U.S Department of Homeland Security issues alert on hospital ransomware attacks

April 13, 2016

In the wake of recent ransomware attacks on hospitals, the Department of Homeland Security's Computer Emergency Readiness Team (US-CERT) issued an alert regarding ransomware and recent variants. The alert notes that already this year, destructive ransomware variants, such as Locky and Samas, have infected computers belonging to health care facilities and hospitals. US-CERT states that the alert is "to provide further information on ransomware, specifically its main characteristics, its prevalence, variants that may be proliferating, and how users can prevent and mitigate against ransomware."

The alert further describes the nature of ransomware and the proliferation of variants, noting that due to the lucrative success of ransomware attacks, more sophisticated variants have emerged since 2012. Specifically, in early 2016, a destructive ransomware variant, Locky, has been observed infecting computers belonging to health care facilities and hospitals in the United States, New Zealand and Germany. The alert cautions that this ransomware "...propagates through spam emails that include malicious Microsoft Office documents or compressed attachments (e.g., .rar, .zip)...[and the]...malicious attachments contain macros or JavaScript files to download Ransomware-Locky files."

Information is also provided regarding CryptoLocker, a variant that typically causes a user to become infected by opening a

malicious attachment from an email. The alert notes that the malicious attachment contains Upatre, which is a downloader that infects the user with CryptoLocker as well as GameOver Zeus, a trojan that steals data. CryptoLocker, the alert warns, "encrypts files on the infected system, and requests that a ransom be paid."

While reports have indicated that some hospitals have paid the ransom at a relatively low amount to regain access to their data, US-CERT cautions: "Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed." Indeed, in this alert, US-CERT discourages organizations from paying the ransom and recommends reporting instances of fraud to the FBI at the Internet Crime Complaint Center.

US-CERT also recommends the following preventative measures for organizations to protect their systems:

- Employ a data backup and recovery plan for all critical information. Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Use application whitelisting to help prevent malicious software and unapproved programs from running. Application whitelisting is one of the best security strategies as it allows only specified programs to run, while blocking all others, including malicious software.
- Keep your operating system and software up-to-date with the latest patches. Vulnerable applications and operating systems are the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
- Maintain up-to-date anti-virus software, and scan all software downloaded from the internet prior to executing.
- Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
- Avoid enabling macros from email attachments. If a user opens the attachment and enables macros, embedded code will execute the malware on the machine. For enterprises or organizations, it may be best to block email messages with attachments from suspicious sources.
- Do not follow unsolicited Web links in emails.

Additional resources and links on these topics are provided in the alert.

Authors