eMazzanti Technologies Issues Dark Web Sextortion Scam Warning

NYC area IT security consultant advises the public not to pay or fall for cyber-criminals' false sextortion scam threats

Hoboken, New Jersey -- (Cision) October 4, 2018 — eMazzanti Technologies, a NYC area IT security consultant and MSP, issued a warning today regarding an email "sextortion" scam based on stolen passwords obtained from the dark web. The company helps customers deal with this and numerous evolving cyber-security threats.

The advisory comes in response to increasing emails targeting computer users that threaten embarrassment and demand payment. The emails cite real user passwords purchased on the dark web as leverage to back their fictitious blackmail attempts.

"People are very concerned," stated Almi Dumi, CISO, eMazzanti Technologies. "We've received multiple calls from customers who feared it was a legitimate threat since the emails referred to valid credentials obtained on the dark web."

The sextortion scam email messages claim to have been sent from a hacker who has breached the recipient's computer and used its webcam to record a video of the victim visiting a porn website. The criminal threatens to email the video to the recipient's contacts unless they pay a substantial extortion fee, usually in Bitcoin.

Ignore the Sextortion Scam Email

eMazzanti urges customers to ignore threatening sextortion scam emails. A company cyber-security expert explained that criminals send large numbers of these fraudulent emails hoping to persuade a small percentage of victims to pay the sextortion fee based on their false claims. The company recommends these steps as a sensible response:

How to Respond to a Sextortion Email
- Don't reply to the email or click any links.
- Ignore and delete the email immediately.
- Do not pay the extortion fee.
- Reach out to eMazzanti Technologies for dark web ID protection.
- Inform the FBI if you want to help catch the criminals.

(The FBI recommends reporting any scams like these to IC3.gov, the FBI's Internet Crime Complaint Center.)

Dark Web Search

Sextortion scam criminals use stolen passwords to add credibility to their threats. These passwords are usually purchased on the dark web from hackers who obtained them in numerous recent security breaches. If an individual's information has been stolen in a past breach, they may be more vulnerable to this type of attack.

eMazzanti Technologies offers services related to Dark Web identity protection. In addition to performing a thorough dark web search and domain monitoring, the company goes a step further and provides assistance with remediation and improving its clients' security posture.

Avoid Becoming a Sextortion Scam Victim

eMazzanti recommends these steps to avoid falling prey to sextortion scams and other cyber-security threats:
- Check if personal information is being sold on the Dark Web from past security breaches.
- Cover the camera lens and disable the microphone on computers when not in use.
- Change passwords regularly.
- Use two-factor authentication.
- Subscribe to security announcements.

Boost Cyber-security Awareness

Security awareness is very important and the responsibility of everyone. eMazzanti urges business leaders to make this information available to ALL employees. In addition, they should test the organization's security posture regularly. Information security threats evolve quickly, so should the organization's controls and cyber-security awareness.

Keeping up with threats to sensitive data requires that individuals and organizations stay vigilant. Accordingly, anyone charged with data security who is unsure about what to do may call the IT security professionals at eMazzanti Technologies

Related resource information:

Staying Safe in the Shadow of the Dark Web

The dark web: What your business needs to know

About eMazzanti Technologies

eMazzanti's team of trained, certified IT experts rapidly deliver increased revenue growth, data security and productivity for clients ranging from law firms to high-end global retailers, expertly providing advanced retail and payment technology, digital marketing services, cloud and mobile solutions, multi-site implementations, 24×7 outsourced network management, remote monitoring and support.

eMazzanti has made the Inc. 5000 list eight consecutive years, is a 2015, 2013 and 2012 Microsoft Partner of the Year, 2016 NJ Business of the Year, 5X WatchGuard Partner of the Year and one of the TOP 200 U.S. Microsoft Partners! Contact: 1-866-362-9926, info@emazzanti.net or http://www.emazzanti.net Twitter: @emazzanti Facebook: Facebook.com/emazzantitechnologies.