Journal of Applied Technology and Innovation
Vol. **09,** Issue **2**, 2025**,** pp. **23-32**
e-ISSN:2600-7304-ISSN
DOI: https://doi.org/10.65136/jati.v9i2.28

Detection and Mitigation Techniques for Fileless Attacks Using LOLBins in Modern Windows Environments.

Nor Azlina Abd Rahman [1]*, Jalil Md Desa [1]

[1] School of Computing, Asia Pacific University of Technology & Innovation, Kuala Lumpur, Malaysia
*Corresponding Author: nor_azlina@apu.edu.my

Abstract

Fileless malware is becoming popular with cyber attackers innovating on how to attack the target victim by avoiding antivirus and EDR mechanisms. The Living of the Land Binaries (LOLBins) are become the target for exploitation by the attacker and particularly dangerous as the programs are legitimate utility files and are present by default in the operating system. Since LOLBins are legitimate operating system files and any exploitation to LOLBins files are hard to detect. Lolbins exploitation is the focus of this research paper, which is accompanied by several examples of LOLBins exploitation such as Emotet and Chaes that use these strategies. It also discusses how attackers interact with LOLBins, some of which are using PowerShell, Mimikatz and Windows Management Instrumentation (WMI). Some of the LOLBins exploitation detection techniques investigated are behavior and log analysis, file integrity check, network traffic, and UEBA. The different difficulties involved in identifying the use of LOLBins in attacking the system have been discussed, and they include: The circumvention of security tools; Achieving privilege elevation; Movement from one component of the system to another; Other forms of concealment. This research serves to investigate the behavior of LOLBins in attacks and their detection focusing on current and future developments in monitoring and threat hunting to counter the threats posed by fileless malware.

Keywords: *LOLBins, fileless, Autoruns, WMI, Mimikatz.*

1. Introduction

As a result of advancement in security systems, the attackers are now devising new ways that will enable them to evade the antivirus or end detection response system (EDR). Indeed, one of the ways that attackers employ in their aggression is fileless malware. This method has been used since early 2000. It can be used to run code a user is unaware of, or which has not installed any malware on the victim's system or prompted users. The process of such an attack involves the use of the programs that are initially contained in the system for instance PowerShell, or the weaknesses of the applications in the machine [1]. Specifically, LOLBins (Living off the Land Binaries) is a kind of fileless attack.

In a LOLBins attack, the use of binaries will perform unlawful action with legal commands on a system. Not only do they download malware and malicious code while going unnoticed, but they also continue to stay in the system unnoticed. An attacker may increase the likelihood they avoid detection if using LOLBins, however in leveraging standard cloud services (such as GitHub, AWS S3 bucket, Dropbox, Google Drive and so on). LOLBins are obscure to be detected because they are genuine and are pre-installed tools [2, 3].

2. Malwares That Exploited LOLBins

2.1 Emotet

Emotet original job was a banking trojan whose purpose is to enjoy bank account details and banking cards numbers from a user's computer. This malware makes extensive use of PowerShell This is because Emotet employs a form of worm type functionality in order to spread to the other connected devices within the compromised computer [4].

2.2 Chaes Malware

This malware attacked the customers' credential data of the largest e-commerce website in Latin America; consists of username and password, bank record, debit or credit card numbers, and other financial details. The Chaes attack chain, in fact, consists of several stages at which the use of LoLbins and other legitimate applications is regarded as a means to avoid the identification by antivirus (AV) systems.

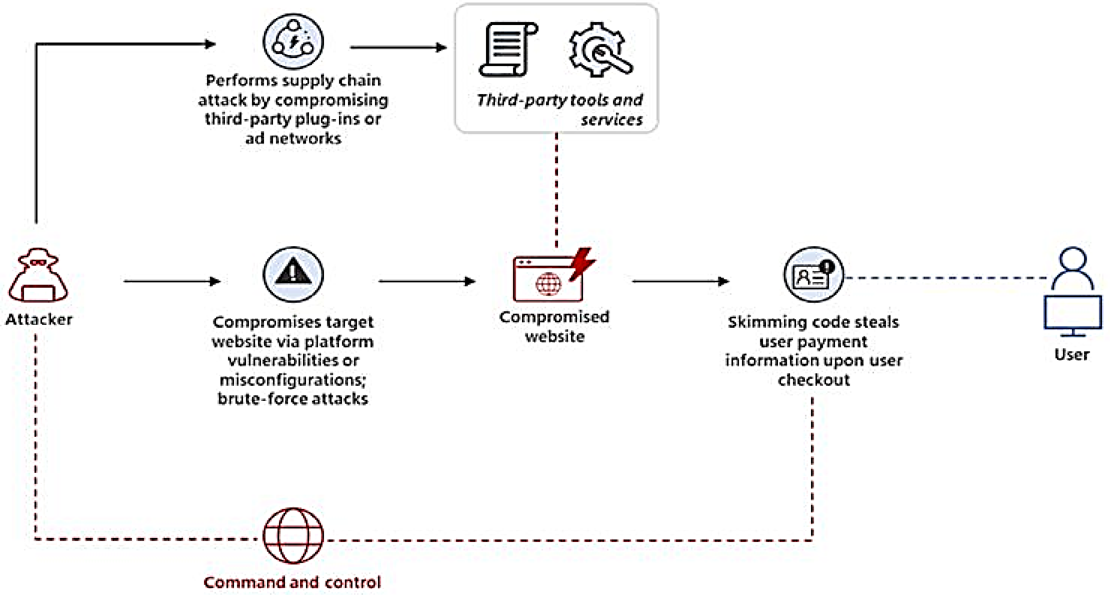

Performs supply chain attack by compromising third-party plug-ins or ad networks
Third-party tools and services
Attacker
Compromises target website via platform vulnerabilities or misconfigurations; brute-force attacks
Compromised website
Skimming code steals user payment information upon user checkout
User
Command and control

Figure 1. Chaes attack chain

Attackers take advantage of such holes in order to install skimming scripts or as a result of web application supply chain attacks involving identification of flaws in third-party components or compromised advertising platforms. As it has been pointed by the source offered by Microsoft, a major challenge arises from the client-server networking.

3. How Lolbins Are Exploited

3.1 Exploiting Legal System Tools

As it was pointed out before, the tricks on which LOLBins attacks rely on most do not arouse suspicion as they are legitimate tools of the system. As stated before the commands used in these system build-ins will not trigger the security system and team because they are recognized by it. PowerShell, WMI; Windows Management Instrumentation; and command line are probably the most significant.

3.2 Leveraging Preexisting Vulnerabilities

These also incorporate the present flaws in the target system. Potentially damaging elements can manipulate the system, gain access to data they are not supposed to access and perform operations that the system is supposed to implement. Exploiting these vulnerabilities also makes the hacking process less Fun, since the attackers don't need to create the hacking structures from ground.

3.3 Hiding Malicious Code in Normal Files

A common practice amongst attackers is to introduce malware code in standard formats like .pdf,. dox and .exe. Since this file is seemingly innocent, many users will download and run it, and at that point, the malware is installed into the victim's computer [5].

4. Lolbins Manipulation

Attackers utilize the system's legal applications for LOLBins attack to probe the network, run the compromised code from a distance, and brute force passwords in addition to making the most of the system's weaknesses. These tools are processed collectively not singularly to get into the system and ensure they retain their ingress on the violated network. Unfortunately, to be able to utilise these tools, an attacker is required to be of a better skill level. Some of the tools used for LOLBins attacks include:

4.1 PowerShell

PowerShell is the most used tool in this type of attack according to previous research conducted by various scholars. This scripting language allows the attacker to get the victim's systems to execute his or her commands. PowerShell can also download code and more importantly, execute code. PowerShell is trusted by the system hence when it is used, attackers can breach a system's security measures discreetly [5].

4.2 Mimikatz

Mimikatz is a strong hacking tool by utilizing which attacker can steal the passwords and other critical data of the OS. It also offers the attacker the permissions of other components in the network in regard to the affected system.

4.3 WMI (Windows Management Instrumentation)

WMI facility is very useful for the system administrators and these administrators can do different tasks at faster manner, but an attacker also can take the advantages of WMI as like as a legal admin can. An attacker can also query the metrics and then upload the malicious code, then all the computers that is conneted to the network will get infected. This tool also ensures the attacker permanent connectivity to the network [6] form different tasks at fast pace, but an attacker can exactly take the benefits of WMI that a legal admin can. An attacker can also query the metrics and then upload the malicious code, then all the computers that are connected to the network will get infected. This tool also guarantees persistent access of the attacker to the network [6].

4.4 Msiexec

Msiexec is a command prompt which is primarily used for formation and de-formation of software applications on the Windows operating system. These files contain installation information comprised of to be installed files, registration data and features and updates on the application. Since software generation companies give the installer their products too, so the installation process could get done more safely. Through the Msiexec file, the users can actually control several command-line prompts. Another reason forcing normal users denies the execute permission from accessing Msiexec is that it installs applications that can also be installed via Msiexec. Another important function of Msiexec is that it can contact remote servers; therefore, if a cyberattack closes to Msiexec, they can embed undesirable payloads or set up and configure tools as well as applications to the assaulted framework distantly. If wrongly set up, then, an attacker will be able to interact with this file. Thus, if an attacker obtains access to the Msiexec, attacker can take privileges and overcome normal measures taken to prevent attackers from gaining access. That which you have seen above are only functions of the MSI file's ability and are not limited only to these. DLL files can also be registered and unregistered by them. When a DLL file is registered, the name and location of the file are stored in the registry section of Windows, so this tool needs to be secured and the means of accessing it cannot be made generally available. It is recommended to block the executable of MSI files for all users to prevent the risk of attack through this [9]. Here are some of the commands which can be used by MSI:

- msiexec /quiet /i cmd.msi
- msiexec /q /i http://192.168.100.3/tmp/cmd.png
- msiexec /y "C:\folder\evil.dll"
- msiexec /z "C:\folder\evil.dll" [10].

4.5 Wscript

Wscript.exe is a real file in Windows e, and is understood by the common name, Windows Script. As it can be deduced by its name, this file introduces Windows to scripting functions. Thus, it is an effective scripting file that can be used in a way which will bring many advantages to attackers as soon as they gain access to it. The executable processes of this file are to be installed in System32 by default, system32 is a Windows folder that stores the files of windows operating system. But if the attacker has found this file, he wants to exploit it then they will either change the path of this file or the name of the file. As we know, if they decided to change the name the new name that they will be replacing it with will be very close in name. One way to know if a malicious activity is being performed is to look at the icon of the process in Windows Task Manager. When one comes across a process name with a system icon around it, there should be an alert for a cyber analyst.

Malicious use of wscript file is particularly applied if the attacker is in competition with the firm to fraud credit card numbers and other related financial data as is evident from the Chaes malware case study. Cyber criminals can use files which contain viruses and share them online or use the pretense of giving an update, sharing trojans and other types of viruses. In this particular case, the intruders first Fake Phishing E-mail having Microsoft.doxc file with a Macro feature of Microsoft Word was used [11].
Here are two commands which can be used by Wscript:

- wscript //e:vbscript c:\ads\file.txt:script.vbs
- echo GetObject("script:https://raw.githubusercontent.com/sailay1996/misc-bin/master/calc.js") > %temp%\test.txt:hi.js && wscript.exe %temp%\test.txt:hi.js [12].

4.6 InstallUtil

One way to approximate execution of codes by a Windows trusted file, InstallUtil.exe. This is a command-line-based file which can easily be used to install resources, especially those which have used .NET class binaries. Software that is applied in the computer can be installed and uninstalled by command prompt through InstallUtill.exe. It would be obvious for Microsoft to sign this .exe file as a legitimate and safe one to run those malicious .NET executables that slip past the AppLocker. Any graphic program can be executed without being noticed because AppLocker policies can originate from Windows Folder. Chaes malware has used InstallUtil file to download the malware content [13].

5. LOLBins exploitation detection

A large number of bad deeds and attacks are instantly described by traditional security measures and tools such as firewalls, EDRs, and antivirus. When choosing a SOC (Security Operation Center) system and tools with high functionality, it is possible to detect LOLBins attacks, which are quite difficult. A threat intelligence team who can work proactively to discover more bad patterns and actions is required. Here are some ways for detecting LOLBins attacks [7]:

5.1 *Behavioral Analysis*

The analysis of the behavioral patterns done in the system requires the application of sophisticated security applications; the most important aspect that should get much attention is the unusual command-line because most of the activities are accomplished in PowerShell. New connections should also be observed as these attacks are carried out from remote locations in their very nature. The other feature which should be looked for is unusual process behavior [2, 7].

5.2 *Log Analysis*

Although this type of attack does not produce a large number of logs, or nearly any at all, system logs should not be overlooked. Specific considerations are Abnormal Command-Line Arguments, Extra Access to Network or Files or the Processes, which is started by LOLBins utilities and must be observed by security staff. Misuse of the system is identified by the parent-child relationship of the running processes and streams as well as network abnormal of the processes. Thus, more data write to the system, organizations should set it up for centralized logging and after that, the threat-hunting teams can perform additional analysis [2,7].

5.3 *File Integrity Monitoring*

The file integrity monitoring tools enable an organization to address the second threat since the modification of the root files by invaders is recognizable. Second, entries of new files associated with LolBins should also be examined. All the changes that are known to affect binaries, scripts and system configuration files for being clued to detect malicious activities should be investigated [2].

5.4 *Network Traffic Monitoring*

Network anomalies or parts of the network traffic that appear to be an indication of security abuse should be discovered through the use of behavior-based network traffic analysis systems. To assess the validity of the data, an investigation to connect to known malicious IP addresses or domains and other unusual traffic should be performed, since it might mean data exfiltration [2].

5.5 *User and Entity Behavior Analytics (UEBA)*

Any UEBA solutions which are augmented with machine learning algorithms to develop normal behavior baseline for users and systems should be used. This is useful in tracking unprecedented activities such as odd and repetitive command sequences and frequent visits to system sensitive components. Efforts to prioritize escalations by users and their activities should also be observed [2].

6. Issues in LOLBins exploitation detection

Lolbins exploitations are hard to detect by antivirus or End Point Detection and Response (EDR) System. This is due to:

6.1 Bypassing Security Measures

They are regarded as legal scripts in the system and as a result, attackers are able to engage in all sorts of negative activities, yet the security system remains oblivious and does not sound alarming. It gives them the opportunity to ignore application controls, for example, WDAC (Windows Defender Application Control).

6.2 Execution with Legitimate Processes

Attackers synchronize malicious activities with legal procedures; this makes it hard to distinguish between the wicked deed the system is performing and an allowed one.

6.3 Increment of Privileges

Basically, by using LOLBins the attackers gain higher privileges on weak systems or, in the case of system vulnerabilities. Targeting exposure like un-patched or misconfigured script in those situations gives the attacker better control of victim's systems from the vertical point of view. The most ordinary method of the privileges' escalation is the UAC (User Account Control) bypass.

6.4 Lateral Movement

As has been observed, with different LOLBins, attackers can move from one different system in a network or different device in possession of the network to another. Once the attackers identify some means of exploiting the mentioned system weaknesses and navigating through the system, they are able to identify potential profitable assets [2].

6.5 Remote Access and Command Execution

Threat actors execute commands on focus points from a distance. It can then use built-in programs on Windows such as PowerShell and WMIC (Windows Management Instrumentation Command-line) and control them to run payloads on the systems.

6.6 Supporting Obfuscation

By operating within the parameters of a system's properly coded on/off switches and pull-through features such as PowerShell, the attackers can trick the system in several ways. For example, one of the characteristics that PowerShell offers is encoding Base64. Base62 is used to convert binary string into printable human text string. As has been discussed, base64 enables attackers to transfer binary data in protocols that fail to support binary format but are intended to support text format. Base64 can both be encoded and decoded through the command line [2, 8].

7. Mitigation of LOLBins Attacks

Traditional control systems like firewalls and Antivirus cannot tackle a LOLBins attack and there is a need to find new ways. In order to defend against the LOLBins attack, the threat intelligence team that utilizes an active approach is ready to address the LOLBins attack. The management of this type of attack is simplified by the fact that; For this attack type, human intelligence will be more effective.

One of the most efficient methods in order to prevent the attack utilizing LOLBins it is necessary to monitor the users and the system. Arrangements, such as parent-child relationships between processes and unnormal network behaviours of the processes can be suspicious items. It is better to log the systems centrally to make security teams able to do advanced investigation [14].

Application whitelisting can be very powerful for the illicit utilization of LOLBins. In turn, the role of these applications is to restrict possible actions with LOLBins. Whereas the type of limitation can be a bit of a problem in this case, its extent can be quite tricky.

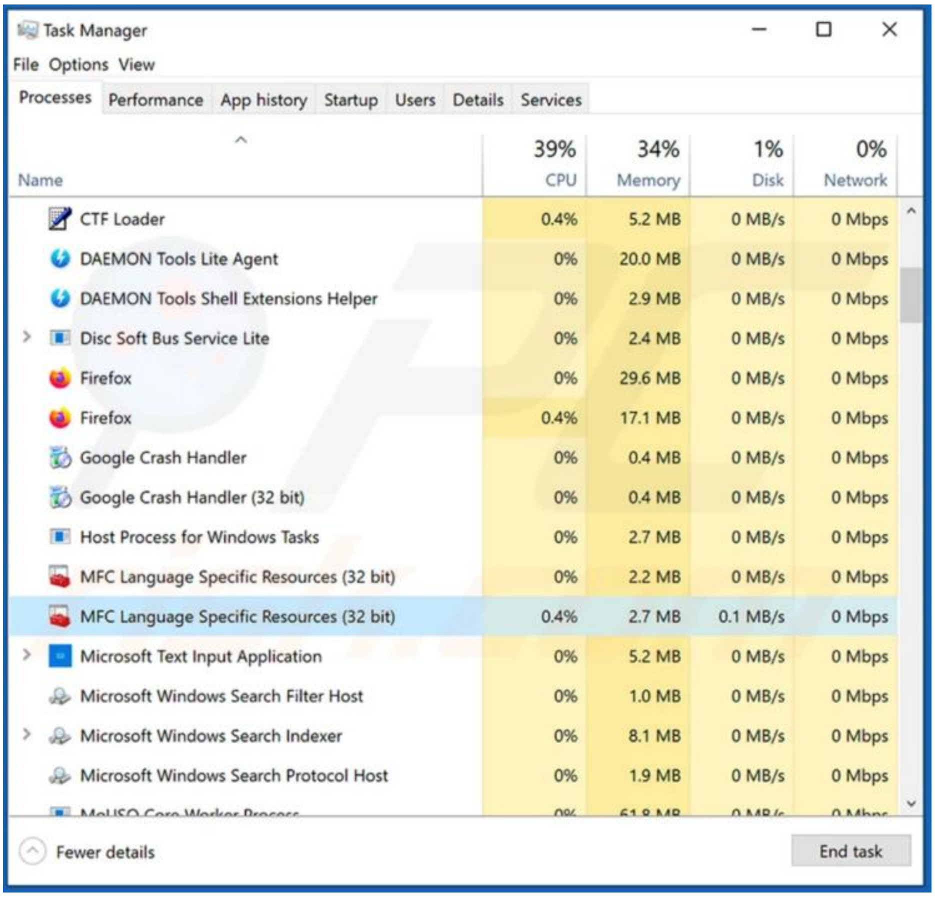
Current security policies are also mandatory in this area. In this way, the security of the organization would be more stable as compared to the centralized security. These policies should review web sites and e-mail for example. NGIPS – next generation intrusion prevention systems and a powerful EDR solution can add more layers of protection as well [2]. It is important to educate people, they should not open such e-mails, they should particularly not download attachment from such e-mail.

Additionally, software and tools should be downloaded only from official or valis sources only. Equally, programs should be updated with the products of legitimate developers. Powerful anti-spyware should also be installed too. These programs, therefore, should be updated, and should be in regular usage [15].

Removal of Chaes Malware

The malware removal can be a complex task. This section will be discussing on the malware removal steps that focusing on Chaes malware that exploiting LOLBins [15]:

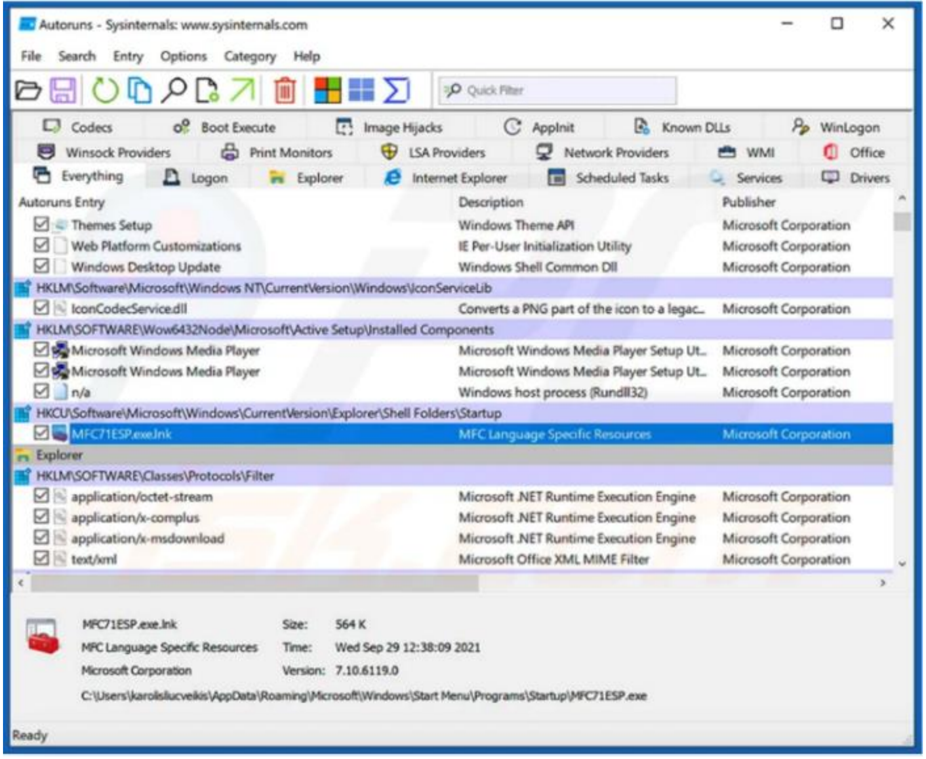
- Firstly, is to identify the name of the malware. Figure 2 shows an example of a suspicious process that is listed in task manager.



Name	39% CPU	34% Memory	1% Disk	0% Network
CTF Loader	0.4%	5.2 MB	0 MB/s	0 Mbps
DAEMON Tools Lite Agent	0%	20.0 MB	0 MB/s	0 Mbps
DAEMON Tools Shell Extensions Helper	0%	2.9 MB	0 MB/s	0 Mbps
Disc Soft Bus Service Lite	0%	2.4 MB	0 MB/s	0 Mbps
Firefox	0%	29.6 MB	0 MB/s	0 Mbps
Firefox	0.4%	17.1 MB	0 MB/s	0 Mbps
Google Crash Handler	0%	0.4 MB	0 MB/s	0 Mbps
Google Crash Handler (32 bit)	0%	0.4 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks	0%	2.7 MB	0 MB/s	0 Mbps
MFC Language Specific Resources (32 bit)	0%	2.2 MB	0 MB/s	0 Mbps
MFC Language Specific Resources (32 bit)	0.4%	2.7 MB	0.1 MB/s	0 Mbps
Microsoft Text Input Application	0%	5.2 MB	0 MB/s	0 Mbps
Microsoft Windows Search Filter Host	0%	1.0 MB	0 MB/s	0 Mbps
Microsoft Windows Search Indexer	0%	8.1 MB	0 MB/s	0 Mbps
Microsoft Windows Search Protocol Host	0%	1.9 MB	0 MB/s	0 Mbps
MoUSO Core Worker Process	0%	61.8 MB	0 MB/s	0 Mbps

Figure 2. Suspicious Process in Task Manager

- Next step is to download a program called Autoruns. This application is used to view the auto-start application as shown in figure 3.



Autoruns Entry	Description	Publisher
☑ Themes Setup	Windows Theme API	Microsoft Corporation
☑ Web Platform Customizations	IE Per-User Initialization Utility	Microsoft Corporation
☑ Windows Desktop Update	Windows Shell Common Dll	Microsoft Corporation
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\IconServiceLib		
☑ IconCodecService.dll	Converts a PNG part of the icon to a legac...	Microsoft Corporation
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components		
☑ Microsoft Windows Media Player	Microsoft Windows Media Player Setup Ut...	Microsoft Corporation
☑ Microsoft Windows Media Player	Microsoft Windows Media Player Setup Ut...	Microsoft Corporation
☑ n/a	Windows host process (Rundll32)	Microsoft Corporation
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Startup		
☑ MFC71ESP.exe.lnk	MFC Language Specific Resources	Microsoft Corporation
Explorer		
HKLM\SOFTWARE\Classes\Protocols\Filter		
☑ application/octet-stream	Microsoft .NET Runtime Execution Engine	Microsoft Corporation
☑ application/x-complus	Microsoft .NET Runtime Execution Engine	Microsoft Corporation
☑ application/x-msdownload	Microsoft .NET Runtime Execution Engine	Microsoft Corporation
☑ text/xml	Microsoft Office XML MIME Filter	Microsoft Corporation

```
MFC71ESP.exe.lnk                  Size:     564 K
MFC Language Specific Resources   Time:     Wed Sep 29 12:38:09 2021
Microsoft Corporation             Version:  7.10.6119.0
C:\Users\karolisliucveikis\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\MFC71ESP.exe
```

Ready

Figure 3. User-Interface of Autoruns Program

- After the Autorun application is downloaded, the computer should be restarted in 'safe mode.'
- Extract the downloaded files and then run the Autoruns.exe file as shown in figure 4.

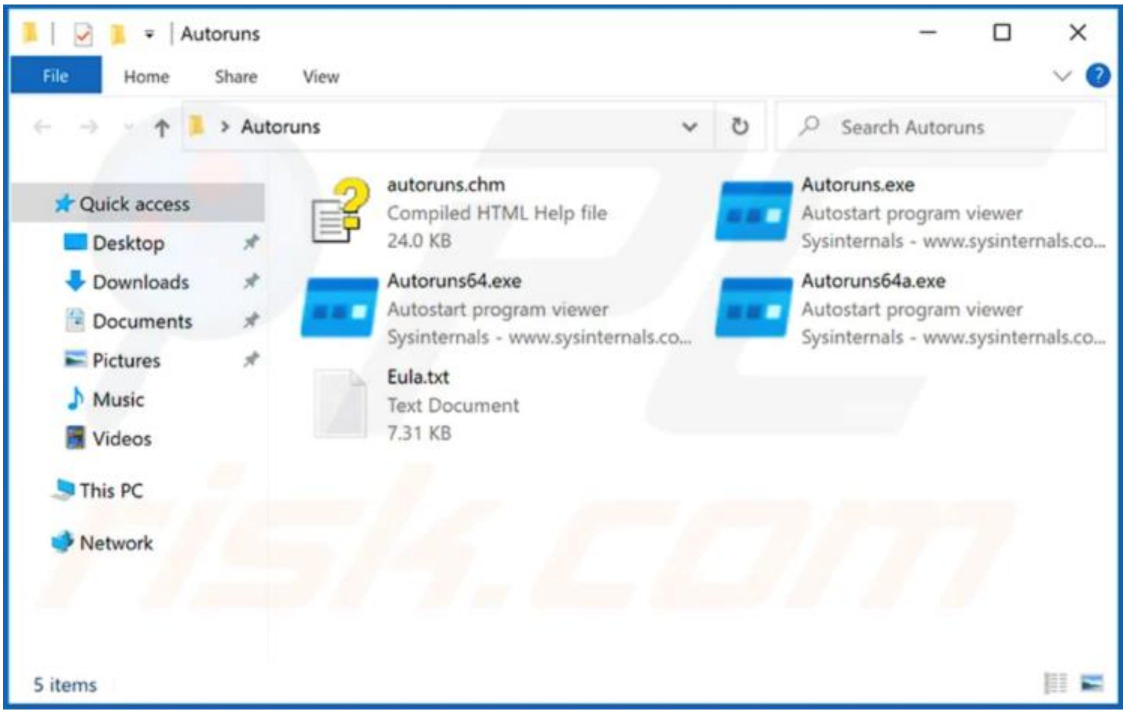
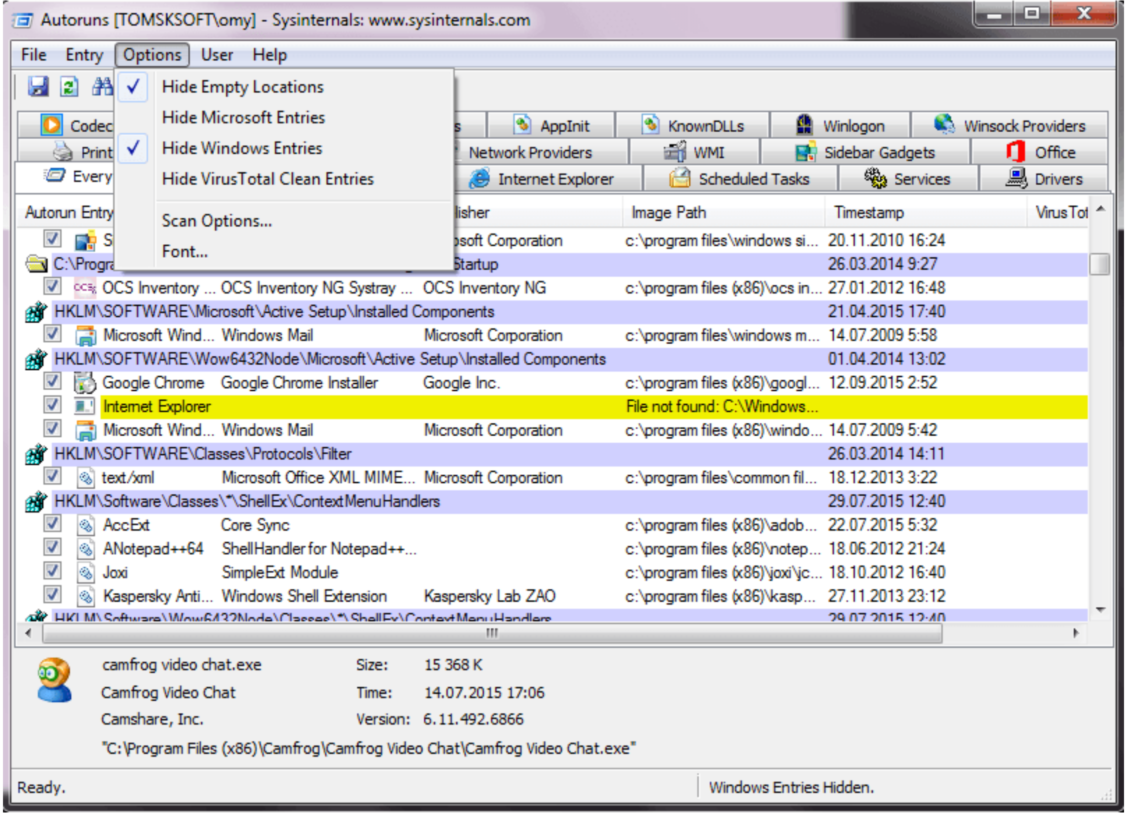


Figure 4. Extraction of Autornus.exe file

- Click the "Option" menu and uncheck the 'Hide Empty Location' as shown in figure 5.



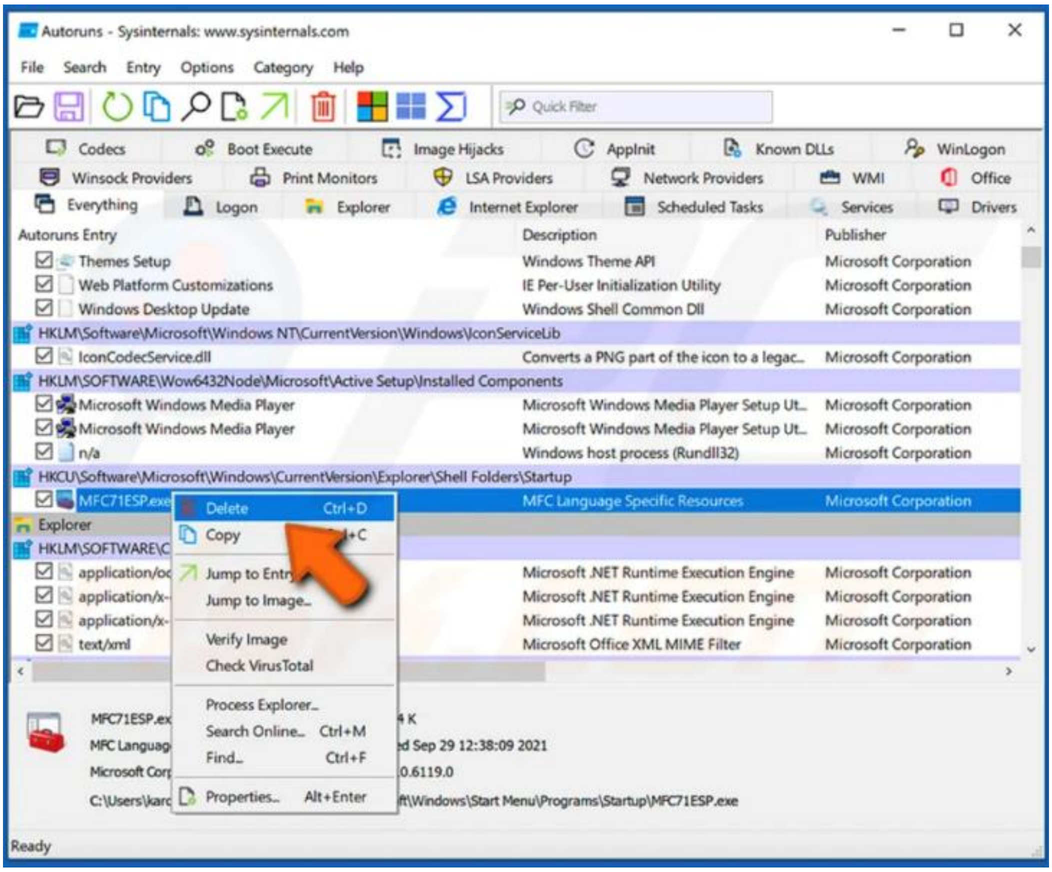
Autorun Entry		lisher	Image Path	Timestamp	VirusTot
☑ S		osoft Corporation	c:\program files\windows si...	20.11.2010 16:24	
C:\Progra		Startup		26.03.2014 9:27	
☑ OCS Inventory ...	OCS Inventory NG Systray ...	OCS Inventory NG	c:\program files (x86)\ocs in...	27.01.2012 16:48	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				21.04.2015 17:40	
☑ Microsoft Wind...	Windows Mail	Microsoft Corporation	c:\program files\windows m...	14.07.2009 5:58	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				01.04.2014 13:02	
☑ Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\googl...	12.09.2015 2:52	
☑ Internet Explorer			File not found: C:\Windows...		
☑ Microsoft Wind...	Windows Mail	Microsoft Corporation	c:\program files (x86)\windo...	14.07.2009 5:42	
HKLM\SOFTWARE\Classes\Protocols\Filter				26.03.2014 14:11	
☑ text/xml	Microsoft Office XML MIME...	Microsoft Corporation	c:\program files\common fil...	18.12.2013 3:22	
HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers				29.07.2015 12:40	
☑ AccExt	Core Sync		c:\program files (x86)\adob...	22.07.2015 5:32	
☑ ANotepad++64	ShellHandler for Notepad++...		c:\program files (x86)\notep...	18.06.2012 21:24	
☑ Joxi	SimpleExt Module		c:\program files (x86)\joxi\jc...	18.10.2012 16:40	
☑ Kaspersky Anti...	Windows Shell Extension	Kaspersky Lab ZAO	c:\program files (x86)\kasp...	27.11.2013 23:12	
HKLM\Software\Wow6432Node\Classes\*\ShellEx\ContextMenuHandlers				29.07.2015 12:40	

camfrog video chat.exe Size: 15 368 K
Camfrog Video Chat Time: 14.07.2015 17:06
Camshare, Inc. Version: 6.11.492.6866
"C:\Program Files (x86)\Camfrog\Camfrog Video Chat\Camfrog Video Chat.exe"

Ready. Windows Entries Hidden.

Figure 5. Unhide Empty Location

- Carefully check all the files that are listed in Autoruns application and identify the malware file to be eliminated. At this final step, extra attention is needed to ensure the system files will not being deleted by mistake.



Autoruns Entry	Description	Publisher
☑ Themes Setup	Windows Theme API	Microsoft Corporation
☑ Web Platform Customizations	IE Per-User Initialization Utility	Microsoft Corporation
☑ Windows Desktop Update	Windows Shell Common Dll	Microsoft Corporation
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\IconServiceLib		
☑ IconCodecService.dll	Converts a PNG part of the icon to a legac...	Microsoft Corporation
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components		
☑ Microsoft Windows Media Player	Microsoft Windows Media Player Setup Ut...	Microsoft Corporation
☑ Microsoft Windows Media Player	Microsoft Windows Media Player Setup Ut...	Microsoft Corporation
☑ n/a	Windows host process (Rundll32)	Microsoft Corporation
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Startup		
☑ MFC71ESP.exe	MFC Language Specific Resources	Microsoft Corporation
Explorer		
HKLM\SOFTWARE\C		
☑ application/oc	Microsoft .NET Runtime Execution Engine	Microsoft Corporation
☑ application/x-	Microsoft .NET Runtime Execution Engine	Microsoft Corporation
☑ application/x-	Microsoft .NET Runtime Execution Engine	Microsoft Corporation
☑ text/xml	Microsoft Office XML MIME Filter	Microsoft Corporation

MFC71ESP.ex | 4 K
MFC Languag | d Sep 29 12:38:09 2021
Microsoft Corp | 0.6119.0
C:\Users\karc | ft\Windows\Start Menu\Programs\Startup\MFC71ESP.exe

Figure 6. Deleting the malware file.

8. Conclusion

The rise of fileless malware, particularly through the exploitation of Living off the Land Binaries (LOLBins), poses a significant challenge to traditional security measures. LOLBins leverage legitimate system tools and processes, allowing attackers to operate discreetly and bypass conventional antivirus and EDR systems. This study highlights the various techniques and tools used in LOLBins attacks, emphasizing how attackers can exploit vulnerabilities, manipulate system commands, and conceal malicious code. Despite the complexity of detecting LOLBins-based intrusions, there are effective strategies available, such as behavioral analysis, log monitoring, file integrity checking, and network traffic analysis. However, these detection methods require sophisticated security frameworks and proactive threat intelligence to identify unusual patterns and anomalies.

The key challenge lies in the fact that LOLBins exploitations seamlessly blend with legitimate system processes, complicating the task of distinguishing malicious actions from authorized ones. To counteract these sophisticated threats, organizations must employ a multi-layered defense strategy that integrates advanced monitoring tools, centralized logging, and machine learning algorithms to detect subtle deviations in user and system behavior. Moreover, continuous threat hunting and vulnerability assessments are crucial to stay ahead of evolving attack techniques. The ongoing research and development of enhanced security protocols and tools will be essential to address the risks posed by LOLBins and mitigate the impact of fileless malware in the future. In conclusion, vigilance, adaptability, and proactive defense are key in the battle against LOLBins and similar advanced cyber threats.

References

[1]. Cynet. (2020). What Are LOLBins and How Do Attackers Use Them in Fileless Attacks? https://www.cynet.com/attack-techniques-hands-on/what-are-lolbins-and-how-do-attackers-use-them-in-fileless-attacks/

[2]. Oleksandra Rumiantseva. (2023). Using Living Off the Land Binaries in Cyber Attacks & Their Detection. https://socprime.com/blog/what-are-lolbins/#How_Can_LOLBins_be_Used_for_Cyber_Attacks

[3]. Sidechannel. (2021). LOLBins: how native tools are used to make threats stealthier. https://www.sidechannel.blog/en/lolbins-how-native-tools-are-used-to-make-threats-stealthier/

[4]. Malwarebytes.(n.d.).Emotet.https://www.malwarebytes.com/emotet

[5]. Kiteworks. (n. D.). Living-Off-the-Land (LOTL) Attacks: Everything You Need to Know. https://www.kiteworks.com/risk-compliance-glossary/living-off-the-land-attacks/

[6]. Fred O'Connor. (n. d.). What you need to know about WMI attacks. ttps://www.cybereason.com/blog/fileless-malware-mi#:~:text=Instead%2C%20fileless%20malware%20attacks%20take,they%20carry%20out%20are%20trusted.

[7]. Sapphire. (2023). Lolbins: How To Detect & Mitigate Use On Cyber Attacks. https://www.sapphire.net/cybersecurity/lolbins/

[8]. Anthony Critelli. (2022). Base64 encoding: What sysadmins need to know. https://www.redhat.com/sysadmin/base64-encoding#:~:text=Fundamentally%2C%20Base64%20is%20used%20to,formats%20and%20require%20simple%20text.

[9]. crowdstrike. (n. d.). 8 Lolbins Every Threat Hunter Should Know.Pdf. Https://go.crowdstrike.com/rs/281-OBQ 66/images/WhitepaperHuntingForLOLBins2023.pdf

[10]. wietze. (2022). LOLBAS-Project/LOLBAS. https://github.com/LOLBAS-Project/LOLBAS/blob/master/yml/OSBinaries/Msiexec.yml

[11]. Tomas Meskauskas. (2022). How to remove wscript.exe virus. https://www.pcrisk.com/removal-guides/15192-wscript-exe-virus

[12]. frack113. (2022). LOLBAS Wscript.yml. https://github.com/LOLBAS-Project/LOLBAS/blob/master/yml/OSBinaries/Wscript.yml

[13]. MITRE ATT&CK. (n. d.). System Binary Proxy Execution: InstallUtil. https://attack.mitre.org/techniques/T1218/004/

[14]. sapphire. (2023). LOLBINS: HOW TO DETECT & MITIGATE USE ON CYBER ATTACKS. https://www.sapphire.net/cybersecurity/lolbins/

[15]. Tomas Meskauskas. (2023). How to remove Chaes malware from your operating system. https://www.pcrisk.com/removal-guides/19484-chaes-malware