



Evasive Methods Against Healthcare

12/10/2020





- Detection Methods
- Fileless Malware
- Living off the Land
- MITRE | ATT&CK
- WMI
- Example Campaigns
- Remediation
- Summary
- References



Slides Key:



Non-Technical: Managerial, strategic and high-level (general audience)



Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)





Signature Based

Signature-based detection relies on a preprogramed list of known indicators of compromise (IOCs). An IOC could include malicious network attack behavior, content of email subject lines, file hashes, known byte sequences, or malicious domains. Signatures may also include alerts on network traffic, including known malicious IP addresses that are attempting to access a system.



Anomaly Based

Anomaly-based detection is used for changes in behavior. Anomaly-based detection relies upon observing network occurrences and discerning anomalous traffic through heuristics and statistics.









Fileless Threats 101:

Characteristics of a Fileless Attack



Has no identifiable code or signature and particular behavior that traditional security software detects.



Is a memory-based threat, resides in the computer's RAM.



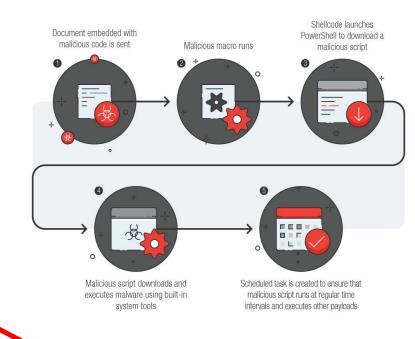
Takes advantage of processes in the system to facilitate an attack.



Could be used with other kinds of malware.



Could bypass whitelisting, as it takes advantage of allowed applications in the system.



LIVING OFF THE LAND

Image sources: TrendMicro







Windows Registry Manipulation

Windows registry manipulation involves the use of a malicious file or link that, when clicked on, uses a normal Windows process to write and execute fileless code into the registry.

Memory Code injection

Memory code injection techniques involve hiding malicious code in the memory of legitimate applications. While processes that are critical to Windows activity are running, this malware distributes and reinjects itself into these processes.

Script-Based Techniques

Scripts provide initial access, enable evasion, and facilitate lateral movements post-infection. Attackers will use scripts directly on the machine or embed them in Office documents and PDFs sent to the victims as email attachments.



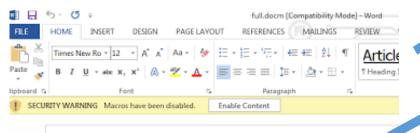




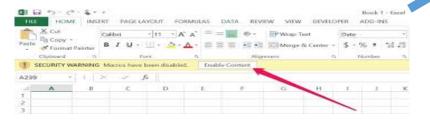


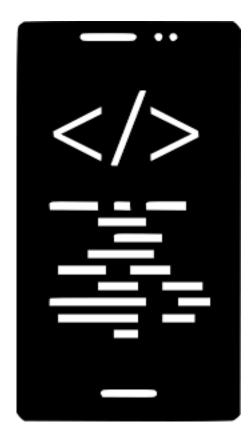


A fileless attack can start "traditionally" via malicious macro code (e.g. JavaScript or VBScript) embedded in archives, other seemingly normal files, and approved applications such as Office documents (e.g. Microsoft Word and Excel) and PDFs.









JScript | VBScript | Flash







is normally used for legitimate purposes but can also be abused by malicious actors.

- powershell.exe.
- bitsadmin.exe
- •certutil.exe-
- •psexec.exe
- •wmic.exe
- •mshta.exe
- mofcomp.exe
- •cmstp.exe
- windbq.exe
- •cdb.exe
- msbuild.exe
- •csc.exe
- regsvr32.exe

Most of the LoLBin and LoLBas techniques make use of PowerShell commands that execute a script directly in memory.

Can be used to easily install fake certificates for manin-the-middle (MITM) attacks, and to download base64 or hexadecimal encoded files disguised as certificates before decoding them.

Is often used as part of the exploitation of a CVE or Office macro to download files in place of PowerShell.







Image sources: Github









GOAL

to document every binary, script and library that can be used for Living Off The Land techniques. Github

Submission Requirements

- executing code
- downloading/upload files
- bypass UAC
- compile code
- getting creds/dumping process
- surveillance (keylogger, network trace)
- evade logging/remove log entry
- side-loading/hijacking of DLL
- pass-through execution of other programs, script (via a LOLBin)
- pass-through persistence utilizing existing LOLBin
- persistence (Hide data in ADS, execute at logon etc)

MITRE | ATT&CK





Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
	31 items	56 items	28 items	59 Items			17 items	13 items	9 items	21 items
-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
t Public-Facing	CMSTP	Accessibility Features	Manipulation	Binary Padding	Bash History	Application Window	Application Deployment	Automated Collection	Data Compressed	Communication Through
cation	Command-Line Interface	AppCert DLLs	Accessibility Features	BITS Jobs	Brute Force	Discovery	Software	Clipboard Data	Data Encrypted	Removable Media
vare Additions	Control Panel Items	Applnit DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	Browser Bookmark Discovery	Distributed Component Object Model	Data from Information	Data Transfer Size	Connection Proxy
cation Through vable Media	Dynamic Data Exchange	Application Shimming	Applnit DLLs	Clear Command History		File and Directory	Exploitation of Remote	Repositories	Limits	Custom Command and Control Protocol
phishing	Execution through API	Authentication Package	Application Shimming	CM		File and Directory	Services	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic
hment	Execution through Module	BITS Jobs	Bypass User Account Control	Co			Logon Scripts	Data from Network	Exfiltration Over	Protocol Protocol
phishing Link	ink Load	Bootkit	DLL Search Order	Co A			Pass the Hash	Shared Drive	Command and Control	Data Encoding
phishing via	Exploitation for Client Execution	Browser Extensions	Hjacking	0	ITR		Pass the Ticket	Data from Removable	Channel	Data Obfuscation
:0	Graphical User Interface	Change Default File	Dylib Hijacking				Remote Desktop	Media	Exfiltration Over Other Network Medium	Domain Fronting
ly Chain iromise	InstallUtil	Association	Exploitation for	Co.			Protocol	Data Staged	Exfiltration Over	Fallback Channels
ed Relationship		Component Firmware	Privilege Escalation				Remote File Copy	Email Collection	Physical Medium	Multi-hop Proxy
Accounts	Launcheti	Component Object Model	Extra Window Memory Injection	De			Remote Services	Input Capture	Scheduled Transfer	Multi-Stage Channels
Accounts	Local Job Scheduling	Hijacking	Injection File System	A	FO 0	1	Replication Through Removable Media	Man in the Browser		Multiband Communication
	LSASS Driver	Create Account	Permissions Weakness Hooking		T&C	K.,	Shared Webroot	Screen Capture Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking			$\mathbf{I} \propto \mathbf{C}$		SSH Hijacking			Part Knocking
	PowerShell	Dylib Hijacking	Image File Execution							Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Options Injection		l Tactics, Technic		Taint Shared Content			Remote File Copy
	Regsvr32	File System Permissions	Launch Daemon		mon Knowledge	100	Third-party Software			Standard Application
	Rundli32	Weakness	New Service	Fit			Windows Admin Shares			Layer Protocol
	Scheduled Task		Path Interception	File System Logical Children		System Information Discovery System Network	Windows Remote Management			Standard Cryptographic
	Scripting	Directories	Plist Modification	Gatekeeper Bypass						Protocol
	Service Execution	Hooking	Port Monitors	Hidden Files and Directories	Authentication	Configuration Discovery				Standard Non-Application Layer Protocol
	Signed Binary Proxy Execution	Hypervisor	Process Injection	Hidden Users	Interception	System Network Connections Discovery				Uncommonly Used Port
		Image File Execution Options Injection	Scheduled Task	Hidden Window						Web Service
	Signed Script Proxy Execution	Kernel Modules and	Service Registry	HISTCONTROL		System Owner/User Discovery System Service				
	Source	Extensions	Permissions Weakness	Image File Execution Options						
	Space after Filename	Launch Agent	Setuid and Setgid	Injection		Discovery				

An open framework and knowledge base of adversary tactics and techniques based on real-world observations, provides a structured method to help you answer these questions.

MITRE | ATT&CK°



Matrices Tactics ▼ Techniques ▼ Mitigations ▼ Groups Software

Resources ▼

Blog **♂**

Contribute

Search Q









There are many advantages of using WMI to an attacker:

- It is installed and running by default on all Windows operating systems.
- For code execution, it offers a stealthier alternative to running psexec.
- Permanent WMI event subscriptions run as SYSTEM.
- Defenders are generally unaware of WMI as a multipurpose attack vector.
- Nearly every operating system action is capable of triggering a WMI event.
- Other than storage in the WMI repository, no payloads touch disk.



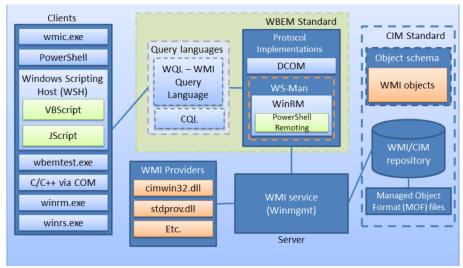


Image source:BlackHat

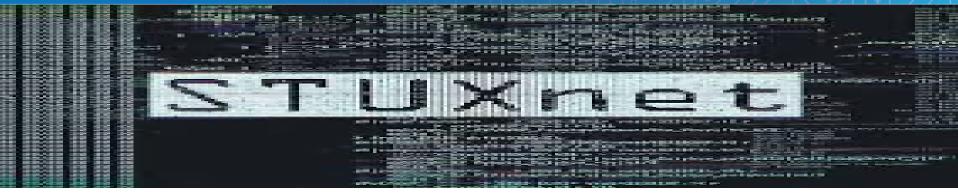
Great Source



https://www.blackhat.com/docs/us-15/materials/us-15-Graeber-Abusing-Windows-Management-Instrumentation-WMI-To-Build-A-Persistent%20Asynchronous-And-Fileless-Backdoor-wp.pdf







Stuxnet, one of the most sophisticated worms of 2010, affected nuclear processing facilities in Natanz, Iran and used WMI to enumerate users and spread to available network shares. It also used MOF (Managed Object Format) files, the means for creating and registering providers and events for WMI.



https://www.youtube.com/watch?v=0SjMgnGwpq8



T1064 - Scripting

T1197 - BITS Jobs

T1105 - Remote File Copy

TA0005 - Defense Evasion

T1073 - DLL Side-Loading

T1218 - Signed Binary Proxy Execution

T1096 - NTFS File Attributes



T1027 - Obfuscated Files or Information

T1027 - Obfuscated Files or Information

Astaroth

Fileless campaign that completely lives off the land. All of the relevant functionalities reside in scripts and shellcodes that are almost always coming in encrypted. are then decrypted, and run while only in memory. No malicious executable is ever written to the disk.

Astaroth attack chain 2020

- Spear-phishing email contains URL to archive file containing a shortcut file that invokes obfuscated BAT commands to drop a one-line JavaScript.
- The one-line JavaScript, which is run using explorer.exe, fetches the main script and runs it in memory.

flow 11 times.

The main script also uses bitsadmin.exe to download three more binary data. which it combines to form the first-stage malware

> which loads the first-stage malware code using DLL hijacking technique.

decrypts and combines three ADS streams in desktop.ini to form the second-stage malware.

The second-stage malware

- The third-stage malware is injected into userinit.exe using the process hollowing technique. The injected code reads and decrypts, the final-stage malware code, which is Astaroth.
- Astaroth reads and decrypts various plugins from the ADS streams in desktop.ini. The plugins allow Astaroth to steal email passwords, steal browser passwords, and enumerate installed security software.



T1192 - Spearphishing Link T1023 – Shortcut Modification T1064 - Scripting

link JavaScript

Second-stage

malware code

Third-stage

malware code

Process

hollowing

Userinit.exe

Steal browser

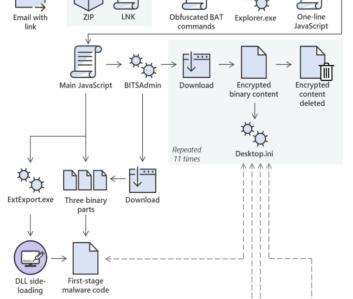
Using bitsadmin.exe, the main script downloads encrypted binary content, with it copies to the ADS of desktop.ini. It deletes the downloaded binary and starts the process again. It repeats this

ExtExport.exe

The script calls ExtExport.exe,

The first-stage malware

in turn reads and decrypts the third-stage malware.



T1129 - Execution Through Module Load T1140 - Deobfuscate/Decode Files or

Information T1093 - Process Hollowing T1055 - Process Injection

T1503 - Credentials from Web Browsers T1003 - Credential Dumping

Image source: Microsoft



Astaroth

Enumerate





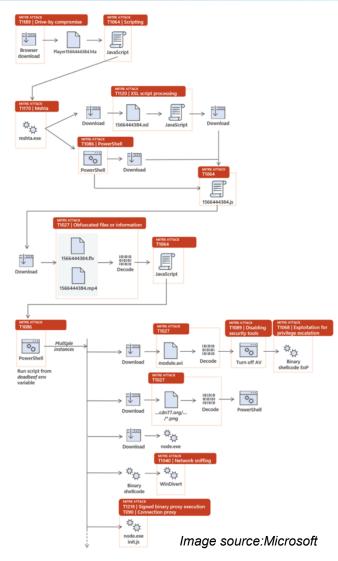
Nodersok

- 1. Victim runs an infected HTA (HTML application) file via an infected ad or download.
- JavaScript code in the HTA file downloads a secondstage component.
- Second-stage component launches a PowerShell command.
- 4. PowerShell commands download and run additional encrypted components

Nodersok Tools

Node.exe: This an implementation of Windows' Node.js framework that is used by many web applications. This means it will go over the heads of most and slip detection.

WinDivert: Packet capture utility and would not raise any red flags regarding detection.







Zloader is spread through aggressive email campaigns where the email contains a malicious attachment with a provocative title referring to either COVID-19 or seeking a job, and invoices with links to infected Microsoft Word files. In the case of the invoice email, users will download the malware installer when they

click the "Enable Content"

button on the document

Altered integers with ASCII characters to comprise a script to download malicious DLLs.



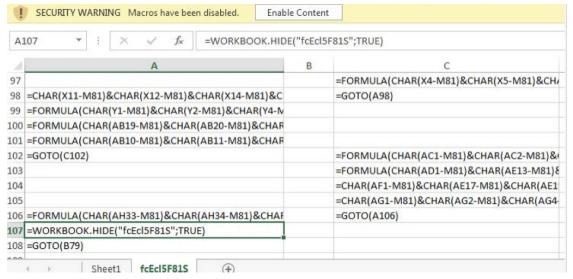


Image sources: eSentire and VMWare Carbon Black







Signature + Anomaly (Behavior) Detection

- **Endpoint hardening:** Since fileless attacks originate at the endpoint, it's important to have an advanced endpoint security solution that provides essential defenses like vulnerability assessment, exploit/memory protection, desktop firewall, and URL filtering.
- **Machine learning:** Security analytic solution using advanced, adaptive, and state-of-the-art machine learning, deep learning, and artificial intelligence techniques.
- **Application containment**: Blacklisting solution that blocks unauthorized applications and code from running on servers, desktops, and fixed-function devices.
- Behavior monitoring: Anomaly detection and customized rules.
- Interactive threat hunting: Endpoint detection and response (EDR) tool that automatically and proactively
 investigates and responds to abnormal behavior on endpoints and searches for fileless attack footholds.
- **Single-console centralized management:** Security management through platform that provides control, visibility, reporting, and actionable dashboards across hundreds and even thousands of nodes enterprisewide.
- **Integration with partner technologies**: Third-party partners who offer additional advanced technologies, helping you gain the advantage over adversaries.







According to 2019 Data Breach Investigations Report, it takes on average of 6 months to identify a compromise.

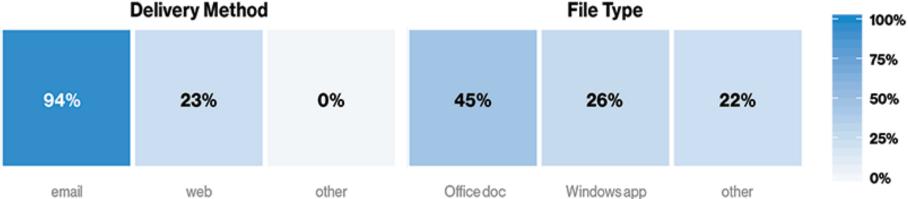
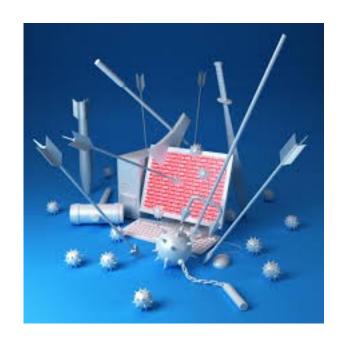


Image sources: Bluefin.com





Stealth is one of every threat actor's primary objectives, and fileless malware, LOLBins, and WMI functions provide perfect camouflage for malware that wants to hide in plain sight. This leaves plenty of time for an attacker to do their worst and maximize damage to the target network. We would do ourselves a disservice to think that these techniques aren't being utilized in the Healthcare sector. In order to truly protect our systems we have to utilized both signature and behavior detection methods.





Reference Materials





- Bring your own LOLBin: Multi-stage, fileless Nodersok campaign delivers rare Node.js-based malware
 - o https://www.microsoft.com/security/blog/2019/09/26/bring-your-own-lolbin-multi-stage-fileless-nodersok-campaign-delivers-rare-node-js-based-malware/
- Dismantling a fileless campaign: Microsoft Defender ATP's Antivirus exposes Astaroth attack
 - o https://www.microsoft.com/security/blog/2019/07/08/dismantling-a-fileless-campaign-microsoft-defender-atp-next-gen-protection-exposes-astaroth-attack/
- InfoStealers Weaponizing COVID-19
 - o https://www.lastline.com/labsblog/infostealers-weaponizing-covid-19/
- New TA505 Phishing Campaign Using LOLBins to Distribute Backdoor Malware
 - https://securityintelligence.com/news/new-ta505-phishing-campaign-using-lolbins-to-distribute-backdoor-malware/
- What Are Living Off the Land Attacks?
 - https://logrhythm.com/blog/what-are-living-off-the-land-attacks/
- Living Off The Land Binaries and Scripts (and now also Libraries)
 - o ht https://github.com/api0cradle/LOLBAS
- 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/
- · Hunting for LoLBins
 - https://blog.talosintelligence.com/2019/11/hunting-for-lolbins.html
- How Do Attackers Use LOLBins In Fileless Attacks?
 - o https://www.sentinelone.com/blog/how-do-attackers-use-lolbins-in-fileless-attacks/
- Cyber researchers confirm Russian government hack of Democratic National Committee
 https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html





- What Is Fileless Malware?
 - o https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html
- Monitoring with PowerShell: Preventing PowerShell based attacks (LoLBas)
 - o https://www.cyberdrain.com/monitoring-with-powershell-preventing-powershell-based-attacks-lolbas/
- Keep An Eye on LOLBins
 - https://isc.sans.edu/forums/diary/Keep+An+Eye+on+LOLBins/26502/
- · Abusing Microsoft Windows Utilities to Deliver Malware for Fun and Profit
 - o https://www.blackhat.com/docs/us-15/materials/us-15-Graeber-Abusing-Windows-Management-Instrumentation-WMI-To-Build-A-Persistent%20Asynchronous-And-Fileless-Backdoor-wp.pdf
- · An intro into abusing and identifying WMI Event Subscriptions for persistence
 - o https://in.security/an-intro-into-abusing-and-identifying-wmi-event-subscriptions-for-persistence/
- · Abusing Windows Management Instrumentation (WMI) to Build a Persistent, Asyncronous, and Fileless Backdoor
 - o ht https://github.com/api0cradle/LOLBAS
- ZLoader: What it is, how it works and how to prevent it | Malware spotlight
 - https://resources.infosecinstitute.com/topic/zloader-what-it-is-how-it-works-and-how-to-prevent-it-malwarespotlight/
- TA505
 - o https://attack.mitre.org/groups/G0092/
- Latest Astaroth living-off-the-land attacks are even more invisible but not less observable
 - https://www.microsoft.com/security/blog/2020/03/23/latest-astaroth-living-off-the-land-attacks-are-even-more-invisible-but-not-less-observable/
- A survey of emerging threats in cybersecurity
 - o https://www.sciencedirect.com/science/article/pii/S0022000014000178





- Threat Intel Versus Threat Hunting, What's the Difference?
 - o https://www.activecountermeasures.com/threat-intel-versus-threat-hunting-whats-the-difference/
- Abusing Windows Management Instrumentation (WMI)
 - o https://www.youtube.com/watch?v=0SjMgnGwpq8
- Malware spotlight: Nodersok
 - https://resources.infosecinstitute.com/topic/malware-spotlight-nodersok/
- What Is Endpoint Detection and Response (EDR)?
 - https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint/what-is-endpoint-detection-andresponse.html
- Attack Detection Fundamentals: Discovery and Lateral Movement Lab #5
 - o https://labs.f-secure.com/blog/attack-detection-fundamentals-discovery-and-lateral-movement-lab-5/
- How Do Attackers Use LOLBins In Fileless Attacks?
 - o https://www.sentinelone.com/blog/how-do-attackers-use-lolbins-in-fileless-attacks/
- · What Is Stuxnet?
 - o https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html
- A Decade of WMI Abuse an Overview of Techniques in Modern Malware
 - o https://www.bitdefender.com/files/News/CaseStudies/study/377/Bitdefender-Whitepaper-WMI-creat4871-en-EN-GenericUse.pdf





Upcoming Briefs

Securing RFID In Healthcare



Recipients of this and other Healthcare Sector Cybersecurity Coordination Cen products are highly encouraged to provide feedback to HC3@HHS.GOV">HC3@HHS.GOV.



Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to

HC3@HHS.GOV">HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

