Trickbot to Ryuk in Two Hours

Published: 2020-03-25 · Archived: 2026-04-05 15:55:31 UTC

A few days ago, I ran a Trickbot sample in the lab and was quite surprised what occurred. The attackers ran Cobalt Strike across multiple machines within 30 minutes and confirmed hands on activity within 60 minutes. They did additional recon and testing before deploying Ryuk. The attackers were able to go from Trickbot on one machine, to installing Ryuk on multiple machines, in just over two hours. Read below for the TLDR, Timeline, Summary and IOCs.

Lab Systems

There's a bunch of systems in the lab but I will specifically be talking about 3 of them.

- Workstation1 – Trickbot was executed on this Windows 10 workstation.
- Workstation2 – Lateral movement to this Windows 10 workstation via Cobalt Strike.
- Domain Controller (DC) – Lateral movement to this 2012 R2 server via Cobalt Strike.

TLDR

The actors initiated Cobalt Strike within 30 minutes of the Trickbot execution. From there, they attempted to copy & execute a Cobalt Strike beacon using SMB to the other machines on the network. Next, came a Bloodhound scan to find attack paths in the environment. The attacker then moved laterally via Cobalt Strike to a Domain Controller and then started running recon scripts such as PowerView. Twenty minutes later, a RDP session started on the Domain Controller. The attacker then ran a test method to verify Ryuk would work, then mapped all C$ administrator shares to the Domain Controller using Network Scanner. The attackers then dropped/ran Ryuk and waited about 10 minutes before logging off and killing the Cobalt Strike connection.

Timeline

19:24 UTC – Ran Trickbot sample from Any.Run on Workstation1

19:29 Trickbot written to AppData (screenshot shows Trickbot location)

.

A scheduled task was created, which runs at startup and every 20 minutes after install.

.

19:41 Trickbot recon commands run

- ipconfig /all
- net config workstation
- net view /all

- net view /all /domain
- nltest /domain_trusts
- nltest /domain_trusts /all_trusts

19:42 Trickbot sends task list and output of above commands to 203.176.135[.]102. Trickbot gtag ono35.

.

.

19:53 Cobalt Strike is initiated on Workstation1.

C2 – 206.81.5[.]253 / norulless.com

.

ETPRO Cobalt Strike signature fired for this activity. This rule is not available for the free ET ruleset.

.

C2 IP was first scene by RiskIQ on 3-21, so this appears to be pretty fresh.

.

19:56 Cobalt Strike run on Workstation2. File was copied over SMB and run as a service. Defender blocked this beacon but I allowed it 🙂 Two ET signatures fired each time they copied an EXE over SMB and executed it.

19:57 BloodHound is run on Workstation1

.

.

CyberChef

19:57 Creates BloodHound output files and zips them up.

.

19:59 Cobalt strike initiated on DC. File was copied over SMB and run as service.

.

20:16 PowerView run

.

20:16 Additional Recon activity via Cobalt Strike on DC

.

.

CyberChef

20:18 Possible lsass dump using rundll32.exe (Cobalt Strike default session uses rundll32.exe)

20:24 RDP connection is being tunneled over 443. Source of the tunneling is 195.123.242[.]48

.

20:25 RDP activity starts on DC. This next sequence appears to be the actors testing to see if Ryuk would run successfully. The grub.info.test folder is dropped.

.

20:33 Runs start.bat which runs Get-DataInfo.ps1

.

.

Here's a snippet from Get-DataInfo.ps1. The full script can be downloaded here.

20:34 – Netscan.exe is dropped and run

.

It appears netscan and it's exact path were used in a SWIFT Ukraine APT attack according to THOR.

.

THOR Scanner

20:35 Test results are zipped using 7z

.

20:59 RDP login to DC from DC as the same user. They used the IP address of the DC and not 127.0.0.1. The attacker went from tunneling through Workstation1 to running rdp/vnc locally on the DC.

20:50 The attacker then used Network Scanner to scan for devices on the local subnet and then right clicked on each C$ to map the drive. The attacker maps all machines to the DC as file shares.

21:34 The attacker then turned off Defender real-time protection via the local security policy.

.

21:34 Ryuk dropped

.

C:\\Users\\Administrator\\AppData\\Local\\Temp\\1\\fx1-318.exe

21:35 Ryuk is run, which runs the following commands before encrypting all systems included the mapped C$ shares.

- net.exe stop “samss” /y
- WMIC.exe shadowcopy delete
- vssadmin.exe Delete Shadows /all /quiet
- bcdedit /set {default} recoveryenabled No
- bcdedit /set {default}
- bootstatuspolicy ignoreallfailures
- icacls “C:*\” /grant Everyone:F /T /C /Q (this is done for all mapped drives)

21:35 We see multiple binaries run with “8 LAN” as the parameter shortly after Ryuk is run, which according to BleepingComputer designates the use of Wake-on-Lan (WoL). Ryuk will look at the arp table and then initiate a WoL packet to each system. If the system responds, Ryuk will attempt to mount the C$ admin share and then encrypt it.

.

Here is a listing of the binaries that seemed to do Ryuks bidding. Ryuk was initiated by the highlighted binary.

.

According to THOR at least a few of these are considered to be RYUK binaries

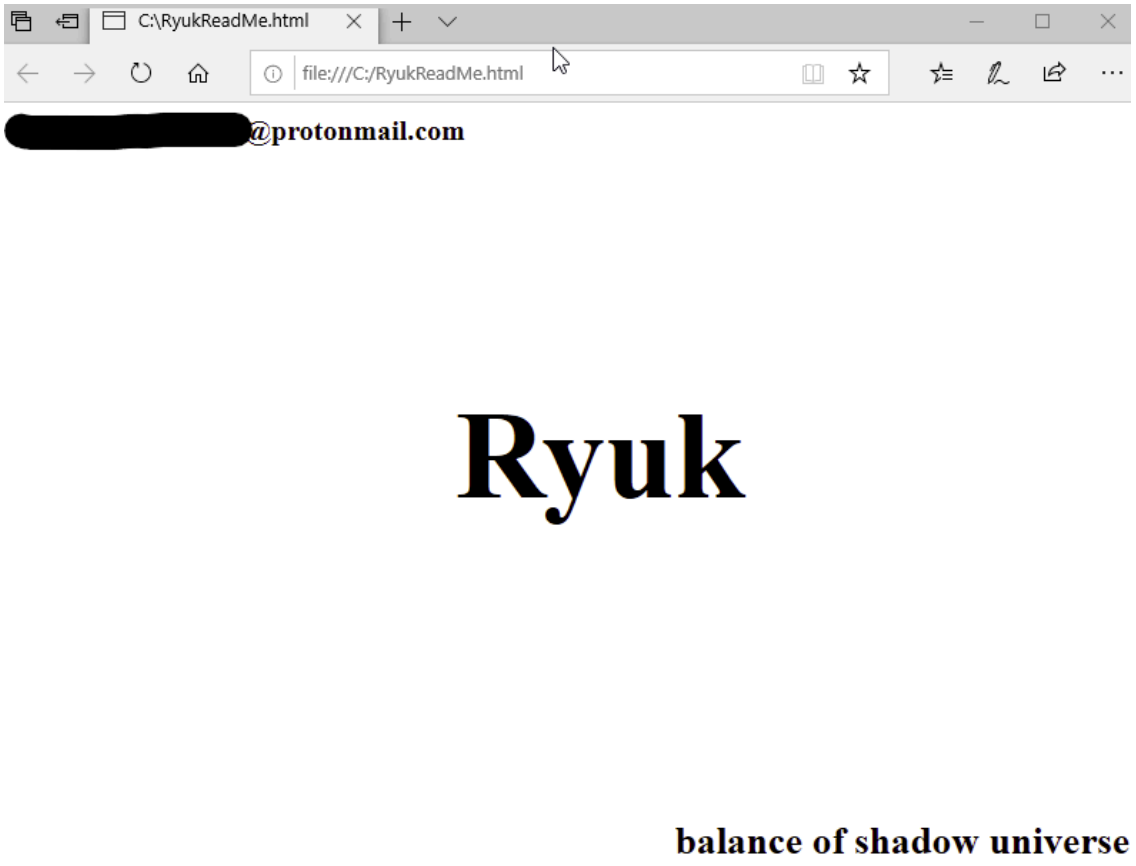
.

21:46 Cobalt strike drops off across all machines.

By this time all systems are encrypted with Ryuk. This is what the DC looks like after the drives were mapped and Ryuk run.

.

Screenshot of the Ryuk ransome page



Here is the email response I received when contacting them. They are asking for around $300k…

Summary

Ryuk actors move fast and usually use Offensive Security Tools such as Cobalt Strike, PowerView and/or Empire. This is the first time I've ever heard or seen Ryuk move this fast so I was very excited to watch it unfold in front of my eyes. Another interesting point is the use of Network Scanner. I've seen this used by low level ransomware groups all the way up to this Ryuk group; it seems to be a favorite. Something else to note is the use of US IPs for C2 and tunneling so geo blocking will not help you here. Make sure you can detect Trickbot, Cobalt Strike, Empire, and PowerView in your environment and make sure you test on a regular cadence because these tools change.

If you have any questions or want additional information please feel free to use the Contact Me page. A HUGE shout out to all the people working on Hybrid Hunter, this tool is fantastic and I can't wait to see it continue to improve. Thanks for reading!

IOCs

All IOCs including binaries are in MISPPriv Event ID 65678 and CIRCL OSINT feed via UUID 5e78dc2c-afc8-411f-94a5-40bb950d210f.
