TDCI’S SECURITIES DIVISION ISSUES CYBERSECURITY INVESTMENT ADVISER REGISTRANT ALERT: RANSOMWARE

On March 31, 2016, the U.S. Department of Homeland Security, in collaboration with the Canadian Cyber Incident Response Centre, issued a joint alert on ransomware.¹ Less than one month later, anti-malware maker Enigma Software reported that April 2016 was the “worst month for ransomware on record in the U.S.”² In an effort to increase awareness to this ever-growing cybersecurity threat, the Tennessee Securities Division issues this Cybersecurity Alert on ransomware.

What is Ransomware?

According to the U.S. Computer Emergency Readiness Team (“US-CERT”), ransomware is a specific type of malicious program (i.e., a virus) where the victim’s computer, network, and/or files become strongly encrypted to the point they are effectively rendered useless. Shortly after the victim realizes what happened, the victim typically receives a message demanding a ransom in exchange for restoring access to the affected systems.

How is Ransomware Spread?

According to US-CERT, ransomware can be spread through e-mails that contain the malicious program or contain links to an infected website, or through messages or links sent through social media; however, in some recent variants, ransomware is spread by means of a “drive-by download attack,” which occurs when an attacker covertly “injects” an ordinary website—usually a trusted or popular website—with malicious code, which, in turn, is downloaded and installed on unsuspecting visitors’ computers. An October 2014 article in SecurityWeek magazine explains that many drive-by download attacks target users running out-of-date or older versions of common software programs; users who fail to promptly install the most current security patches also can easily fall victim to this method of attack.³

Impact

According to Kaspersky Lab, cybersecurity experts found that in 2015, one in three business computers were exposed at least once to an internet-based attack; during that same timeframe, more than 50,000 corporate machines fell victim to ransomware attacks.⁴ Businesses, however, haven’t been the only target. According to the FBI, victims have included hospitals, school

---

² Enigma Software, “April 2016 was the Worst Month for Ransomware on Record in the US” http://www.enigmasoftware.com/april-2016-worst-month-ransomware-record-us/
districts, state and local governments, and law enforcement agencies. In short, anyone with a computer and internet access could potentially become the next victim of a ransomware attack.

**Solutions**

Enigma Software and US-CERT provided recommendations to help minimize the impacts of a ransomware attack, including:

1. **Backup** your data regularly to an external device that isn’t regularly connected to the network. Keep in mind that ransomware will target anything connected to an infected computer or network; unless the computer or network has been completely wiped clean of any trace of the malicious program, the ransomware will easily spread to any device connected, even after infection.

2. **Update** your software. Keep your operating system and software up-to-date with all the latest patches, especially critical security patches.

3. **Maintain** up-to-date anti-virus software, and ensure virus updates are downloaded automatically.

4. **Think** before you click. Do not click on unfamiliar links sent in unsolicited messages or e-mails: social media accounts can be hijacked, and e-mails can be spoofed, so even a trusted sender could really be a wolf in sheep’s clothing.

5. **Contact** your local FBI field office immediately if you become the victim of a ransomware attack. Do NOT pay the ransom. According to the FBI, paying a ransom does not guarantee you will regain access to your data; in a number of instances, individuals who paid the ransom were never provided with decryption keys.

More than anything, have a plan. There are a number of resources on ransomware that contain useful considerations for both before and after a ransomware attack. While there is no certain way to protect against ransomware attacks, preventative preparation has the potential to mitigate impact.

---
