eMazzanti Technologies Issues US-Cert Ransomware Warning

NYC area IT security consultant urges organizations to take preventative measures to guard against recent variants of ransomware

Hoboken, New Jersey -- (Cision) April 8, 2016 — eMazzanti Technologies, a NYC area IT consultant and MSP, issued a security warning today regarding threats to computer networks from recent ransomware variants. The warning was prompted by an alert from the Department of Homeland Security, US-CERT or United States Computer Emergency Readiness Team on March 31, 2016.

According to the US-Cert Alert (TA16-091A), "In early 2016, destructive ransomware variants such as Locky ransomware and Samas were observed infecting computers, which included healthcare facilities worldwide." eMazzanti is urging organizations to take preventative measures to ensure uninterrupted business operation and avoid the potential serious negative consequences of ransomware infections.

"Ransomware can cause significant downtime in addition to the loss of data," stated Almi Dumi, Project Lead, eMazzanti Technologies. "We urge our customers and others to take the necessary steps to prevent ransomware infections and mitigate their effects."

Here is the full text of the warning:

Ransomware Warning

eMazzanti Technologies wants to alert businesses and organizations to the increased threat of ransomware infection as has been stated by The United States Department of Homeland Security, in collaboration with the Canadian Cyber Incident Response Centre.

Infections can be devastating in their effects and recovery can be a difficult process. Organizations suffering a ransomware attack may require the services of an experienced data security and recovery professional.

US-CERT and eMazzanti recommend that users and administrators implement the following preventive measures to protect their computer networks from ransomware infection:

- Use a data backup and recovery plan for all critical and operational information. Perform and test backups regularly.
- Keep operating system and application software up-to-date with security patches.
- Maintain anti-virus software with current updates and scan all software downloads before running.
- Employ application whitelisting to prevent malicious software from running.
- Use permission settings to prevent users from installing and running unauthorized software, applying the principle of "Least Privilege" to all systems.
- Avoid enabling macros coming from email attachments. Block email messages with attachments from untrusted sources.
- Do not click links in unsolicited emails.

eMazzanti urges businesses and organizations experiencing a ransomware attack to work with qualified data security and data recovery professionals to minimize downtime and the loss of data. We discourage organizations and individuals from paying ransoms. Doing so does not guarantee the release of files.

eMazzanti's customers are advised that eCare network security solutions should detect and block ransomware. But, to avoid being victimized, do not open Word attachments in email unless you know the person you are receiving it from, or visit websites not known to be secure. Please let us know if you think you may be subject to a ransomware attack.

Additional Ransomware Information from US-Cert

Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. Ransomware variants often attempt to extort money from victims by displaying an on-screen alert. Users are told that unless a ransom is paid, access will not be restored.

Ransomware is often spread through phishing emails that contain malicious attachments or through visiting an infected website. Crypto ransomware, a malware variant that encrypts files has also been spread through social media, such as Web-based instant messaging applications.

The authors of ransomware instill fear and panic into their victims, causing them to click on a link or pay a ransom. Ransomware displays intimidating messages similar to, "All files on your computer have been encrypted. You must pay this ransom within 72 hours to regain access to your data."

Recent Variants

In early 2016, the Locky ransomware variant was observed infecting computers belonging to healthcare facilities. It spreads through spam emails that include compromised Microsoft Office documents or compressed attachments.

The destructive Samas ransomware variant was used to infect and damage healthcare facilities networks in 2016. Unlike Locky, Samas spreads through vulnerable web servers.

Impact

Businesses infected with Ransomware often suffer negative consequences, including:

- Disruption to operations, including sales and customer support
- Temporary or permanent loss of business-critical information
- Costs to restore systems and files
- Loss of reputation

Paying the ransom does not guarantee the release of encrypted files nor does decrypting files ensure the removal of the original malware. Systems infected with ransomware are often simultaneously infected with other malware.

Professional Help Available

New Internet threats surface regularly. eMazzanti's trained IT security experts are ready to help organizations deal with ransomware and other security issues. A security-first mindset and proactive approach is necessary to keep networks and assets safe in today's threat-rich IT environments.

Related resource information:

Employee Devices Bring Added Security Concerns

eMazzanti Technologies Issues DROWN Attack Warning

About eMazzanti Technologies

eMazzanti's team of trained, certified IT experts rapidly deliver cloud and mobile solutions, multi-site implementations, 24×7 outsourced network management, remote monitoring and support to increase productivity, data security and revenue growth for clients ranging from professional services firms to high-end global retailers.

eMazzanti has made the Inc. 5000 list six years running, is a 2015, 2013 and 2012 Microsoft Partner of the Year, and a 5X WatchGuard Partner of the Year. Contact: 1-866-362-9926, info@emazzanti.net or emazzanti.net Twitter: @emazzanti Facebook: Facebook.com/emazzantitechnologies.