Ransomware Called #1 Growing Security Threat on Manhattan Chamber of Commerce Program

eMazzanti Technologies CEO, Carl Mazzanti discusses nature and persistence of ransomware threat on blogtalkradio broadcast

Hoboken, New Jersey -- (Cision) June 24, 2016 — A NYC area IT security expert and eMazzanti Technologies CEO, Carl Mazzanti, discussed the topic of ransomware on a June 15, 2016 blogtalkradio business program sponsored by the Manhattan Chamber of Commerce, calling ransomware the number one growing security threat.

In the interview, Mazzanti discussed the nature and persistence of the ransomware threat. How infections occur and methods to prevent them, including education and IT security tools, were explained in response to questions asked by program host, Bruce Hurwitz. Anyone interested in the topic can listen to the recorded program online.

"Ransomware is the #1 growing IT security threat because people are making money," stated Mazzanti. "It's a business run by criminals who hold data hostage for money. They are smart enough to get some percentage of people to open a ransomware trigger."

Here are a number of relevant points that Mazzanti made during the program:

- Criminals almost always use a file as a trigger that may sit idle for long periods until activated. Antivirus products are not very effective against ransomware.
- Ransomware is often acquired through drive-by downloads from a website or by opening a harmless looking email attachment. The subject line might be something as simple as 'Invoice'. An accounts payable person may open the attachment because it's their job.
- When the trigger file is opened, it makes a call to open or download something else that encrypts data on the computer and requests the ransom.
- If the individual or organization doesn't have backups, they may be obliged to pay the ransom. Even when the infected machine is rebuilt using backup files, the trigger may still be sitting in the same infected file. Unless something changes, the file lock-up will happen again.

"People call eMazzanti after getting get hit. Then they're hit again a month or two later," related Mazzanti. "Even when the ransom is paid and the files are decrypted, that computer can turn into a dissemination point to other networks."

Mazzanti explained how 'sandboxing' is a way to determine which files are triggers. For example, WatchGuard Technology's Advanced Persistent Threat data security tool uploads and executes files in question and blocks or lets them pass through.

He also mentioned strategies for preventing ransomware infections:

- Educating users about ransomware is essential.
- Often, they can easily detect a malicious website by looking at the URL in the link.
- Users should look for misspelled names or poor link formatting.
- They should carefully check email addresses that tip off disguised or fraudulent messages.
- If they don't know the sender of an email, they should delete it.
- Employees should know who the business is contracting with and not open email attachments from others.
- There are a number of security tools that may or may not help prevent ransomware infections.

Responding to a question from host, Bruce Hurwitz, Mazzanti explained that everything connected to a network is a potential point of access for ransomware. A common way is through USB keys, often left on the sidewalk.

Pedestrians pick up the USB key and seem compelled to plug it into their computer to investigate. One company did a similar thing as a training exercise to show employees how they just compromised the system.

People handing out music CDs or DVDs are a simple dissemination point. "You'll see it with Times Square musicians who say, 'Take my CD,'" Mazzanti related. "Most people will take it. It's just a matter of time before they put it in their computer."

What to do if you are the victim of a ransomware attack:

- Call a data security professional for assistance.
- Contain the breach as quickly as possible.
- Recover to a state where you can operate.
- Put preventative measures in place as quickly as possible to prevent a repeat attack.

The program concluded with a warning that if an organization is hit by ransomware, there is a high probability that it will happen again. As long as there is a way that criminals can profit, they are a target.

Related Resources

[3 things businesses can learn about email security from the Panama Papers hack]

[eMazzanti to Show Legal IT Security, Compliance and Collaboration Solutions at NYC LegalTech Event]

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.