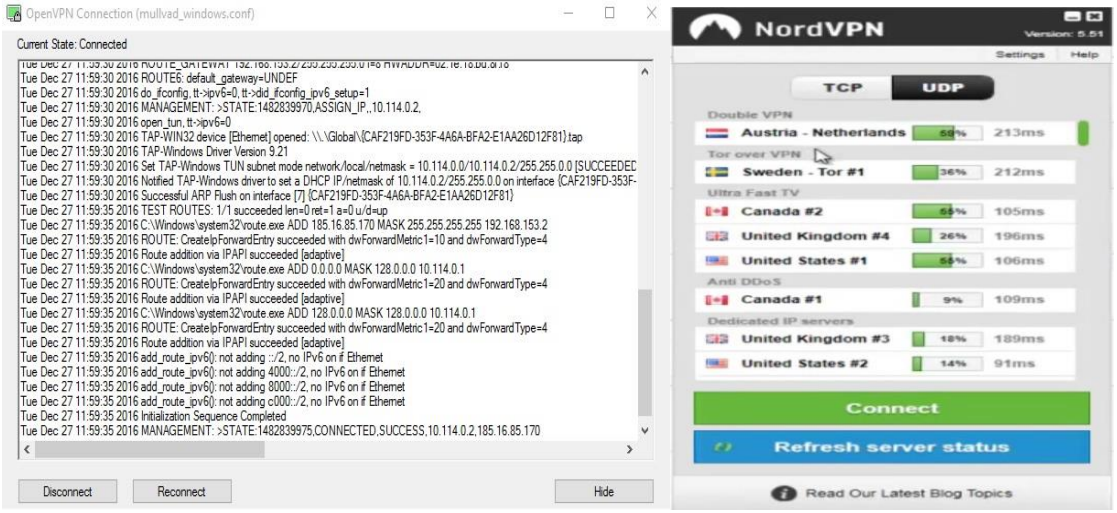
Various corporations offer solutions for this issue, commonly known as Virtual Private Network services providers. These corporations offer the VPN solutions for users that wish to establish a secure connection over an insecure network, access content not allowed in their country (region specific) or simply hide their online sharing activities that are banned in some Countries such as P2P sharing.

As far as cybercriminal activities go, there are various things they take in mind prior to buying a VPN subscription with the most important being:

- VPN provider being in Countries where legal legislation isn't defined regarding internet and online activities
- VPN doesn't keep logs that could assist get the user identified
- Require a small amount of personal information in order to sign up
- Accepts payments that can't get traced back to the user, such as cryptocurrencies like Bitcoin.

A couple more factors cybercriminals take in mind are:

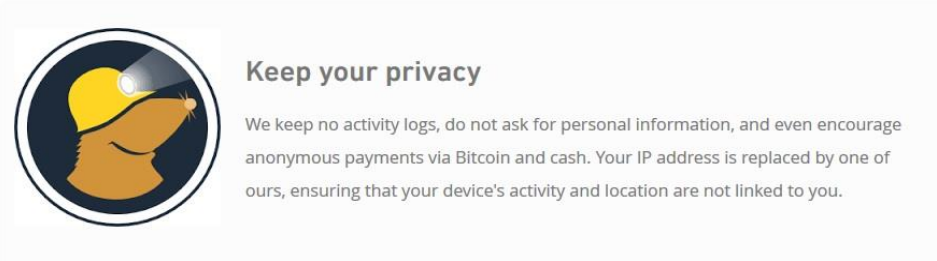
- VPN provider having multiple servers in different countries; thus, allowing them to change their IP to different ones
- VPN provider supporting all VPN protocols; with the most popular being openVPN.
- VPN provider offering protection from DNS leaks; Some VPN providers offer their own application that has embedded a Kill switch so it shuts down if the connection fails and protects user from revealing his true IP or their ISP's DNS server.



Picture 38: At left: OpenVPN connecting to VPN providers server, at right: Custom software from NordVPN.

These factors are taken into serious consideration by cybercriminals since some of the VPN service providers will give out information from their logs to law enforcements regarding user activities. These types of actions will actually disable every operation security measure taken.

One example of a VPN service provider handing over information of a cybercriminal occurred in 2011 by a service provider named “HideMyAss” a company located in the United Kingdom after a court order handed to FBI logs containing information that lead to the arrest of Cody Kretsinger (known as recursion) that was able to access unauthorized servers belonging to Sony Pictures Corporation. Several years after this case many VPN service providers advertise that they in fact keep no logging activities of their users thus if forced to court they wouldn’t have any information to hand over. These are actually the VPN service providers most of cybercriminals use. On another note its seems digital currency is accepted by the majority of VPN service providers thus giving an extra level of anonymity between user and VPN service provider. Almost every major VPN service provider advertises in their main webpage that they in fact do not keep logs and accept digital currency payments. A monthly VPN subscription starts as low as 5 USD and can go up to 30 USD. .



Picture 39: Screenshot from Mulvad’s VPN company website.

Based on IP’s monitored getting a TOR exit node it seems the most favorite VPN service provider’s users use to access TOR network are:

- Mullvad
- NordVPN
- PerfectPrivacy
- VIP72
- SecureVPN

Extensive research on multiple VPN providers has been carried through by testing, terms and conditions policy crosschecking and actual cases. The table below describes every VPN provider that cybercriminals use to operate.

Best VPN Providers								
VPN Service Name	Location	Data Collected	IP/ Web Activit	IP Logs Delete	DMCA Policy	P2P Allowed?	VPN Protocols Offerd	Crypto-currencies
BTGuard	Canada	"Personal Information"	No	N/A	Does not respond to DMCA	Yes	PPTP OpenVPN	Bitcoin
MULLVAD	Sweden	Litteraly nothing - You click "create account" and you get an account number. ZERO	No	N/A	Does not respond to DMCA	Yes	PPTP OpenVPN	Bitcoin
NORDVPN	Panama	E-mail address Username/password Billing infomraiton	No	N/A	Does not respond to DMCA complaints	Select servers	PPTP L2TP OpenVPN TCP	Bitcoin
PRQ	Sweden	E-mail address	No	N/A	Does not respond to DMCA	Yes	OpenVPN	Bitcoin
Private Internet Access	USA	E-mail Address Payment Data Optional temporary cookie	No	N/A	DMCA Compliant (Reminder: No logs means no data to turn over)	Yes	PPTP OpenVPN IPSEC/L2TP	Bitcoin
SHADEYOU VPN	Netherlands	Username/password	No	N/A	DMCA Compliant (Reminder: No logs means no data to turn over)	Yes	PPTP OpenVPN L2TP	Bitcoin
TorGuard	USA	"TorGuard collects personally identifiable information... for ordering products and services."	No	N/A	DMCA Compliant (Reminder: No logs means no data to turn over)	Select servers	PPT OpenVPN L2TP SSTP	Bitcoin
OCTANEVPN	USA	Name Address E-mail address Payment info	No	N/A	DMCA Compliant	Yes	PPTP OpenVPN IPSEC	Bitcoin
SLICKVPN	USA	E-mail Username/Password Apache Webserver Data Payment Data E-mail corresponance Google analytics Temporary cookies	No	N/A	DMCA Compliant	Yes	OpenVPN	Bitcoin
SECUREVPN.TO	*multiple locaions	"Personal Information"	No	N/A	DMCA Compliant (Reminder: No logs means no	Yes	OpenVPN (UDP/ TCP)	Bitcoin Litecoin Feathercoi

Picture 40: Screenshot from www.deepdotweb.com a website for news and tips from the Deep web.

3.3.2 Proxies

As previously stated, Virtual Private Networks are the first line of protection cybercriminals use to cover their tracks and protect their identity. Another popular solution in getting anonymized are proxy servers.

Proxy servers are intermediate computers that act as a “proxy” between the user and the internet. Proxy servers where initially used for traffic filtering and accelerating data transmission, but they are broadly used by cybercriminals since they offer a great level of anonymity. (Alisdair, 2015)

When a cybercriminal uses a proxy server the IP provided by the proxy server will be shown in his activities and not his private one. However just like VPN providers some proxy servers keep log files with users IP, logon/ logoff times, this is why cybercriminals never connect directly to a proxy server.

There are four types of proxy servers:

- HTTP Proxy server, which are the most known form of proxy servers, they are broadly used this is why they may be referred to just as a proxy servers. Using and setting up an HTTP proxy server is quite easy since every browser can run this form of proxy server.

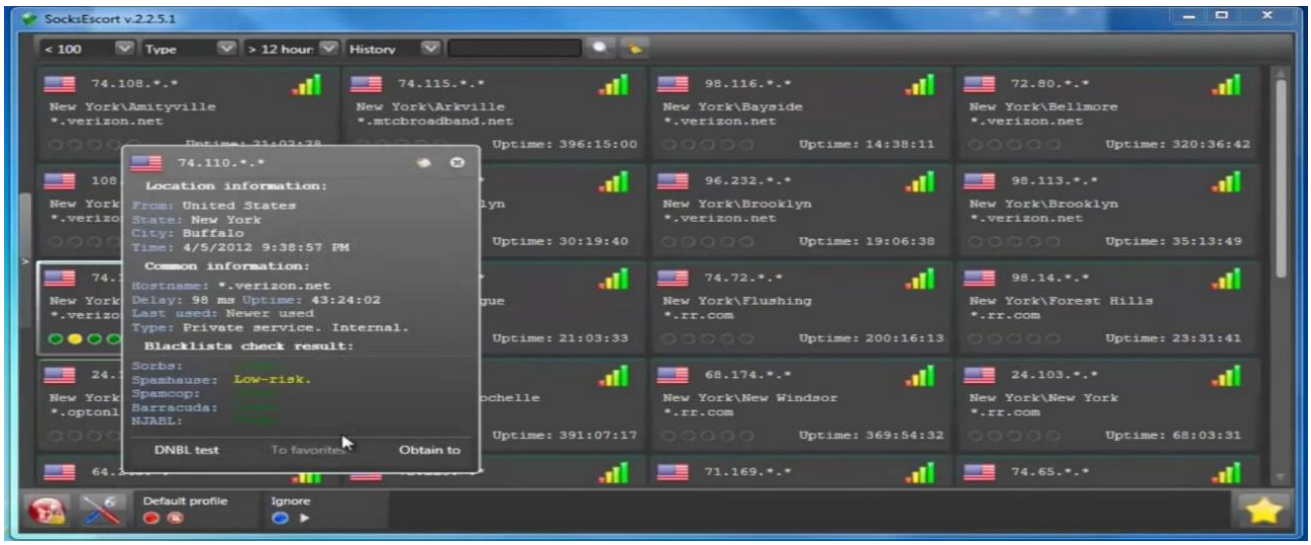
- Socks proxy servers, that can be categorized in socks 4 proxy and socks 5 proxy. The main difference between socks 4 proxy and socks 5 is that socks 4 proxy only supports TCP applications whilst socks 5 proxy supports both TCP and UDP applications. These types of proxies are mostly used by cybercriminals and there are a lot of companies offering socks proxies packages of clean and non-blacklisted IP's. The advantage of socks proxy is that user can forward all his traffic via this proxy however socks proxy can't run on its own as additional software is required. The most used and famous socks proxy tool is proxifier and application that allows users to proxify each application through the proxy.(Viano, 2016)
- Anonymizer or CGI proxy server, it is used through browsers and using them to proxify other applications isn't advised. Anonymizer on the other hand, is fairly easy to work with and can be chained with different types of proxies as well.
- FTP proxy servers, these are mostly used in corporations based on the firewall installed, that prevents direct access to the internet.

Proxies can be acquired both legally and illegally and the same applies to the IP's of the proxy servers. Some IP's will come from compromised computers or servers and usually they are sold in the deep web with 48 hours' guarantee. Although as previously mentioned there are several companies offering complete packages of socks 5 proxies that accept digital currencies. Most of these companies offer their own solution upon proxyfying application and IP blacklist checking.

Examples of transparent socks 5 proxies legitimate providers are:

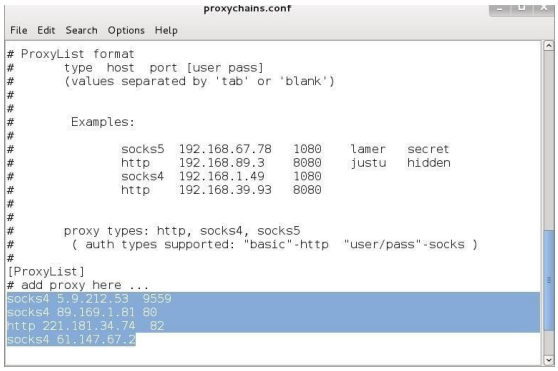
- Vip72.com
- Sockscescort.com
- Luxsocks.ru

Picture 41: Screenshot from www.socksescort.com website advertising socks proxies and custom software.



Picture 42: Custom software curtasy of Socksescort, real time proxy blacklist checking and switching.

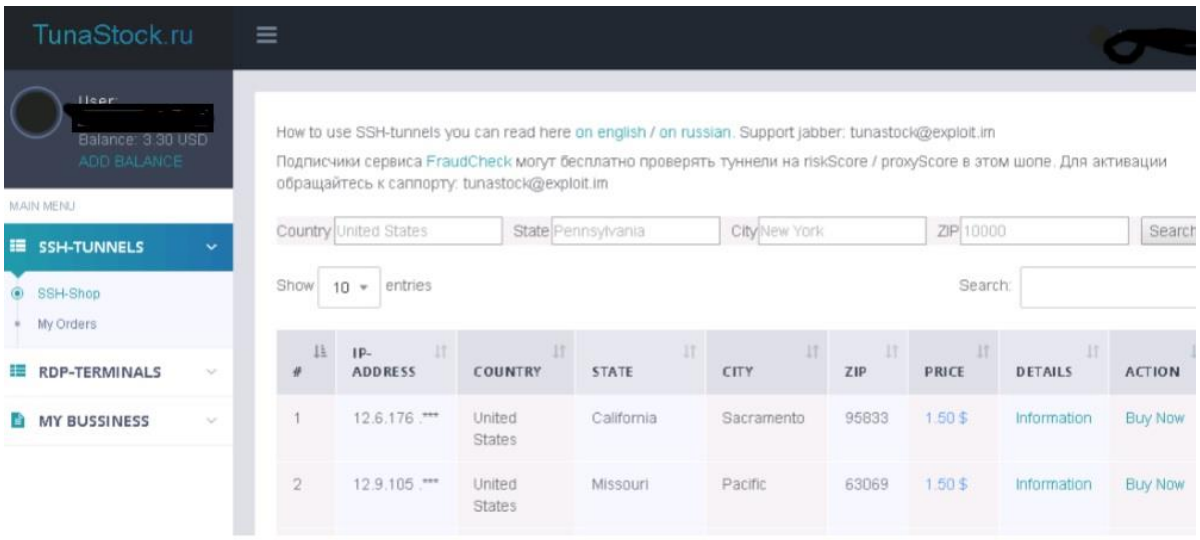
These proxies are sold in the form of a subscription with or without specific amount of proxies to use. Socks proxies are from around the globe so cybercriminals can select a clean IP close to their needs. Cybercriminals that work with proxies like to use multiple proxies together in order to increase the difficulty of being tracked, this is known as a proxy chain.



Picture 43: Proxy chaining in kali Linux via terminal.

3.3.3 Secure Shell and Windows Remote Protocol

Last but not least two remote methods of accessing legitimate or compromised servers. Secure Shell is a secure remote connectivity protocol in TPC/IP network, it allows users to work securely in an unsecure network. Secure Shell doesn't provide a graphical user interface and can be accessed through third party applications. In cybercrime accessing via SSH servers is used as a part of a simplified operation security since it its quite easy to implement. Users connect remotely to the client and then using various applications and configuring their browser can send their traffic through the servers IP. One major SSH store selling hacked SSH details in Clearnet is www.tunastock.ru. This site has been around for a while and offers over 50.000 hacked SSH details as low as 1,50$ per item.



Picture 44: Screenshot from Tunastock.ru marketplace.

Windows Remote Desktop, broadly known as RDP, is a remote desktop protocol from Microsoft that provides graphical user interface to users. Both protocols where created to remotely access, troubleshoot or maintain servers, but cybercriminals use them as a part of their operation security since these RDP IP's are usually clean to work with (non-blacklisted). On the other hand, some RDP IP's come from Datacenters IP's and don't appear as residential ones which is a red flag in cybercrime. Using RDP's in the cybercrime world is easy as most of the time users don't feel the need to create and maintain a high-level operation security. Accessing RDP's is easier than setting up SSH client and send traffic through the servers IP. (Clough, 2015)

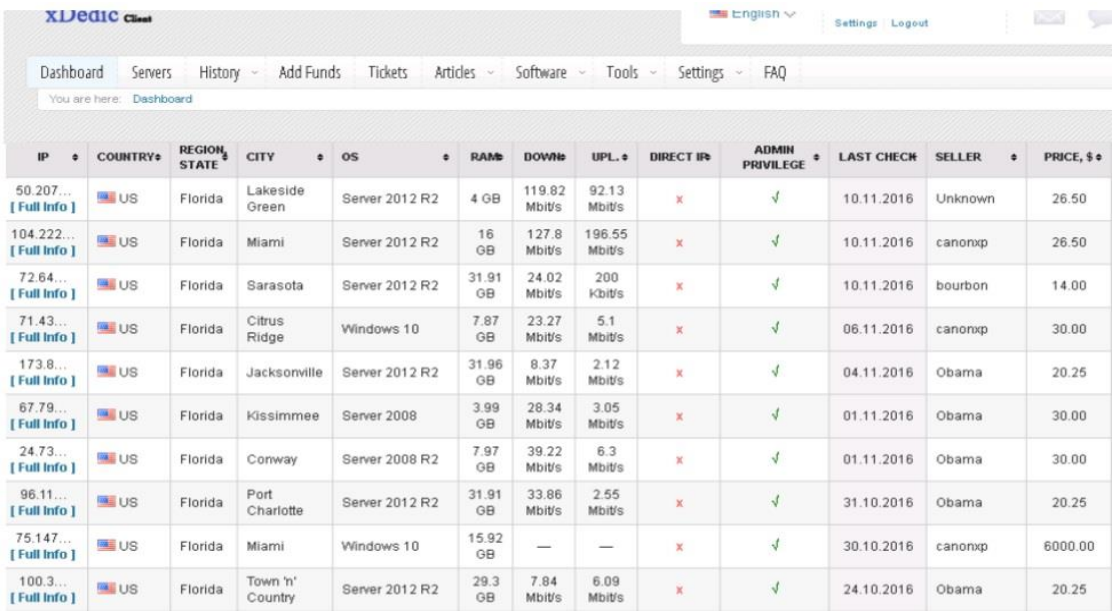
Picture 45: Windows Version of RDP.

In both remote connectivity methods three items are needed:

- IP of the server
- The Username of the user
- The password of the user

The same principle applies to remote protocols as with Virtual Private Networks and Proxies, users interested in them can buy them both legitimately or cracked RDP's from the deep web. One example of a website in Clearnet that recently moved to deep web selling illegally acquired RDP servers is www.xdedic.biz, a Russian website that only accepts bitcoin payments.

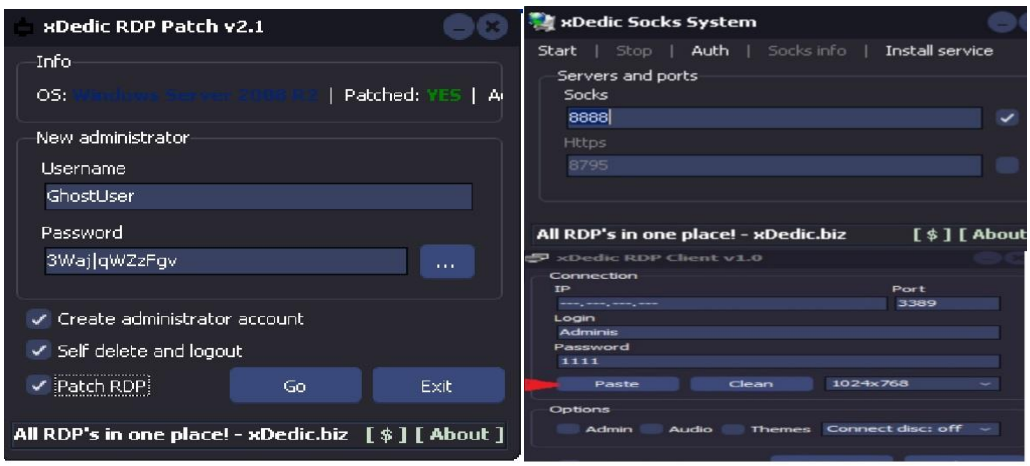
It is a complete underground marketplace that actually facilitates in selling and purchasing RDP servers. Apart from its illegal purpose it offers scam protection and high quality support. In xdedic marketplace users can select an RDP over 75.000 available cracked RDPS that may be from universities, corporations, even foreign governments. By reverse searching the university IP's one can locate the origin of the cracked webserver. A stunning fact is that there are over 800 RDP's from universities in the Information technology field that their login information is a combo of "admin -1234 or admin -admin". It goes without saying that there are over 1500 cracked Greek RDPs. Moreover, there are IP's from 8 Greek information technology related universities with clean non-blacklisted IP's and admin rights.



IP	COUNTRY	REGION, STATE	CITY	OS	RAM	DOWN	UPL.	DIRECT IP	ADMIN PRIVILEGE	LAST CHECK	SELLER	PRICE, $
50.207... [Full Info]	US	Florida	Lakeside Green	Server 2012 R2	4 GB	119.82 Mbit/s	92.13 Mbit/s	x	√	10.11.2016	Unknown	26.50
104.222... [Full Info]	US	Florida	Miami	Server 2012 R2	16 GB	127.8 Mbit/s	196.55 Mbit/s	x	√	10.11.2016	canonxp	26.50
72.64... [Full Info]	US	Florida	Sarasota	Server 2012 R2	31.91 GB	24.02 Mbit/s	200 Kbit/s	x	√	10.11.2016	bourbon	14.00
71.43... [Full Info]	US	Florida	Citrus Ridge	Windows 10	7.87 GB	23.27 Mbit/s	5.1 Mbit/s	x	√	06.11.2016	canonxp	30.00
173.8... [Full Info]	US	Florida	Jacksonville	Server 2012 R2	31.96 GB	8.37 Mbit/s	2.12 Mbit/s	x	√	04.11.2016	Obama	20.25
67.79... [Full Info]	US	Florida	Kissimmee	Server 2008	3.99 GB	28.34 Mbit/s	3.05 Mbit/s	x	√	01.11.2016	Obama	30.00
24.73... [Full Info]	US	Florida	Conway	Server 2008 R2	7.97 GB	39.22 Mbit/s	6.3 Mbit/s	x	√	01.11.2016	Obama	30.00
96.11... [Full Info]	US	Florida	Port Charlotte	Server 2012 R2	31.91 GB	33.86 Mbit/s	2.55 Mbit/s	x	√	31.10.2016	Obama	20.25
75.147... [Full Info]	US	Florida	Miami	Windows 10	15.92 GB	—	—	x	√	30.10.2016	canonxp	6000.00
100.3... [Full Info]	US	Florida	Town 'n' Country	Server 2012 R2	29.3 GB	7.84 Mbit/s	6.09 Mbit/s	x	√	24.10.2016	Obama	20.25

Picture 46: Screenshot from xdedic.com marketplace.

On top of that Xdedic offers its own tools for accessing, creating socks 5 proxy of the RDP in question and actually offering a tool that allows multiple remote users to access the same RDP. This is an excellent script since the victim isn't aware that someone is using his server. This tool is targeting non-datacenter windows versions that allow only one user per remote connection. Also, one useful tool as well, is a custom made one that offers the ability to automate the RDP as a socks proxy. This leaves the user to freely use the victims IP and conduct illegal activities without logging remotely to his computer.



Picture 47: Screenshot from xdedic's custom made application on windows based OS.

3.4 Selecting and Securing Browser vulnerabilities

In order to have a completely secure and anonymous presence one last customization has to be made. Every user in order to access and be able to browse online has to use a web browser which in a nutshell is a software application that is able to show content from the world-wide web. There are several browsers produced by different companies but all of them assist the same purpose; being able to view URL's. An example of a secure web browser is already mentioned in this thesis, TOR browser.

Even though TOR has been proven to be an excellent browser at a security- privacy concerned environment, this is being the only browser cybercriminals use. It is known that cybercriminals sometimes commit the crime of identity theft, by impersonating a different person. In order to surf online and impersonate a legitimate user cybercriminals need the IP to match the victim's town/ country, an issue solved by VPN's and socks proxies, but furthermore they need a browser that isn't in the TOR network and doesn't have as many antifingerprinting, anti-canvas modifications and add-ons that the average user doesn't use. On top of that online websites will red flag a user that denies any fingerprinting and his IP originates from possibly a blacklisted TOR server.

As with every bit of software goes some browsers are more secure that others and others are easily customizable to be somewhat secure. Browsers are generally large and complicated pieces of software and one flaw on the code can potentially lead to being abused by crackers. This logic however can be reverse engineered so law enforcements could use the same browser vulnerabilities to track cybercriminals.

It is well known that several companies are tracking information of internet users for several purposes including online advertising, behavior analysis, online fraud protection, identity theft

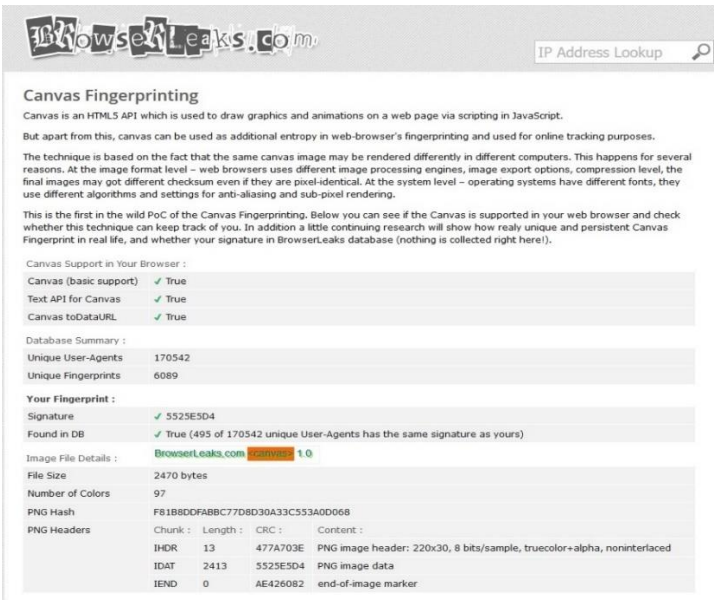
protection and account hijacking in general. Big data analytics are used by companies for various purposes.

When a user installs a web browser in his computer, a browser fingerprint (may also be referred to as an instance) is created to the specific installation of the browser in the specific computer or device. Browser fingerprinting is information and browser related properties collected about a computer or a mobile device for the main purpose of identification. Fingerprints can be used in order to partially or fully identify users or devices regardless of cookies and JavaScript status. Browser fingerprinting consists of information regarding the computer operating system, system fonts, browser add ons, browser version, screen dimensions.

This is based on the assumption that a browser fingerprint remains the same and is in fact unique regardless of updates on the operating system or the browser itself.

Browser fingerprinting could be categorized in four major heads:

- JavaScript, a cross platform object oriented scripting language that is broadly used for content in the internet. JavaScript has been exploited in order to get information regarding navigator and screen; information about operating system, browser name, browser version, screen resolution and color depth. JavaScript can be exploited further with the combination of HTML5 canvas element in order to provide more information regarding the user agent and finally the end user. Canvas fingerprinting actually draws graphics and animation on a web page via JavaScript scripting. In simple words, it draws images based computers hardware specification, operating system and browser fingerprint so this canvas fingerprint can't be duplicated in any way. Several websites offer canvas fingerprinting crosschecking.

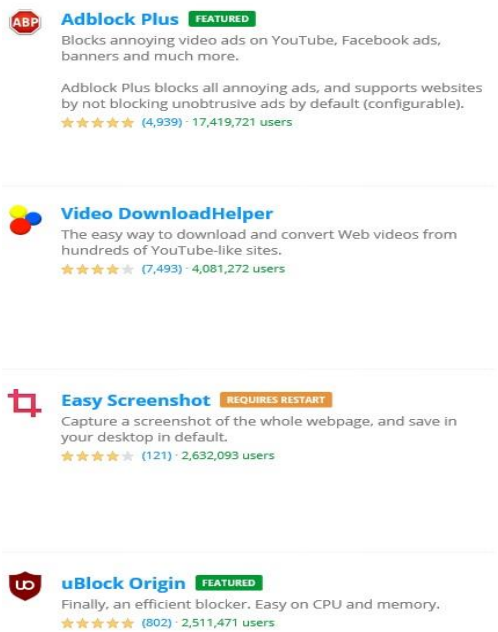


Picture 48: Screenshot from analysis on Canvas Fingerprinting.

- Plugins, are a bit of software that offers extra features to the browser that it doesn't include by default. Famous examples of plug ins are Adobe's flash player and Oracle's Java. Plugins API's are able to access both software and hardware properties on the computer-device. Both plugins are cross platform, although flash player is preferred when tracking and not java since java content requires user permission to run.

Picture 49: Screenshot that requires user action to activate Java in webpage.

- Extensions – Add- ons, these are software components that adds additional functions to a web browser. Add-ons could be about, pdf viewers, automated one click video downloaders, ads and pop up blockers and also privacy related add ons. There are several add-ons that assist limiting or completely eliminating getting fingerprinted. No Script is an add-on currently preinstalled in TOR browser bundle and assists as an enhancement in user's privacy and security by blocking JavaScript. Another example of a popular add-on is User agent switcher an add-on that lets the user spoof his user agent.



Picture 50: Screenshot from Mozilla Firefox Add-ons Library.

- Headers, it is already known that information is shared between client and server at all times. On the browser environment side, several bits of information are shared such as IP address, HTTP headers and user Agent String.

HTTP Headers :

Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding	gzip, deflate, br
Accept-Language	el-GR,el;q=0.8,en-US;q=0.5,en;q=0.3
Dnt	1
Referer	https://browserleaks.com/
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0

TOR Relay Details :

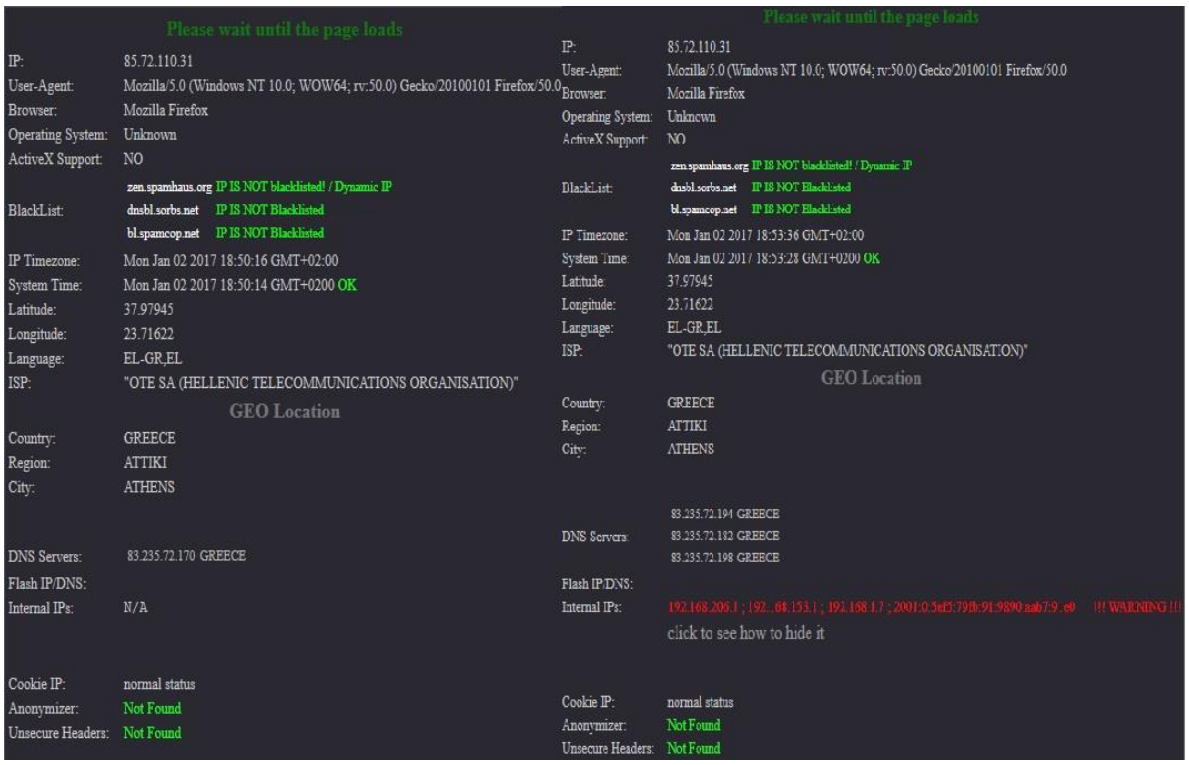
Relays	Your IP is not identified to be a TOR Relay

Picture 51: Screenshot from www.browserleaks.com where HTTP headers are verified match.

Furthermore, several anti-fraud companies and mostly payment processors that offer this type of service, have a repository of browser fingerprints. If fraud occurs with a specific browser fingerprint, evidence is stored and the browsers fingerprint gets flagged and blacklisted. Having the user's unique browser fingerprint in blacklist means that future fraud attempts can be prevented.

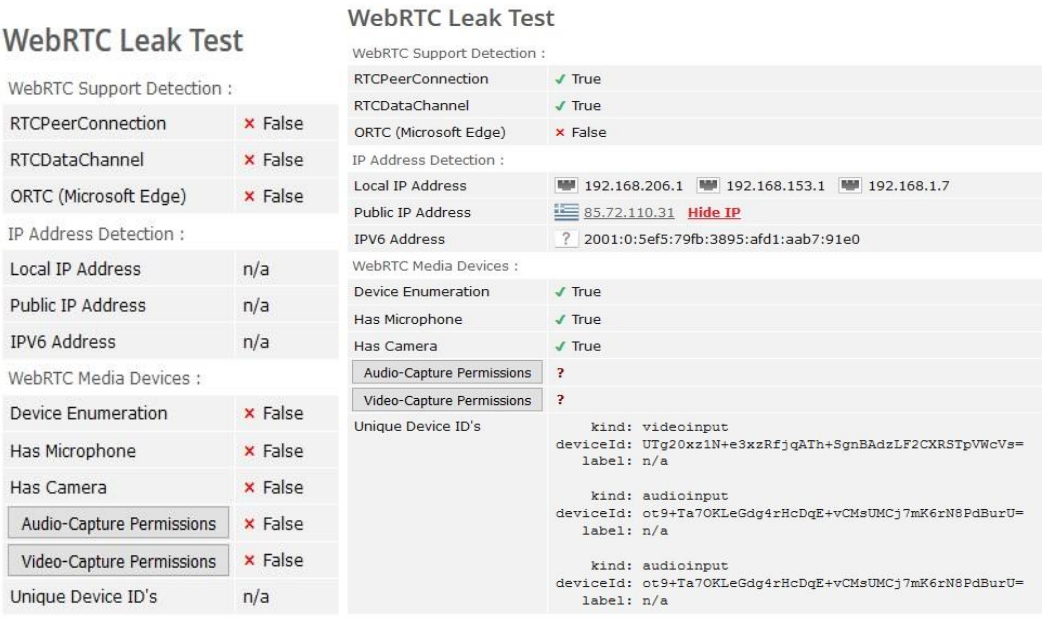
All these factors should be taken into serious consideration by cyber criminals in order to protect their identity and reveal only spoofed or non-linkable amount of information from their browsers. By doing so they will have a non-linkable browser but with enough amount of information so that websites wouldn't put a flag on that users IP or browser fingerprint.

One major factor that changed cybercriminals preferences regarding their most used browsers is WebRTC leaks or RTC Peer Connection. WebRTC is an experimental technology currently prefixed in numerous web browsers available publicly. RTC refers to real time communication that works in a combination of standards, protocols and JavaScript APIs, that allow peer to peer audio, video and data sharing between browsers. WebRTC is able to leak two characteristics; the first one is the ability to reveal the users private (internal) IP address and unmask any obfuscation IP application. Furthermore, if a user has and uses a VPN subscription, RTC leak will reveal his real IP, his IPv6 address if applicable and his internal IP on his router configuration thus making useless his primary layers of security. The second function of webRTC is to show media devices registered in the computer. That means if a user has a microphone or a camera or in fact any type of device connected it will reveal its unique device ID.



Picture 52: Using www.check2ip.com at left webRTC leaks are patched where on the right one can see the internal IP and IPv6 as well.

Above there is an example of Mozilla Firefox user agent with webrtc leaks patched and webrtc leaks on their preset status, currently revealing the users internal IP address. Also included is the IPv6 address of the user. In this scenario, the user didn't use any VPN services, if however, he did, this real IP from his ISP will be shown as well.



Picture 53: Extended test on webRTC leaks where the user's unique device ID shows up on the right.

Web RTC leaks occur on all stock browsers. However, webRTC browser leaks can be prevented by customizing some browsers. On the other hand, some browsers are unable to switch off the web RTC leaks and users rely on third party applications and add-ons that may or may not work at all times.

One example of a browser that is capable of being customized is Mozilla Firefox. Using the browsers graphical window and entering about:config in the address line one can disable webRTC leaking on both IP and hardware information. The user has to manually customize some browser options in order to completely disable webRTC leaks. The same applies to every Firefox version available in Linux distributions. Example of browsers that can't have webRTC disabled is google chrome and Microsoft edge, however there are some third-party add-ons that offer to disable but at the current time of writing this thesis they don't seem sufficient.

Based on the above information Mozilla Firefox is the most preferred browser in terms of protecting one's identity and being able to spoof a large amount of information; exactly what a cybercriminals toolkit needs. By adding some useful add-ons available for the Mozilla browser cybercriminals are able to change their http headers, useragent, disable webRTC, have cookies at specific folder or automatically delete cookies and of course use blockers for flash and java objects.

Some examples of popular add-ons are:

- User Agent Switcher, an add-on that lets the user spoof his browser and information shared. That means that user can use Mozilla Firefox in a windows operating system and with this add-on virtually change his user agent to a safari one from an OSX operating system.
- Modify Headers, is a specifically useful add-on that is able to modify and add HTTP request headers so a user can completely spoof his user agent and geolocation.
- No script and flash block, are both blockers for JavaScript, java and flash objects.
- Cookie safe and closenforget, are both cookie management add-ons, that a user can change their permissions transfer them to another browser or completely eliminate them.

Some cybercriminals prefer to use Firefox portable bundled the aforementioned add-ons since it is easily manageable. Firefox portable is 95megabytes and doesn't need to get installed. It supports all Firefox's add-ons and it doesn't create any common files in Microsoft windows. Portable Mozilla Firefox is also known in deep web as "portafox".

One major flaw that this setup has is that the user has to manually make a lot of changes in order to create a fake "unique" fingerprint. However, security related companies have studied those free add-ons and blacklisted the preset canvases offered in an attempt to limit online fraud.

3.5 Custom Developed Applications

So far in this thesis it has been studied how cybercriminals utilize free or paid for software in order to hide their identity in order to commit fraud. Some online fraudsters have created applications and virtual machines in order to automate the procedure of setting up and maintaining proper operation security. These types of applications – software is sold in the deep web or in a very specific part of the Clearnet. Several cracked versions appear from time to time but they are unstable and most of the times contains malware. This is in fact software developed by cybercriminals for cybercriminals. (DeepDotWeb, 2016)

3.5.1 FraudFox

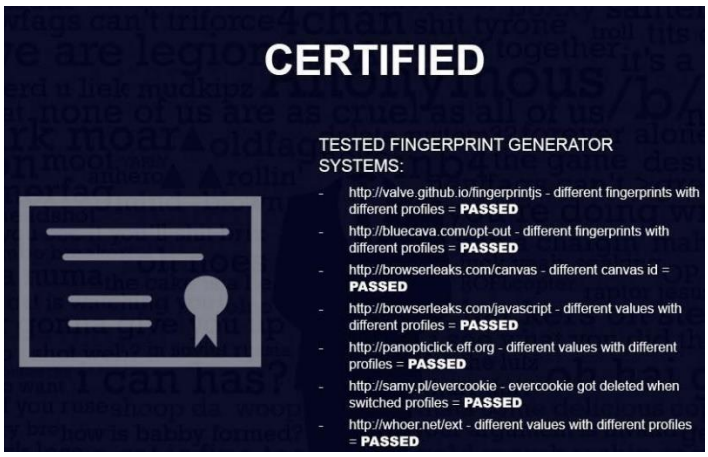
The first and quite popular among online fraudsters was developed by an unknown individual that claims to be a programmer with nickname “Hugo Chavez” or “Hugo” and its name is Fraud Fox (FF). Fraud Fox is advertised to be the first all in one tool for user agent, device spoofing and IP & DNS leak free virtual machine ever created. Its marketing campaign and promotion is based in the fact that Fraud Fox is able to assist both seasoned cybercriminals by saving tremendous amount of time having and maintaining multiple vm’s as much as for new cybercriminals that would like to start and scale their business.

Fraud Fox is sold in a form of monthly subscription that costs 99 USD. It’s main purpose isn’t for cracking or any intrusion related cybercriminal attack but it is known to be a great tool to cybercriminals that commit online economic crimes, included the act of identity theft and stolen credit card usage.

Picture 54: FraudFox logo.

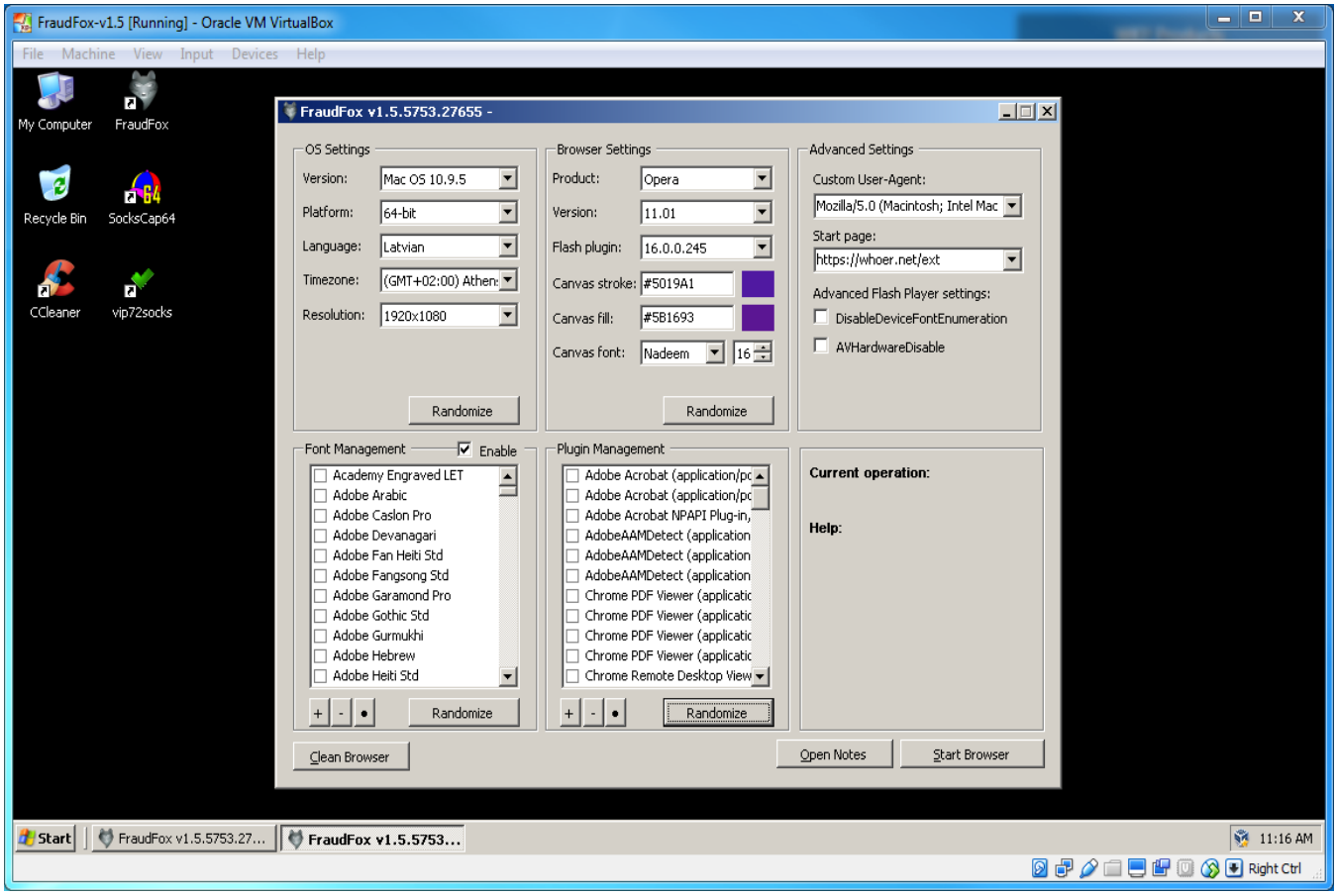
Fraud Fox is available to import for two virtualization software’s, Vmware Workstation (and fusion) and Oracle’s Virtual Box. However, its developer insists on using only the virtual box versions due to the fact that it is open source when compared to Vmware workstation.

Looking inside fraud fox, it is a completely edited and customized Microsoft windows XP version, that is able to spoof every single bit of information needed. Furthermore, Fraud Fox has been tested with every new fingerprinting method available and has passed all up to date tests.



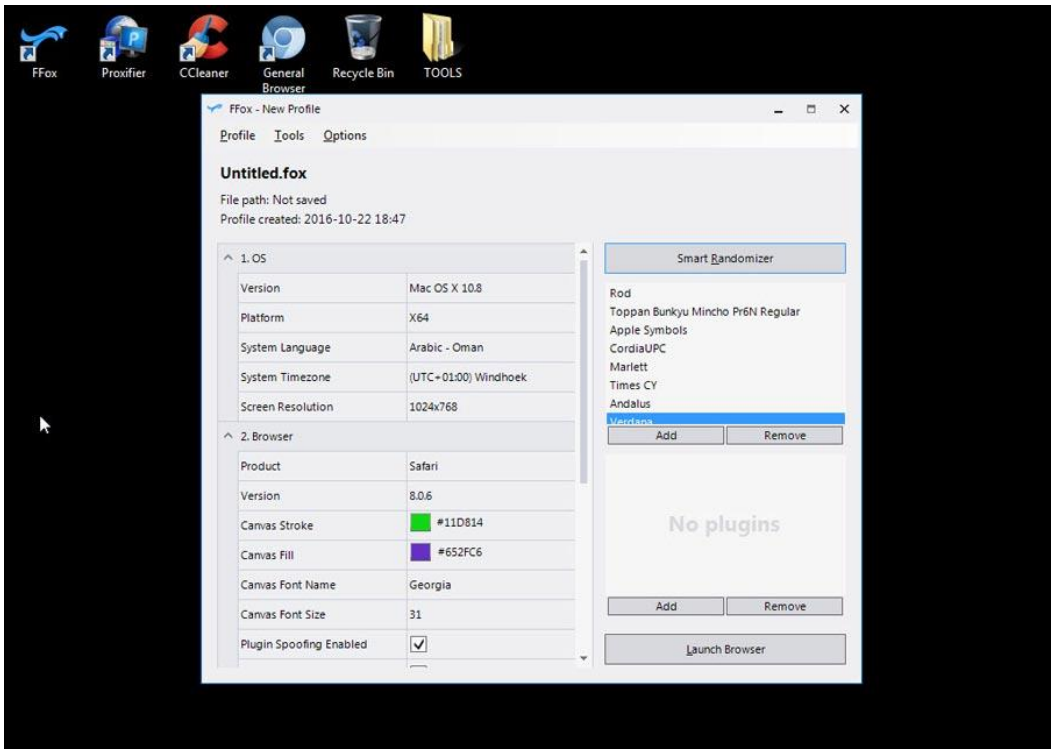
Picture 55: Screenshot from FraudFox sales thread in AlphaBay marketplace.

Embedded inside the virtual machine are various VPN software such as openVPN and proxifiers such as sockscap64 that allows the user to easily manage and maintain his VPN subscriptions and socks proxies. On the browser spoofing factor Fraud Fox is able to successfully spoof every information related and even more it's able to spoof plugins. Of course, included inside are tools that clean the Fraud Fox of cookies and files such as Bleach bit and CCleaner.



Picture 56: Screenshot from FraudFox version 1.5, which is currently outdated since 2.1 is the latest.

Using all the embedded spoofing tools one can create countless fake “unique” fingerprints and bypass blacklists, or limitations that could occur on a blacklisted fingerprint. Fraud Fox keeps profiles so users can switch between those profiles without having to input all the necessary information again, this means if a cybercriminal is using two stolen credit cards one from US and one from Germany, he can switch between these setups IP’s and browser fingerprints in seconds. Profiles created within Fraud Fox are saved in a special encrypted folder with. fox extension.



Picture 57: Creating and importing a .fox profile in FraudFox.

Also, inside Fraud Fox there are custom developed kill switches that will prevent any leakage on VPN, socks proxy for IP related issues and DNS. On top of that embedded are real time IP blacklist check tools in order to verify the IP’s status.

Fraud Fox is the most popular developed tool in deep web with thousands of sales and subscriptions. It is so popular in the deep web that lately several “sellers” appear to sell Fraud Fox subscriptions at a discounted price and actually defraud other fraudsters. There are several guides as well on how to work with Fraud Fox and the developer has started some threads in specific forums that users may post bugs or request specific add-ons. This is also due to the fact that it’s developer continuously updates the file system and the embedded utilities with the most up to date tools. Fraud Fox started from version 1.0 and is now on 2.1 beta and as announced by its developer the upcoming version will have embedded features of form grabbers in order to make phishing webpages managing easier to criminals. Overall Fraud Fox isn’t resource hungry apart from hdd

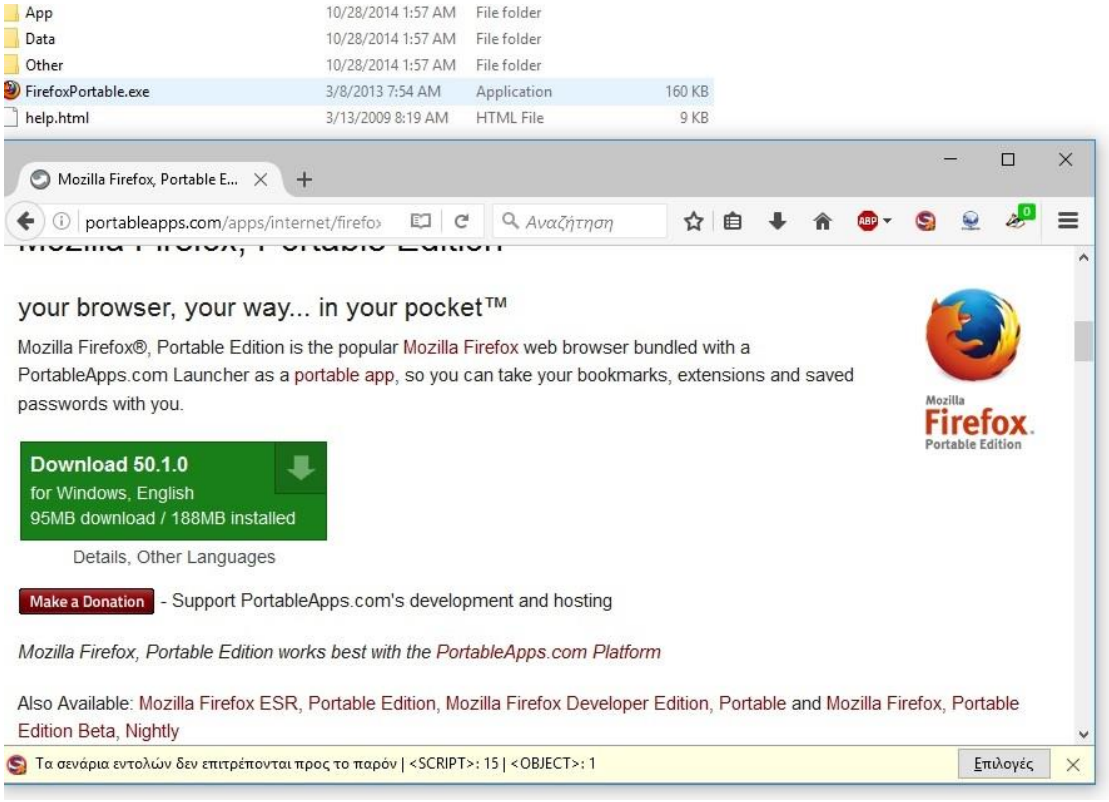
space since the first compressed versions where close to 1,2gigabytes but now the latest version is close to 3,2gigabytes.

So far Fraud Fox has been a step forward from all fraud detection algorithms and is yet to receive any blacklists.

3.5.2 Ghost Box

The second application was created by a long time deep web seller with the nickname "spreadforbooooey", commonly known as "spread" or "SFB". It is based on the same principle of Fraud Fox, as it is a customized windows XP version as well. Ghost Box marketing campaign is based on the logic that the virtual machine does almost the same as Fraud Fox but comes with a onetime fee of 60USD. Ghost Box is actually marketed that it will save time setting up a fraudulent virtual machine and not on the fact of avoiding blacklists. Ghost Box main target group is new cybercriminals that are having issues setting up a "fraudulent virtual machine".

Having a closer look in the Ghost Box layout one would see that it simply contains applications and spoofers that are available online and no custom work or applications are embedded to it. This means that some browser fingerprints blacklists will occur.



Picture 58: Ghost Box embedded browser with add-ons on the right.

On another note the creator hasn't added any features regarding VPN or socks proxy and the browser currently used is Firefox Portable customized with free available add-ons.

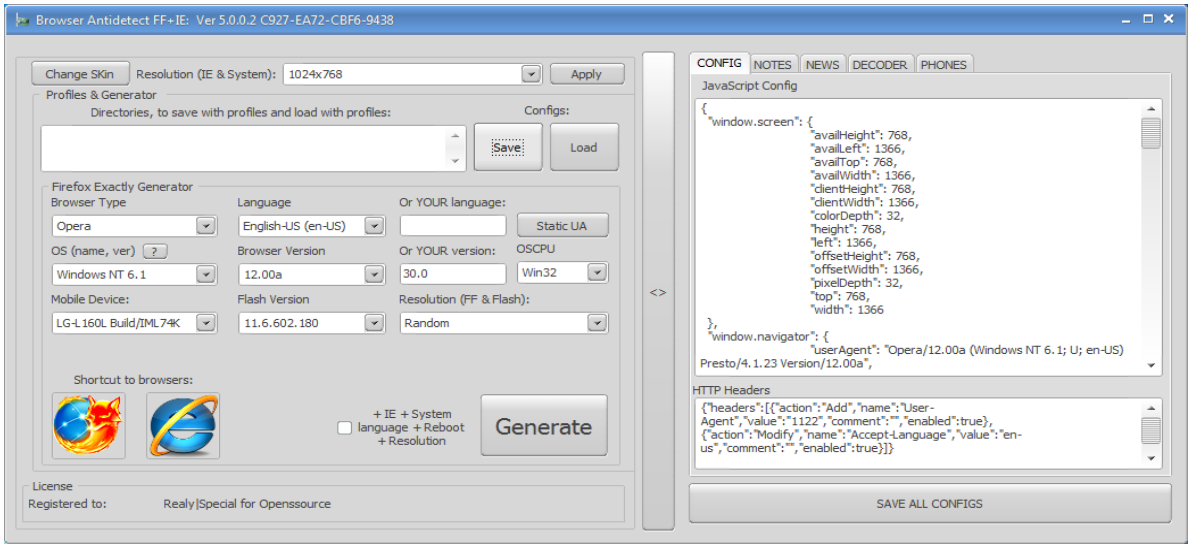
Several programs in Windows XP where uninstalled and java and flash player has been removed completely from the operating system.

Another issue is that there is currently only one version available for Oracle's Virtual Box and it doesn't support VMware's Workstation. Ghost Box is very light compared to Fraud Fox and has received only 2 updates so far. Users are advised to not update any components or applications inside Ghost Box since there are issues with stability. As for disc space, it's close to 1 gigabyte. The creator of Ghost Box has announced a new upgrade coming up on late 2017 with the name Wrath Box that is claimed to be equal as Fraud Fox. Even though both software's where created for the same purpose and belong in the same application family there is no need to compare them since Fraud Fox is superior in construction, spoofing, custom applications and regular updates.

3.5.3 Antidetect

Close the same family of software created to assist fraud is a Russian made tool named Antidetect (may be named in Russian forums in deep web as "FFTools"). Antidetect project started at 2013 it has received many updates so far. Antidetect is sold in Russian Darknet markets and in Clearnet on www.antidetect.org, a website that only accepts digital currency payments. There isn't a specific creator of the tool, but as they claim in both deep web and clear net Antidetect was created by a team of security developers working in commercial protection systems.

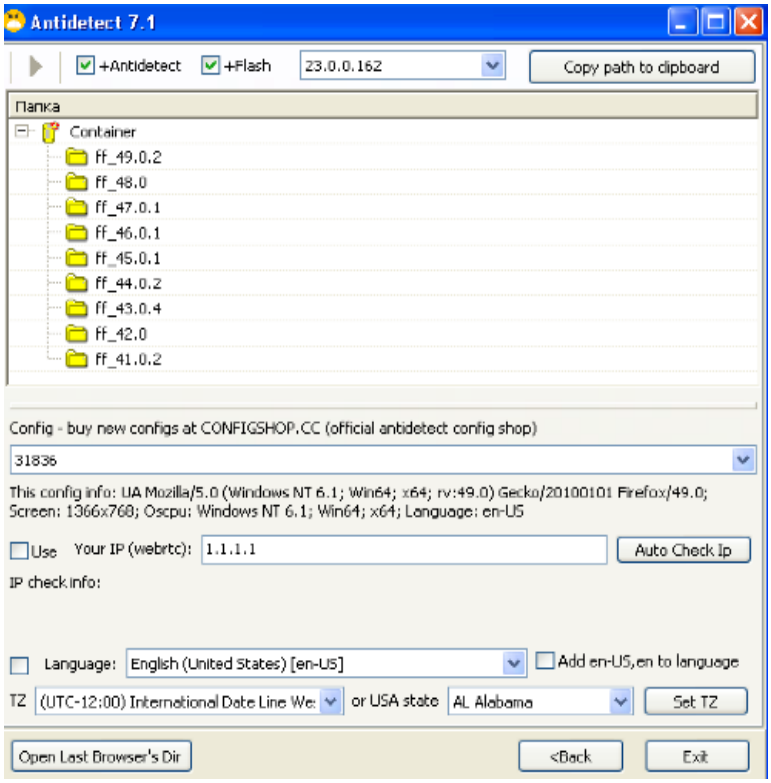
Looking inside antidetect one would find an edited Mozilla Firefox Portable browser or internet explorer with a custom-made program able to spoof several amounts of information. Legally it is advertised to be the world's most secure browser.



Picture 59: Antidetect's version 6 customization panel.

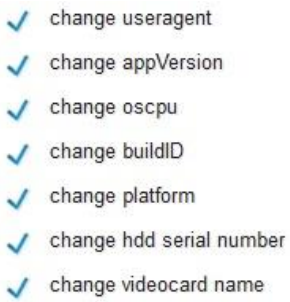
Antidetect browser is meant to be used in both host or guest machines, but it is obvious that the user would need to create and customize one.

Being only a browser antidetect doesn't offer any security features regarding operation security such as VPN, socks proxies not even basic encryption. Antidetect is sold in a one-time fee of 600USD and every update should be paid for again in full. One major disadvantage of antidetect is that it can only be used in one PC because it is designed to lock in a specific Hardware ID setup. Antidetect has evolved the last couple of years starting from version 0.9 it is currently in version 7.1, a newer version that claims that can be embedded in every browser publicly available thus eliminating the need of using Firefox portable. Version 7.1 is also able to spoof the WebRTC a great add-on that FraudFox's latest version hasn't embedded yet.



Picture 60: Antidetect version 7.1 panel.

In the latest update, antidetect 7.1 allows users to buy configured canvas and browsers fingerprints from real phished individuals. There is a dedicated website selling them, www.configshop.cc in a fixed price of 3 USD.



Picture 60: Screenshot from www.antidetect.net where extra spoofing features are advertised.

Showing **1-50** of **46,593** items.

ID	User-agent	OS	Browser	Screen	Language	Day(s)	Flash	Price	Buy
70012	Mozilla/5.0 (iPhone; CPU iPhone OS 10_2 like Mac OS X) AppleWebKit/602.1.50 (KHTML, like Gecko) CriOS/55.0.2883.79 Mobile/14C92 Safari/602.1	IPhone	Chrome	414:736	en-sg	0 day(s)	NO	3$	Buy
69996	Mozilla/5.0 (iPhone; CPU iPhone OS 10_0_1 like Mac OS X) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Mobile/14A403 Safari/602.1	IPhone	Safari	375:667	en-gb	0 day(s)	NO	3$	Buy
69995	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/602.3.12 (KHTML, like Gecko) Version/10.0.2 Safari/602.3.12	Mac OS	Safari	1366:768	en-us	0 day(s)	NO	3$	Buy
69994	Mozilla/5.0 (iPhone; CPU iPhone OS 10_2 like Mac OS X) AppleWebKit/602.3.12 (KHTML, like Gecko) Version/10.0 Mobile/14C92 Safari/602.1	IPhone	Safari	414:736	en-sg	0 day(s)	NO	3$	Buy
69993	Mozilla/5.0 (Linux; Android 6.0.1; SM-J700H Build/MMB29K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.91 Mobile Safari/537.36	Android	Chrome	360:640	en-GB,en-US;q=0.8,en;q=0.6	0 day(s)	NO	3$	Buy
69992	Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) YaBrowser/16.11.0.2708.10 Mobile/13G36 Safari/601.1	IPhone	Safari	375:667	ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4	0 day(s)	NO	3$	Buy
69991	Mozilla/5.0 (Linux; Android 4.4.2; GT-N7100 Build/KOT49H) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.91 Mobile Safari/537.36	Android	Chrome	360:640	en-GB,en;q=0.8,en-US;q=0.6,ms;q=0.4	0 day(s)	NO	3$	Buy
69990	Mozilla/5.0 (iPhone; CPU iPhone OS 9_2_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13D15 Safari/601.1	IPhone	Safari	320:568	en-sg	0 day(s)	NO	3$	Buy
69989	Mozilla/5.0 (iPhone; CPU iPhone OS 10_2 like Mac OS X) AppleWebKit/602.3.12 (KHTML, like Gecko) Version/10.0 Mobile/14C92 Safari/602.1	IPhone	Safari	375:667	en-gb	0 day(s)	NO	3$	Buy
69988	Mozilla/5.0 (Linux; Android 6.0.1; SM-N920I Build/MMB29K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.91 Mobile Safari/537.36	Android	Chrome	412:732	en-SG,en-US;q=0.8,en;q=0.6	0 day(s)	NO	3$	Buy

Picture 61: Screenshot from www.configshop.cc selling phished canvases.

Antidetect's new update is close into spoofing exactly the same amount of information as Fraud Fox does on the user agent part.

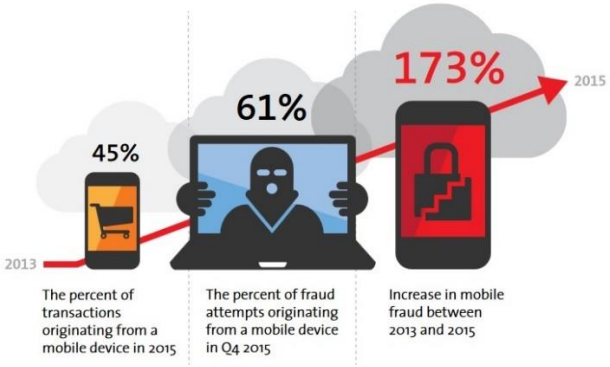
3.6 Futureproofing online fraud

The chapter above was an attempt to analyze the current operation security followed by cybercriminals up to date. Written in detail is every aspect of how cybercriminals built the correct infrastructure in order to maintain high level of anonymity and be able to bypass security systems. In conclusion to the above chapter, it seems cybercriminals always try to be ahead of the online security industry in order to remain free and conduct their business. Cybercriminals use every resource to the best way possible, a useful example the utilization of cloud infrastructures. (Goodman,2016)

As society evolves and smart devices are used on a day to day basis a lot of individuals use them as a computer alternative. Online shops, retailers and banks offer websites mobile friendly and even mobile application in order to create a better user experience. Using technologies that computer doesn't have such as fingerprint read or retina scanner those application seem to the user somewhat more secure. Using a smart device either mobile phone or a tablet one can access websites, make purchases, keep their accounts up to date. Today mobile commerce is a huge part of ecommerce.

The same principle follows a significant amount of cybercriminals. The last couple of years cybercrime has moved from computer crime and evolved to mobile crime. Mobile fraud is divided into two categories, the first being emulator based and the second being physical mobile phones.

One would ask, why migrate to mobile fraud. There are several discussions regarding this in a majority of forums in the deep web, but the answer is usually the same. Mobile applications and mobile commerce is just starting to grow so by default it has less security features and algorithms compared to regular ecommerce. There are reports of several cybercriminals that are able to bypass security on several websites that they were unable to when trying from a computer setup. What seems stunning is that even though fraudulent machine preventions algorithms are in a position to blacklist a mobile device's IMEI or serial number they are unable to predict fraudulent behavior. Using one of the aforementioned algorithms one can see that using the same IP, same country location and time zone in both computer and mobile device, the fraud score in the mobile device is always lower. (Ali & Hudaib, 2015)



Picture 62: Screenshot from Symantec 2015 research regarding cybercriminal modes of operation.

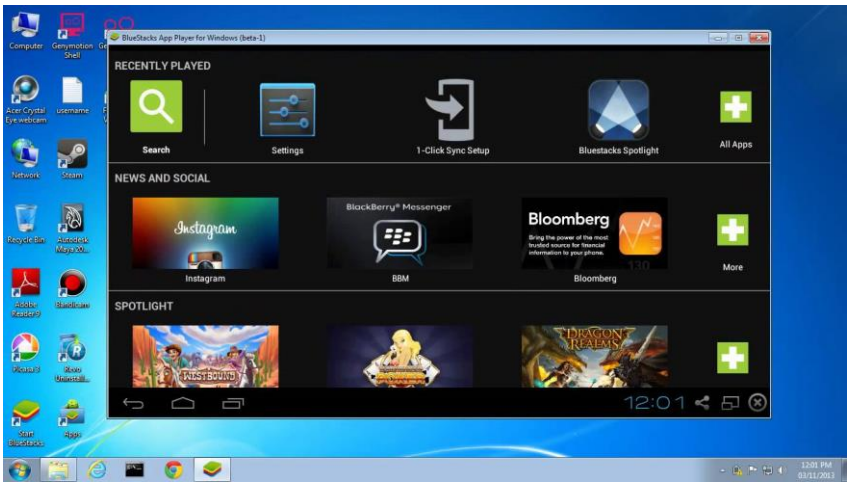
3.6.1 Operation security with mobile phones emulators

Today available there are several mobile emulators for computer, created mainly for the purpose of testing apps in several mobile operating systems in a wide range of screen sizes. Most emulators are about Googles operating system for mobile phones; Android. Some applications come in a form of free and others in a form of freenium or paid for.

Cybercriminals follow the same logic when using virtual machines but instead run the emulator in either the guest or via Remote Desktop protocol. They are still able to spoof IP and DNS leaks via their computer setup that was previously analyzed. Several guides are available in deep web in order how to be successful in setting up android emulators.

Based on these guides and information it seems the most preferable emulators are:

- Blue stacks, an easily fouled emulator that is able to run in a guest setup in a virtual machine. Blue stacks emulator will get the IP of the computer, so it is easier to setup and use. Blue stacks seem to be the most user-friendly emulator software.
- Genymotion, it was developed to assist developers and it seems there are a lot of locks in the software. Genymotion has an embedded verification system that will not run in the guest machine based on the virtual hardware ID for security reasons. Genymotion is mostly used with remote desktop protocol.
- AMIDuOS, offers only two versions of android and it is quite simple to use, although not preferred due to this fact.
- Andy, is a the last application used, it doesn't have a lot of fans due to some crashing issues in several setups.



Picture 63: Screenshot of Bluestacks running on windows host machine.

3.6.2 Operation security with smartphones

The same principles apply when cybercriminals use actual smartphones. Buying an android smartphone is quite easy, although specific brands and models are preferred since it is required that the user has root access. Android operating system is easily customizable with IMEI spoofers, location spoofers, and VPN and socks proxy capabilities it's the easiest and fastest operation security available today.

As in terms of being mobile, cybercriminals either use prepaid SIM cards with data plans or simply find a location with free wireless, such as universities or coffee places. (Senker, 2015)

The smartphone described above is often known as an android burner, since after many fraudulent transactions the IMEI and browser fingerprint does get blacklisted. One major flaw of this operation security scenario is because of the blacklists, users still need to keep buying new mobile

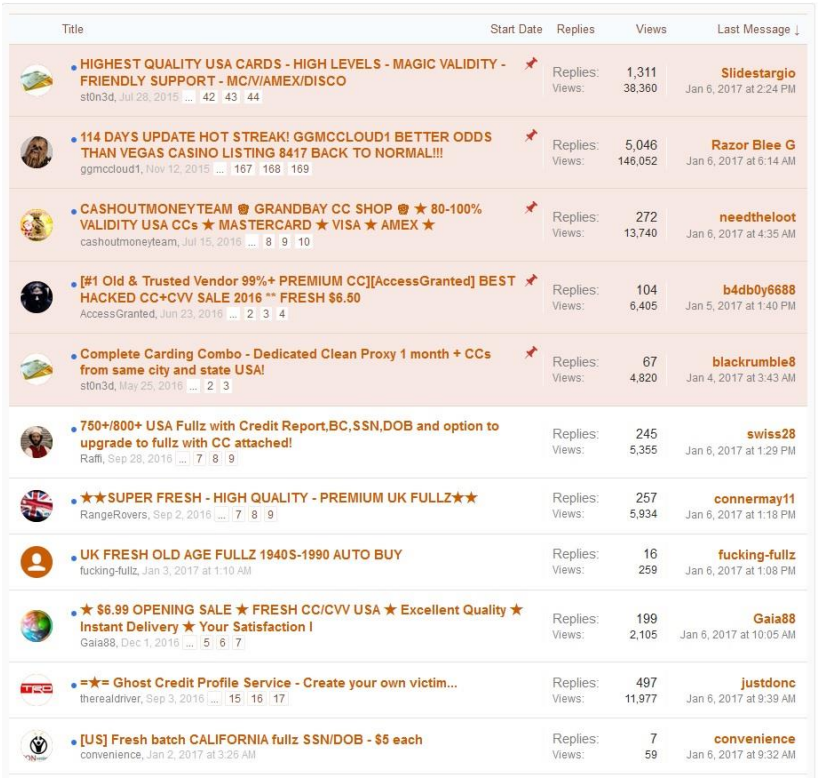
phones to use. On average an android burner could last up to 6 months depending of usage. On a final note, encryption is pretty hard to maintain in a smartphone since high amount of resources is needed that these types of smartphones do not have.

3.7 Using acquired data, cybercrime in 2017

Having proper operation security and using VPS to run spamming and phishing campaigns is of no use if the criminal cant utilize them or sell through proper channels.

The first thing cybercriminals do is use them on their own in order to test their data/products/items. Time has shown that later on successful cybercriminals scale up their business by creating a team and actually selling to other criminals. Many are the times that sellers go in their own apart from the darknet markets and create their own marketplaces in order to sell phished and illegally acquired data both in deep web and in clear net.(Ali & Hudaib, 2015)

There is always huge demand for stolen credit cards and there are plenty online criminal groups to fulfill these demands. There are literally hundreds of stores selling stolen credit card data. Some of them are even buyer/user friendly by accepting refunds if the card data is invalid, or dead. Dead is a situation where the card has some information that are faulty so it is actually of no use to the criminals.



Picture 64: Screenshot from AlphaBay marketplace Where sellers advertise stolen credit cards.

The most used and favorite thing cybercriminals do, is use stolen credit cards to make purchases. The purchased items could be either physical, laptops, handsets, tablets expensive electronics or in virtual state, like gift cards or digital currency. This operation is known in the cybercriminal world as carding. In fact, carding is the number one online fraud carried away globally.

Stolen credits cards could be either phished online, or have their data stolen physically via tapping a payment gateway point of sale or even an ATM. Lately a new form of stolen credit cards arose utilizing contactless chips embedded inside the credit card based on NFC chip. (Ali & Hudaib, 2015)

Stolen credit cards are sold in deep web based on the amount of information they contain. The more information they have about the cardholder, the easier it is for cybercriminals to bypass additional security questions that may pop up.

In order to have a closer look in the stolen credit card world one would have understand the credit card basics. Cards issued by banks are divided into 4 basic categories:

- Credit cards, that are cards that give the owner credit to make purchases and their limit is defined by their contract. These types of credit cards are the most wanted since they can be divided in lots of categories with many limits and balances. There are premier credit cards, gold credit cards, silver, platinum and business credit cards that may have a spending limit up to 50.000 euro. A seasoned cybercriminal could be able to cash out close to 65-70% of that cards spending limit before the card getting cancelled.
- Debit cards, are cards that are linked in the owner's bank account, so a user can spend up to the amount the bank account has. As far as debit cards goes, there is always an argument between sellers as some cards could burn pretty quick if the cardholder has and actually checks his online banking. Also with text messaging notifications and emails the cardholder could cancel his card faster than he would with his credit card.
- Prepaid cards, these where a new wave mostly in Europe, marketed by Banks and Monetary institutions that they make online purchases safer. The logic behind them is that the user can "charge" the amount he wishes to spend and no more than that, so if someone has the info he can't spend more than the pre-charged amount.
- Virtual Prepaid cards, following the same logic as the prepaid card above, virtual prepaid cards can be issued by banking and monetary institutions. Virtual prepaid cards do not have a physical form and can online be used online. (Ali & Hudaib, 2015)

Based on the financial institution that supports payment processing card are divided in:

1. American Express, that unlike all others are 15 digit cards and start with 3XXX
2. Visa cards, having 16 digits and starting with 4XXX
3. MasterCard, having 16 digits and starting with 5XXX
4. Discover card, having 16 digits and starting with 6XXX

These institutions do not issue credit cards, they are only responsible to provide a network where a transaction will take place. They don't have a lot of differences, as some of them are accepted in retailers with more ease than others.

Another difference these institutions have is upon their terms and conditions as to how they treat their clientele. Visa will chargeback faster in case of a customer complaint that his card was stolen rather than MasterCard that may take up to 40 days to process the customer's request. Based on the above statement it seems MasterCard is the most favorable among cybercriminals due to longer chargeback time. However, the chargeback could occur in a very fast manner, it all comes down to the cardholder finding out and notifying his issuing bank in a timely manner. (Malufu, 2013)

Looking at the cards anatomy the card has two sides where it has information about the cardholder. Furthermore, in the front side, there is the logo of issuer Bank, usually an EMV chip that offers PIN protection, a 15 or 16-digit card number known as Primary Account number (PAN), the expiration date, the name of the cardholder and finally the company that is responsible to process the payment.

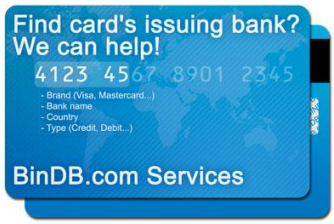
On the back, there is a three-digit code that is called a Card Verification Value or CVV/CVV2. Also on the back there is the Magnetic strip that contains a string of the credit cards data. The information inside the strip is referred to as Dump. Dump contains in cleartext all the information the card has in its front side. The Magnetic strip is easily cloned and their information are sold in underground marketplaces.

However, it is obvious that the cards Magnetic strip doesn't contain the cardholders PIN number. In new type of cards with the EMV chip, Dump is separated in two parts, named track 1 and track 2. Track 1 is encrypted in the chip thus useless to cybercriminals, but track 2 is being sold as it can be written in the magnetic strip.

EMV chip in credit cards is used widely in Europe, Asia, Pacific Countries, Australia, Africa, Malaysia, Latin America, the Caribbean and Canada. However, it was supposed to be embedded in the United States of America, but it is still in a transitional face where roughly 25% of the cards are EMV compliant. The same figure applies for the merchant stores in US.

Picture 65: Detailed analysis of cards issued by banks containing EMV chip.

Banks and financial institutions responsible of issuing credit cards have a unique identified of their cards. The first 6 digits on a 15 or 16 credit card number is called Bank identification number(BIN). This number is used so the four major institutions (visa, MasterCard, American express and discover) recognize the issuing bank. Every Bank has a unique BIN on each institution. Cybercriminals, categorize credit cards by their BIN. The logic behind this is that some banks have higher level clientele thus having greater possibilities of the card having a high spending limit.



Picture 66: Screenshot from www.bindb.com a BIN checker.

On the following pages an attempt is made based on information on several cards selling marketplaces and the deep web regarding credit card categorization.

First in line are plain credit cards with basic information known as CC that contain, only the credit card number and expiry date. It doesn't contain any information regarding cardholders name, address, phone number neither the CVV2. However sometimes they may contain the name of the cardholder but at a different price range. This type of card tends to get extinct since there isn't a lot of demand. This type of card starts at 1 USD and can go up to 5 USD per piece.

Second in line are cards with more information known as CVV or pizza. The term pizza arose from United States cybercriminals that used to card hundreds of dollars' pizza places with just one credit card. These mostly contain information about the name of the cardholder, the credit card number, CVV2, address and email of the victim.

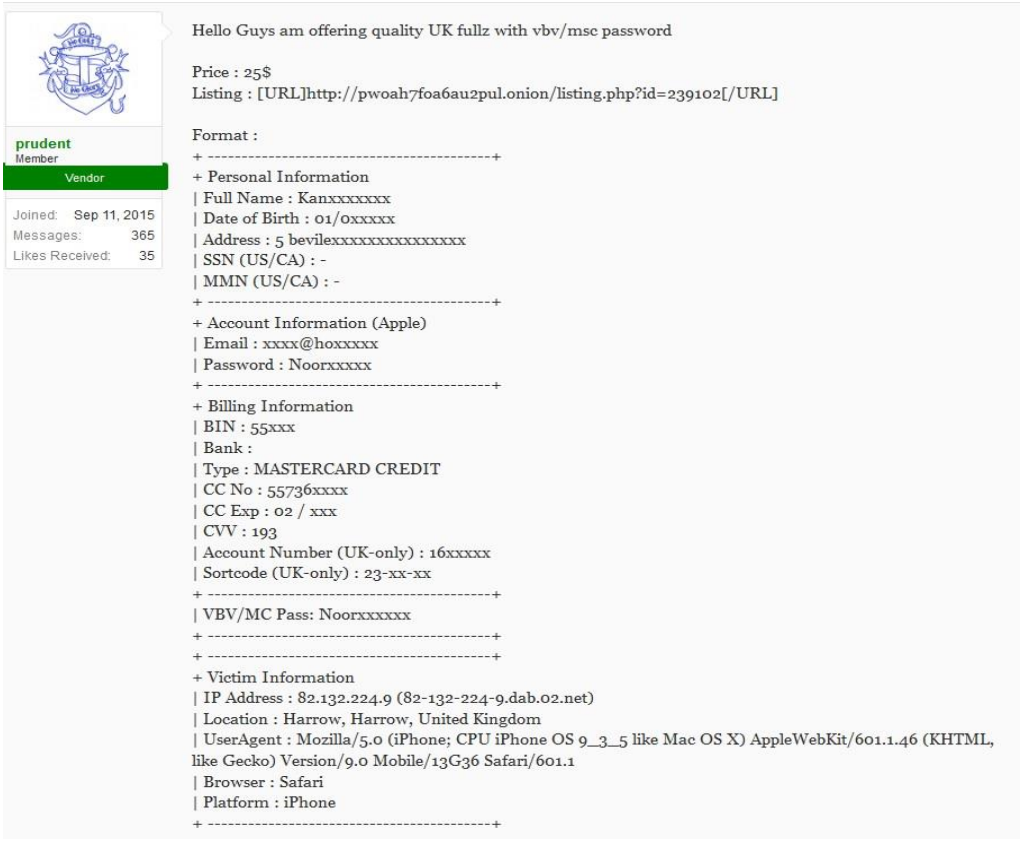
These are mostly targeted for older and less secured payment processors. These cards are also used in conjunction with social engineering. Cybercriminals buy the CVV online and then try to make a purchase from retailer via phone call pretending to be the legitimate cardholder. The payment processor and gateway that call centers have, requires very little amount of information as low as the card number, expiry date and CVV2. This way they can card and ship items at specific locations or even drive by and pick them up from a store. It goes without saying that they are able to bypass every security block that could pop up upon checking out online. However, this form of carding is only intended for native speakers and same sex as the cardholder. As an extreme scenario imagine an individual from Russia, calling a major retailer in the United States asking to buy a high priced electronic device and requesting to charge a female's American credit card. CVV are usually sold between a price range of 6-15 USD.

Picture 67: Screenshot from an illegal seller advertising CVV's or pizzas.

Lastly, these are considered to be top of the line credit cards, known as fullz. The term fullz means that they contain every bit of information needed to bypass every security check available. Fullz come in a form that is Fraud Fox ready, so criminals buy the fullz, import data in their Fraud Fox VM and the customization to the victim's time zone, language, addons, plugins, useragent will occur automatically.

Using fullz compared to the described above types of cards is somewhat easier, and cybercriminals could target higher level retailers and retailers that have strong antifraud mechanisms. The information above such as Mothers Maiden name, sorting number, date of birth and mobile phone number listed in banks files are the ones needed in order to bypass every check that bank may request upon purchase. (Montague, 2010)

Furthermore, fullz come in a specific format for direct importation as follows:



Picture 68: Screenshot from AlphaBay market of freshly phished fullz by apple.com phishing page.

Since fullz are usually known to be a slam dunk they are sold in a way higher priced manner with prices starting from 25$ to even 100$.

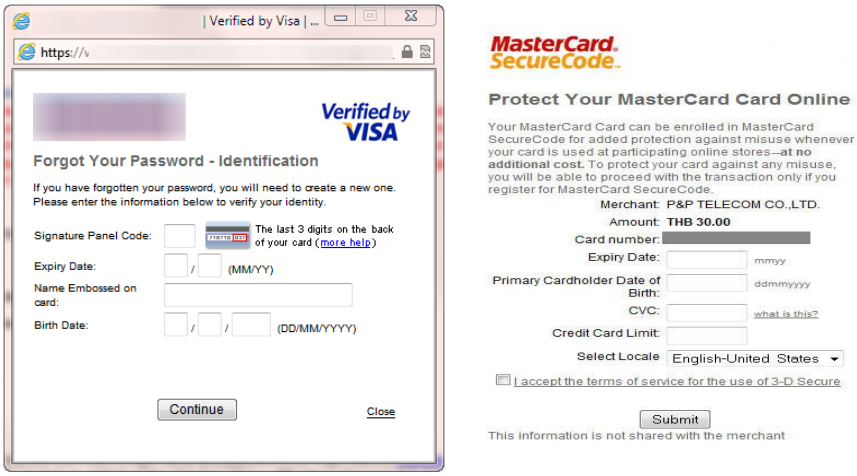
In the illegal world cards are also categorized based on the security features each Banking institution or Country has implemented.

Security features such as:

- AVS cards, are cards that could be credit cards or debit cards. The issuing bank in these types of banks has implemented a security feature named Address Verification System. Upon making a purchase with a merchant the billing address should match the one there is in the Banks records, otherwise payment will not get authorized. AVS system is implemented in United States, United Kingdom, Australia and Germany. (Malufu,2013)
- Non AVS cards, these types of cards are often sold with the name “bill=ship”. This means that cybercriminals could simply put a different name as the cardholders and also a different address than the one registered in the banking system. These types of cards are mostly from China, Brazil and Africa.
- VBV, is a security feature implemented by VISA with cooperation with the issuing bank. VBV derives from Verified by Visa and it was created as an extra layer of security prior to

completing the online purchase where the cardholder in the final stage of payment will be redirected to his banks website and has to enter very personal information such as his birthdate, his mother's maiden name, his address or his phone number. In VBV security feature a password is created that can be reset by answering correctly the above questions. VBV is bypassed with fullz and is mostly used in Europe. If there are three failed attempts to reset the VBV password there is a lockdown on the card for security reasons. The only way re- reset the cards VBV password is by calling the issuing bank and answering more security questions. Sold in underground marketplaces are cards that are non vbv. Non vbv is a term cybercriminals use in order to point that the issuing bank hasn't implemented extra security in their cards.

- MCSC, is the same feature as vbv, only developed from MasterCard in cooperation with the issuing bank. It stands for MasterCard Secure Code and the same features apply upon registering and changing the mcsc password as with VBV. Once again fullz are able to bypass this security feature.



Second step in password reset

Picture 69: Screenshot from Barclays VBV and MCSC bank verification.

Verified By Visa and MasterCard Secure code are known as 3Dsecure implementation. 3D Secure is based on a three level verification process :

- The merchant store
- The Bank that issued the card
- The institution that supports the payment(visa, or mastercard)

However as already mentioned they are easily resettable by cybercriminals. This lead to a new implementation of 3D Secure systems awaiting to be embedded to new cards known as 3D Secure 2.0. It is considered to fix those security issues that the initial protocol had and will be publicly available in the middle of 2017.

Cybercriminals buy credit cards based in a lot of criteria's such as:

- Issuing Bank, cybercriminals tend to buy specific cards from an issuing Bank they know of, so that they know upfront the security questions that might get triggered.
- Payment Processor, it all comes down to their target. If the payment processor is outdated and doesn't require checks, cybercriminals wouldn't use fullz, but cvv instead.
- Age of cardholder, This is mostly requested by seasoned cybercriminals, since they target the age group of 50+ because based on their theory these individuals do not check their ebanking and purchases made until their monthly hard copy statement arrives. On top of that this age group seems to be in a better economic state than younger individuals thus leaving the possibility of having larger spending limits. Age groups of 18 to 30 aren't preferred at all since it seems most of them have ebanking application in their smartphones and their spending limits are very low. Usually on young individuals their logins aren't consistent on the same user agent or IP thus giving more possibilities of security checks popping up.
- Card price factor and buying in bulk, cybercriminals tend to buy 5 or more cards per purchase so they try to find a seller that would offer discounts on bulk orders of 5 or more cards.
- Having drops. Drop is a name for a residential address that is most of the times on the same country of the legitimate cardholder that cybercriminals can ship stolen goods. These Drop addresses could belong to other cybercriminals or to individuals that are unaware of the scheme running in the background. Another factor cybercriminals take in mind is if the retailer is able to ship items to the drops address's Country. Drop addresses are there in order to cover the cybercriminals tracks.
- Card has been checked trough an online checker. There are several sites in deep web and in Clearnet that have embedded illegal merchant accounts that make a 1,5$ test authorization charge in order to see if the payment will go through. If the test authorization happens the card is considered live, otherwise it is considered to be dead. There are a lot of websites in the internet that offers this service with the most preferable being try2check and robocheck. These types of websites charge from 3 up to 8$ per credit card check. However, opinions are divided upon both seller and buyer checking the card since it could potentially raise red flags and bank could contact the legitimate cardholder regarding his suspicious transaction. Since more of these merchant's accounts are in Countries where the legal legislation isn't harsh in online crimes, several Banks block cards upon being checked.

3.7.1 Carding with Dumps

Physical carding is the action of using stolen card data in order to rewrite them to counterfeit credit card and perform physical transactions at a point of sale.

Sold in the deep web are skimmers for almost every type of point of sale, with the most preferred being VeriFone POS. Cybercriminals have come to a point where they sell edited VeriFone POS and admin page in order for user to handle the dumps. On an even more gentle approach cybercriminals have actually created a very small piece of equipment that they put inside the POS charger and records and forwards the dumps to a specific email or FTP. As far as ATM goes, the process of installing illegal equipment in order to steal dumps is known as skimming. Very few individuals can actually see the skimmer, since it is usually installed in a completely transparent way. Some ATM skimmers are known to have cameras in order to capture the PIN number of the cardholder and some can record keystrokes although, no credit cards with PIN are sold in illegal marketplaces.

Picture 70: At left: preconfigured verifone POS, At right: ATM skimmer installed.

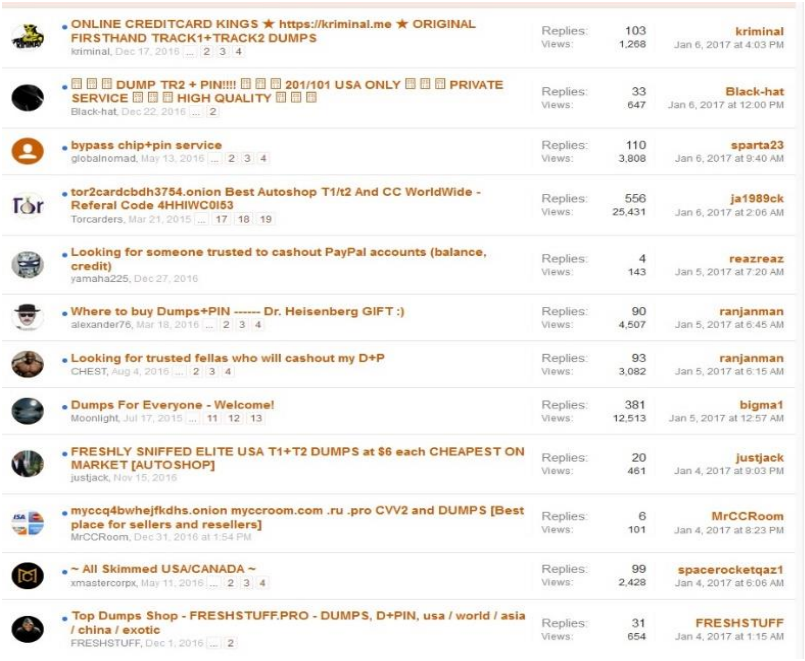
Based on the chip and pin factor cybercriminals theoretically would be unable to use the dumps. However, there is a specific failsafe created for legitimate cardholders that cybercriminals are abusing in order to get purchase authorizations.

When a legitimate cardholder goes to make a transaction at a point of sale, he gives out his card that is entered in a point of sale and then if the card has an EMV chip embedded, an authorization request will come up and ask for the cardholders Personal Identification Number, or PIN. If the PIN is correct the authorization request will be granted and the payment will get processed, thus completing the purchase.

However, if for some reason the chip is faulty, destroyed or is malfunctioning there is an automated failsafe that after three failed attempts to verify the chip condition the transaction will go through via the magnetic strip thus not requesting a PIN number. This term is known in the credit card

security and POS manufacturers as technical fallback. The transaction will get an authorization as well but this time it will have bypassed the encrypted track1 information. Sometimes cashiers might ask for identification of the cardholder in order to complete the transaction if PIN isn't requested at the time of purchase

In order to be successful in carding with dumps cybercriminals have to maintain and follow a specific work around. As it turns out buying dumps from stolen credit cards is the easiest part.



Picture 71: Sellers advertising Dumps/ track1 or track2 data. On their threads they post tips as well for their buyers.

The second part is writing the information in a different credit card. It seems there are two options for this:

1. Several darknet sellers offer custom made cards with Chip and bank logos that could contain the cybercriminals information. Although, creating, printing and shipping the credit card to the cybercriminal is time consuming and the dumps bought could be useless by that time.
2. Write the dumps information in a prepaid card from a monetary institution. Prepaid cards are preferred because they cost less and they are easier to locate. There are also a lot of ways cybercriminals approach this way, they sometimes use prepaid cards that don't have cardholders name at all, or use prepaid cards from monetary institutions that they register in their name or in the name of a fake identification they have in their possession in order to show if asked.

Picture 72: Tool for writing, editing, and cloning track1 and track 2 data in magnetic strips.

After writing the dumps in the aforementioned cards they usually drive far away of their location and try to use the cards to top up gift cards or buy high value electronics. Cybercriminals scale their operation by carrying more than one card with stolen dumps.

In general carding with dumps is very country specific thus not preferred, since a lot of cybercriminals are worried about security cameras and the fact that the cashier may get suspicious regarding non-pin payment. Carding with dumps is very popular amongst US based cybercriminals.

Paying with stolen contactless data is also one thing cybercriminals use with dumps. Transferring their dumps to applications for android devices such as track2nfc and the most popular modded application cvv2nfc they can make purchases at contactless points of sale.

Picture 73: Track 2 nfc mobile application in android device.

Since contactless payments are fairly new most of the times cashiers do not ask for further ID verification. Carding with contactless dumps amongst the cybercriminal world is considered to be fairly easy although not many prefer this way because of the small amount of profitability it offers.

Contactless payments can occur up to a certain amount that has been setup from the Banking institution. Examples of these amounts for Europe are 25 euro per transactions or 30 GBP and 25USD for the United States.

3.7.2 Virtual Carding

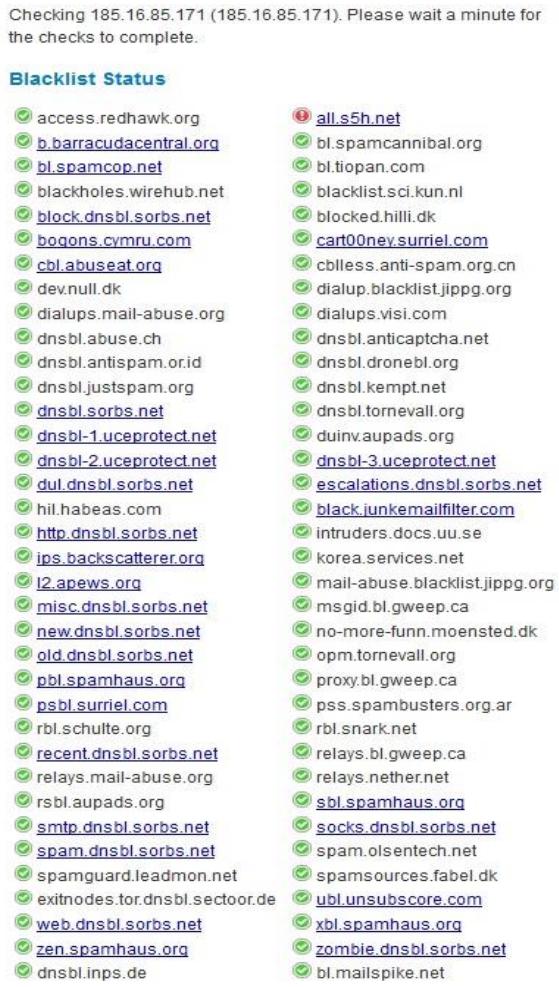
Virtual carding is the process of using stolen credit card data in order to profit. These types of transaction are known to merchants and security specialists are Card Non Present transactions (CNP). There are a lot of ways cybercriminals approach virtual carding. Cybercriminals that do virtual carding are generally split in two categories; carding items online and shipping them to a safe location as previously stated, or carding virtual items that are sold online and there is no actual trace back to the criminal. (Montague, 2010)

In both cases cybercriminals, must user proper operation security. Extensive research regarding operation security has been done in the above chapter. In order to card online stores cybercriminals must select a sock 5 proxy that it's IP is clean and not blacklisted. There are several ways where this information can be verified online with the most popular being:

1. www.whoer.net
2. www.blacklistcheck.net
3. www.check2ip.com.
4. www.leaktest.net
5. www.detect.cc
6. www.panopticlick.eff.org

Having a blacklisted IP or DNS leakage, are issues that could bring errors to the procedure. Furthermore, IP blacklisting checks are done in order to verify that this specific IP hasn't been used in any illegal activities such as spamming. If an IP has been a part of an illegal operation it should be flagged. Based on the dynamic logic of the IP this means that the previous user that was assigned this IP could blacklist it, but this fact can't be verified or taken into consideration by algorithms.

An IP can remain blacklisted for up to 90 days until the server clears off its blacklist. Having a clean IP is essential when cybercriminals target high level retailers or payment gateways. Consistency of the IP is also wanted, since new machine learning algorithms will raise flags if a user logs in continuously from different IP's. Also, it is important that this IP is close to the victim's home address.



Picture 74: Blacklist checks on www.whatismyip.com .

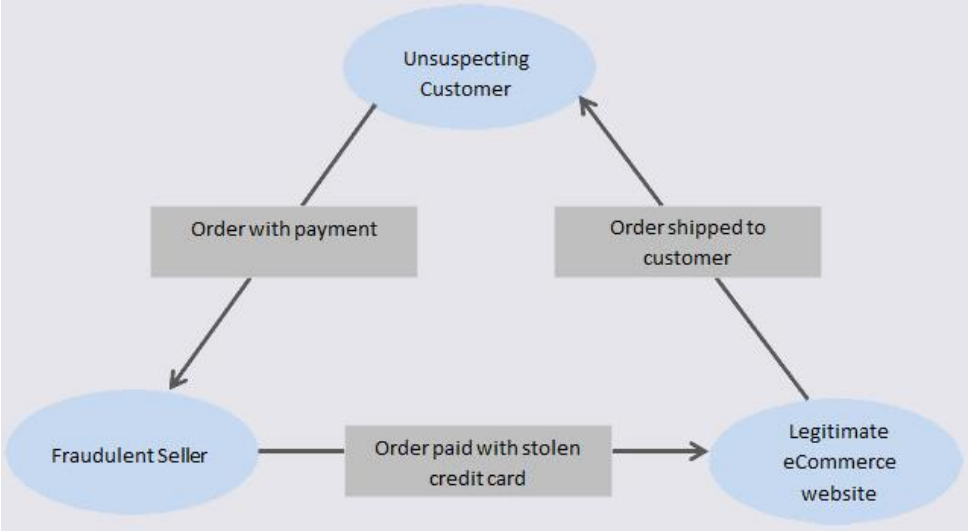
After buying the type of stolen card they wish for and setting up their socks proxy or RDP and their user agent settings, second in line is creating an email with the victim's name. It is clear that cybercriminals continuously commit the crime of identity theft. The email provider could be both a free one or a paid for that accepts digital currencies. After that they register at their targeted retailer and try to make a purchase. If the order gets accepted and shipped they try to reorder using the same setup. They keep doing it until the card is no longer valid; thus, canceled by its legitimate owner. This operation is known to the underground communities as "milking".

In the cybercriminal communities, it there is a common understanding that carding online gift cards and digital codes in general is even more difficult and could occur to order cancelations or extra identity verification. This is due to unusual buyer patterns that may try to make an extremely high value purchase. One major factor that seems to be amongst these societies is that seasoned cybercriminals do not tend to steal electronic devices but other types of items, such as kitchenware, or home appliances. This is due to the fact that the websites selling these items seem to have less security features than the electronics ones.

However, many of them report success in carding electronics as well, although a significant factor is that this type of information can only be verified by retailers themselves.

Upon receiving their stolen goods, they are mostly sold locally or online with plenty of options such as Gumtree, eBay, Craigslist and receive either cash or payment via payment processor such as PayPal. These types of fraudsters do keep seller accounts with great feedback in order to lure buyers faster. Stolen goods are usually sold at 65-70% of the actual face value.

During the last years, some cybercriminals teams have scaled up and automated this procedure that is usually known as drop shipping. Cybercriminals primarily put a listing of an item they don't have at their possession at that time using their seller accounts. When a legitimate user makes the purchase on the seller account controlled by them, cybercriminals then use the stolen credit card and ship the product directly to the unaware buyer. This way eliminates the needs of having physical drop addresses.



Picture 75: Carding directly to victims addresses.

Seasoned cybercriminals tend to use stolen credit cards in specific times of a month. Prefereable dates start at the fifth of every month up to the twenty fifth. This is due to the hypothesis that the victim doesn't have online banking and is waiting for his monthly credit card statement that arrives via post where he will understand that he got scammed. Cybercriminals hope that by that time they would have "milked" the card in every possible way.

3.8 Bank Transfers, Bank Drops

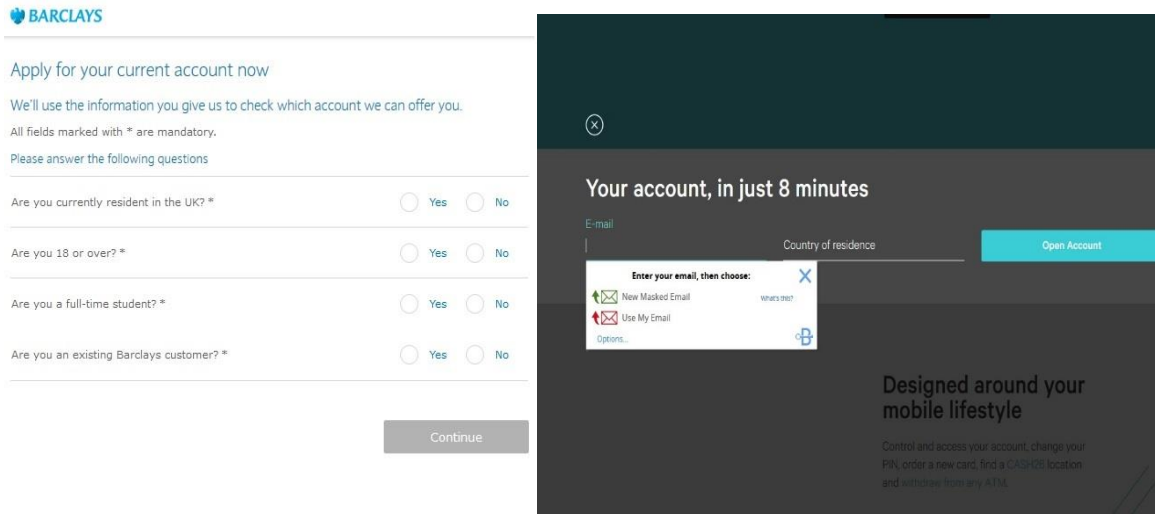
Phished information, sometimes contains data regarding ebanking login details, or they may be harvested by a botnet or a spreaded malware. Cybercriminals in fact to have ways of monetizing by doing online transfers from stolen ebanking credentials.

There are two was the online banking scheme is approached, the first one is committing identity theft and opening online a bank account in a victim's name.

The second one is transferring via SEPA transfer or wire transfer the amount to the previously opened bank account or any bank account controlled by them.

Several cybercriminals offer to sell opened ready to use bank accounts ready to receive transfers and several more are selling ebanking credentials.

As previously stated cyber criminals target banks that offer to open online a bank account or monetary institutions that offer to give an iban to the user. The first think these types of companies ask is for a mobile phone number and photos of the individual's identity card and proof of residency. This is due to the know your customer act (KYC) that is a process of identifying and verifying the actual identity of a customer. Know Your Customer started as early as 2002 but only in 2012 it started being mandatory. (Montague, 2010)



Picture 76: At left: Online Bank account feature at Barclays UK. At right: Registering at a monetary institution www.number26.com that issues IBANS and debit cards in cooperation of Deutche Bank.

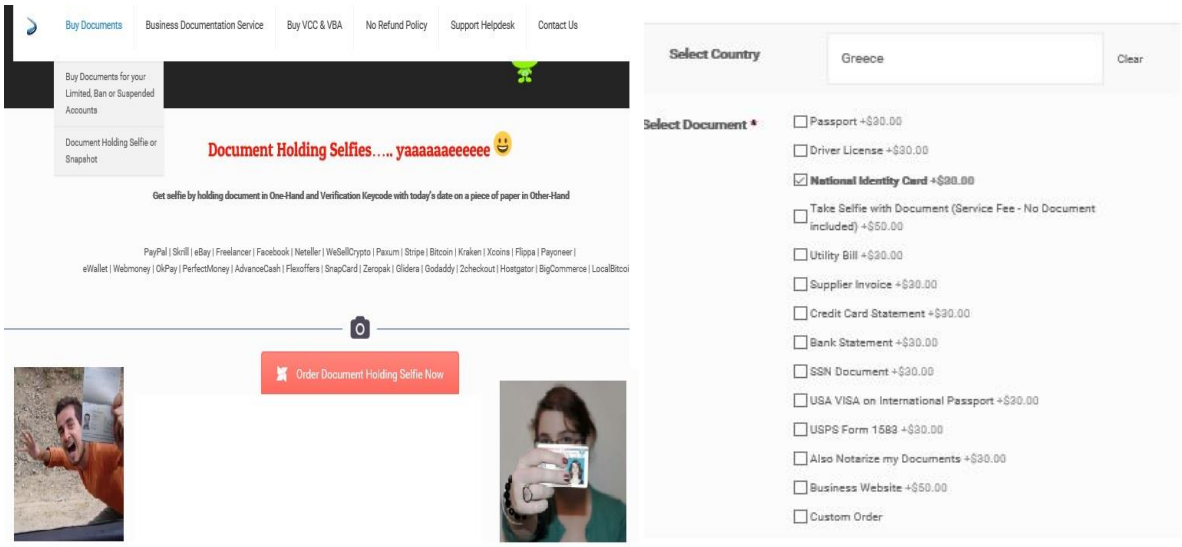
Based on the above prerequisitories getting a preactivated sim online is fairly easy. As for getting an individual's identification was supposed to bring an end to money laundering and money transfers of illegal nature. However, cybercriminals do a have two ways around this:

1. Get the data of an actual person that where phished or in some way tricked to hand them over. Several individuals do have saved as an attachment photos of their identification or they have uploaded them in the cloud, such as their drobox accounts. Cybercriminals that utilize email leads and sell these identities or passports online with prices starting from 30 USD up to 100 USD.

2. Buy counterfeit scanned documents containing fake information with a counterfeit photo. There are several sellers both in deep web and Clearnet that offer these types of photoshop skills and metadata add ons in order of high level verification purposes.
   By adding fake metadata in a picture such as the location where the photo was taken, the address, the date and device used, cybercriminals create strong counterfeit documents that will pass every verification. Some sellers actually offer the "selfie" feature that modern banks may request, that is the user holding his printed ID upon his face.

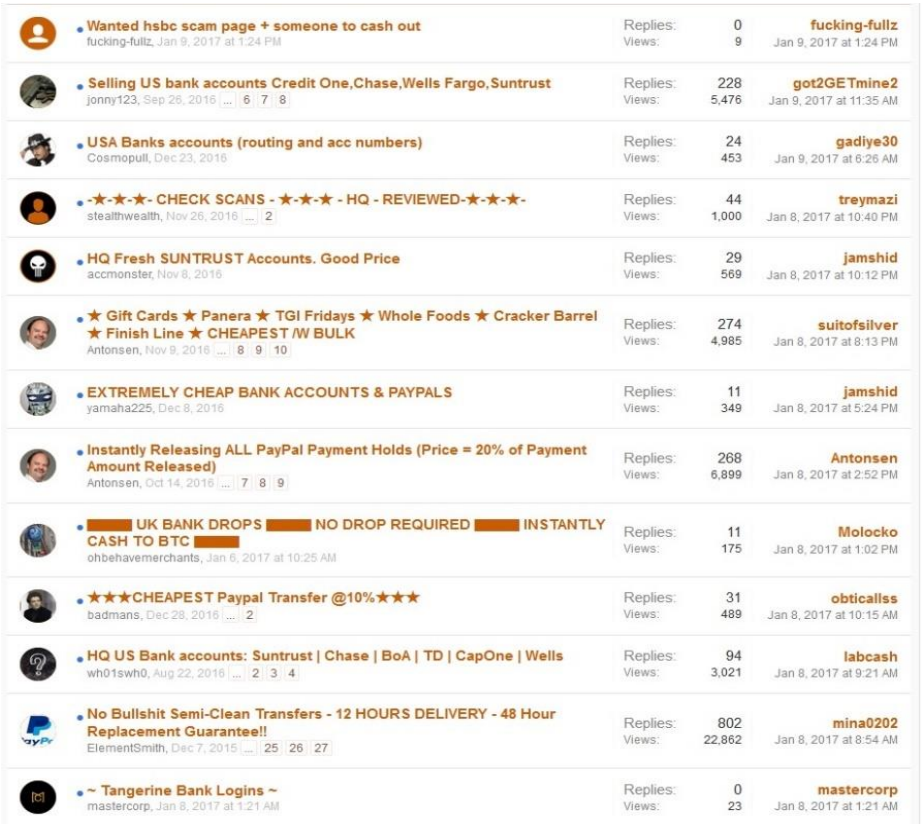
Moving a step forward this counterfeit information can be used in several Countries in order to open online a legitimate business. Business accounts and Bank drops are sold at very high prices based on the Banking institution that issued the bank drop. After opening the bank account online and verifying it, cybercriminals use the online banking options to either order debit cards and ship them to a safe location, or just make money transfers.

If the person's information that was used to open a bank account are legitimate and in good standing cybercriminals tend to apply for credit cards and loans. If the credit card gets approved, cybercriminals max out the credit card and move to a new victim. Since the victim is unaware of a credit card in his name he is unable to cancel it until he gets notified by the issuing bank.



Picture 77: Screenshots from Russian site www.secondeyesolution.ru that provides fake documents with metadata.

Tied with Banking systems and Bank drops are Payment Processors and Payment Gateways in general. One payment processor that is targeted is PayPal, a monetary institution that acts as intermediate between buyer and seller. On PayPal users input their credit card information once and from that moment on they are able to make payments online and transfers to other PayPal account holders.



Picture 78: Selling illegal PayPal trasnfers.

Cybercriminals abuse PayPal's system, by creating fake accounts and using stolen credit cards to make transfers from one account to another. PayPal transferring services are quite popular among online fraudsters.

Bottom line, having multiple bank drops is useful for cybercriminals since they are opened in made up or other individuals names that obviously protects the cybercriminals operation security. Bank drops don't have an average amount of life since it depends on how cybercriminals use them. Some Bank drops last up to two months while other could last up to years.

Complete bank drop packages with sim number, scans of the victim, debit card and ebanking access are sold from 300$ up to 2000$ depending on the issuing bank. Some of the most favorable banks are located in United Kingdom, United States and in Germany, although native speakers are needed if account gets locked.

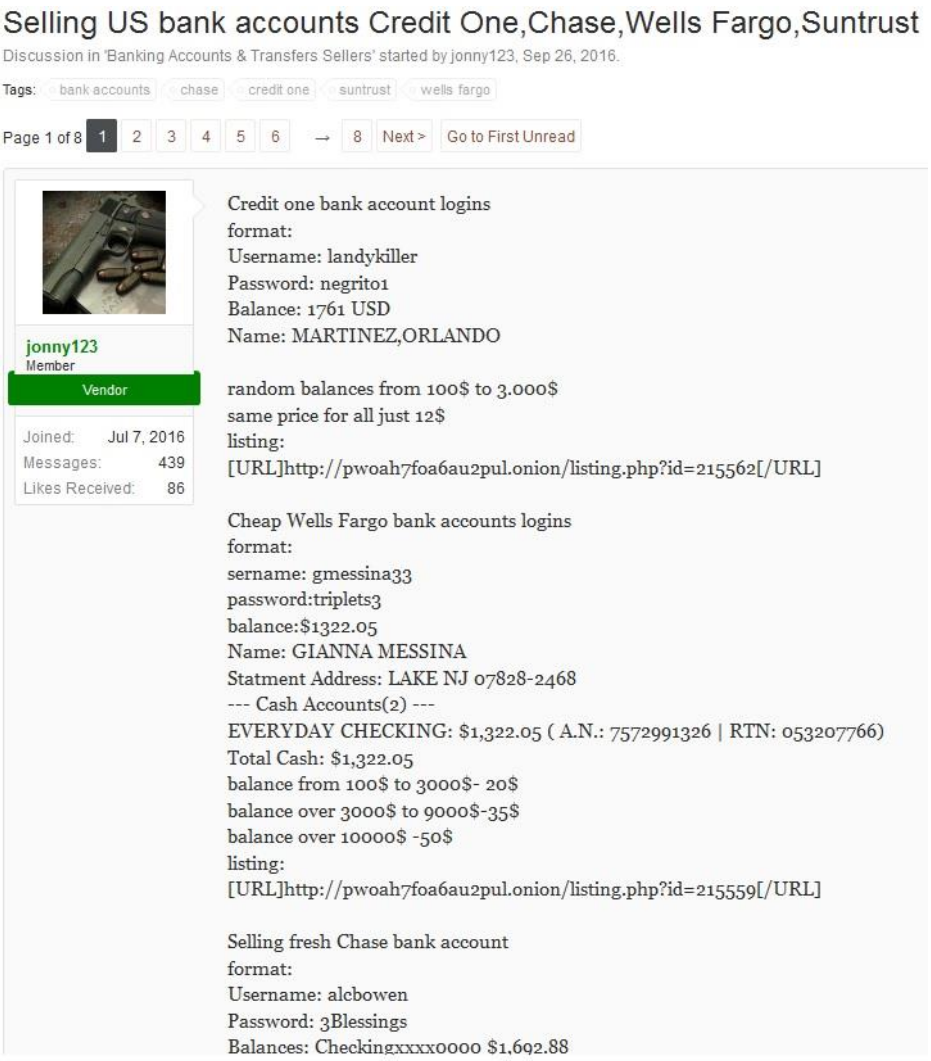
Buying cracked ebanking logins and transferring to a bank drop controlled by cybercriminals is easy but it will lead to the bank drop getting closed if a report is filled. Ebanking accounts and login credentials are sold in the same layout as fullz are sold so cybercriminals can bypass additional checks. Some banks have implemented additional token verification that might be in a form of a unique random numerical calculator or via text message.

Cybercriminals bypass this feature by a procedure called aging. Cybercriminals choose a clean non-blacklisted static IP and log in and log off, in the victim's time zone and simply browse

through the victim's bank accounts and history. After 5-6 days that enough cookies have been built up of the cybercriminal browsing the victims bank accounts, transfers and payments from the same IP and user agent he is in a position to send a transfer without extra security features popping up.

This is due to the fraud algorithm that now recognizes the fraudulent logging in times and IP's as legitimate. Stolen ebanking credentials are sold based on the amount the bank accounts have. Also the issuing bank is a key point when cybercriminals make transfers from accounts, so specific banks with lower security implementation in their e-banking systems are preferred.

If the aging process fails, cybercriminals try to create or buy bank drops on the same bank as the victim. Transferring funds from the same bank between two different customers might not require extra verification, however this is up to the banks security measures implementation.



Picture 79: Screenshot from AlphaBay where a seller sells US bank accounts details.

Cash out is the procedure where cybercriminals wish to withdraw fraudulently created money. Cybercriminals have several ways of cashing out their bank drops. They can use the debit card linked to the bank account or they can send them to another bank account and cash out through there. However most of them prefer exchanging these illegally acquired money to bitcoin and then after tumbling withdrawing them to their legitimate bank accounts. Digital currency actually assists cybercriminals in a lot of ways on their activities overall.

3.9 Account Take Over

Cybercriminals that have a large amount of botnets or run massive spamming campaigns gather information apart from credit card information, email details and ebanking login credentials. Information about social media accounts, or accounts in websites that come in a form of a subscription or even iTunes, iCloud accounts, or Xbox live accounts are sold for profit. Many are the times that some of these accounts might have balance on them, a form of gift card ready to be redeemed or even a linked credit card.

Websites that have lower security are most targeted. Account take over is the procedure where a cybercriminal, uses a fraudulent acquired account and changes a part of the information so that user will never have access to the account again. These changes might be a simple mobile phone change, or deleting the legitimate owners email and adding a fraudulent one as primary. If the legitimate owner tries to take over control of his accounts his information would have been changed to a point where he will not be able to answer security questions or basic information regarding account status.

Some examples of accounts being sold in the deep web that can be ATO'ed are Walmart, amazon, PayPal, grub hub, deliveroo, uber. All these type of company accounts have one similarity; they have a linked credit card from the victim that they do not need to enter the details upon making a new purchase. These types of accounts could also have attached a form of a gift card a recurring subscription or even some form of credit. Examples of the subscription based accounts could be Netflix, skype, online newspapers, Microsoft office 365 and lots of more options. On plenty situations the gift cards attached could be transferred in a new account so cybercriminals exploit that loophole as well. As for physical products, cybercriminals after doing the account takeover purchase items to safe locations controlled by them. Due to the high amount of popularity several account cracking tools with wordlists are sold in deep web in order to run in virtual private servers. Accounts are sold in prices starting from 3$ up to 50$ depending on the status, the age of the account and the linked credit cards.

Pages: -1- 2 ->
To page: 1 Go

Amazon Balance	Gift Balance	Country	Credit Card	Card Exp	Mail domain	Last order	Uploaded	Seller	Price ($):	
N/A	$8.31	United States	+	sa xxxx3527 07/2020 | Marcus Ash | Marcus Ash 4000 ACE LN # 349 LEWISVILLE ; 75067-8054 United States 9726076651 ; Visa xxxx8401 04/2018 | Anisa | Marcus Ash 4000 ACE LN # 349 LEWISVILLE	@gmail.com	September 15, 2016, $0.00, Sep	7 Jan 2017	WTS	3	
N/A	$25	United States	+	sa xxxx2305 11/2019 | Leigh Centore | Leigh Centore 65 CARRELL RD RANDOLPH ; 07869-2922 United States 9734613250 ; Visa xxxx2028 Expired 08/2015 | Leigh Centore | Leigh Centore 65 CARRELL RD RANDOLPH ; 07869-2922 United States 9734613250 ; Discover xxxx3794 09/2021 | Leigh K Centore | Leigh Centore 65 CARRELL RD RANDOLPH ; 07869-2922 United States 9734613250 ; Discover xxxx0986 07/2018 | Leigh K Centore | Leigh Centore 65 CARRELL RD RANDOLPH	@aol.com	December 26, 2016, $41.74, Dec	7 Jan 2017	WTS	4	

Picture 80: Screenshot from www.slilpp.com where amazon accounts are sold.

Since computer outsourcing and the cloud in general is preferred, several individuals and cybercriminals are using these services.

Cybercriminals based on bad security implementation and the fact that most cloud providers are based on authentication and Access Control to the stored data find them as easy targets. Based on these unsecure mechanisms cybercriminals can get the data or even resell the storage space after it has been ATO'ed. This is due to the fact that the data inside the cloud aren't in any way encrypted at least for the popular cloud providers such as Amazon S3 & simpleDB, Microsoft Azure and Google App Engine Datastore. (Agudo, Nunez, Giamatteo, Rizomiliotis & Lambrinoudakis)

3.10 Cybercriminal Modus Operandi in 2017

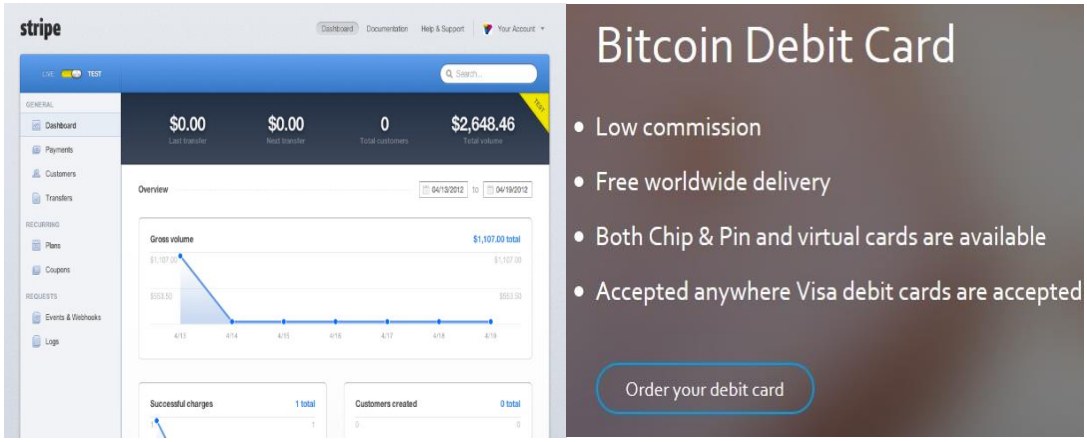
As payment processors and security measures evolves, cybercriminals are adopting this transitional phase as well. Every time a security feature is added cybercriminals try to locate the vulnerability that they can abuse. Based on research in darknet markets apart from being an illegal seller or carder, several cybercriminals are running a fake web shop.

This operation occurs based on identity theft once more and on online resources. Cybercriminals create fake websites of selling merchandising. On top of that they create merchant accounts on multiple payment processors on a victim's name and try to run a legitimate looking business. There are several options such as PayPal, Stripe or shopify. The last two offer the option of creating easily a web shop. Using their payment processors cybercriminals can create a legitimately looking online webstores.

The logic behind running a fake web shop is that cybercriminals do have control of the web shops merchant bank account and they have control of the payment processor gateway as well. Furthermore, cybercriminals select a lower and not advanced payment processor for their webstore, thus giving them the ability to actually use with ease stolen credit cards to run their campaigns.

There are two ways these webstores currently run:

1. Webstores that are built to run only one month. Cybercriminals create the fake webstore and start charging using stolen credit cards. After a significant amount, has reached their bank drop they close the store or it gets closed due to abuse. However by the time the webstore gets closed cybercriminals may have gained thousands $ of fraudulent money.
2. Webstores that are built to be semi legitimate. On these stores cybercriminals run both stolen credit cards and virtual prepaid cards they create themselves in order to pose as legitimate customers. Prepaid cards that can be topped up via bitcoin can be found all over Clearnet. This way the fake webstore can be alive much longer since cyber criminals do an analogy of 3 legitimate transactions and 1 fraudulent thus leaving room for plausible deniability on the chargeback that might occur. Several times chargebacks occur on legitimate merchants and retailers so, the store stays in business and doesn't get closed as opposed to the first option.



Picture 81: At Left: Screenshot of Stripe Merchant account on the right: Screenshot from www.bitplastic.com

4.Effectiveness of Cybersecurity today

Based on the current situation and the huge steps cybercrime has taken over the past years, law enforcements and authorities try to inform individuals on how to protect themselves, protect victims of cybercrime, monitor illegal marketplaces and organize a righteous legal legislation that will try to put boundaries to online crime. It is clear that every nation globally should prioritize taking measures regarding cybersecurity. However, combating online crime with laws seems so far quite difficult because legal legislation seems to be always a step behind cybercriminals and their operations. This is to be expected in a way since creating and establishing a legal framework on online crime requires both legal experts as well as cybersecurity experts that they by default have few common grounds.

The generic approach upon legal legislation and the difficulty in tracking down online evidence are two significant factors. In order to get a comprehensive understanding of how measures are taken one would have to approach this issue from multiple aspects.

4.1 Cybersecurity as a global concern

The first aspect is Governmental legislation and country specific law enforcement awareness. As it happens in Europe in general, legal legislation regarding cybercrime isn't followed in the same manner by every European country, since some of them have already implemented legal framework while others are yet to fulfill it. However, every European country has to follow the same European legal framework and cooperate with each member.

In Europe, four key actions have been taken so far starting from:

1. 2001, where a framework was created upon combating online fraud and counterfeiting currencies. This was the first convention carried away by the council of Europe that was signed by every country member of the European union. On top of that 100 more countries signed the petition and implemented the basic framework in their local legal legislation.
2. 2002, where basic standards where implemented between phone communication providers regarding privacy
3. 2011, where the issue of online child pornography was addressed thoroughly
4. 2013, where Europe as the rest of the world had to face multiple cyber-attacks in their information systems.

As far as organizations responsible of awareness, monitoring and reporting issues in Europe are:

1. Internet Organized Crime Threat Assessment (IOCTA), a Europol's team mainly targeting online fraud, child pornography and cracking
2. Euro just, a department responsible of coordinating investigations and prosecutions between country members, recently took action regarding online crimes
3. Europol, specifically European Crime Center known as EC3, that was founded in 2013 and its main purpose is to do analysis of the current situation, custom digital forensics and provide general cyber intelligence for future legal legislation. EC3 has a toll-free number so European citizens can report any online security issues they may be facing.
4. Joint Cybercrime Action Taskforce, known as J-CAT, launched in 2014 is responsible of fighting cybercrime in collaboration with EC3 within and outside European Union.
5. Computer Emergency Response Team for EU institutions, known as CERT-EU that was founded in 2012.

It is clear that these types of organizations would be unable to do research, use leads and track down cybercriminals if there isn't a country based local enforcement agency handling cybercriminal offences. On top of that it seems that only lately individuals or corporations started contacting local authorities regarding online crimes. Not contacting law enforcements is a serious issue with cybercrime since no research and investigation will occur regarding the attack thus no leads or patterns will come to light.

Also, the aforementioned organizations in an attempt to educate further law enforcers around Europe organize conferences in order share information regarding current attacks and typical cybercriminal behavior. Truth of the matter is that these actions aren't enough to either protect or put cybercriminals in a tough spot.

Two European cybersecurity studies from IOCTA in 2016 and a 2015 study from Europol's EC3 report a rapid increase in cybercrime in 2015 compared to 2014. Based on the above reports cybercrime has increased over 45% than the previous year and its character is actually changing by being more aggressive. The same statistics are verified as well from a 2015 white house report regarding cybersecurity in the United States.

Looking the matter in a country specific situation inside Europe it seems countries that have changed their structure by offering their services online thus paperless and having a strong digital economy are the main target. Countries such as United Kingdom, Germany, France, Netherlands, Belgium, Sweden, Denmark, Austria, Finland are cybercriminals European targets.

Every country seems to have its own way of creating developing and maintaining a specific cybercrime department. It goes without saying that the pace of implementing a cybersecurity or a cybercrime division goes along with the current situation that every country is in. Theoretically, some countries that are having a serious cybercrime heat should implement faster cybercriminal laws and responsible departments to track down cybercriminals.

However, this isn't the case. Taking a closer look in the majority of the European countries it seems that some of those countries haven't actually taken the correct measures in order to combat cybercrime. Moreover, the majority has created one department responsible of handling cybercriminal cases and inform citizens regarding pending threats.

Seeing how these departments are organized one can understand that in most Countries the personnel is understaffed and there are too many cases that never actually get investigated.

On the other hand, several European countries haven't setup the department in question at all or they are in the making, thus leaving room for cybercrime to grow. This action leads to

cybercriminals having the feeling that they can keep evolving their operations without any repercussions.

Since cybercriminals can commit crimes from one country and the outcome of the crime be in another they feel safer being in countries that are doing small steps towards cybercriminal legislation. Having only one department responsible of handling cybercriminal cases or not having one at all could be the reason as to why cybercriminal behavior is becoming more aggressive each year. (Wild, MacEwan & Weinstein, 2011)

Bottom line, although there are organizations lead by the European committees they must be supported by local authorities having the specific target of combating cybercrime. This is due to each country member approaching cybersecurity in a different way thus leaving the opportunity cybercriminals need.

Looking close to European examples it seems countries like Germany, France, Cyprus, Greece, Malta, Belgium, Netherlands, Sweden, Austria and Finland have created one department regarding cybercrime and cybercriminal behavior. Even though Germany has strong digital economy and a huge wave of cybercrime it seems the steps regarding combating it nationwide are fairly small.

One example of a European country facing a tremendous heat of cybercrime as well is United Kingdom, that recently created two new dedicated teams of IT, cybersecurity specialists and digital forensics investigators that are already handling some forms of cybercriminal behavior.

Moreover, United Kingdom has four head departments regarding cyber security assessment and analysis.

- National Cyber Security Centre, NCSC that launched in 2016 based in the 2016-2021 UK cybersecurity strategy, it's part is to organize every governmental organization regarding combating cybercrime in the UK
- National Cyber Crime Unit (NCCU), that is leading and coordinating every investigation regarding cybercrime in UK
- Action Fraud, a dedicated line for cybercrime that has online features of reporting both anonymously and with personal information online crimes
- Fraud and Linked Crime Online (FALCON), a team of cybersecurity specialists consisting of detectives that mainly support businesses and corporations that were attacked by cybercriminals.

United Kingdom's government divided the UK into 14 different cybercriminal departments under the supervision of the above four. The latest new additions in the cybercriminal justice departments in UK are:

- South East Regional Organized Crime Unit (SEROCU), that is responsible of economic cybercrimes carried away in the UK
- Metropolitan Police Cyber Crime Unit (MPCCU), that is responsible for cybercriminal offences and social engineering attacks.

These two departments even though they are fairly new have already made over 700 arrests of cybercriminals in the UK.

On the other side of the globe, looking at United States of America, the situation compared to Europe is different.

In the US, there are dedicated departments to combat cybercrime in every state, thus meaning that there are in fact 50 departments responsible and all of them have to answer to major governmental organizations such as:

- National Security Agency of the Homeland Security, responsible of monitoring illegal marketplaces. Collecting intelligence and stepping up when cybercriminal behavior is hand in hand with terrorist threats.
- Secret Services, where few information is available regarding its history and its operations. The first role of Secret Services was to investigate and prevent counterfeiting, however due to technological advancements it has evolved to monitoring cybercriminal behavior mostly in areas of banking and finance.
- Federal Bureau of Investigations. Responsible of organizing all cybercrime units around the United States, monitoring and linking online information regarding suspicious individuals. Furthermore, FBI has multiple departments handling different cybersecurity issues, such as National Cyber Forensics and Training Alliance that was founded in 1997 and its purpose is to bring together law enforcements, private industry and academia in order to share information and intelligence with the main purpose of stopping cyber threats. Also Cyber Division's Cyber Iniative and Resource Fusion, that handles very complex identity and economic online crimes.
- Interpol, has a dedicated team responsible of communicating with other global organizations regarding cybercrimes carried away globally in order to track down cybercriminals. Also, supported from Interpol the Internet Crime Complaint Center, known as IC3.

- National Cyber Investigative Joint Tasks Force, with main purpose of tracking down cybercriminals since 2008. Based on the United Stated Congress it is also the only one task force responsible of sharing information across the globe.
- Computer Crime and Intellectual Property Section, dedicated to work around intellectual property crimes carried around US
- Computer Emergency Response Team.

All the above departments statewide and countrywide assist each other and collaborate in long range and complex cybercriminal offences.

On top of that several states have dedicated toll free lines to assist individuals and corporations that may be victims of cybercrime. Not only that but in the spirit of promoting cybersecurity several states have created departments called “Defense Centers” in order to assist new businesses grow online without the fear of cyberthreats or cyberattacks getting in the way. Of course, this is in conjunction with the Department of Defense and the Department of Homeland Security. (Michigan, 2015) Other attempts to promote cybersecurity statewide are, lectures in high schools and universities, free courses on being safe online and sometimes there may be courses that lead to IT security certifications. (FBI, 2016)

Picture 82: taken from Michigan State actions regarding combating cybercrime. (Michigan,2015)

As fast as legal legislation goes, an attempt to cover every cybercriminal aspect of methodology and attacks was submitted to the US congress in the October of 2006.

Looking at how United States is handling cybersecurity and cybercrime in general compared to Europe it seems that US has started pretty early to develop mechanisms to promote cybersecurity. US holds a record as well to the first created organization to combat cybercrime at 1997. However regardless of those mechanisms United States, Europe and the rest of the globe face tremendous loses due to cyberciminal operations.

4.2 Economic Impact of Cybercrime

Economic cybercriminal offences could hurt three types of entities:

1. Individuals
2. Corporations
3. Banks and Monetary institutions

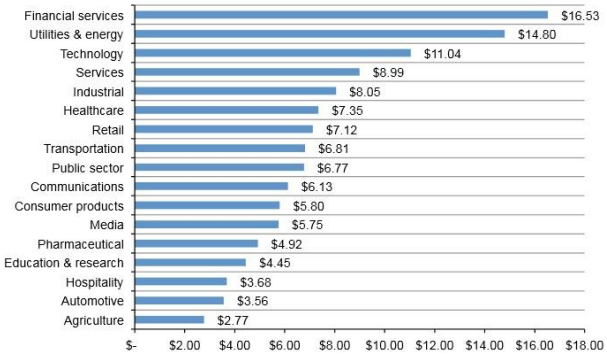
This categorization is due to the fact that the first two entities will try to get compensated from the third entity.

In the cybercriminal mindset, the same excuse seems to come up stating that every company or individual will get compensated as soon as proof of cybercriminal attack is verified. On top of that the excuse that corporations and banking institutions are insured is an opinion widely shared upon deep web. These excuses carry an amount of truthfulness even though in many situations this isn't the case.

Even though if individual falls under cybercriminal attack and faces economic loses he should get compensated there are countless registered cases where Banking institutions denied to offer a refund. Several key points make the verification of online fraud quite difficult and the fact that most of the times no arrests are made due to the nature of the crime the loss goes to the Banking institution.

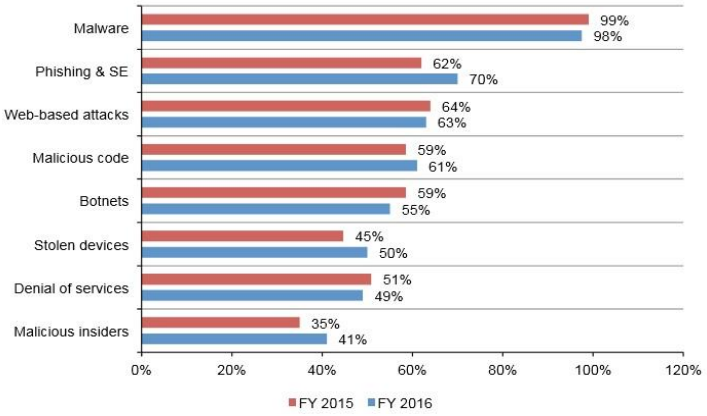
Cybercrime victims often take cases to court in order to claim them loses but it is a very time consuming situation on both participants since investigating and prosecuting cybercrime is often a very slow procedure. The outcome of those trials very, based on the information regarding the executed cybercrime.

Corporations could face economic loses as well regardless of company size and the industry sector they belong to. A recent 2016 study on 252 companies from Ponemon institute suggests that financial services suffer the most with 16,53 billion dollars loses.



Picture 83: Screenshot from Ponemon's institutes report. 252 companies took place in the analysis.

Based on the same Ponemom study it seems companies and corporations in general do have two expensive consequences of cybercrime; Information loss and economic theft. Described below are the top attacks that took place in 2015 and in 2016 to corporations. It seems social engineering attacks and phishing attacks increased significantly. (Ponemon, 2016)



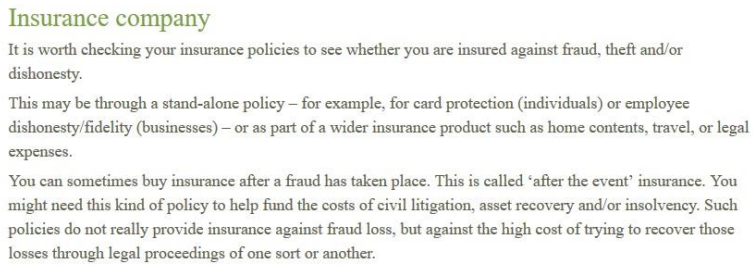
Picture 84: How attacks grew in 2016 based on Ponemons Study.

Both individuals and corporations in order to get compensated have to reach out to their banking institution or insurance companies respectively. Regardless of the contract the above entities have signed banking institutions and several insurance companies have to comply to consumer credit act on European law or in the consumers act in the country they are located.

Based on the consumer acts several individuals are able to claim back fully or partially the stolen amount by cybercriminal operations up to a certain amount defined in the legal legislation of each Country.

A significant example is in UK's legal system where there is the section 75 of consumer credit act that states that individuals can get compensated from amounts of £100 up to £30,000 that used in cybercriminal operations. However, these types of laws mostly protect credit cards, so issues come up if a victim had money stolen from his debit or even prepaid card. These situations often go to court in order to get settled but as previously stated are time consuming.

As far as corporation compensation goes, the majority of them are insured but it seems a small percentage has covers for cybercrime that is an extra expense in the usual package covers, thus leaving no room for compensation. However due to the rise of cybercrime several insurance companies offer to their clients an after the event insurance, that covers a part of the loss.



Picture 85: Insurance claim for after the event coverage scheme.

Companies, corporations and online merchants try to protect their assets from cybercriminal operations. Most of the online stores seem to have implemented the extra verification that the majority of card issuers offer, 3Dsecure that is the verified by visa or the MasterCard secure code. As previously stated certain stolen cards known as fullz contain the information needed to bypass the security features thus leaving the security measure useless to merchants.

Several online merchants had to add a team of security- fraud analysts in order to keep an eye on all orders and verify the given information. This operation is time consuming so legitimate buyer orders could take some time to get verified. Fraud analyst is a quite new term, it is in fact a cyber security analyst that is a specialist in payment gateways and measuring risk score or actually analyzing patterns to see the legitimacy of the information provided. Fraud analysts where initially

hired widely by the banking sector in order to review transactions manually and approve or block transactions that may be of fraudulent nature. Fraud analysts are in fact a mixture of IT and economics.

In an attempt to find the golden line between securing purchases, reviewing orders and keeping the clientele happy major online stores tried to implement algorithm based security layers. Maxmind is a tool that is able to calculate every bit of information and provide a general fraud score in the range of 0,01 up to 99. If the fraud score is above the threshold, then it gets blocked and a manual review is requested from a fraud analyst. Based on the terms and conditions of the online store the fraud analyst could require some more information like pictures of identity card or picture of the credit card used but cybercriminals bypass this feature easily.

Maxmind is able to:

- See information regarding IP, such as blacklists, geolocation, dns leakage. It is able to see proxies, tor exit nodes VPN servers. Maxmind provides detailed information regarding the ISP, the time zone, address, postal code, area, risk factor and other useful information.
- Do email age verification, by seeing the age of an email account one can verify pending fraudulent transactions. Based on the detailed review in the above chapter cybercriminals

always create a new email account in the same manner as the victim. Email age verification has actually been a key point to stopping online fraud.

- View user agent settings, times zones, fonts, add-ons, information that can however be spoofed.

The second tool embedded in Maxmind algorithm, comes by the name of minFraud and offers information regarding:

minFraud Factors subscores

Subscore	Risk assessment factor
AVS	Address verification result
Billing address	Billing address
Billing address distance	Distance between IP and billing locations
Browser	User agent and accept language HTTP headers
Chargeback	Chargeback data and IP address
Country	High risk country associations
Country mismatch	Mismatches between billing country, shipping country, IIN country, and IP address country
CVV	Card security code result
Email address	High risk email associations
Email domain	Email domain
Email tenure	Tenure of customer on email domain
IIN	IIN / region mismatch or merchant specific risk for IIN
IP tenure	Tenure of customer on IP address
Order amount	Merchant specific order amount
Phone number	Telephone number
Shipping address distance	Distance between shipping address and IP address location
Time of day	Local time of day of the transaction in the IP address location

Picture 86: Information taken into consideration by maxmind algorithm.

Maxmind is a great tool widely used by merchants around the globe in order to minimize fraud. However, maxmind isn't foolproof. There are several cases where the maxmind algorithm has failed. Companies such as amazon, asos, Microsoft stores, apple, tesco use on a daily basis the maxmind algorithm. CEO of amazon Jeff Bezos, has announced that a new machine learning algorithm will be implemented in the amazon checkout process to do predictive analysis on purchases. Machine learning is currently used in amazon's cloud known as AWS.

Bottom line, even though there are tools out there that can protect merchants, cybercriminals do in fact have the means to bypass them.

The last party taking place in compensating fraudulent transactions are the bank institutions themselves.

Each banking institution has to agree and comply to the laws of every state they are offering their services. This leads to banking institutions having to respect the consumer rights upon proof of fraudulent transactions. Banking institutions try to protect their assets and sometimes deny to offer refund in large amounts, that often will lead to court.

If a banking institution receives the order to compensate a victim their first attempt is to do a chargeback. Chargeback is actually reversal of charges the cybercriminals did on the victim's credit card. Looking into the chargeback case closely, if a cybercriminal bought something from an online retailer received it and the victim realized his card was used and filled a report, the bank will chargeback the amount from the online retailer and give it back to its legitimate owner. However, this means actual loss to the online store that can't prove that this transaction was fulfilled and not part of a cybercriminal operation.

On the other hand, if the monetary institution is unavailable to fulfil the chargeback request, banking institutions return the fraudulently taken amount from their insurance claims. The last option could take up to 90 days in order to get fulfilled.

5 Conclusions

Cybercriminals are walking hand in hand with new technological advancements. It is a general understanding that as societies evolve and move towards the digital era and the internet of things, so will cybercriminals. A recent example comes to verify this assumption with the first ddos internet of things attack taking place in 2016 (Mirai botnet).

A textbook cybercriminal doesn't exist, some of them could be very well knowledgeable while others may be having basic computer skills. Its illegal underground marketplaces in the internet and in the deep web that makes online crime look easy to carry out. Every tool needed to commit online fraud is sold, so it guiding, information sharing or even resources exchange. Online crime doesn't have any more rogue criminals, teams have been organized and it attracted regular real life organized crime as well, this is why online crime is getting more aggressive every year.

Cybercriminals can and will find major opportunities for economic fraud, theft, utilization and monetization of illegally acquired data and other forms of information. Software vulnerabilities, badly secured infrastructures, weaknesses in encryption systems are cybercriminals bread and butter. Recent example the yahoo attack that got one billion email accounts compromised, one billion accounts with two-way factor authentication disabled. However on the yahoo case it seems there is online security illiteracy on a tremendous amount of users.

Cybercrime is a very lucrative operation for cybercriminals and todays security mechanisms doesn't seem to put a stop to their operations. On the contrary, cybercrime is considered to cost the global economy ~ 500 billion USD every year and is moving upwards every year. It is considered that this crime wave will reach up to 2 trillion USD by the end of 2019.

Looking the matter from a legal point of view, legislation is fairly new, untested to time and quite generic. Legal legislation faces difficulties since internet fraud doesn't have boundaries like traditional crime and gathering data and conducting investigations is still at an early stage. It's shocking that the legal legislation worldwide doesn't cover at all the cybercrime victims end and rely on local legal legislation, banking sector, court orders and insurance policies. Every country should take measures and protect these individuals.

Cybercrime isn't victimless. Either it is an individual, an online business or a banking institution that suffered from ransomwares or economic crimes, these people are paying the price of the online crime. There is a need of a global organization that will support these victims.

Every country is in a different situation regarding cybercriminal law and every country has a different way of prosecuting cybercriminals thus a different structured cybercrime department.

Cybercriminal departments around the globe need one global repository of cybercriminals acts and investigations. It could be that two cybercriminal departments of two countries are chasing the same fraudster without their knowledge. Today there isn't a mechanism where cybercriminal departments share information. This causes lost resources since combined forces will assist to finally getting results. This miscommunication is well known among fraudsters and its time it comes to an end.

Cybercrime has become a major issue and new types of jobs were created in order to combat online crime. Specific law solicitors regarding online crimes, special digital forensics investigators, online fraud detectives, security and cybersecurity analysts, white hat crackers with the same purpose; making online fraud difficult to fraudsters and maintaining a certain level of cybersecurity. However recent studies show that few online merchants and retailers are taking measures regarding combating it.

Corporations, online stores, merchants and the banking sector need to approach cybersecurity in a different manner. So far, the methods deployed where targeted to treat and patch the known issue/vulnerability. However, the IT departments should approach this is issue in a completely different way; by preventing, detecting and mitigating. The path should follow the line of consideration regarding susceptibility, resilience, wellness, vulnerability and lastly recoverability.

Achieving a certain level of cybersecurity isn't by simple implementation of the correct form of technology, it's also about providing awareness to the public so everyone will know and protect their selves in the digital world. Having individuals being aware regarding everyday online risks is essential. Finally, individuals should report issues to authorities regarding online crimes, it is shocking that only lately cases actually reach law enforcements agencies even in 2017.

It is a fact based on statistics that cybercrime will grow the upcoming years, however by applying correct countermeasures and being proactive in cybersecurity aspects cybercrime could be measured since if left unattended it could pose as a threat to the global security and economic growth in general.

6. Bibliography

1. Agudo, I., Nunez, D., Giammatteo, G., Rizomiliotis, P. & Lambrinoudakis, C. (2011) Cryptography goes to the cloud, Retrieved 7 January 2017 from: http://www.eng.it/ricerca/file/2011%20Crypto_STAVE.pdf
2. Anti-Pishing Working Group (2015) Global Phishing Survey: Trends and new methods, Retrieved 6 December 2016 from: https://docs.apwg.org/reports/APWG_GS_1H2015.pdf.
3. Ali, A. & Hudaib, Z. (2015) Selection Guide & Penetration Testing for Banking systems Online Payments notes: Selection Guide for Cyber Defense & Penetration testing for Banking, CreateSpace Independent Publishing Platform, Indiana, United States of America.
4. Alisdair, G. (2015) Cybercrime: Keys issues and Debates, Routledge Publishing, London, United Kingdom.
5. Attrill, A. (2015) Cyberpsychology, Oxford University Press, Oxford, United Kingdom.
6. Bleaken, D. (2010) Botwars: The fight against criminal cyber networks Retrieved 7 November 2016 from: http://spectrum.library.concordia.ca/9769548/1/bleaken.pdf .
7. Clough, J. (2015) Principles of Cybercrime (second edition), Cambridge University Press, Cambridge, United Kingdom.
8. DeepDotWeb (2016), Retrieved 12 December 2016 from : https://www.deepdotweb.com/
9. Dieterle, D. (2015) Intermediate Security Testing with Kali Linux 2.0, CreateSpace Independent Publishing Platform, Indiana, United States of America.
10. Donaldson, S., Siegel, S. & Williams, C. (2015) Enterprise Cybersecurity: How to build a Successful Cyberdefense Program Against Advanced Threats, Apress Publishing, New York City, United States of America.
11. Eilam, E. (2005) Reversing: Secrets of Reverse Engineering (1st edition), John Wiley and Sons Publishing, New Jersey, United States of America.
12. Elisan, C. (2012) Malware, Rootkits & Botnets; A Begginer's Guide, MCGraw-Hill Education, Pennsylvania, United States of America.
13. Engerretson, P. (2013) The Basic of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (2nd edition), Syngreess- Elsevier Publication, Amsterdam, Netherlands.
14. Erickson, J. (2015) Hacking: The Art of Exploitation (3rd edition), Amazon media Publishing, California, United States of America.

15. European Cybercrime Center (2015), First year report, Retrieved 30 November 2016 from :https://www.europol.europa.eu/publications-documents/european-cybercrime-center-ec3-first-year-report .
16. Federal Bureau of Investigations (2015) Internet Crime Report, Retrieved 11 November 2016 from: https://pdf.ic3.gov/2015_IC3Report.pdf .
17. Frisby, D. (2014) Bitcoin: The Future of Money, Unbound Publishing, London, United Kingdom.
18. Goodman, M. (2016) Future Crimes: Inside The Digital Underground and the Battle For our Connected World, Corgi Publishing, London, United Kingdom.
19. Holt, T. , Bossler, A. & Seigfried-Spellar, K. (2015) Cybercrime and Digital Forensics: An introduction, Routledge Publishing, London, United Kingdom.
20. Hubbard, D., Seiersen, R. & Geer, D. (2016) How to Measure Anything in Cybersecurity Risk, John Wiley and Sons Publishing, New Jersey, United States of America.
21. Jewkes, Y. & Yar, M. (2009) Handbook of Internet Crime, Willan Publishing Limited, London, United Kingdom.
22. Kaspersky (2016) Kaspersky Labs report in IT threat evolution, Retrieved 16 November 2016 from: https://securelist.com/files/2016/05/Q1_2016_MW_report_FINAL_eng.pdf .
23. Kennedy, D., O'Gorman, J. & Kearns, D. (2011) Metasploit: The Penetration Tester's Guide (1st edition), No Starch Press, California, United States of America.
24. Kirwan, G. & Power, A. (2013) Cybercrime: The Psychology of Online Offenders, Cambridge University Press, Cambridge, United Kingdom.
25. Krebs, B. (2015) Spam Nation: The Inside Story of Organized Cybercrime- From Global Epidemic to Your Front Door, Sourcebooks Publishing, Illinois, United States of America.
26. Lickiewicz, J. (2011) Cyber crime phsycology proposal of an offender psychological profile. Recognition, analysis, prevention, patterns and usual unusual behavior.

    Retrieved 19 October, 2016 from: http://www.forensicscience.pl/pfs/87_Lickiewicz.pdf .
27. Luttgens, J., Matthew, P., & Mandia, K. (2014) Incident Response & Computer Forensics (3rd edition), MCGraw-Hill Education, Pennsylvania, United States of America.
28. Malufu, K. (2013) Ebanking Security: How secure is electronic Banking?, Lambert Academic Publishing, Saarbrucken, Germany.
29. Marion, N. (2016) Introduction to Cybercrime: Computer Crimes, Laws and Policing in the 21st Century, Greenwood Publishing Group - Praeger Security International, California, United States of America.

30. Michigan Cyber Civilian Corps (2015), Cybersecurity report and assessment, retrieved 19 December 2016 from: http://www.michigan.gov/som/0,4669,7-192-78403_78404---,00.html .
31. Microsoft (2015) Microsoft Security Intelligence report in Cybercrime and Cybersecurity, Retrieved 14 November 2016 from : https://www.microsoft.com/security/sir/default.aspx.
32. Mitrou, E. (2016) Course notes from Online Criminal law, Retrieved 10 October 2016 from : https://eclass.hua.gr/courses/DIT197/ .
33. Montague, D. (2010) Essentials of Online Payment Security and Fraud Prevention (1st edition), John Willey & Sons, New Jersey, United States of America.
34. Osborne, M. (2014) Cyber Attack, Cybercrime, CyberWarface-CyberComplacency: Is Hollywood's blueprint for Chaos Coming true, CreateSpace Independent Publishing Platform, Indiana, United States of America.
35. Ponemon (2016) Ponemon's study and assessment in Cybersecurity, cybercrime and data breach, retrieved 8 December 2016 from: https://securityintelligence.com/cost-of-a-data-breach-2016/ .
36. Portnoy, M. (2016) Virtualization Essentials (2nd edition), Sybex Publishing – John Willey & Sons, New Jersey, United States of America.
37. Rashmi, S. (2014) Profiling a Cyber Criminal. Retrieved 22 October, 2016, from : http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf .
38. Regalando, D., Harris, S. & Harper, A. (2015) Gray Hat Hacking: The Ethical Hacker's Handbook (4th edition), MCGraw-Hill Education, Pennsylvania, United States of America.
39. Schneier, B. (2016) Blog post and newsletter feed Retrieved 28 November 2016 from: https://www.schneier.com/ .
40. Senker, C. (2015) Cybercrime and the Darknet: Revealing the hidden underworld of the Internet, Amazon media Publishing, California, United States of America.
41. Shackelford, J. (2016) Cybersecurity 101: What You Absolutely Must Know! – Volume 1: Learn How to Not be Pwned, Spear Phishing and Zero Day Explois, Cloud Security Basics, and much more, CreateSpace Independent Publishing Platform, Indiana, United States of America.
42. Shukla, P. & Mehra, N. (2015) The Unrevealed Secrets of Hacking and Cracking – Hack Before You Get Hacked, Unicorn Books, New Delhi, India.
43. Smith, J. (2016) Tor and The Dark Net: Remain Anonymous and Evade NSA Spying, Pinacle Publishers, Orpington, United Kingdom.
44. Stryker, C. (2012) Hacking the Future: Online Anonymity, Privacy and Control, Gerald Duckworth Publishing Limited, London, United Kingdom.

45. Symantec (2016) Internet Security Threat report, Retrieved: 22 November 2016 from: https://www.symantec.com/security-center/threat-report .
46. Tipton, H. & Nozaki, M. (2016) Information Security Management Handbook, volume 6 (6th edition), AuerBach Publications – CRC Press, Florida, United States of America.
47. Viano, E. (2016) Cybercrime, Organized Crime and Societal Responses: International Approaches, Springer Publishing, New York City, United States of America.
48. Wall, D. (2007) Cybercrime: The transformation of Crime in the Information Age (1st edition), Polity Press, Cambridge, United Kingdom
49. Wild, C., MacEwan, N. & Weinstein, S. (2011) Electronic and mobile Commerce Law: An analysis of Trade, Finance, Media and Cybercrime in the digital Age (1st edition), University of Hertfordshire Press, Hatfield, United Kingdom.
50. Yar, M. (2013) Cybercrime and Society (2nd edition) , Sage Publishing , California, United States of America.