FORTALICECLIENTADVISORY

The Threat of Ransomware

Updated October 2019

Fortalice

Fortalice

Executive Summary

Ransomware: What is it?

A new brand of security disaster has threatened the cyber world. Ransomware, an opportunistic brand of malware, has become an extraordinary threat to U.S. businesses and individuals over the course of the last few years.

In 2017, a ransomware attack on FedEx's Dutch units cut its' profit by 79 cents per share, leaving a negative financial impact on the company almost 40 times worse than that of Hurricane Harvey[i]. Between July 2015 and July 2016, researchers found that 133 healthcare organizations, 115 finance organizations, and 67 government organizations (including law enforcement groups and federal agencies) had ransomware on their corporate networks.[ii]

Recently, some variants of the malware have expanded to include data exfiltration, participation in Denial of Service attacks (DDoS), and anti-detection components[iii]. Others now target smart phones and other personal Internet of Things (IoT) devices.

Unfortunately, human error – such as clicking on a link embedded in a phishing e-mail or browsing an infected site – is most commonly to blame for the infiltration of ransomware into systems. Victims are generally chosen at random and risk losing far more than data in the event of an attack: they may experience financial loss as a result of paying ransoms and legal fees, hiring third-party experts, lost productivity, etc. On average, ransomware creators earned profits of $1,077 per victim in 2017 – a 266% increase from 2015, when authors only profited about $295 per victim.[iv]

HOW DOES IT WORK?

In a ransomware attack, data on the victim's computer is locked, typically by encryption. The threat actor then requires a ransom – usually in the form of bitcoin, or some other form of virtual currency, to maintain anonymity on behalf of the hacker. Unlike other types of hack attacks, victims are usually made aware of the breach by the hackers themselves, and informed their files will only be unlocked and decrypted when the described fee is paid. Upon receiving payment, the attacker typically provides a key which should decrypt the user's files.

FOR EXAMPLE…

In 2017, a large, global malware attack affected multiple organizations around the world. The ransomware named "WannaCry" was a malicious code introduced to networks via a phishing email which contained a Word attachment with an encrypted archive. Developers of the ransomware were able to use a tool developed by a National Security Agency to exploit vulnerabilities in Microsoft Windows XP.

WannaCry infected more than 200,000 computers worldwide[v]. The American software Symantec observed 22 million attempts to infect machines and, at one point, was blocking a whopping 200k attacks per hour[vi]. Once opened, the ransomware spread quickly and typically demanded ransoms of around $300 bitcoin[vii]. Total overall losses were estimated to be in the billions, making it one of the most damaging incidents involving ransomware to ever occur. Shockingly, this incident could have been largely prevented: a solution to fix the vulnerability had previously been released by Microsoft, however, most organizations opted out of updating their systems.

TIPS

1. Backup Data

Ransomware attacks prey on the unfortunate fact that many individuals and organizations neglect to backup websites and data, so if it becomes encrypted and held for ransom, the victim is at the mercy of the attacker. Having backups gives the

victim an opportunity to restore the data that has been encrypted without having to pay the ransom or running the risk of having corrupted data returned to them after decryption.

2. Don't pay the ransom

Paying the ransom only provides more incentive for these types of attacks. Also, even if you pay the ransom, there is no guarantee your files will come back undamaged, if at all. One-in-five businesses did not get their data back after financially complying with hackers.[viii]

3. Contact No More Ransom

The FBI at IC3.gov or the Europol project may actually have the key to unlock your files. Both are a free service to you. Law enforcement and security researchers have joined forces to help people who have been attacked by ransomware get their data back from criminals without paying a dime. The Europol project is called the No More Ransom initiative and the website has links to decryption codes for a number of various ransomware strains. They have helped over 200,000 ransomware victims recover their files.

4. Train employees

Make sure staff is thoroughly trained to avoid pitfalls like falling prey to social engineering, or phishing e-mails, and urge them to avoid clicking unknown links or visiting unknown websites. Let them know the importance of reporting suspicious e-mails as soon as possible, as well as who said emails should be reported to.

5. Be cautious with personal information

Never provide sensitive data via text, e-mail or any other form of electronic messaging, and be wary of unsolicited phone calls.

6. Keep systems patched

Ensure you've patched all systems in your network, including all mobile devices, software, operating systems and applications, including cloud locations and content management systems (CMS).

7. Segment networks

Organize and separate data to limit the amount of data a ransomware attack will be able to access, in the event of a breach.

8. Monitor third parties

Vet who has access to your company's network and ensure third parties are vigilant in keeping up with the best cybersecurity practices. Restrict access to common ransomware entry points, like personal e-mail and social media accounts.

Scary Headlines from 2019

McAfee: “Ransomware Attacks Double in 2019”

ZDNet: “Over 500 US schools were hit by ransomware in 2019”

Cybercrime Magazine: “Cybersecurity Ventures predicts that there will be a ransomware attack on businesses every 14 seconds by the end of 2019, and every 11 seconds by 2021. This does not include attacks on individuals, which occurs even more frequently than businesses.”

9. Use reliable anti-virus software and a firewall

Maintain a fortified firewall and enlist a well-known, proven, and current security software.

10. Use a VPN

When accessing public Wi-Fi, always use a virtual private network (VPN). This prevents other malicious actors on the same network from gaining access to your information and/or credentials.

CONTACT FORTALICE

Contact Fortalice

Fortalice Solutions, LLC. remains the cybersecurity and intelligence operations expert companies and people turn to regarding efforts to strengthen their privacy and cybersecurity. If you'd like to step up your cybersecurity defenses or need help complying with existing or future regulations, give us a call. We are highly skilled in disaster planning and recovery, incident response exercises and cyber risk assessment and we are standing by to aid you and your team.

Contact:
Watchmen@FortaliceSolutions.com
Or call our offices at 877.487.8160 and anyone on the Fortalice team can help.

[i] https://www.insurancejournal.com/news/national/2017/09/20/464842.htm
[ii] https://info.bitsighttech.com/bitsight-insights-ransomware
[iii] https://www.cisecurity.org/ransomware-facts-threats-and-countermeasures/
[iv] https://www.symantec.com/about/newsroom/press-kits/istr-22?om_ext_cid=biz_social_pr_vanity-istr22-press-kit
[v] https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/
[vi] https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/
[vii] https://securelist.com/kaspersky-security-bulletin-2016-story-of-the-year/76757/