Journal of Forensic Sciences
And
Criminal Investigation
ISSN: 2476-1311

Juniper PUBLISHERS key to the Researchers

Review Article
Volume - 9 Issue 5 - July 2018
DOI: 10.19080/JFSCI.2018.09.555775

J Forensic Sci & Criminal Inves

Using Security Intelligence in Corporations

Nikola Protrka* and GrgaJovanovski

University of Police College, UK

Submission: June 28, 2018; **Published:** July 13, 2018

*Corresponding author: Nikola Protrka, University of Police college, Senior Lecturer, Court Expert for IT, UK, Email: nprotrka@fkz.hr

Abstract

This paper explains security intelligence and how corporations use it to maintain the security of information systems by analysis of malicious content. Most famous threats to corporate information systems and departments that fight against these threats are explained, as well the tools for collecting data for analysis. Most common public available services for analysis are explained, and commercial brand-named tools. Dynamic and static analysis are divided and explained also, with awareness of security incident.

Keywords: Security Intelligence; Malicious Content; Analysis; Threats; Cybercrime.

Introduction

Collecting security intelligence is one of the most important parts of corporate information security. To protect against attackers, a corporation needs to collect information about the attackers and tools they use for attacks.

Without security intelligence, the corporation is literally blind to possible attacks or even the advanced persistent threats that are already on their network. Security intelligence gives the insight into what is happening in the information system and if some attack is underway. Once the information security team collects enough information about the tools and malware the attackers use it can carry out malware analysis to find out even more information about the attacker. “The purpose of malicious software analysis is to provide you with the information you need to respond to a network incursion. Your goals will be to find out what happened and make sure you found all the infected machines and files [1]. To protect the corporation from malicious threats, it is necessary within the corporation to analyze malicious content coming from different communication channels, such as email and Internet.

Malicious content analysis can be divided into dynamic analysis and static analysis. The dynamic analysis implies launching malicious files and tracking their behavior on the system. Monitoring involves reviewing the connection of malicious files to the Internet and checking the processes that the malicious file is triggering and what the processes are doing. Static analysis does not imply launching malicious files, but its content is reviewed here. An advanced static analysis uses a disassembler, which allows you to view the instructions of a malicious program.For static and dynamic analysis corporations can use an internal lab for analysis, but ready-made tools that can be used free of charge or solutions from other information security companies.

Intelligence Gathering Tools

Corporations must continuously monitor the security of their information system. To be able to do that, they must collect data about the system and analyze it. The quality of security intelligence depends on the tools that the corporation uses. These types of tools can achieve prices up to a couple of hundred thousand dollars, but their price does not guarantee total security [2]. It only guarantees that the information security team will get accurate and timely information about the security of the information system.

Splunk

Splunk is one of the main tools for data collection. It can collect different types of information about different types of devices. Every device that generates logs can be tracked via Splunk. Apart from collecting logs, the main part of Splunk is the ability to analyze raw information. Splunk gives the ability to visualize information and insert information into graphs. It also gives the ability to send alerts when a certain change happens in a system. Because of all of these abilities, Splunk is used in information security. A typical implementation of Splunk corporate security is monitoring e-mails and network traffic. With Splunk, it is possible to track all e-mails that exit or enter the corporate information system. Once monitoring has been established, criteria that trigger an alert can be set. An example of such a criterion is if an email with a corporate domain that is not sent from the corporate e-mail server appears. That means someone is pretending to be part of the corporation to get some information or compromise the system[3]. Once the information security team has received an alert on such an e-mail, it can alert the employee who has received this mail that this is not a legitimate e-mail but a malicious one.

In the financial industry, Splunk is most useful for tracking database access. Banks' databases are a key part of their business, as they have information on bank customers, accounts, and cards. The database will send logs to Splunk every time someone logs in or tries to log in to the database. The log will contain information about the username, which database someone attempted to access, with which user rights and at what time. Every employee who wants to access the database must get approval. To get the approval, there must be a justified business reason for the database access[4]. After obtaining approval, it is saved to the location Splunk has access to. Splunk will compare the information it receives from the database and the list of all who currently have the approval. If a user accesses the database and does not have the approval, the information security team will be alerted. The team can then investigate what has happened. As much as it is important to collect information, it is also important not to collect a lot of information. If the information security team receives a large amount of information, they will not be able to react promptly because processing this information will take too long. Splunk information must be summarized and timely, only after a possible incident is detected, a greater amount of information will be analyzed surrounding that incident[5].

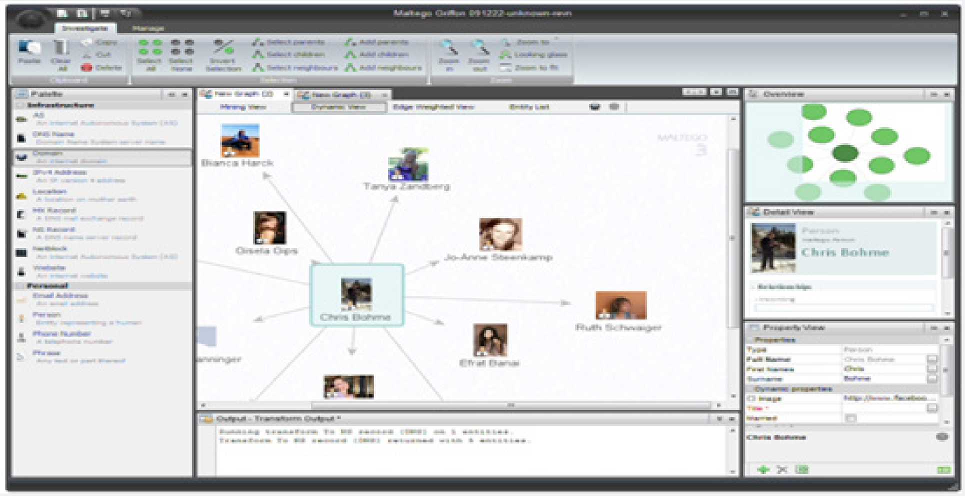
IBM Qradar

IBM Quadra is a SIEM system. SIEM systems are solutions that collect security intelligence from different devices and analyze anomalies. If they detect an anomaly in the system operation, they inform the security team and provide all available information about the event. IBM Quadra is a solution for large corporations that have a large number of logs. It collects logs of various devices such as network devices, computers, servers, security cameras, and applications. Quadra compares logs with a baseline. By comparing, it can detect security anomalies, device behavior changes, and events that can endanger the system[6]. These events are analyzed and presented to the information security team in simple form with essential aggregated information.

Radar is also used to analyze the security level of a device. It analyses the current security patch status on devices and provides insight into what a particular device or application is vulnerable to.

Maltego

Maltego is a platform that allows the use of OSINT. OSINT refers to all unclassified information and includes everything that is freely available on the web. OSINT is different from a closed type of intelligence or confidential information. Common OSINT resources include social networks, forums, business websites, blogs, videos, and news. Connecting data with a person on Maltego is shown in the picture below (Figure 1). Maltego allows visualization of the relationship between different information. It can display relationships between people, social networks, corporations, organizations, websites, DNS names, documents, and files. Malte go can be used for corporate purposes after malware analysis[7]. All information such as domains and IP addresses can be linked via the Malte go platform to the location and people who have some connection with this domain. It gives the possibility of rapid progression of the investigation into the purpose and cause of the attack. Since Malte go is used in defense against malware, the corporation can analyze itself and see which information is available about them and if there is something sensitive that is part of the publicly available information. It may ask the person who disclosed that information to remove them or by legal means request the removal of this information.



```
Running transform To MX record [DNS] on 1 entities.
Transform To MX record [DNS] returned with 5 entities.
```

Figure 1: Connecting Data About A Person.

How to cite this article: Nikola P, GrgaJovanovski. Using Security Intelligence in Corporations. J Forensic Sci & Criminal Inves 2018; 9(5): 555775. DOI: 10.19080/JFSCI.2018.09.555775.

Malware analysis laboratory

The malware Analysis Laboratory enables the security team to launch malicious software in a secure environment to understand what it does and what it takes to protect from the threat posed by a malicious program. If done well, the lab can be a powerful tool for quick understanding and protection from new threats or unknown actors. [5].If a corporation decides to analyze in its own laboratory, such a laboratory needs to be prepared for conducting the analysis. It is important that the laboratory is separated from corporate computers and networks, and that access is allowed only to information security personnel.There are several elements of such a lab.

Virtual Machines

The core of the lab itself is virtual computers. It is necessary to prepare and install several virtual computers with different operating systems, such as Windows XP, Windows 7, Windows 8, Windows 10. If a corporation uses Apple computers, it is necessary to obtain a few computers running the Mac OS operating system, so samples that attack Apple computers can analyze. The same goes for the Linux operating system.Some malicious programs behave differently on different operating systems, so several versions need to be installed. In addition, it is necessary to prepare another virtual computer that will serve for the static analysis.To be able to return to the original state without infection, snapshots should be applied. Therefore, the snapshot is set up after the installation of the tools, so it is possible to return to the previous state when the analysis is finished.In order not to infect other corporate computers, it is necessary to separate the network segment that contains the computers for analysis from the corporate network. It is most desirable to get a separate connection to the Internet just for the analysis computers.

Tools for Dynamic Analysis

After installing virtual computers for dynamic analysis, several tools need to be installed.

a. Process Monitor

b. Reshot

c. ApateDNS

d. FakeNET

e. Wireshark

Along these tools, some basic tools need to be installed, such as Internet browsers, document management tools, and unzipping tools. This is because the malicious file does not have to be in the .exe format, it can be inside a document or as a .jre file so it is necessary to install the tools that will be able to run such a file.

Tools for Static Analysis

On a computer that is configured for static analysis, it is useful to have several programs listed below. All these tools must be able to analyze the code without starting the sample, but for security, it is best to run these tools on a virtual machine.

a. Strings

b. PE studio

c. PEID

d. PE view

e. UPX

f. Resource Hacker Like on dynamic analysis computers, it is useful to install basic programs.

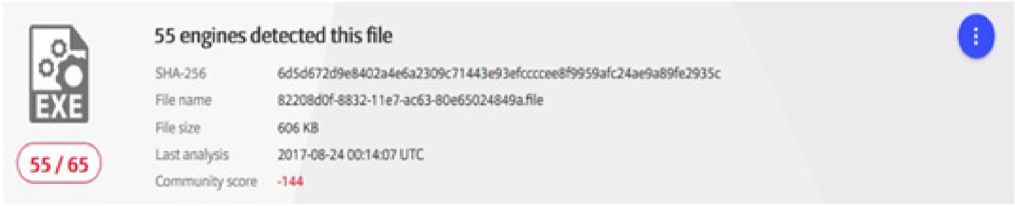
Publicly Available Tools for Malware Analysis

There are several malware analysis tools available through the Internet. Some of them are available free of charge, while most of them are paid solutions. The best-known tools are VxStream Hybrid Analysis from Payload Security, Virus Total from Google and Malwr based on the Cuckoo Sandbox platform. In most cases, the analysis with publicly available tools is sufficient as they provide enough information to determine what kind of malicious code it is and what protection measures are to be taken. The only case in which it is not recommended to upload to publicly available tools is when there is a suspicion that malicious content is intended for a corporation and may contain information sensitive to its business.Each of these free tools has its paid version and provides additional features. Virus Total in its paid version offers download of samples analyzed on the platform, while Hybrid Analysis has this in its free version. For this paper, Virus Total and Vx Stream Hybrid Analysis will be used. Malwr will not be used because it is unreliable lately and does not reveal enough sample information.

Virus Total

Virus Total is a platform launched in 2004, and Google has bought it in 2012. Virus Total gives the ability to analyze computer files and Android applications. The file is scanned with a series of antivirus solutions and provides feedback for each antivirus, whether the file is malicious and under what name it is categorized. In addition, it provides detailed information on the file type and its contents. Locky will be analyzed on this platform. Locky is a ransomware that encrypts files on both internal and external drives and requires a certain amount of money to decrypt. After the payment, it sends a key to decrypt the files. After uploading the file, the first display contains: file type in the form of an icon, number of antiviruses detecting that the file is malicious, SHA-256 file hash, file name and file size, date and time of the last file analysis, and number of users who rated the file malicious (Figure 2). Using the SHA-256 hash, it is possible to find out whether the sample was uploaded to another platform for analysis. Label 55/65 states that the sample is known to most antiviruses, so in the case of sample launch there is a great chance that antivirus will stop the sample from running on the computer.

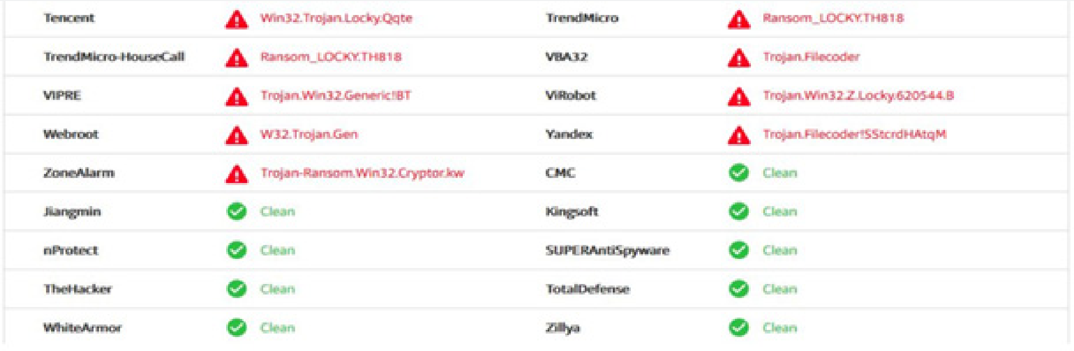
How to cite this article: Nikola P, GrgaJovanovski. Using Security Intelligence in Corporations. J Forensic Sci & Criminal Inves 2018; 9(5): 555775. DOI: 10.19080/JFSCI.2018.09.555775.



55 engines detected this file

SHA-256	6d5d672d9e8402a4e6a2309c71443e93efccccee8f9959afc24ae9a89fe2935c
File name	82208d0f-8832-11e7-ac63-80e65024849a.file
File size	606 KB
Last analysis	2017-08-24 00:14:07 UTC
Community score	-144

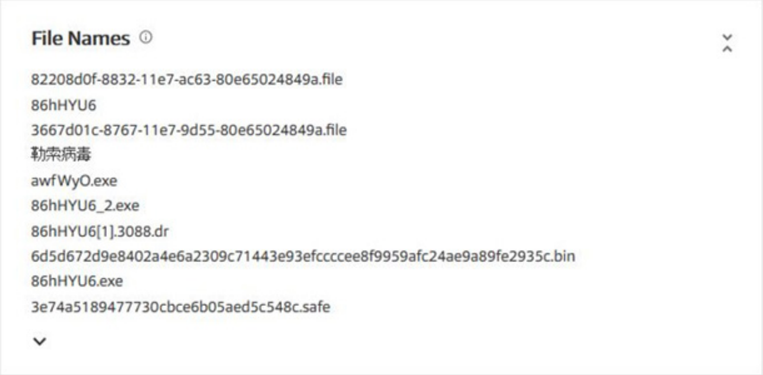
Figure 2: Basic Information of The Sample.



Tencent	Win32.Trojan.Locky.Qqte	TrendMicro	Ransom_LOCKY.TH818
TrendMicro-HouseCall	Ransom_LOCKY.TH818	VBA32	Trojan.Filecoder
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.Z.Locky.620544.B
Webroot	W32.Trojan.Gen	Yandex	Trojan.Filecoder!SStcrdHAtqM
ZoneAlarm	Trojan-Ransom.Win32.Cryptor.kw	CMC	✓ Clean
Jiangmin	✓ Clean	Kingsoft	✓ Clean
nProtect	✓ Clean	SUPERAntiSpyware	✓ Clean
TheHacker	✓ Clean	TotalDefense	✓ Clean
WhiteArmor	✓ Clean	Zillya	✓ Clean

Figure 3: List of Antiviruses and Detection Rates.

The following image Figure 3 shows several antiviruses that have or have not detected that the sample is malicious. It is visible that TrendMicro and Vi Robot successfully detected the sample as Locky, while Kingsoft and Total Defense antiviruses indicated that the sample was clean. This knowledge is very useful to ascertain whether the current corporate antivirus system is able to defend the corporation from this threat.Under the card details, there is information about the file. The most interesting part of the basic analysis are the names under which this sample appeared (Figure 4). All file names have something in common, they have the same SHA-256 hash.Interestingly, this sample has different extensions such as. safe and.dr, but they are still .exe type files. It can be concluded that in the case of the. safe extension, the attacker tried to hide the actual file extension and replaced it with an extension that does not look malicious.Virus Total also displays the compile time in the details, but in most cases, it is incorrect because it is possible to change compile time when writing code.



File Names

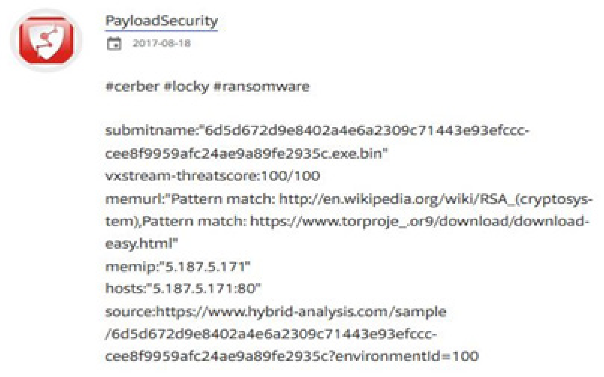
82208d0f-8832-11e7-ac63-80e65024849a.file
86hHYU6
3667d01c-8767-11e7-9d55-80e65024849a.file
勒索病毒
awfWyO.exe
86hHYU6_2.exe
86hHYU6[1].3088.dr
6d5d672d9e8402a4e6a2309c71443e93efccccee8f9959afc24ae9a89fe2935c.bin
86hHYU6.exe
3e74a5189477730cbce6b05aed5c548c.safe

Figure 4: Sample Names.

The compile time of this sample is 02.03.2013, but it is certainly incorrect because this sample first appeared in 2010. The last tab shows user comments. Most of the comments consist of the malicious code name and help with the basic analysis if it is not possible to conclude what the type is. If the sample was uploaded on Hybrid Analysis, a Payload Security comment will appear that will have the type of malicious code and additional information as well as the link on the Hybrid Analysis platform where that same sample was analyzed. The picture shows such a comment (Figure 5).In conclusion, Virus Total is a very reliable and fast tool for basic file analysis and quickly determining whether the file is malicious. It is useful in determining the

How to cite this article: Nikola P, GrgaJovanovski. Using Security Intelligence in Corporations. J Forensic Sci & Criminal Inves 2018; 9(5): 555775. DOI: 10.19080/JFSCI.2018.09.555775.

effectiveness of the corporate antivirus, and for quick analysis where the only information needed is whether the sample is malicious or not. If a deeper analysis of files is needed, Hybrid Analysis and manual dynamic and static analysis is used



PayloadSecurity
2017-08-18

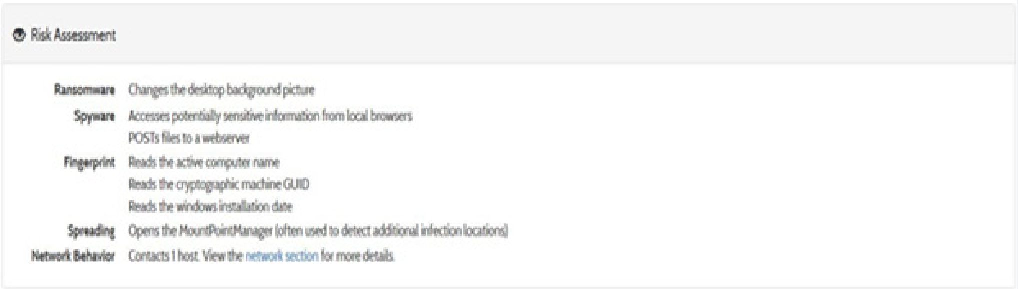
#cerber #locky #ransomware

```
submitname:"6d5d672d9e8402a4e6a2309c71443e93efccc-
cee8f9959afc24ae9a89fe2935c.exe.bin"
vxstream-threatscore:100/100
memurl:"Pattern match: http://en.wikipedia.org/wiki/RSA_(cryptosys-
tem),Pattern match: https://www.torproje_.or9/download/download-
easy.html"
memip:"5.187.5.171"
hosts:"5.187.5.171:80"
source:https://www.hybrid-analysis.com/sample
/6d5d672d9e8402a4e6a2309c71443e93efccc-
cee8f9959afc24ae9a89fe2935c?environmentId=100
```

Figure 5: Payload Security Comment.

Hybrid Analysis

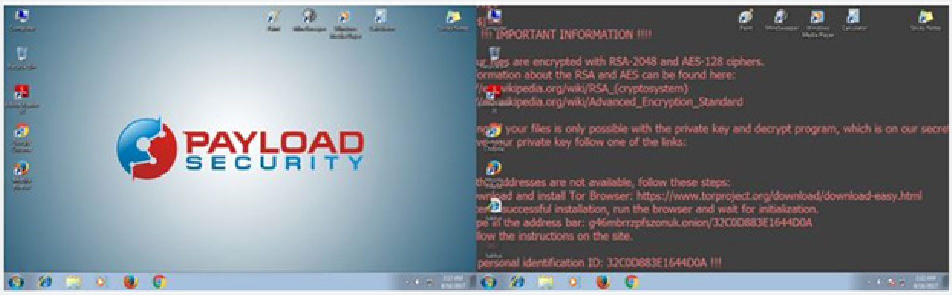
Hybrid Analysis is a platform for dynamic and static file analysis. While Virus Total only checks if antiviruses detect given malware, Hybrid Analysis runs a file on a virtual computer and tracks its behavior. In addition, it uses scripts to run files that simulate human behavior, so the malicious file cannot recognize it is running in an automated virtual environment.Hybrid Analysis allows uploading different file types and can scan files that are somewhere online and have their link.On the Hybrid Analysis platform, a Locky sample will be analyzed that was also analyzed on the Virus Total platform.The following Figure 6 shows the risk rating that is the first part of the platform and has key information about what the platform found out from the analyzed file. This sample changes the background of the desktop, so it is immediately possible to conclude that it is a ransomware. The reason for the background change is to inform the user that all the files on the computer are encrypted and the payment method to receive the decryption key. The image also shows that the file at runtime contacts one address on the Internet.Another, most interesting part are the screenshots (Figure 7).That were recorded by the platform before and after launching the code. This is very useful because it is possible to see if malicious code left some visual traces after starting.



Risk Assessment

Ransomware	Changes the desktop background picture
Spyware	Accesses potentially sensitive information from local browsers POSTs files to a webserver
Fingerprint	Reads the active computer name Reads the cryptographic machine GUID Reads the windows installation date
Spreading	Opens the MountPointManager (often used to detect additional infection locations)
Network Behavior	Contacts 1 host. View the network section for more details.

Figure 6: Risk Assessment.



!!! IMPORTANT INFORMATION !!!!

ur files are encrypted with RSA-2048 and AES-128 ciphers.
ormation about the RSA and AES can be found here:
/en.wikipedia.org/wiki/RSA_(cryptosystem)
//en.wikipedia.org/wiki/Advanced_Encryption_Standard

ng of your files is only possible with the private key and decrypt program, which is on our secre
ve your private key follow one of the links:

the addresses are not available, follow these steps:
wnload and install Tor Browser: https://www.torproject.org/download/download-easy.html
ter a successful installation, run the browser and wait for initialization.
pe in the address bar: g46mbrrzpfszonuk.onion/32C0D883E1644D0A
llow the instructions on the site.

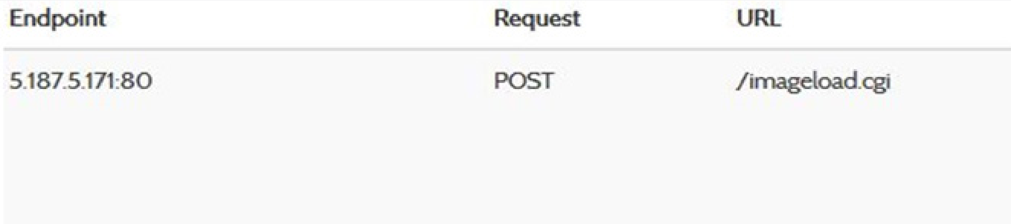
personal identification ID: 32C0D883E1644D0A !!!

Figure 7: Screenshots.

How to cite this article: Nikola P, GrgaJovanovski. Using Security Intelligence in Corporations. J Forensic Sci & Criminal Inves 2018; 9(5): 555775. DOI: 10.19080/JFSCI.2018.09.555775.

Screenshots

The last part is the network section that shows what the sample contacted. In this case, it contacted one address. Malicious files have two types of addresses that they contact. One is the payload address from which the malicious code will be downloaded[8]. It uses the HTTP GET command to download. Payload addresses are quite commonly used because they allow the first file to have no malicious indications, but its task will be to download and run the malicious code, so the first file can avoid detection. The second type of domains that the malicious file can contact is the C&C domain. To this domain the malicious code sends information it has collected from the victim's computer and in some cases gives control of the infected computer. It can be recognized if the protocol used is the HTTP with the POST command. In this case, it is possible to see POST at IP address 5.187.5[.]17image load. cgi. Figure 8 shows the HTTP POST request. In some cases, Hybrid Analysis is not able to detect all the malicious domains contacted. They can be detected in Dynamic Analysis using the Wireshark tool.



Endpoint	Request	URL
5.187.5.171:80	POST	/imageload.cgi

Figure 8: Http Post Request.

Malware Analysis with Commercial Tools

Sample analysis with commercial tools is a quick and reliable way of detecting whether the sample is malicious. In most tools, there are three types of analysis platforms. An e-mail platform that intercepts any message sent from outside the corporate network and analyzes its structure and attachments in search of malicious files or links. A network traffic platform that intercepts the download of each file and analyzes it before permitting the download[9]. The analysis platform serves to analyze the samples that the information security team chooses, it is very similar to the Hybrid Analysis platform.

Fire Eye

FireEye is a company founded in 2004 and it is currently one of the world's most well-known information security companies. It offers various solutions, such as email analysis platform, traffic analysis platform, computer agents, and penetration testing.The FireEye EX device is used for electronic mail analysis. It resides between the external e-mail server and the internal e-mail server. Any message coming from an external address and has successfully passed the email server filter is analyzed in the virtual environment of this device. If the mail is not malicious, it will be forwarded to the server and then to the recipient. If the mail is malicious it is put in quarantine and EX notifies the information security team, it provides detailed information about the structure and type of the malicious code.The FireEye NX device is used for network traffic analysis. It resides after the web proxy and analyzes web traffic[10]. All traffic and downloaded files are analyzed before the download is allowed. If the file is malicious, it is quarantined, and the device informs the information security team. Like EX, it provides detailed information on the structure of the malicious code.

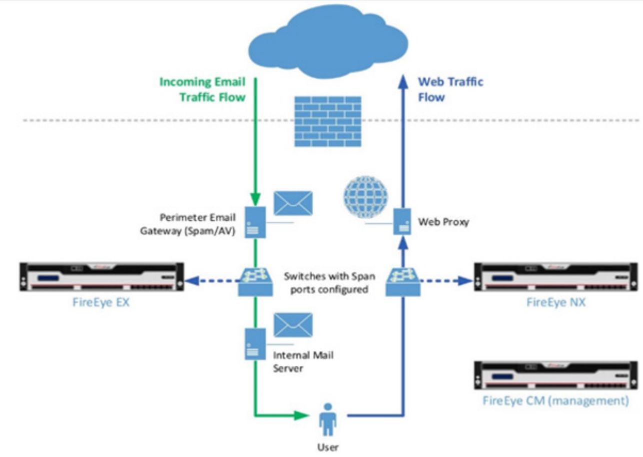
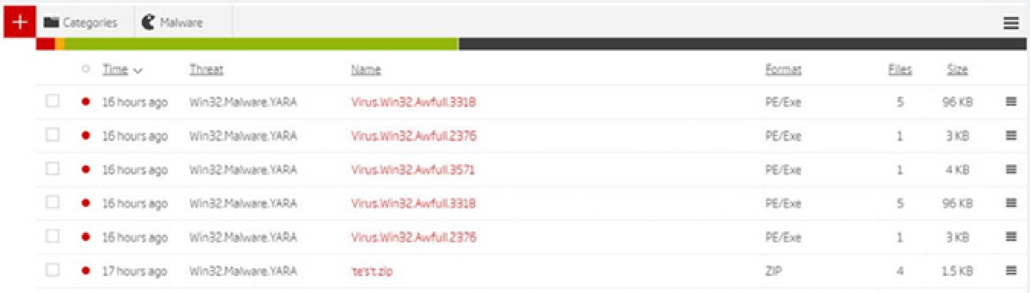

Incoming Email Traffic Flow
Web Traffic Flow
Perimeter Email Gateway (Spam/AV)
Web Proxy
Switches with Span ports configured
FireEye EX
FireEye NX
Internal Mail Server
FireEye CM (management)
User

Figure 9: Sample Names.

Figure 9 shows the way to connect the EX and NX devices to the corporate network. The FireEye HX device is used for endpoint security. Agents are deployed on the corporate computers and then HX can monitor those endpoints. HX can monitor what is happening on each endpoint, what processes are running, and which files are being accessed. The information security team can implement certain rules by which for example if a process with a certain name is run the HX will notify the team and stop the execution. It can also stop files with certain hashes or names from being run. FireEye HX collects information about the network connections made from and to the endpoint, which files where opened, which process was running and registry changes. It can usually save logs up to five days. It also supports quarantining the endpoint if that endpoint is infected. When an endpoint is quarantined all network, connections are blocked by the agent and the endpoint can only communicate with the HX. This protects other endpoints from the infections and gives the information security team the ability to analyze the endpoint.

Reversing Labs

Reversing Labs is an information security company based in Croatia. Like FireEye, they have different solutions for information security. The main part is the Titanium Core platform for malicious content analysis. It analyzes files in a virtual environment by static analysis and can analyze millions of files per day. A1000 is a device for malicious content analysis in the security operations center. It uses Titanium Core for analysis. It can work with a large file spectrum and can use reputation-based analysis, so it can detect that the file is malicious even before the main analysis.The following Figure 10 shows a list of analyzed files and short information about them.The N1000 is a device that connects the email analysis platform and the network traffic analysis platform. It also uses Titanium Core.



		Time	Threat	Name	Format	Files	Size	
□	●	16 hours ago	Win32.Malware.YARA	Virus.Win32.Awfull.3318	PE/Exe	5	96 KB	≡
□	●	16 hours ago	Win32.Malware.YARA	Virus.Win32.Awfull.2376	PE/Exe	1	3 KB	≡
□	●	16 hours ago	Win32.Malware.YARA	Virus.Win32.Awfull.3571	PE/Exe	1	4 KB	≡
□	●	16 hours ago	Win32.Malware.YARA	Virus.Win32.Awfull.3318	PE/Exe	5	96 KB	≡
□	●	16 hours ago	Win32.Malware.YARA	Virus.Win32.Awfull.2376	PE/Exe	1	3 KB	≡
□	●	17 hours ago	Win32.Malware.YARA	'te'st.zip	ZIP	4	1.5 KB	≡

Figure 10: List Of Analyzed Files And Short Information About Them (Reversinglabs).

Defense Code

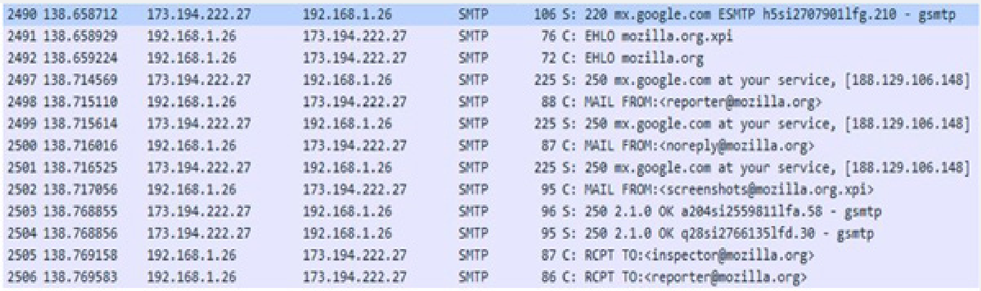
Defense Code is a Croatian company that deals with computer security. It offers two products to corporations to increase the level of information security.The first is Thunder Scan that does source code analysis and provides insight into all the vulnerabilities in that code. Supports C #, Java, PHP, ASP, VB.Net, Visual Basic, VBScript, Java script, Android Java, IOS Objective C, PL / SQL. It is extremely useful for corporations that issue their software solutions because most of these solutions have many vulnerabilities[11].The second one is Web Scanner, which is an automated platform for penetration testing of web pages. It attacks the designated website with different techniques to find vulnerabilities, and after the attack, it shows a report on types of vulnerabilities. Corporations can test the vulnerability of their websites with this tool.

Dynamic Analysis

Dynamic analysis means running malicious code and observing what it is doing and how it behaves. It is most commonly done in virtual computers because it is easy to get back to the state before the infection. In some cases, malicious code will recognize that it is running in a virtual environment, so it will not start, in these cases, it is necessary to have dedicated physical computers to run the analysis.

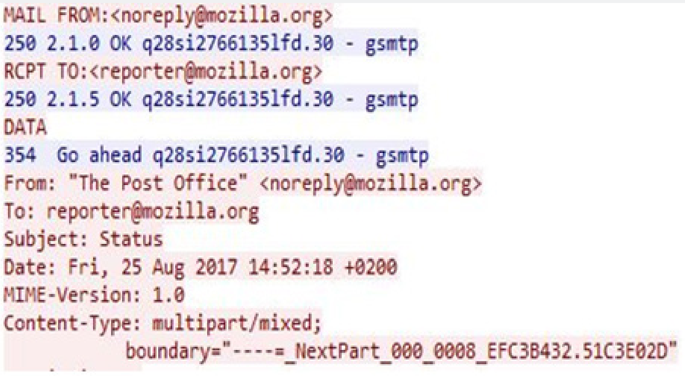
Network Traffic

Wireshark is used to capture network traffic within a virtual computer. Before launching potentially malicious files, it is necessary to start Wireshark and start the packet capture on the network interface that is connected to the Internet.In the static analysis of this sample, it was apparent that the sample would attempt to start communication, while dynamic analysis can verify whether this is true.After successfully running the sample, in Wireshark, there is a large amount of SMTP traffic[12]. This is the first indicator that it is malicious because the Windows operating system without the SMTP agent installed will not send and receive SMTP traffic. The following picture Figure 11 shows SMTP traffic.By selecting line number 2506, and right clicking to select Follow TCP Stream it is possible to analyze the entire communication with which that package is linked. The following Figure 12 shows the TCP packet stream. It is apparent that the sample attempted to send an email to reporter@mozilla.org but from the fake address noreply@mozilla.org. In addition, the message has a subject Status, which is one of the subjects that My Doom uses in its malicious e-mails, and the same subject was shown in the static analysis[13].



```
2490 138.658712  173.194.222.27  192.168.1.26    SMTP  106 S: 220 mx.google.com ESMTP h5si2707901lfg.210 - gsmtp
2491 138.658929  192.168.1.26    173.194.222.27  SMTP   76 C: EHLO mozilla.org.xpi
2492 138.659224  192.168.1.26    173.194.222.27  SMTP   72 C: EHLO mozilla.org
2497 138.714569  173.194.222.27  192.168.1.26    SMTP  225 S: 250 mx.google.com at your service, [188.129.106.148]
2498 138.715110  192.168.1.26    173.194.222.27  SMTP   88 C: MAIL FROM:<reporter@mozilla.org>
2499 138.715614  173.194.222.27  192.168.1.26    SMTP  225 S: 250 mx.google.com at your service, [188.129.106.148]
2500 138.716016  192.168.1.26    173.194.222.27  SMTP   87 C: MAIL FROM:<noreply@mozilla.org>
2501 138.716525  173.194.222.27  192.168.1.26    SMTP  225 S: 250 mx.google.com at your service, [188.129.106.148]
2502 138.717056  192.168.1.26    173.194.222.27  SMTP   95 C: MAIL FROM:<screenshots@mozilla.org.xpi>
2503 138.768855  173.194.222.27  192.168.1.26    SMTP   96 S: 250 2.1.0 OK a204si2559811lfa.58 - gsmtp
2504 138.768856  173.194.222.27  192.168.1.26    SMTP   95 S: 250 2.1.0 OK q28si2766135lfd.30 - gsmtp
2505 138.769158  192.168.1.26    173.194.222.27  SMTP   87 C: RCPT TO:<inspector@mozilla.org>
2506 138.769583  192.168.1.26    173.194.222.27  SMTP   86 C: RCPT TO:<reporter@mozilla.org>
```

Figure 11: List Of Analyzed Files And Short Information About Them (Reversinglabs).



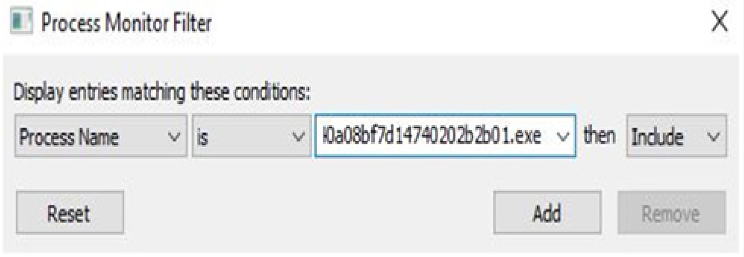
```
MAIL FROM:<noreply@mozilla.org>
250 2.1.0 OK q28si2766135lfd.30 - gsmtp
RCPT TO:<reporter@mozilla.org>
250 2.1.5 OK q28si2766135lfd.30 - gsmtp
DATA
354  Go ahead q28si2766135lfd.30 - gsmtp
From: "The Post Office" <noreply@mozilla.org>
To: reporter@mozilla.org
Subject: Status
Date: Fri, 25 Aug 2017 14:52:18 +0200
MIME-Version: 1.0
Content-Type: multipart/mixed;
           boundary="----=_NextPart_000_0008_EFC3B432.51C3E02D"
```

Figure 12: TcpPacket Stream.

Monitoring Processes

When the sample is started, it is possible to keep track of what the sample is doing and what functions it calls.

In the static analysis, the conclusion was that the sample would try to open or create a new file and modify the Windows registry keys. The process monitor tool is Proc Mon that is part of the System Internals tool. After starting the sample, it is necessary to make a filter in Proc Mon to make it easier to keep track of what the sample is doing. On the Filter tab, select Filter ... and in the next window, the settings must be exactly like in the picture, with the exception that the process name must be the same as the sample name. The image Figure 13. shows the filter settings. Finally, select Add and OK. Only the events that the sample has run will now appear in the main window. There are many operations with the Windows Registry, it is apparent that the sample changes the registry keys, as shown in Figure 14. My Doom searches for potential email addresses in different text files so it is possible for Proc Mon to show that it is opening one of the .txt files. The image Figure 15 shows the process of opening the .txt file. The following picture (Figure 16). Also shows the SMTP traffic that the sample tries to establish to send its copy to as many addresses as possible found in the text files.

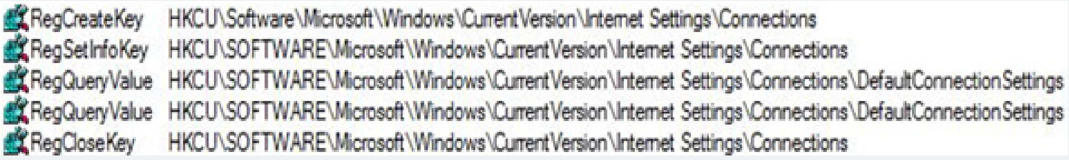


Process Monitor Filter

Display entries matching these conditions:

Process Name: is: l0a08bf7d14740202b2b01.exe then Include

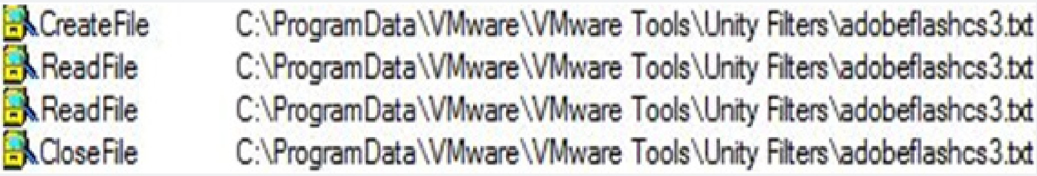
Figure 13: Filter Settings.



```
RegCreateKey    HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
RegSetInfoKey   HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
RegQueryValue   HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
RegQueryValue   HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
RegCloseKey     HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
```

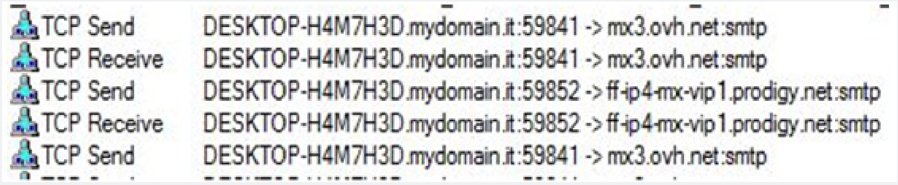
Figure 14: Changes In The Registry.

How to cite this article: Nikola P, GrgaJovanovski. Using Security Intelligence in Corporations. J Forensic Sci & Criminal Inves 2018; 9(5): 555775. DOI: 10.19080/JFSCI.2018.09.555775.



```
CreateFile    C:\ProgramData\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt
ReadFile      C:\ProgramData\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt
ReadFile      C:\ProgramData\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt
CloseFile     C:\ProgramData\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt
```

Figure 15: The Process of Opening a Txt File



```
TCP Send      DESKTOP-H4M7H3D.mydomain.it:59841 -> mx3.ovh.net:smtp
TCP Receive   DESKTOP-H4M7H3D.mydomain.it:59841 -> mx3.ovh.net:smtp
TCP Send      DESKTOP-H4M7H3D.mydomain.it:59852 -> ff-ip4-mx-vip1.prodigy.net:smtp
TCP Receive   DESKTOP-H4M7H3D.mydomain.it:59852 -> ff-ip4-mx-vip1.prodigy.net:smtp
TCP Send      DESKTOP-H4M7H3D.mydomain.it:59841 -> mx3.ovh.net:smtp
```

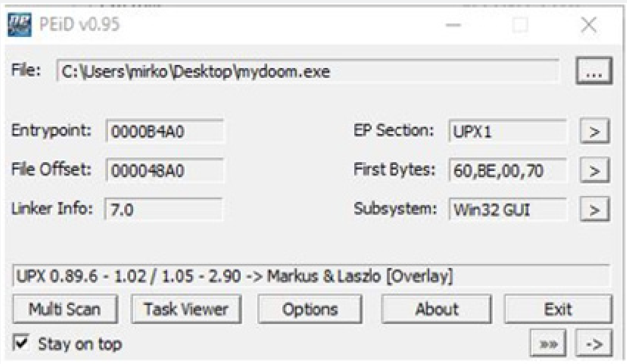
Figure 16: SMTP Traffic

Static Analysis

Static analysis is used if dynamic does not show enough information or it is needed to know exactly how the malicious code works. Simple static analysis has a few steps described in this paper. Advanced static analysis requires disassembly and it will not be described in this paper. An example of static analysis will be shown on the My Doom worm sample.

File Unpacking

Most malicious code authors hide the original code, so it could not be analyzed. The obfuscated code has its sub-category called packed code and that code can be read after unpacking.The type of packaging can be checked with the PEID program. After uploading the potentially packaged file, it will show the type of packing. Figure 17 shows the interface of the PEID program with an already loaded sample. PEID has successfully detected the packer as UPX Packer.UPX is one of the most popular packers and it is easy to unpack it with the UPX tool.This command will unpack the mydoom.exe file and save the unpacked file to the same directory under the name mydoom_clean.exe: upx -d mydoom.exe -o mydoom_clean.exe.The followingFigure 18 shows that UPX has successfully unpacked the file so it is now possible to continue the analysis.



PEiD v0.95

File: C:\Users\mirko\Desktop\mydoom.exe

Entrypoint: 0000B4A0

File Offset: 000048A0

Linker Info: 7.0

EP Section: UPX1

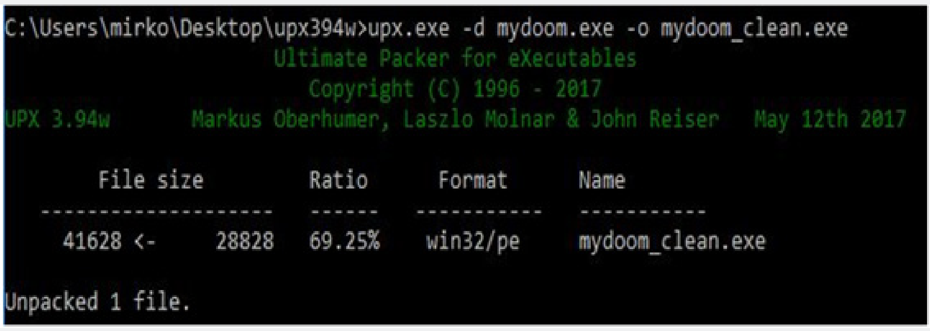
First Bytes: 60,BE,00,70

Subsystem: Win32 GUI

UPX 0.89.6 - 1.02 / 1.05 - 2.90 -> Markus & Laszlo [Overlay]

☑ Stay on top

Figure 17: PEID Interface.

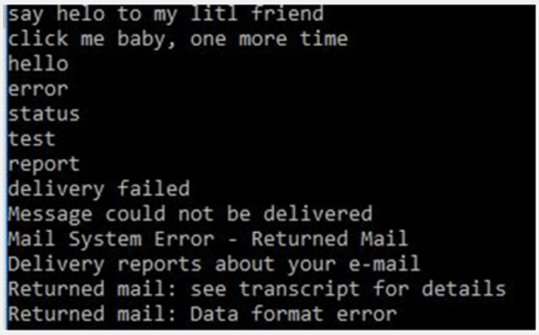


```
C:\Users\mirko\Desktop\upx394w>upx.exe -d mydoom.exe -o mydoom_clean.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2017
UPX 3.94w       Markus Oberhumer, Laszlo Molnar & John Reiser   May 12th 2017

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     41628 <-     28828   69.25%    win32/pe     mydoom_clean.exe

Unpacked 1 file.
```

Figure 18: Information After Unpacking.

Strings

One of the essential parts after unpacking is to find some meaningful strings inside the code. These characters can reveal a lot about how the malicious code works and provide relevant information about the type of malicious code.The string of characters from the .exe file can be extracted with the tool Strings. The command is:strings64.exe mydoom.exe.An interesting section of the Strings command is shown in Figure 19. Most of the sentences mentioned were the subject or body of the e-mails that spread the most famous worm named MyDoom. There are many strings that can be read in this sample. Most of them are domains to which the worm has spread.

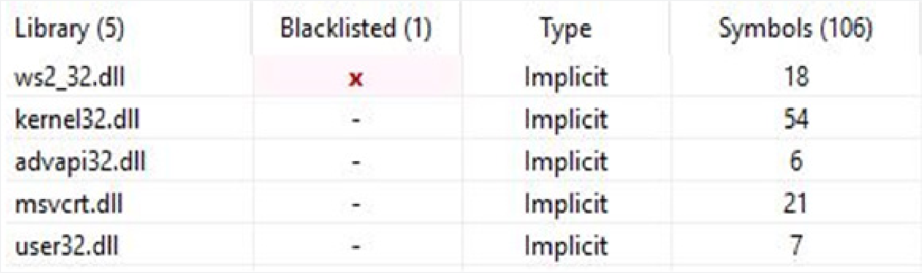


```
say helo to my litl friend
click me baby, one more time
hello
error
status
test
report
delivery failed
Message could not be delivered
Mail System Error - Returned Mail
Delivery reports about your e-mail
Returned mail: see transcript for details
Returned mail: Data format error
```

Figure 19: The Result of the Strings Tool

Linked Libraries

There are three ways to link program libraries. One of them is a static connection, where all the code from the library is transferred to the program. Another way is to dynamically connect, where all required code from the library is loaded when the program runs. The last way is connecting at startup, where the code from the library is called only when the function in a program is requiring it. The last way is best known for malicious codingbecause it is impossible to analyze the code without running it.Pestudio makes it possible to check the dynamically linked code. The sample loads 5 libraries: kernel32.dll, advapi32.dll, msvcrt.dll, user32.dll and ws2_32.dllFigure 20 shows the loaded libraries.If a sample loads advapi32.dll it also means that it is doing a change in the Windows Registry, so it is needed to check them in the dynamic analysis which keys have been changed. This sample uses advapi32.dll and loads RegCreateKeyEx, which is responsible for creating a registry key and RegSetValueEx, which is responsible for changing a key. It is known that this sample will create and modify the registry keys. The sample uses ws2_32.dll, which means that it will attempt to start a communication with an address or domain.



Library (5)	Blacklisted (1)	Type	Symbols (106)
ws2_32.dll	x	Implicit	18
kernel32.dll	-	Implicit	54
advapi32.dll	-	Implicit	6
msvcrt.dll	-	Implicit	21
user32.dll	-	Implicit	7

Figure 20: Loaded Libraries.

It calls the accept and bind functions, which allows it to listen to a specific port. Connect and send functions allows it to merge and send data to a remote address; it is often used to connect to a C&C address. The Inetaddr function converts the IP address into a format that is readable to other functions. Gethostbyvalue and Gethostvalue functions allow the sample to do DNS searches.The last that the sample is using, and relevant in the analysis, is kernel32.dll. The CreateFile function creates a new or opens an existing file. CreateFileMapping allows access to a file via a memory address. FindFirstFile and FindNextFile allow a search of the file system. GetWindowsDirectory returns the location of the Windows operating system installation. It is possible to conclude that the sample will attempt to create a file in the Windows directory.Functions give a lot of information about what some malicious code will try to do. It is difficult to analyze all the functions that some program loads, but the above functions are some of the most important in analyzing malicious files.

Program Resources

Some programs use visual operating system resources and can be checked by the Resource Hacker tool. Resources are in the.rscr part of the program.After uploading the sample to the program, it is apparent that it uses the email icon as a program icon. The reason for this is confusing the user. Image Figure 21 displays the Resource Hacker tool result.

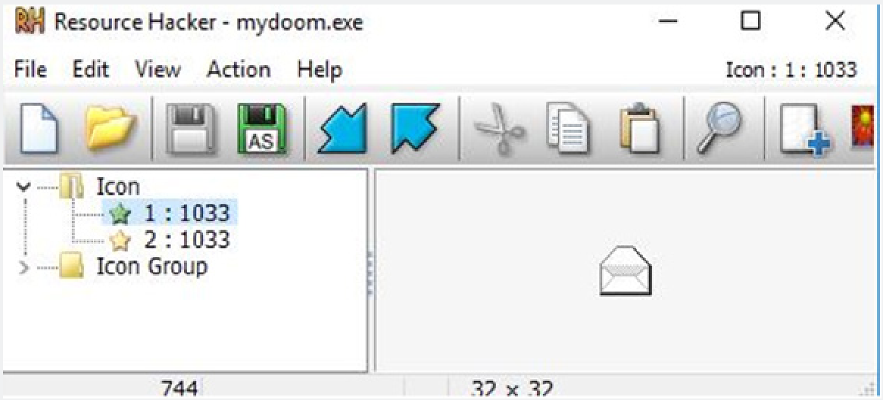


Figure 21: Resource Hacker Result.

Conclusion

Security intelligence is an essential part of corporate information security. It requires the collection of information and a thorough and quick analysis.The corporations can use many tools at its disposal for security intelligence gathering and malware analysis. For the best results, open source and commercial tools should be used together.By analyzing the malicious content used in attempts to attack a corporation, it is possible to establish better security controls. The analysis has certain steps and tools described in this paper. The most important thing in the analysis is to get as much information as possible about the attack and its methods. It is useful to keep a database of all analyzed samples.The rise of computer threats to the corporation also increases the number of defense methods. It is important to educate users about security and how to recognize the attack, as they are the first line of defense and most often the first attack targets for the attacker to gain further access to the system. It is a recommendation to educate corporate users annually, as the state of technology and type of attack often change.

References

1. Liska A (2014) Building an intelligence-led security program. Syngress.
2. Crump J (2015) Corporate security intelligence and strategic decision making. Crc press.
3. Sikorski M (2012) Practical malware analysis. No starch press.
4. Dewdney AK (1989) Computer recreations: of worms, viruses and core war, scientific american110-113.
5. Bilandžić M, lucić D, (2014) A predicting business opportunities and/or threats – business intelligence in the service of corporate security. Collegium anthropological 38(1): 25-33.
6. (2007) Zakon o informacijskoj sigurnosti.
7. (2008) Metodologija penetracijskoj testiranj.
8. (2014) Analiza računalnog kriminaliteta za.
9. (2016) Verizon data breach investigations report.
10. Wielenga G (2010) Interview: intelligence gathering software on the net beans platform.
11. Al damati R (2015) Deployment architectures for fireeye nx and EX.
12. (2018) Malware Analysis Platform.
13. (2013) What is OSINT and how can your organization use it.

DOI: 10.19080/JFSCI.2018.09.555775