

eMazzanti Technologies Issues Locky Ransomware Warning

NYC area IT security consultant warns customers and the public to take extra precautions to avoid data loss in light of new data security threat

Hoboken, New Jersey -- (Cision) February 26, 2016 — eMazzanti Technologies, a NYC area IT consultant and MSP, issued a warning today regarding a new ransomware virus that has infected hundreds of thousands of computer networks worldwide.

The company urges business and home computer users to take extra precautions to avoid being victimized by the malware threat, called Locky, that encrypts their data, holding it hostage until a ransom is paid.

"Locky is wreaking havoc across the net," stated Almi Dumi, Project Lead, eMazzanti Technologies. "We urge our customers and others to take the necessary steps to avoid losing data. We advise computer users not to open email attachments they are not expecting or from senders they do not recognize."

Here is the text of the warning:

Locky Ransomware Warning

"eMazzanti Technologies wants to bring to your attention a very serious threat that is infecting computer networks and spreading across the Internet.

There is a new ransomware strain out this week dubbed "Locky." The professional-grade malware enters a network as a Microsoft Word email attachment embedded with malicious macros, making it difficult for antivirus software to detect. When the Word document is opened, the content of the document appears scrambled and the user may see a message directing them to enable macros if the text is unreadable.

eMazzanti's eCare [network security solutions](#) should detect and block the virus in most cases, but to avoid being victimized, please do not open Word attachments in email unless you know the person you are receiving it from and are expecting an attachment. Especially do not enable Macros. Please let us know if you think you may be subject to this attack."



Additional Information about Locky

Locky encrypts data on an infected system using Advanced Encryption Standard (AES) encryption, and then leaves a blackmail letter (which is localized in several languages) asking for payment to get the data back. It also searches for any network share and encrypts data on those remote shares as well. A cloud backup may get infected as well when it synchronizes the encrypted files.

Currently, researchers have not found a way to decrypt files Locky has locked. It is estimated that Locky infects more than 100,000 systems per day.

In most cases, Locky arrives in an email that includes an Office document with a malicious macro. If the document is opened, it tries to infect the user's computer with the ransomware. Other variants sometimes arrive as a .zip file, which contains some malicious JavaScript. The emails are mainly fake invoices.

Analysis showed that 26 out of 55 AV scanners were able to detect Locky. eMazzanti utilizes the most advanced Gateway Anti-Virus (AV) solution in order to detect and prevent this particular variant from reaching customers.

eMazzanti further advises that malware changes and evolves quickly, which is why signature-based AV often can't keep up with the latest threats. To combat this problem, APT Blocker (Advanced Persistent Threat) is available as another layer of protection to detect brand new, never before seen malware files. Even if the file used to deliver Locky changes, its behaviors won't. That's why this solution can catch new threats that signatures might miss.

Another solution, HTTPS Deep Inspection has the ability to run [security scans on encrypted web traffic](#) to detect and block the virus despite an encrypted webmail connection. eMazzanti's solutions have several [features that can help prevent these various forms of ransomware](#). However, these protections only work if they are turned on and configured properly.

Related resource information:

[Employee Devices Bring Added Security Concerns](#)

[The best way to prepare for disasters and security breaches](#)

About eMazzanti Technologies

eMazzanti's team of trained, certified IT experts rapidly deliver cloud and mobile solutions, multi-site implementations, 24x7 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.

2015 | 2013 | 2012 Microsoft
Partner of the Year



Inc. 500 | 5000
2015 | 2014 | 2013 | 2012 | 2011 | 2010



ShoreTel Sky
Partner of the Year