Cyber Crime Unit

Ryuk Ransomware Infections

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 TLP: GREEN 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/.

July 26, 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 26, 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. 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. Analysis of evidence from infected networks has revealed the creation of new user accounts and privilege escalation several days prior to encryption. Additionally, network logs indicate the presence of remote attackers at least two weeks prior to encryption.

Analysis of volatile data and memory dumps recovered from infected machines indicates the attackers are using WSMAN to implement PowerShell scripts. Ad_driver.sys has also been observed, which is linked to Anti-forensics processes activated when the presence of memory dump code is detected. Network activity also indicates the attackers are using Advapi for web-based logins, hijacking the Explorer.exe process. Advapi32.dll, a source of cryptographic functions in windows and used in the SMB exploit Eternal Blue, was also observed. The presence of advapi32.dll in a suspicious program may be an indicator of ransomware, as it is used for non-trivial cryptographic functions such as encryption/decryption of files.

Infected organizations are encouraged to not pay a ransom to criminal actors. Organizations who believe they have observed the following Indicators of Compromise should contact the fusion center at 1-800-434-8007 or lafusion.center@la.gov.

Indicators of Compromise

- Traffic to or from Pastebin.com (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, or 8082
- Outbound and Inbound traffic to ports 5985 or 16993
- Unusual remote connections either through RDP, LogMeIn, or TeamViewer
- Installed services with unusual names/created scheduled tasks with unusual names or paths
- Unusual files in user's roaming directories
- Advapi32.dll process being used as a hook for Explorer.exe
- The presence of ad_driver.sys in \\C\Users\ADMINI~1\AppData\Local\Temp\1\
- Creation of new user accounts with broad privileges
- Odd processes such as svchost.exe tied to open ports, including port 80

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.