WILMERHALE

Ransomware Prevention Highlighted at FTC Technology Workshop

SEPTEMBER 9, 2016

The Federal Trade Commission kicked-off its series of fall technology events with an afternoon workshop exploring ransomware on Wednesday, September 7. While malicious computer code is nothing new, infiltrating computer systems and then encrypting them to hold data hostage until users pay-up has become an especially appealing criminal enterprise. Ransomware has hit everything from police departments to major medical centers, and according to FTC Chairwoman Edith Ramirez, the threat has become "the most profitable malware scam in history" and is "increasing at an alarming rate." As a representative from the FBI's Cyber Division would warn, success is breeding success.

Chairwoman Ramirez hoped that the workshop would increase awareness of the ransomware threat among consumers and businesses alike. She reiterated that the FTC's privacy and data security enforcement agenda stresses the importance of good cyber hygiene, as well as addressing vulnerabilities as they arise. "A company's unreasonable failure to patch vulnerabilities known to be exploited by ransomware might violate the FTC Act," she cautioned.

The Importance of Backups and Basic Cyber Hygiene

FTC staff focused on what other preparation industry could engage in to protect consumers and businesses. The common refrain was that basic cyber hygiene could largely eliminate the threat of ransomware upfront. Organizations were encouraged to communicate with vendors about ransomware and to stay abreast of guidance from organizations such as NIST and SANS.

Employee training was also identified as key. End users, both average consumers and employees, are repeatedly fooled by the same social engineering spear-phishing attacks. Basic guidance such as not opening unexpected and suspicious email should continue to be drilled into users. FTC Chief Technologist Lorrie Cranor noted efforts have been made to train individuals to avoid malware for over fifteen years, but the visual threat of ransomware may finally scare end users into better practices.

Another way to mitigate the threat posed by ransomware is to inventory and regularly backup essential information. Panelists encouraged both businesses and consumers to think carefully

about:

- Performing backups on a routine schedule;
- Ensuring backups are not connected or otherwise accessible to your system;
- Recognizing that not everything needs to be backed up; and
- Understanding the relative importance of certain types of information and what sort of business or activities would be interrupted by ransomware.

However, panelists cautioned that even backups may not be a "complete panacea," as ransomware evolves to go after backups or otherwise disrupt the ability to recover data.

Putting "Malvertising" on Ad Tech's Radar

While spear-phishing—or personalized emails sent by bad actors—is the primary vector through which ransomware infiltrates computers, malicious advertising campaigns, or "malvertising," were singled out as a growing threat to average consumers. Panelists at the workshop suggested that malvertising may rapidly work to undermine user trust by taking advantage of recognizable websites to deliver infected advertising that redirects users to malicious servers.

FTC staff were especially interested in what legitimate players in the advertising ecosystem could do to protect consumers. Ideas to address malvertising included:

- Networks should implement vetting processes to ensure ads come from trusted sources;
- Links on advertisements should be followed to ensure they come from trusted sources. For example, advertisements for American products likely should not be served from Eastern European servers;
- Ad exchanges should limit ways advertisements can trade places for varying amounts of money; and
- A formal ad certification system should be implemented.

To Pay or Not to Pay, At Least Provide Information to Law Enforcement

The workshop concluded with a conversation of what an organization should do once it is infected by ransomware. Will Bales from the FBI's Cyber Division strongly encouraged companies and individuals not to pay up. He argued that doing so only fuels the growth of ransomware and may make a victim out to be an easy mark for a second pass.

However, there was also recognition by FTC staff and panelists that ransomware has developed into an established, if illicit business model. Engaging with ransomware attackers is increasingly a path many organizations take, but caution was urged. Even Bales acknowledged that the FBI was "sympathetic" to organizations that pay off ransomware, and he made a plea that anyone affected by ransomware should contact law enforcement regardless of the circumstances.

While recognizing that companies may be leery of the potential publicity or inconvenience of reporting an attack, the FBI's representative said that its goal is not to make headlines or otherwise make things worse for a ransomware victim. Panelists noted that anonymous information such as information about where payment is made (for example, a Bitcoin wallet address) and hashed

samples of the malware can be invaluable to law enforcement's ongoing cyber investigations.

With the spate of ransomware incidents now averaging 4,000 per day, businesses and their information security officials must have keep the threat of ransomware in mind. Indeed, according to Chairwoman Ramirez, industry will play a critical role in addressing the threat and adequately protecting consumers' information.