NETWORK SECURITY CMM 528

Intrusion Detection and Log File Analysis

KUSHAL RAHATKAR

TABLE OF CONTENTS

ANALYSIS OF THE THREAT

Background of the Threat

FireEye's HX detected the first ever Cerber Ransomware campaign on June 10, 2016. It detected the distribution of malicious MS Word files linked to the email id. These files had malicious macro attached to them which were written to connect victim to the attacker. And after successful connection, an attacker would deploy a ransomware family member Cerber on the system of victim to launch a ransomware attack.

After noticing, FireEye HX working with CERT – Netherlands launched an intended Cerber infection and successfully shut down the Cerber Command and Control making Cerber Ransomware infective globally.

Process of Propagation and Infection

Propagation

In the figure 1, The process of a propagation of a malware has been explained. At the first, the Document containing the malicious code is opened by the victim. Once the file is opened, the code hidden in the file is executed. The working of a code is not visible on the screen, but it can be seen on the task running on the system. On successful execution of a code, the victim's system gets connected to the system and the ransomware gets installed on the system. This ransomware gets executed by the powershell on the backend which is hidden from the user but can be captured in the Task Manager. Malware encrypts the system important file and creates a DDoS type attack. Typically, in the case of Cerber, it has seen that the executable also deletes backup using Windows utilities like WMIC and/or VSSAdmin.

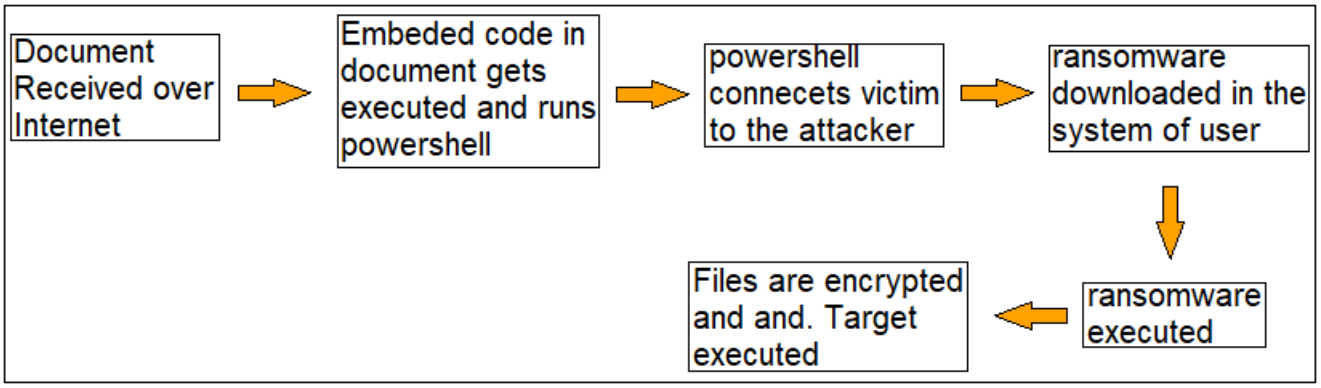

Figure 1

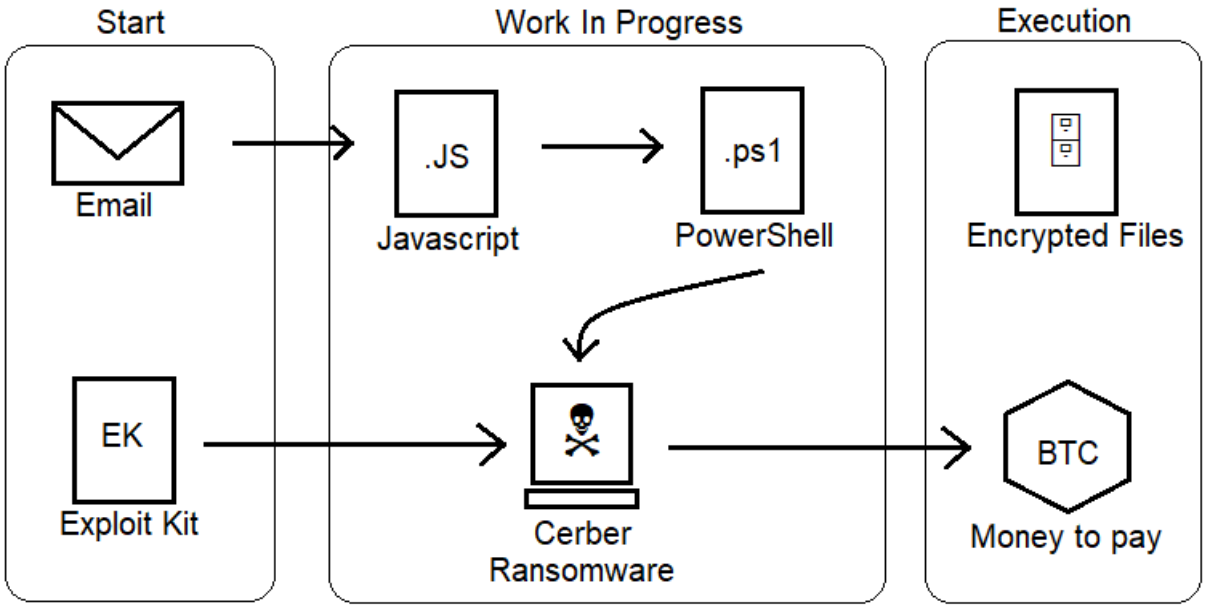

Figure 2

Infection

When a victim is tricked in to opening a malicious application, the script hidden in a file which is called as macro executes VBScrip and VBScript uses PowerShell to connect victim and attackers PC. All this execution is done in hidden mode. The hash of a malware here is constantly changing with respect to time and data bytes. This is used for evasion of hash-based detection system.

❖ Starting Phase of Injection

Once the malware is downloaded and executed, it seems the directory it has been landed in to. If the directory is not %APPDATA%\<VBFILE>, the file creates a copy of itself in %APPDATA% directory having any filename which is mostly selected from the directory of %system32%. If the malware is landed in the perfect directory that is %APPDATA% and knows the names it shouldn't catch to get detected, the malware creates a new copy of itself in %APPDATA% \<VBFILE> using random name selected from %system32%. The malware executes itself from the new location and deletes itself once successfully executed.

❖ Deleting Shadow Files

Volume Snapshot Service, Volume Shadow Copy Service or VSS is a technology offered by windows which is responsible for taking backup of the files or volume. This backup is called as Shadow. Like other ransomwares, Cerber will bypass UAC Checks, delete shadow files, and disable safe booting option as well. Cerber achieves it using following processes

- *Vssadmin.exe "delete shadows /all /quiet"*
- *WMIC.exe "shadowcopy delete"*
- *Bcdedit.exe "/set {default} recoveryenabled no"*
- *Bcdedit.exe "/set {default} bootstatuspolicy ignoreallfailures*

❖ Anti VM Checks

The malware looks for known sandbox filenames, extensions and modules. Which mainly includes sbiedll.dll, dir_watch.dll, api_log.dll, dbghelp.dll, Frz_State, C:\popupkiller.exe, C:\stimulator.exe, C:\TOOLS\execute.exe, \sand-box\, \cwsandbox\, \sandbox\, 0CD1A40, 6CBBC508, 774E1682, 837F873E, 8B6F64BC.

There is also a delay option embedded in a payload which waits before it starts encryption. It helps to identify whether the system is running on sandbox or not. This option is used if none of the mentioned directory is promising.

❖ Persistence

※ Registry is added to avoid shifting of a system on screen saver if it is idle.
※ The ‘CommandProcessor’ autorun key value is replaced with Cerber Payload so that every time cmd.exe is run, payload will be triggered.
※ .lnk file is added in the start-up folder which causes every time the infected user log in, the payload will run
※ Other common persistence methods like run or runonce key are also used
※ Cerber targets 294 file extension

Impact on the system

Once the Cerber ransomware gets fully executed as explained above, it encrypts the data and prevents it from getting accessed by the user. Sometimes, the files get transferred on the machine of an attacker and then the attacker misuses the data leaking and selling it on the deep web market. The victim is forced to pay to get the data back by an attacker which usually do not happen.

The stolen data is also used to create fake profiles and scam people. If a user does not have backup and do not pay the price asked by an attacker, there are chances that the user may lose his data forever.

If the infected user is a well-known company or any organisation, Cerber ransomware may cause entire network collapse. It will hold the ongoing tasks in the network and has the possibility to lose a big amount of money.

Some physical observations of the impact are as follow

1. Cerber changes the operating system wallpaper
2. New files are created on the desktop and only these files are accessible to the user.
3. These files contain the instruction of payment to be made by the victim to get the data back.
4. It gives a countdown timer on the desktop of 7 days. The countdown is for the payment to be made.

Detection and Mitigation methods

❖ Detection Methods

There are three main methodologies to detect the Cerber Ransomware

1. Signature Based Method
2. Behaviour-Based Method
3. Deception

1. Signature-Based Method

In Signature-Based Method, the signature of a malicious file is compared with the signatures captured on the open platforms like VirusTotal. The security applications tries to catch the data from the inside of malicious file without actually running it. Every malicious file has a same backbone with is the real algorithm of a file which makes it run in a certain way. This caught algorithm is captured and checked on open source platform to get the basic idea of Signature-Based Method.

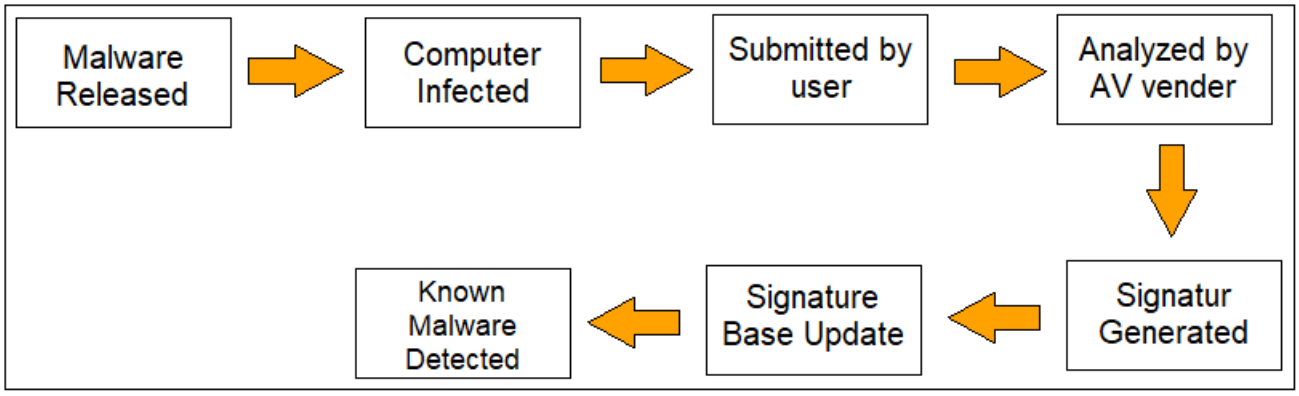

Figure 3

2. Behaviour-Based Method

In Behaviour-Based Method, the way file is acting on the system is observed by the trained modules of security applications.

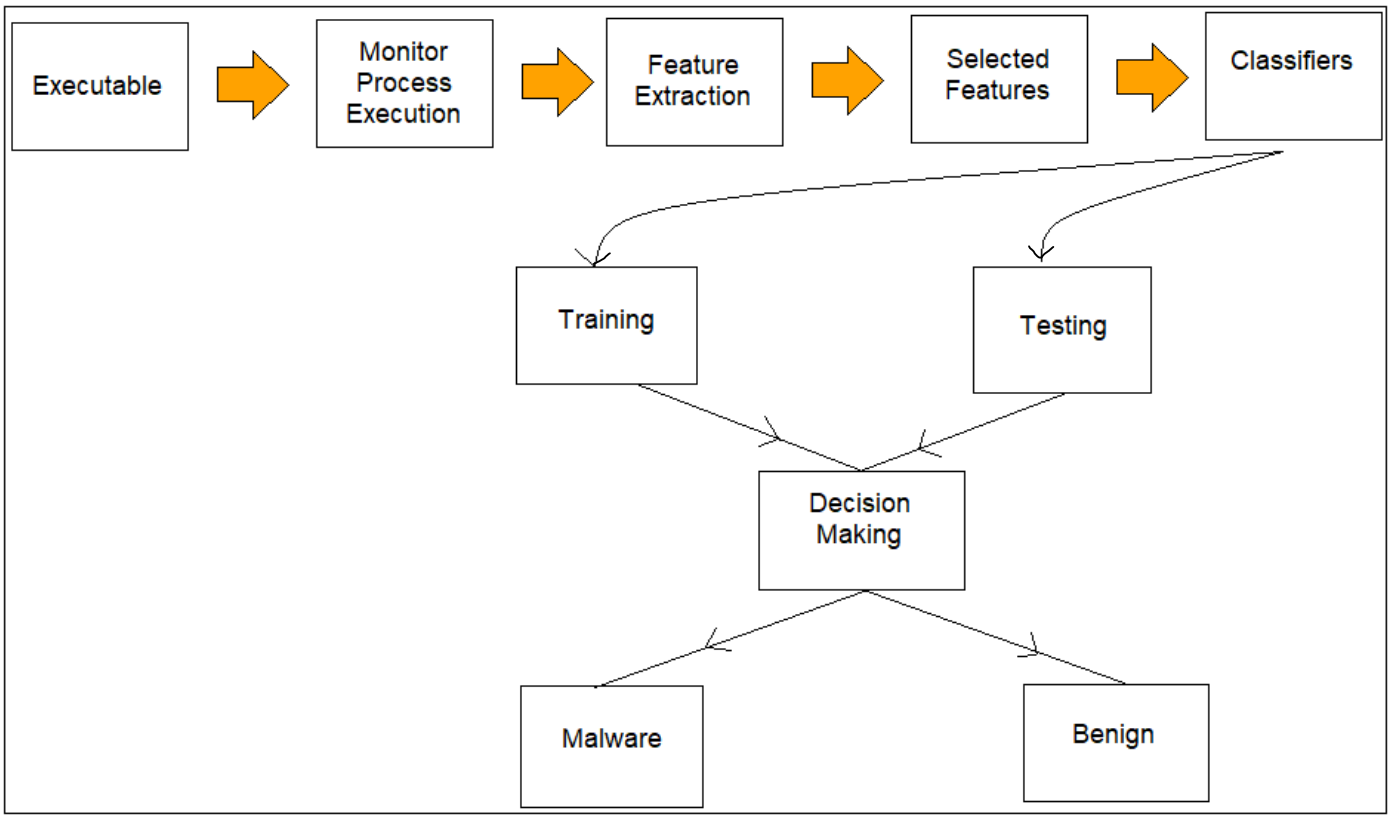

Figure 4

There are three methods in the above methodology

2.1. File System Change

- The way File System is changing in the system.

2.2. Traffic Analysis Change

- The way Traffic is being happening after installing specific file.

2.3. API Calls

- Checks what commands file is executing and triggers if found anything suspicious

3. Deception

In Deception methodology, the attacker is tricked to fall in the pit hole called as HonePot. Here, attacker falls in the system which has nothing to damage, and entire attack fails.

❖ Mitigation Methods

1. Operating system must be actively patched
2. All the application running on Operating System must be up to date.
3. There should be anti-virus and anti-malware programs installed on the system
4. There should be regular backup check on the system
5. HTTP websites shall never be visited unless and until the user does not trust on the website source.
6. Macro running must be disabled in the file system to avoid any code running in the background.
7. Automatic background option must be disabled in the browser.
8. Javascript must be disabled in browsers.
9. If infection happens and the system is in the big network, user must isolate the system as soon as possible and boot it in the safe mode to download the ani-malware programs and try to make system clear.
10. Encrypted files on the system shall never be deleted as there will be a decryption tool available once the malware analysis scientists crack the code.
11. Users should use Linux operating systems over Windows.

FINDINGS FROM DELIVERABLE 1

Description of Methodology Used while Investigating the Threat

Methodology used to investigate the threat is called as STRIDE. STRIDE stands for

- **Spoofing** – hiding self-identity under one's identity
- **Tampering** – the code will be modified by an attacker
- **Repudiation** – All the malicious actions will be hidden
- **Information Disclosure** – data leak
- **Denial of Service** – entire or almost system freezes
- **privilege Escalation** – gets higher level privilege access that is admin.

While investigating the threat, STRIDE methodology was used is because, the attack satisfies every mentioned attribute in the STRIDE. From figure 1 and 2, it can be seen that

- **Spoofing** – because at the very beginning user was redirected to a malicious from a malicious iFrame[1].
- **Tampering** – The file was downloaded in a system called RIG-EK[2] (Exploit kit) which understood the system well.
- **Repudiation** – All the understanding of the system performed by RIG-EK was hidden and not open to see by the user.
- **Information Disclosure** – Loopholes of the system was leaked by RIG-EK to the attacker which led it to download and execute Cerber Ransomware.
- **Denial of Service** – User PC was freeze and was only able to open few files which were having information about the payment to the user.
- **Privilege Escalation** – Cerber Ransomware holds the capacity to execute all the tasks which can only be done by admin user without landing in the Administrator user account

Considering above points, STRIDE is the best suitable methodology to investigate.

Analysis and Discussion of Findings

❖ `Findings using SGUIL and Wireshark

The attack took place between 22:54:42 – 22:55:28.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	21	seconion-...	5.2	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193	49195	6	ET CURRENT_EVENTS Evil...
RT	21	seconion-...	5.13	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193	49195	6	ET CURRENT_EVENTS Evil...
RT	1	seconion-...	5.24	2017-01-27 22:54:42	139.59.160.143	80	172.16.4.193	49200	6	ET CURRENT_EVENTS Evil...
RT	15	seconion-...	5.25	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG...
RT	15	seconion-...	5.26	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG...
RT	15	seconion-...	5.27	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG...
RT	52	seconion-...	5.37	2017-01-27 22:54:44	194.87.234.129	80	172.16.4.193	49203	6	ET CURRENT_EVENTS RIG...
RT	1	seconion-...	5.75	2017-01-27 22:55:17	172.16.4.193	58978	90.2.1.0	6892	17	ET TROJAN Ransomware/C...
RT	1	seconion-...	5.76	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET TROJAN Ransomware/C...
RT	1	seconion-...	5.77	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET DNS Query to a *.top do...
RT	4	seconion-...	5.78	2017-01-27 22:55:28	172.16.4.193	49212	198.105.121.50	80	6	ET INFO HTTP Request to a...

Figure 5

From figure 6, The user triggered 'bing' search saying 'home improvement remodelling your kitchen' from the source www.homeimprovement.com

```
Sensor Name: seconion-import-1
Timestamp: 2017-01-27 22:54:42
Connection ID: .seconion-import-1_2
Src IP:                 172.16.4.193
Dst IP:                 104.28.18.74
Src Port:               49195
Dst Port:               80
OS Fingerprint: 172.16.4.193:49195 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint:   -> 104.28.18.74:80 (distance 0, link: ethernet/modem)

SRC: GET /remodeling-your-kitchen-cabinets.html HTTP/1.1
SRC: Accept: text/html, application/xhtml+xml, */*
SRC: Referer:
http://www.bing.com/search?q=home+improvement+remodeling+your+kitchen&qs=n&sp=-1&pq=home
+improvement+remodeling+your+kitchen&sc=0-40&sk=&cvid=194EC908DA65455B9E9A98285A3313
2B&first=7&FORM=PERE
SRC: Accept-Language: en-US
SRC: User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
SRC: Accept-Encoding: gzip, deflate
SRC: Host: www.homeimprovement.com
SRC: Connection: Keep-Alive
SRC:
SRC:
```

Figure 6

The figure 7 tell the message of IDS as ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2016

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS
Evil Redirector Leading to EK Jul 12 2016"; flow:established,from_server; file_data; content:"|3c 73
70 61 6e 20 73 74 79 6c 65 3d 22 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70
```

Figure 7

Figure 8 tells the malware family which is PsuedoDarkLeech created on 2016/07/12

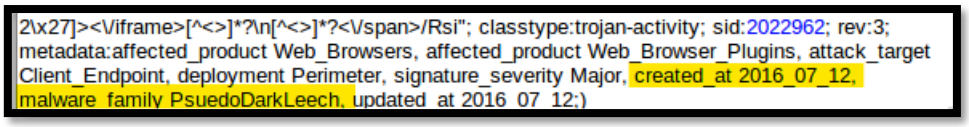

Figure 8

Figure 9 gives us information saying it is RIG_EK kit has been used giving the message highlighted.

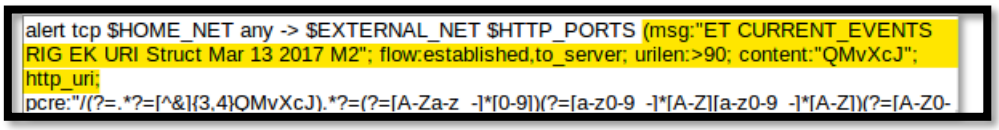

Figure 9

Figure 10 shows that the injection type is Trojan, and it is Ransomware, Cerber

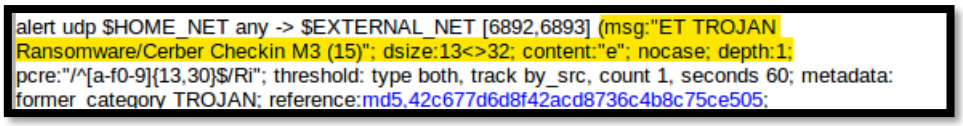

Figure 10

Figure 11 tells some HTTP request has been triggered after infection

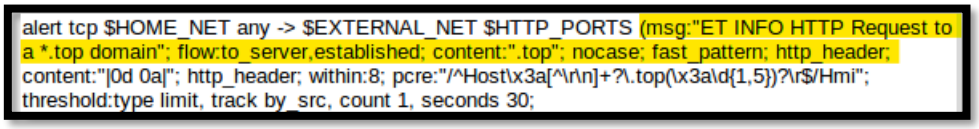

Figure 11

From figure 12, Incident 5.24 from Sguil, the file dle_js.js has been requested. Here the reference website and the Host websites are completely different. The reference website is www.homeimprovement.com and the Host website is retrotip.visionurbana.com.ve. This shows that the file getting displayed on www.homeimprovement.com are getting delivered from retrotip.visionurbana.com.ve which makes things suspicious. That means the file dle_js.js is getting delivered by the host website.

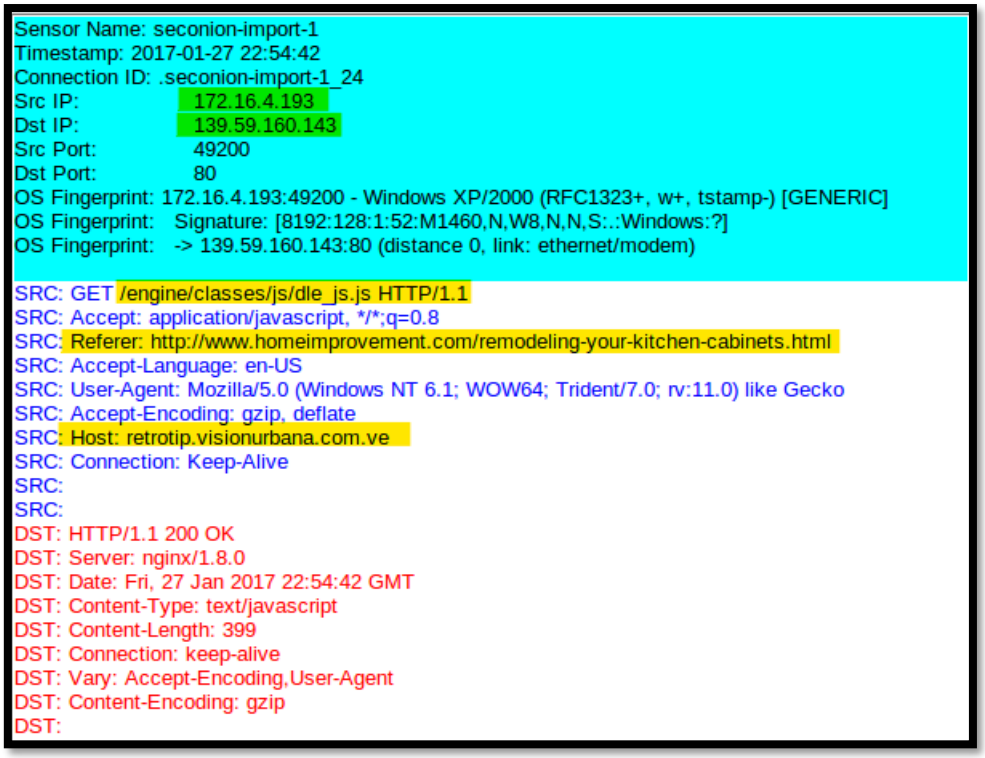

Figure 12

From figure 13, sguil ID 5.25, this is the 1 out of 3 request. Here the referrer is www.homeimprovement.com and the host is someone else that the previous. It is tyu.benme.com.

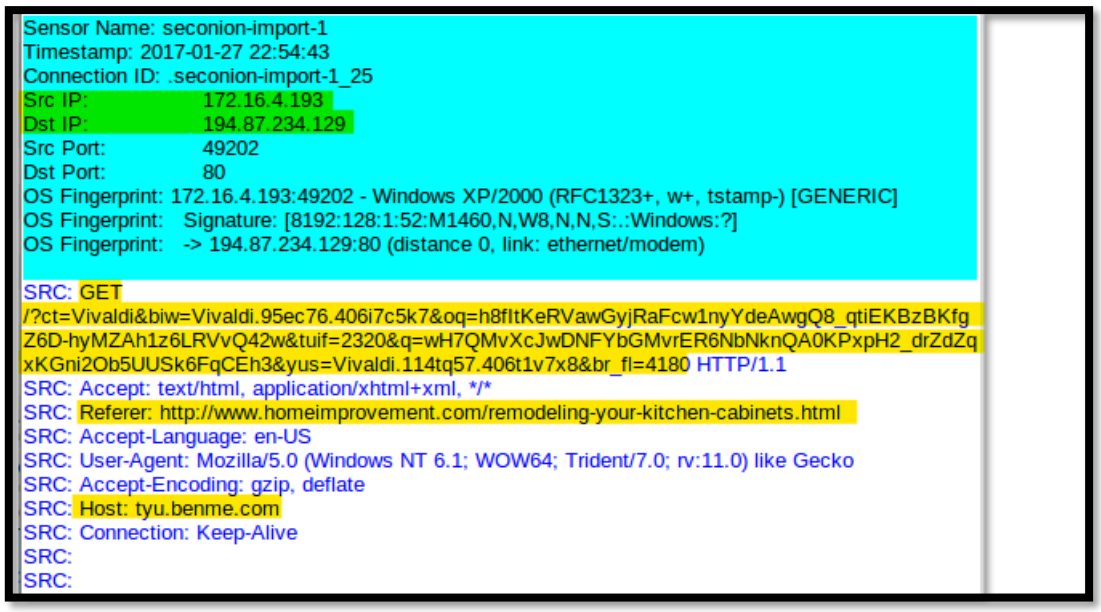

Figure 13

Figure 14 tells the second request caught. The HTTP Request caught here is POST and seems that something is getting upload. Here the Host is same as the first request. If look

closely, the Content type is application/x-www-form-urlencoded. It shows that some data has been sent in a single block to the attacker.

Figure 14

Figure 15 gives the third request of the same IDS, packer. Here the HTTP request is GET again. The referrer URL is different, but the Host is same. This request is very interesting. Here the content type is application/x-shockwave-flash and the file type last sent is CWS.

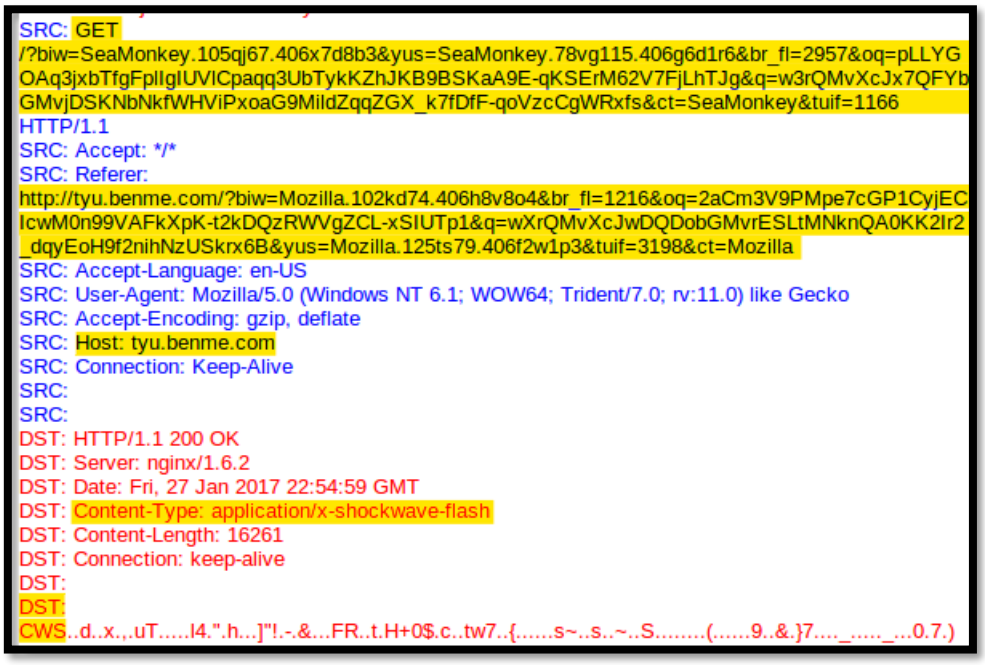

Figure 15

Here the shockwave-flash shows that the file is .swf. The .swf file can run macro within it. This file belongs to the adobe flash.

Here network miner showed that three files has been downloaded on the system. .swf is one of them. (figure 16)

Frame nr.	Filename	Extension	Size	Source host	S. port
4	index.html.1319B475[1].html	html	5 212 B	194.87.234.129 [tyu.benme.com]	TCP 80
10	index.html.4B461872[1].html	html	90 745 B	194.87.234.129 [tyu.benme.com]	TCP 80
95	index.html.67899BE6.[1].swf	swf	16 261 B	194.87.234.129 [tyu.benme.com]	TCP 80

Figure 16

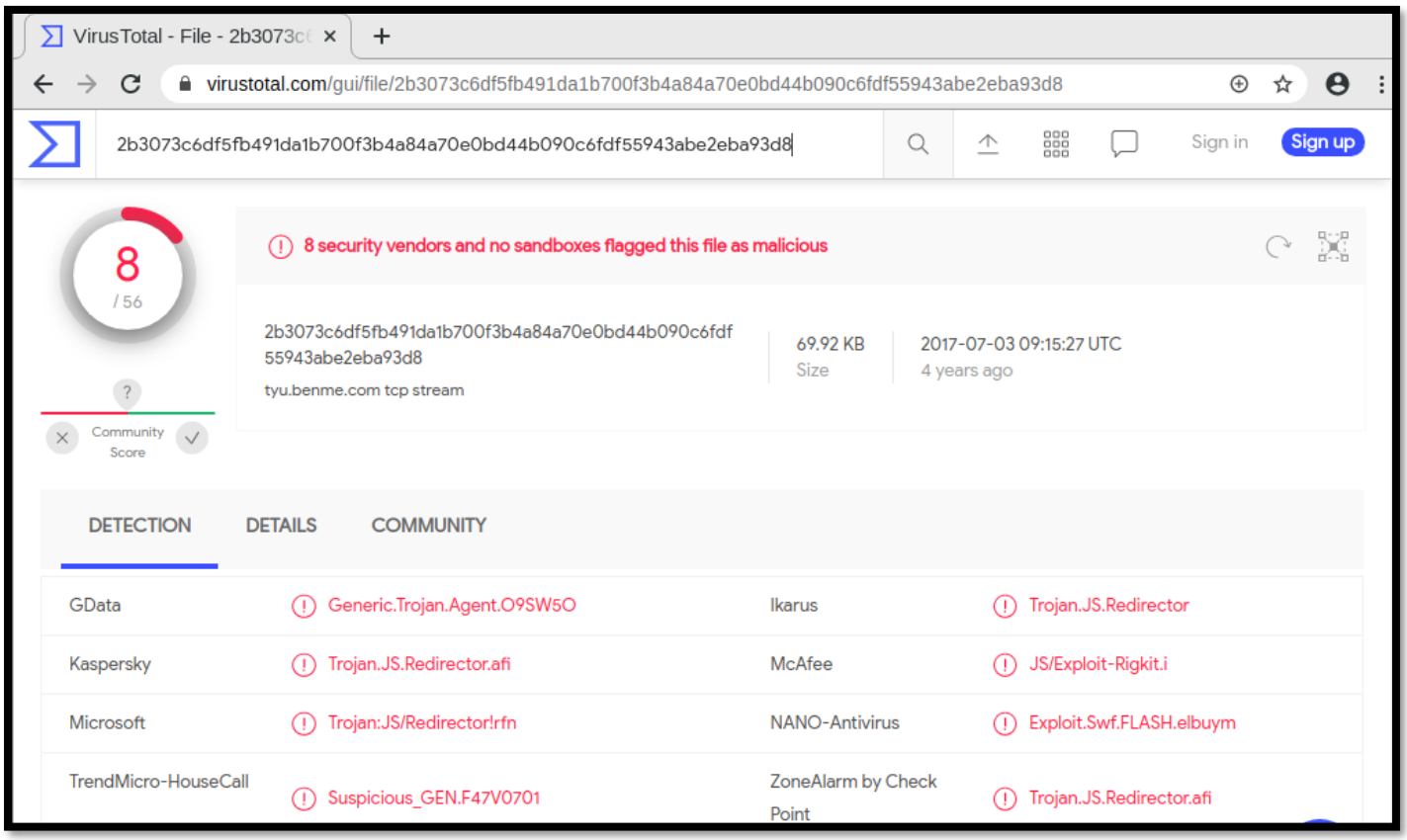

Figure 17

VirusTotal flagged file malicious as well. (Figure 17)

Finding the IDS of figure 10 and considering figure 5, following figure (figure 18) shows that the destination IP address is 90.2.1.0.

RT	1	seconion-...	5.75	2017-01-27 22:55:17	172.16.4.193	58978	90.2.1.0	6892	17	ET TROJAN Ransomware/C...

Figure 18

The Packet Stream for this is not TCP but the UDP as per the Wireshark (figure 19). And this is where the ransomware attack has been triggered.

No.	Time	Source	Destination	Protocol	Length	Info
1	2017-01-27 22:55:17.562378	172.16.4.193	90.2.1.0	UDP	67	58978 → 6892 Len=25

Figure 19

RT	.	seco...	5.410	2017-06-27 13:38:34	119.28.70.207	80	192...	49184	.	ET CURRENT_EVENTS WinHttpRequest Downloading EXE
RT	.	seco...	5.415	2017-06-27 13:38:34	119.28.70.207	80	192...	49184	.	ET POLICY PE EXE or DLL Windows file download HTTP

Figure 20

ST	.	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Event Message
RT	.	seco...	5.27	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	ET CURRENT_EVENTS RIG EK URI struct Oct...
RT	.	seco...	5.37	2017-01-27 22:54:44	194.87.234.129	80	172.16.4.193	49203	ET CURRENT_EVENTS RIG EK Landing Sep 1...
RT	.	seco...	5.75	2017-01-27 22:55:17	172.16.4.193	58978	90.2.1.0	6892	ET TROJAN Ransomware/Cerber Checkin M3 (15)
RT	.	seco...	5.76	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	ET TROJAN Ransomware/Cerber Onion Domain...
RT	.	seco...	5.77	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	ET DNS Query to a *.top domain - Likely Hostile
RT	.	seco...	5.78	2017-01-27 22:55:28	172.16.4.193	49212	198.105.121.50	80	ET INFO HTTP Request to a *.top domain
RT	.	seco...	5.410	2017-06-27 13:38:34	119.28.70.207	80	192.168.1.96	49184	ET CURRENT_EVENTS WinHttpRequest Downl...
RT	.	seco...	5.415	2017-06-27 13:38:34	119.28.70.207	80	192.168.1.96	49184	ET POLICY PE EXE or DLL Windows file downl...
RT	.	seco...	5.420	2017-06-27 13:43:52	145.131.10.21	80	192.168.1.96	49190	ET POLICY PE EXE or DLL Windows file downl...
RT	.	seco...	5.421	2017-06-27 13:43:54	192.168.1.96	49191	143.95.151.192	80	ET CURRENT_EVENTS Terse alphanumeric ex...
RT	.	seco...	5.422	2017-06-27 13:43:54	143.95.151.192	80	192.168.1.96	49191	ET POLICY PE EXE or DLL Windows file downl...
RT	.	seco...	5.428	2017-06-27 13:44:01	192.168.1.96	59029	208.67.222.222	53	ET POLICY External IP Lookup Domain (myip.o...
RT	.	seco...	5.429	2017-06-27 13:44:01	192.168.1.96	49193	198.1.85.250	80	ET TROJAN Backdoor.Win32.Pushdo.s Checkin

IP Resolution | Agent Status | Snort Statistics | System Msg

Reverse DNS Enable External DNS

Src IP:

Show Packet Data Show Rule

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS
WinHttpRequest Downloading EXE"; flow:established,from_server;
flowbits:isset,et.WinHttpRequest; file_data; content:"MZ"; within:2; byte_jump:4,58,relative,little;
content:"PE|00 00|"; distance:-64; within:4; classtype:trojan-activity; sid:2019822; rev:6;
```

Figure 21

From figure 20 and 21, it seems that a .exe file is getting downloaded on the system which is not the which has been infected prior. (Prior IP showed in Pink Highlight)

RT	.	seco...	5.428	2017-06-27 13:44:01	192.168.1.96	59029	208.67.222.222	53	ET POLICY External IP Lookup Domain (myip.o...
RT	.	seco...	5.429	2017-06-27 13:44:01	192.168.1.96	49193	198.1.85.250	80	ET TROJAN Backdoor.Win32.Pushdo.s Checkin
RT	.	seco...	5.431	2017-06-27 13:44:04	62.210.140.158	80	192.168.1.96	49250	ET TROJAN Pushdo.S CnC response
RT	.	seco...	5.438	2017-06-27 13:44:32	208.83.223.34	80	192.168.1.96	49932	ET POLICY TLS possible TOR SSL traffic

Figure 22

From figure 22, attacker has done DNS Zone Transfer and a reverse shell has been installed on 192.168.1.96. and the traffic is being directed through TOR.

Considering figure 21, 21 and 22 it has been concluded that, the cerber attack has no relation with this reverse shell deployed on 192.168.1.96

Legal and Ethical Issues

Understanding whether the intrusion incident is relevant or irrelevant is very difficult. Because both the possibilities contain heavy chances of false positive and false negative. Every scenario of intrusion incident has equal possibility of being true and false. The fine line between the decisions can be drawn understanding the end point of the incident.

In between the legal and ethical issues, there is another issue which is the limitation of technology. To make things work legally, there should be immunity to the people working genuinely in the field of cyber security. A genuine cyber security person can face the trouble whereas the culprit may have the possibility to be fine. Legally, the person creating genuine intrusion incident must be immune. A proper procedure should be followed to grant the immunity in this case. The clarification can be made using technology.

Ethically, things should manage with the help of the available power of machines and knowledge. And beyond this, every person should be morally responsible while managing the incident reports. Misusing the leaked information irrespective of the owner of the machine must be kept in control and hidden from being misused. This should be the moral responsibility of the person who has found the information.

RECOMMENDATIONS

Reflect on work in 1.1 and 1.2

From 1 and 2, the attack followed in the following way

1. The victim visited a website called www.homeimprovement.com. (104.28.18.74)
2. If observed neatly, the website www.homeimprovement.com is not using HTTPS protocol but the HTTP. Which makes it suspicious.
3. This website holds a malicious iframe which redirected the user to the malicious website.
4. The new malicious website is retrotrip.visionurbana.com (139.59.160.143). This file downloaded the javascript file in the system of user. This is the RIG_EK kit.
5. After the output of javascript file received by an attacker, new file was installed which was an adobe file having .aws extension by tyu.benme.com (194.87.234.129)
6. The user got infected by ransomware Cerber.
7. The Cerber was in activity from the attacker having IP address 90.2.10.0
8. Finally, there is a link p27dokhpz2n7nvgr.1jjw2lx.top (198.105.151.50).
9. This link is displaying the webpage on the user's Desktop which gives instruction to the user about the payment.
10. The above point has been stated by studying the .top extension. .top extension is used when the domain is deployed in the root directory of the machine.

Recommendations to improve detection

1. User must use Anti-malware and Anti-virus programs
2. Firewall on the system must be ON
3. There should be applications on the system which will prompt if backdoor activity is going on.
4. Connections going on untrusted websites / IP address must be prompted.

REFERENCES

- MASS.GOV. (2017). Know the types of cyber threats. [online] Available at: https://www.mass.gov/service-details/know-the-types-of-cyber-threats.
- FICHTNER, E. (2022). Top 10 Common Types of Cybersecurity Attacks. [online] www.datto.com. Available at: https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks.
- MALWAREBYTES LABS. (n.d.). Ransom.Cerber. [online] Available at: https://blog.malwarebytes.com/detections/ransom-cerber/ [Accessed 30 Mar. 2022].
- CERBER RANSOMWARE: Everything You Need to Know. (n.d.). Cerber Ransomware: Everything You Need to Know. [online] Available at: https://www.avast.com/c-cerber [Accessed 30 Mar. 2022].
- FireEye. (n.d.). Cerber: Analyzing a Ransomware Attack Methodology To Enable Protection. [online] Available at: https://www.fireeye.com/blog/threat-research/2016/07/cerber-ransomware-attack.html [Accessed 30 Mar. 2022].
- Limited, S. (n.d.). What Is Cerber Ransomware? [online] SiteLock. Available at: https://www.sitelock.com/blog/what-is-cerber-ransomware/ [Accessed 30 Mar. 2022].
- www.pcrisk.com. (n.d.). How to remove Cerber Ransomware [Updated] - virus removal steps (updated). [online] Available at: https://www.pcrisk.com/removal-guides/9842-cerber-ransomware.
- SearchSecurity. (n.d.). 3 Ransomware Detection Techniques To Catch An Attack. [online] Available at: https://www.techtarget.com/searchsecurity/feature/3-ransomware-detection-techniques-to-catch-an-attack.
- BURGESS J, CARLIN D, O'KANE P AND SEZER S. Redirekt: Extracting malicious redirections from exploit kit traffic. Redirekt: Extracting malicious redirections from exploit kit traffic. *2020 IEEE Conference on Communications and Network Security (CNS)*: IEEE; 2020. p. 1-9.
- HOPKINS M AND DEHGHANTANHA A. Exploit Kits: The production line of the Cybercrime economy? Exploit Kits: The production line of the Cybercrime economy? *2015 second international conference on Information Security and Cyber Forensics (InfoSec)*: IEEE; 2015. p. 23-27.

- KURNIAWAN A, RIADI I. Detection and analysis cerber ransomware based on network forensics behavior. *International Journal of Network Security.* 2018; 20(5):836-843.
- MA Z. *The decline of exploit kits as an exploitation strategy.* 2018