cooley.com

FTC: Beware of Ransomware

Cooley Alert

September 22, 2016

Earlier this month the Federal Trade Commission ("FTC") held a workshop on ransomware, and will soon release guidance to businesses on how to mitigate the risk of a ransomware attack. In this client alert, we will explain ransomware in practical terms and provide highlights from the FTC's workshop. In a future alert, we will detail the forthcoming FTC guidance.

What is ransomware?

Ransomware is a form of malware that hackers are able to install on computers of victims and denies the users from accessing their data, typically by encrypting it. Once the data is encrypted, the hacker responsible for the attack notifies the user that in order to regain access to the data, a ransom must be paid- often in the form of cryptocurrency, such as Bitcoin. Alternatively, instead of blocking access, sometimes hackers move the data to external locations or destroy or alter it.

How do hackers infiltrate user networks with ransomware?

One common way in which ransomware infiltrates computers is via spear-phishing email, which is email that appears to be from someone the user knows, but isn't. Rather it is from the hacker, and contains an innocent-looking link or attachment that the user unknowingly opens, enabling the ransomware hijack. A second, and growing, method of delivering malware is via "malvertising"- malicious advertising links on websites that are trusted and clicked by the user. A third and very recent style of malware that is more insidious than the other two relies on network insecurities to penetrate the network rather than mistakes by individual users. This means two things. First, the attacker can penetrate multiple machines, not just the one machine of the individual user. Second, the attacker can deposit malware on servers, which can be much more devastating than on individual machines.

How big of a problem is ransomware?

As FTC Chairwoman Edith Ramirez pointed out, ransomware is "the most profitable malware scam in history." Moreover, the incidence of ransomware attacks is skyrocketing: there have been an estimated 4,000 attacks per day in 2016, a 300% increase from 2015.

Who is likely to be a target of a ransomware hacker?

Anyone can be a target of a ransomware attack. Some examples of organizations that have been targeted by ransomware hackers include commercial companies and ecommerce providers, who

often are inclined to pay quickly in order to get their network back up and running. Other examples include hospitals, universities, and even police departments (some of which have actually paid the ransom).

How does the FTC come into play?

The FTC currently brings enforcement actions under Section 5 of the FTC Act against companies that engage in what the FTC views as unfair or deceptive trade practices by failing to use "reasonable security measures" to reduce the risk of data breaches caused by malware. While the details of the upcoming FTC guidance are still unknown, Chairwoman Ramirez made clear that the FTC would continue to emphasize its focus on good cybersecurity, and this would now include ensuring that businesses responsibly protect their computer systems from ransomware attacks. "A company's unreasonable failure to patch vulnerabilities known to be exploited by ransomware might violate the FTC Act," she warned.

How have other regulatory agencies addressed ransomware?

In July, the Department of Health and Human Services' Office for Civil Rights (HHS OCR) set forth ransomware guidance for entities subject to HIPAA, and announced that ransomware attacks will be presumed to be data breaches (under the theory that the hackers have somehow acquired the data by taking possession or control over it), potentially triggering HIPAA's breach notification requirements. Under the breach notification laws of certain states

(including New Jersey, Connecticut, Florida, Louisiana, and Kansas) *unauthorized access* to personal information constitutes a breach, even if the data accessed was not truly obtained by the hacker.

What can be done to avoid ransomware attacks?

At the FTC's workshop, panelists recommended techniques to mitigate the risks of ransomware attacks that included:

- Deploying current antivirus tools
- Educating and training users about good cybersecurity practices. For example, not opening suspicious or unanticipated email attachments, not enabling office macros for unknown documents, and not visiting websites known for containing malicious software.
- Patching and updating software
- Maintaining frequent backups of essential data and correcting periodic test restorations
- Storing backups on media not connected to the network to stop ransomware from infecting the backups
- Conducting annual penetration and vulnerability testing

What can an organization do if it is infected by a ransomware attack?

While there is no single best response, here are some good ideas:

- Notify the FBI, which does not recommend paying the ransom (since doing so encourages further extortion attempts) but will work with your organization

- When deciding whether to pay, consider that paying the ransom doesn't always mean that your data will be decrypted or returned: the hacker may simply not do it, may demand more money, or may try to decrypt the data and fail

- Notify your cyber-liability insurer to ensure applicable coverage and to receive guidance

- Investigate the incident pursuant to your security incident response plan

- Notify HHS OCR if it regulates your business

- Consult legal counsel to ensure compliance with applicable state and federal privacy laws (for example, HIPAA disclosure and breach notification requirements)

Stay tuned for a follow-up alert when the FTC issues its guidance. Also, join us in our Palo Alto office on October 19 for the First Annual Cooley Cybersecurity Colloquium where one of panels will be "My Entire Network Just Got Encrypted!: Ransomware and Bitcoin Explained, with Avoidance Strategies."