

RANSOMWARE

Ransomware is a form of malware that typically propagates as a Trojan. Once installed onto a computer, it restricts access to the infected computer system in some way so that the user can no longer access it and requires a payment in order to decrypt or release control back to the user.¹



Figure 1: Example of Cryptolocker ransomware demanding a ransom to unlock encrypted files¹

Potential Indicators of Ransomware

Ransomware indicators may or may not be anomalies or incidents dependent on the actor(s). Some prominent indicators for ransomware include the following:

- Suspicious domain names (date gaps, unknown operators, etc.)
- Locked screen or files
- Ransom demand
- The ransomware identifies itself (Linux.Encoder, CoinVault, etc.)
- Changed file name (.lock, .crypt, etc.)²

Actors can use a variety of tactics to achieve their overall objective of cyber system intrusion. If successful, commonly achieved objectives include:

- Loss of control of the compromised machine
- Loss of/ Stolen Personal Identifying Information (PII)
- Loss of/ Stolen Bank Information
- Loss of/ Stolen Username / Passwords
- Loss of file data

Common Vulnerabilities

The following are key common vulnerabilities found within computer systems:

- JBoss application server
- Adobe Flash Player CVE-2015-7645, CVE-2015-8446, and CVE-2015-8651
- Microsoft Silverlight CVE-2016-0034³
- Unpatched systems
- Outdated software
- Limitations of cloud backup
- App Data/ Local App Data folders
- Remote Desktop Protocol (RDP)⁴

Protective/Prevention Measures

Protective/Prevention measures are designed to protect the user against *most* threats. Protective/Prevention measures can include:

- Avoid emails from unknown senders
- Do not click on links or email attachments from unexpected or unfamiliar sources
- Back up important files using the “3-2-1 rule” (create 3 backup copies on 2 different media with 1 backup in a separate location)
- Do not enable macros
- Use “least privileges”
- Segment the network
- Bookmark websites

Mitigation Measures

If ever to be caught with ransomware, the following are best-practice mitigation measure options:

- Immediately disconnect from the network
- Use Windows System Restore to clean the system
- Set back the BIOS clock to provide more time before the countdown increases the ransom
- Do not pay the ransom⁴

¹ Trend Micro (2016). *Ransomware*. Retrieved from Trend Micro Incorporated: <http://www.trendmicro.com/vinfo/us/security/definition/ransomware>.

² Rashid, F. (2016, April 29). *How to Tell if You've Been Hit by Fake Ransomware*. Retrieved from InfoWorld: <http://www.infoworld.com/article/3062552/security/how-to-tell-if-youve-been-hit-by-fake-ransomware.html>.

³ Jackson Higgins, K. (2016, March 22). *Here are 4 Vulnerabilities Ransomware Attacks are Exploiting Now*. Retrieved from InformationWeek: <http://www.darkreading.com/vulnerabilities---threats/here-are-4-vulnerabilities-ransomware-attacks-are-exploiting-now/d-d-id/1324791>.

⁴ Myers, L. (2013, December 12). *11 Things You Can Do to Protect Yourself Against Ransomware, Including Cryptolocker*. Retrieved from WeLiveSecurity: <http://www.welivesecurity.com/2013/12/12/11-things-you-can-do-to-protect-against-ransomware-including-cryptolocker/>.