Data Privacy Detective Podcast – Episode 56: Ransomware and Privacy

Nov 05, 2020

Categories:

Blogs
Podcast
Technology Blog

Authors:

Joseph J. Dehner

Ransomware – a sinister type of cyberattack that installs malware onto a computer system. Once inside a network, the malware encrypts documents, freezing the IT systems of entities and individuals until they pay ransom to regain access to their data. Recent average cost paid to a ransomware syndicate? $333,000, according to Greg Edwards, founder and CEO of CryptoStopper, a leading anti-ransom software provider.

Ransomware surfaced in the late 1980s when the AIDS Trojan was injected through floppy disks. Victims were asked to pay a "license fee" of $189 to a post office box to restore access to their data. Ransomware became ever-more sophisticated. Thanks to Bitcoin and other cryptocurrencies that emerged around 2012, thieves could hide their identity, and attacks mushroomed. Most start through a careless employee who gets phished and permits the villain to enter the enterprise's system. Malware is unleashed to encrypt data, including on back-up copies held within the enterprise.

Ransomware attacks in 2020 show a continuing growth in number and cost. Fileless ransomware appeared, far more likely to succeed than file-based attacks. Smart ransomware disguises itself as though it were Halloween, but it's all trick and no treat. Major 2020 targets are healthcare systems, which cannot risk their patients' health and are pressured to pay substantial ransom to release a freeze of critical data. Cybercriminals now offer Ransomware-as-a-Service, available as kits sold on the dark web that includes everything needed to get into the business of kidnapping data.

Greg Edwards' company CryptoStopper uses detection technology to trick the ransomware code to fix on it as bait, blocking the infection before it spreads. Watcher files defend against attacks. Most clients are B2B, but the company offers a free of charge download to individuals.

When ransomware criminals focused only on encrypting and decrypting data once they were paid, the privacy of data was relatively untouched. This has changed. Now ransomware attackers profit not only from ransom payments but also engage in exfiltration. They acquire and package data for sale on the dark web. Exfiltration releases company and personal data to use by criminals who purchase it for sinister purposes.

Can law enforcement come to the rescue? Occasionally, but most attackers are from areas beyond the reach of Interpol and extradition treaties.

How can enterprises defend and avoid having data breached and resold? Anti-ransomware products are available. Top tips from Greg Edwards to deal with the risk of ransomware beyond an add-on like his company's offering:

- Patch management – update all software and operating system of all devices on a network.
- Keep anti-virus software up to date.
- Keep back-ups in off-site locations.

FBT Gibbons