Ryuk Ransomware Threat Intelligence Report

1/4/2019

Table of Contents

Executive Summary:

The Ryuk variant of ransomware is a new type of ransomware that first appeared in August 2018 and has been used since then in an targeted attack scheme by unknown actors online. The evolution of the attack has taken shape to mimic some of the attack methodologies used by the SAMSAM group (Iran) in locating vulnerable enterprises/organizations through reconnaissance and phishing to then gain a foothold in as a first phase of their attack.

The Ryuk actors then escalate the incursion by loading the ransomware (Ryuk) onto servers in the enterprise and thus locking that business down completely from daily business. The attacks have been seen recently (Dec/January 2018-2019) in attacks against publishing and media corporations such as the LA Times, Chicago Times (Tribune Group) as well as DataResolution Cloud Service. The financial damages to those companies has yet to be determined but due to the attack on the Tribune group, printing of newspapers was degraded or stopped for a time.

The Ryuk actor group uses two probable means to gaining access to internal networks:

1) phishing to infect systems with EMOTET (trojan variant using PowerShell via doc files that use macros to start ps.exe) and then pivot laterally to gain more access.

2) Locating vulnerable systems online using Shodan and other tools to find open RDP sessions and exploits them to escalate the attack.

In both attack vectors the second stage of the attack is to use the access gained to recon the org to locate systems (servers) to infect with Ryuk. The Ryuk infection will then encrypt all data, delete shadow copies and leave a message that the systems have been encrypted and where to send bitcoins.

The malware campaign to date (Aug 2018 to today) has accrued approximately $2,680,077.93 in bitcoin transfers from affected organizations. The average demand for money per each attack, is per the organizations tolerances judged by the actors estimate of what they can afford. This method is a lot like the SAMSAM group.

Recommendations:

Threat intelligence on the malware and the tactics of the group provide the following recommendations for response to this threat:

- Put all IOC’s into HIDS/NIDS
- Block known C2’s
- Assess for vulnerable RDP sessions to the internet (Shodan)
- Block all hashes and C2’s for EMOTET campaigns
- Be aware of ps.exe (powershell) sessions going to the internet

Technical Details:

The malware immediately begins by shutting down A/V systems and specifically SOPHOS and McAfee as well as other processes focusing not only on A/V but backup programs. Early Virus Total assessments as well as Hybrid Analysis online show some signs that the actors had tested early versions of the malware and that it had been detected by SOPHOS and McAfee.

Strings:

stop "Enterprise Client Service" /y
stop "Sophos AutoUpdate Service" /y
stop "Sophos Clean Service" /y
stop "Sophos Device Control Service" /y
stop "Sophos File Scanner Service" /y
stop "Sophos Health Service" /y
stop "Sophos Safestore Service" /y
stop "Sophos System Protection Service" /y
stop "Sophos Web Control Service" /y
stop "SQLsafe Backup Service" /y
stop "SQLsafe Filter Service" /y
stop "Veeam Backup Catalog Data Service" /y
stop "Zoolz 2 Service" /y
stop Antivirus /y
stop BackupExecAgentAccelerator /y
stop BackupExecAgentBrowser /y
stop BackupExecDeviceMediaService /y
stop BackupExecJobEngine /y
stop BackupExecManagementService /y
stop BackupExecRPCService /y
stop BackupExecVSSProvider /y
stop EhttpSrv /y
stop EPSecurityService /y

```
stop EPUpdateService /y
stop MBAMService /y
stop McAfeeEngineService /y
stop McAfeeFramework /y
stop McAfeeFrameworkMcAfeeFramework /y
stop MSSQL$BKUPEXEC /y
stop MSSQLServerOLAPService /y
stop ntrtscan /y
stop PDVFSService /y
stop ReportServer /y
stop ReportServer$SQL_2008 /y
stop ReportServer$SYSTEM_BGC /y
stop ReportServer$TPS /y
stop ReportServer$TPSAMA /y
stop SAVAdminService /y
stop SAVService /y
stop SepMasterService /y
stop Smcinst /y
stop SmcService /y
stop SMTPSvc /y
stop SntpService /y
stop SQLAgent$BKUPEXEC /y
stop SQLAgent$CITRIX_METAFRAME /y
stop SQLSafeOLRService /y
stop swi_service /y
stop tmlisten /y
stop TrueKey /y
stop TrueKeyScheduler /y
stop TrueKeyServiceHelper /y
stop VeeamDeploymentService /y
stop VeeamTransportSvc /y
TerminateProcess
```

Currently a high number of A/V client engines now see the Ryuk malware by hashes. It is assumed that the actor may in fact re-pack the malware to avoid such detection's if not upgrade functionality to have a wider ability to succeed and avoid HIDS/NIDS detection as well.

The malware also requires ADMIN to perform all it’s functions. This need for ADMIN is the reason that Ryuk is a second stage and not a one and done attack. EMOTET infections attain the ADMIN level access and allow the actors to recon the enterprise and determine where to attack as well as what they can access to load Ryuk and encrypt files.

IOC’s:

IP(s) / Hostname(s)

- 104.199.153[.]189
- 104.239.157[.]210
- 187.17.111[.]103
- 195.20.45[.]185
- 200.98.255[.]192
- 23.253.126[.]58
- 68.168.222[.]206
- 89.119.67[.]154

URLs

- bedava-chat[.]com
- bestinfo[.]vv[.]si
- digiturk[.]adsl[.]com[.]tr
- freshmirza[.]tk
- ibrahimreb[.]com
- infocommsystems[.]com
- jaragroup[.]com[.]ar
- klkjwre9fqwieluoi[.]info
- kukutrustnet777[.]info
- kukutrustnet777888[.]info
- kukutrustnet888[.]info
- kukutrustnet987[.]info
- lavanyacreation[.]com
- natufarma[.]net
- radiantjewelcraft[.]com
- sets-hm[.]tk
- veddagroup[.]twomini[.]com

Associated-file-path:

- C:\Users\Public\cjoZX[.]exe
- C:\Users\Public\window[.]bat

Associated-email-addresses:

- WayneEvenson@tutanota[.]com
- WayneEvenson@protonmail[.]com
- stevkramer@protonmail.com
- johnfraz@protonmail.com
- stevkramer@tutanota.com
- johnfraz@tutanota.com
- kurtschweickardt@protonmail.com
- kurtschweickardt@tutanota.com
- wayneevenson@protonmail.com
- wayneevenson@tutanota.com
- steveedelman@protonmail.com
- steveedelman@tutanota.com
- andymitton@protonmail.com
- andymitton@tutanota.com
- kaykienzler@protonmail.com
- bennidiez@protonmail.com
- kaykienzler@tutanota.com
- bennidiez@tutanota.com
- dustinloose@protonmail.com
- dustinloose@tutanota.com
- AdamasVorms@tutanota.com
- AdamasVorms@protonmail.com
- RcsonanaGemmaran@tutanota.com
- RcsonanaGemmaran@protonmail.com
- dfvdc@protonmail.com

- khgvkh@tutanota.com
- yu66MarsellBlan@protonmail.com
- yu66MafrsellBlan@tutanota.com
- BruceSmithh@protonmail.com
- BruceSmithh@tutanota.com
- vejoydyLunde@tutanota.com
- vejoydyLunde@protonmail.com
- RichardsonStan@tutanota.com
- RichardsonStan@protonmail.com
- WillysFranks@tutanota.com
- WillysFrank@protonmail.com
- KangCheonSoo@tutanota.com
- KangCheonSo@protonmail.com
- RaulDrake@protonmail.com
- kaidrake@tutanota.com
- fgbfs@protonmail.com
- fgbf@tutanota.com
- ElaineDeaVille@tutanota.com
- ElaineDeaVille@protonmail.com
- TinaHahn@tutanota.com
- TinaHahn@protonmail.com
- ChrisJohnes@protonmail.com
- ChrisJohnes@tutanota.com
- DeborahPATINO@tutanota.com
- DeborahPATINO@protonmail.com
- CristopherBrandstrom@protonmail.com
- CristopherBrandstrom@tutanota.com
- DANIELEdEBLOIS@tutanota.com
- DANIELEdEBLOIS@protonmail.com
- petterSpurier@protonmail.com

- petterSpurier@tutanota.com
- arWalagnCuad@tutanota.com
- arWalanCuad@protonmail.com
- degrv@tutanota.com
- fhnf@protonmail.com
- taigrizalsec1973@protonmail.com
- arturDale@tutanota.com
- CamdenScott@protonmail.com
- eliasmarco@tutanota.com
- MelisaPeterman@protonmail.com
- MelisaPeterman@tutanota.com

Associated-bitcoin-address:

- 14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
- 1L9fYHJJxeLMD2yyhh1cMFU2EWF5ihgAmJ
- 1KURvApbe1yC7qYxkkkvtdZ7hrNjdp18sQ
- 15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj
- 1LKULheYnNtJXgQNWMo24MeLrBBCouECH7
- 1CN2iQbBikFK9jM34Nb3WLx5DCenQLnbXp
- 14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
- 15FC73BdkpDMUWmxo7e7gtLRtM8gQgXyb4
- 1NQ42zc51stA4WAVkUK8uqFAjo1DbWv4Kz
- 1EoyVz2tbGXWL1sLZuCnSX72eR7Ju6qohH
- 1K6MBjz79QqfLBN7XBnwxCJb8DYUmmDWAt
- 1ChnbV4Rt7nsb5acw5YfYyvBFDj1RXcVQu
- 162DVnddxsbXeVgdCy66RxEPADPETBGVBR
- 12N7W9ycLhuck9Q2wT8E6BaN6XzZ4DMLau
- 1C8n86EEttnDjNKM9Tjm7QNVgwGBncQhDs
- 18eu6KrFgzv8yTMVvKJkRM3YBAyHLonk5G
- 19AE1YN6Jo8ognKdJQ3xeQQL1mSZyX16op

- 1NMgARKzfaDExDSEsNijeT3QWbvTF7FXxS
- 12UbZzhJrdDvdyv9NdCox1Zj1FAQ5onwx3
- 1KUbXkjDZL6HC3Er34HwJiQUAE9H81Wcsr
- 13rTF3AYsf8xEdafUMT5W1E5Ab2aqPhkPi
- 1Kx9TT76PHwk8sw7Ur6PsMWyEtaogX7wWY
- 12vsQry1XrPjPCaH8gWzDJeYT7dhTmpcjL
- 1ET85GTps8eFbgF1MvVhFVZQeNp2a6LeGw
- 1FtQnqvjxEK5GJD9PthHM4MtdmkAeTeoRt
- 1Kx9TT76PHwk8sw7Ur6PsMWyEtaogX7wWY

Malware Hash (MD5/SHA1/SH256)

- c0202cf6aeab8437c638533d14563d35
- d348f536e214a47655af387408b4fca5
- 958c594909933d4c82e93c22850194aa
- 86c314bc2dc37ba84f7364acd5108c2b
- 29340643ca2e6677c19e1d3bf351d654
- cb0c1248d3899358a375888bb4e8f3fe
- 1354ac0d5be0c8d03f4e3aba78d2223e
- 5ac0f050f93f86e69026faea1fbb4450
- 1b465c0e12523747f892b48fa92a30f82e5027199a2aff06587c5269bd99f69a
- 3c8531fc54eca31a79a23bf16d4f528067c89a5e58e1e745a2c5b1b05140f5a8
- 95b228b664dca2e18935444c67c7c7dbda9da7450a18d429cb04f7e311af5fe9
- 46fb27f4cff2d33baae3b1c199797d1f0929bc03166cebd092081e4fe2f9ea6e
- 8d50d9fe17eb36edc9945a2673c1594f58a6e653f5a794058ee42e46d24d83d7
- f21f222d8f62f2223faec375e834efb76f96b73ef70e0ef09024586cf9eef638
- b7e945a8dafc91ebe8c8717ee3107498afc1ad5461599611d2fb07aaa7700aa1
- 88d491bb73d509aacca103919d3a7418f9c6b611ce7dc453e1cacffed9c0f0d5
- 5e4160a133d44a1cf90d72eedd5e6084543521fecbf070d550c6012d294ccb28
- aacfc3e386ed12082923d03fa1120d5fa6bf7b8655ba77e04b96a45434fa9a83
- 235ab3857ba2d2cd09311d6cc7bf1139863022579ea98be2b503921104ee20ac
- 7c1e0597dd5a1e2d48c9cede54843aa7c299f7404630b5a2aafac2eec7358b20
- 9fe66773c84d371ef1b424005996ade4d5e16fb00306a1d54b107b2b2d03fe17

- 695a716f2c43a69bdd03e74058fa23fb77e596bb4f1f3a021d529c85e9564f7d
- 6eca3f416a08fde6688250dbd4ba4dfaa3df95a5d26b6d978dfbd67fbd159619
- 965884f19026913b2c57b8cd4a86455a61383de01dabb69c557f45bb848f6c26
- 8d3f68b16f0710f858d8c1d2c699260e6f43161a5510abb0e7ba567bd72c965b
- 3012f472969327d5f8c9dac63b8ea9c5cb0de002d16c120a6bba4685120f58b4
- b8e463789a076b16a90d1aae73cea9d3880ac0ead1fd16587b8cd79e37a1a3d8
- 9b86a50b36aea5cc4cb60573a3660cf799a9ec1f69a3d4572d3dc277361a0ad2
- 113af75f13547be184822f1268f984b79f35965a1b1f963d23b50a09741b0aec
- 1455091954ecf9ccd6fe60cb8e982d9cfb4b3dc8414443ccfdfc444079829d56
- c51024bb119211c335f95e731cfa9a744fcdb645a57d35fb379d01b7dbdd098e

Dropped Files:

details

"gimap.jar" has type "data"

"org.eclipse.equinox.p2.engine.nl_zh_4.4.0.v20140623020002.jar" has type "data"

"Download_on_the_App_Store_Badge_fr_135x40.svg" has type "data"

"PIXEL.INF" has type "data"

"close.svg" has type "data"

"com.jrockit.mc.components.ui.ja_5.5.1.172852.jar" has type "data"

"org.eclipse.equinox.p2.jarprocessor.nl_zh_4.4.0.v20140623020002.jar" has type "data"

"javaws.jar" has type "data"

"org-netbeans-modules-options-api.jar" has type "8086 relocatable (Microsoft)"

"org.eclipse.e4.ui.workbench.addons.swt_1.1.1.v20140903-0821.jar" has type "data"

"ADEBASE.MSI" has type "data"

"org-netbeans-core-io-ui_zh_CN.jar" has type "data"

"org.eclipse.help.ui_4.0.100.v20140401-0608.jar" has type "data"

"VeriSign_Class_3_Code_Signing_2001-4_CA.cer" has type "data"

"org.eclipse.equinox.p2.touchpoint.eclipse.nl_zh_4.4.0.v20140623020002.jar" has type "data"

"org.eclipse.core.databinding.observable.nl_ja_4.4.0.v20140623020002.jar" has type "data"

"com.jrockit.mc.browser.ja_5.5.1.172852.jar" has type "data"

"org-openide-loaders_zh_CN.jar" has type "data"

"com-sun-tools-visualvm-host-remote_zh_CN.jar" has type "data"

"org-netbeans-modules-queries.jar" has type "data"

source: Extracted File

Virus Total Assessments:

- https://www.virustotal.com/#/file/1b465c0e12523747f892b48fa92a30f82e5027199a2aff06587c5269bd99f69a/detection
- https://www.virustotal.com/#/file/3c8531fc54eca31a79a23bf16d4f528067c89a5e58e1e745a2c5b1b05140f5a8/detection
- https://www.virustotal.com/#/file/95b228b664dca2e18935444c67c7c7dbda9da7450a18d429cb04f7e311af5fe9/detection
- https://www.virustotal.com/#/file/46fb27f4cff2d33baae3b1c199797d1f0929bc03166cebd092081e4fe2f9ea6e/detection
- https://www.virustotal.com/#/file/f21f222d8f62f2223faec375e834efb76f96b73ef70e0ef09024586cf9eef638/detection
- https://www.virustotal.com/#/file/b7e945a8dafc91ebe8c8717ee3107498afc1ad5461599611d2fb07aaa7700aa1/detection
- https://www.virustotal.com/#/file/88d491bb73d509aacca103919d3a7418f9c6b611ce7dc453e1cacffed9c0f0d5/detection
- https://www.virustotal.com/#/file/5e4160a133d44a1cf90d72eedd5e6084543521fecbf070d550c6012d294ccb28/detection
- https://www.virustotal.com/#/file/aacfc3e386ed12082923d03fa1120d5fa6bf7b8655ba77e04b96a45434fa9a83/detection
- https://www.virustotal.com/#/file/235ab3857ba2d2cd09311d6cc7bf1139863022579ea98be2b503921104ee20ac/detection
- https://www.virustotal.com/#/file/7c1e0597dd5a1e2d48c9cede54843aa7c299f7404630b5a2aafac2eec7358b20/detection
- https://www.virustotal.com/#/file/9fe66773c84d371ef1b424005996ade4d5e16fb00306a1d54b107b2b2d03fe17/detection
- https://www.virustotal.com/#/file/695a716f2c43a69bdd03e74058fa23fb77e596bb4f1f3a021d529c85e9564f7d/detection
- https://www.virustotal.com/#/file/6eca3f416a08fde6688250dbd4ba4dfaa3df95a5d26b6d978dfbd67fbd159619/detection

- https://www.virustotal.com/#/file/965884f19026913b2c57b8cd4a86455a61383de01dabb69c557f45bb848f6c26/detection
- https://www.virustotal.com/#/file/8d3f68b16f0710f858d8c1d2c699260e6f43161a5510abb0e7ba567bd72c965b/detection
- https://www.virustotal.com/#/file/3012f472969327d5f8c9dac63b8ea9c5cb0de002d16c120a6bba4685120f58b4/detection
- https://www.virustotal.com/#/file/b8e463789a076b16a90d1aae73cea9d3880ac0ead1fd16587b8cd79e37a1a3d8/detection
- https://www.virustotal.com/#/file/9b86a50b36aea5cc4cb60573a3660cf799a9ec1f69a3d4572d3dc277361a0ad2/detection
- https://www.virustotal.com/#/file/113af75f13547be184822f1268f984b79f35965a1b1f963d23b50a09741b0aec/detection
- https://www.virustotal.com/#/file/1455091954ecf9ccd6fe60cb8e982d9cfb4b3dc8414443ccfdfc444079829d56/detection
- https://www.virustotal.com/#/file/c51024bb119211c335f95e731cfa9a744fcdb645a57d35fb379d01b7dbdd098e/detection

Hybrid Analysis Assessments:

- https://www.hybrid-analysis.com/sample/1b465c0e12523747f892b48fa92a30f82e5027199a2aff06587c5269bd99f69a?environmentId=120
- https://www.hybrid-analysis.com/sample/8d3f68b16f0710f858d8c1d2c699260e6f43161a5510abb0e7ba567bd72c965b?environmentId=120
- https://www.hybrid-analysis.com/sample/3012f472969327d5f8c9dac63b8ea9c5cb0de002d16c120a6bba4685120f58b4?environmentId=120

Appendix:

URL's:

https://www.bleepingcomputer.com/news/security/ryuk-ransomware-involved-in-cyberattack-stopping-newspaper-distribution/

https://niiconsulting.com/Security_Advisories/Security_Advisory_Digest_Aug_2018_Edition_2.0.pdf

https://www.bleepingcomputer.com/news/security/ryuk-ransomware-crew-makes-640-000-in-recent-activity-surge/

https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf

https://resources.malwarebytes.com/files/2018/12/Malwarebytes-Labs-Under-The-Radar-APAC-1.pdf

https://research.checkpoint.com/wp-content/uploads/2018/08/Threat_Intelligence_News_2018-08-27.pdf

https://krebsonsecurity.com/2019/01/cloud-hosting-provider-dataresolution-net-battling-christmas-eve-ransomware-attack/

https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/

https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/27000/PD27951/en_US/McAfee%20Labs%20Threat%20Advisory%20-%20Ransom-Ryuk_v2.pdf

http://www.rewterz.com/rewterz-news/rewterz-threat-advisory-ryuk-evolves-as-a-new-targeted-ransomware

https://www.cyber.nj.gov/threat-profiles/ransomware-variants/ryuk

https://www.maltiverse.com/sample/8d3f68b16f0710f858d8c1d2c699260e6f43161a5510abb0e7ba567bd72c965b