OHIO DIVISION OF SECURITIES
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 Ohio Division of Securities 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 An October 2014 article in *SecurityWeek* magazine explains that many drive-by download attacks target users running out-of-date or older versions of common software programs; users who fail to promptly install the most current security patches also can easily fall victim to this method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

---

[1] US-CERT Alert TA16-091A, "Ransomware and Recent Variants" https://www.us-cert.gov/ncas/alerts/TA16-091A
[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/
[3] Security Week, "The Internet's Big Threat: Drive-by Attacks" http://www.securityweek.com/internets-big-threat-drive-attacks
[4] Kaspersky Lab, "Kaspersky Lab on Business Threats: 2015 Saw the Number of Cryptolocker Attacks Double" http://www.kaspersky.com/about/news/virus/2015/Kaspersky-Lab-on-business-threats-2015-saw-the-number-of-cryptolocker-attacks-double

districts, state and local governments, and law enforcement agencies.[5] 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 – Cincinnati Office (513) 421-4310 or Cleveland Office (216) 522-1400 – 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.[6] While there is no certain way to protect against ransomware attacks, preventative preparation has the potential to mitigate impact.

---

[5] FBI, "Incidents of Ransomware on the Rise" https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise.

[6] Department of Homeland Security United States Computer Emergency Readiness Team, "Ransomware" https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf.

INCIDENT RESPONSE PLAN: RESOURCE 2016

Maintaining an actionable incident response plan is an integral part of cybersecurity preparedness. Creating the plan ahead of time is helpful in two ways. First, it will help you and your company make more informed decisions under the stress of a cyberattack and, second, it will almost certainly allow you to respond much faster. Speed can be of critical importance at the time of an attack. For example, in certain limited instances, law enforcement has been able to reverse a wire transfer when a company realizes quickly enough that it has wired money to a scam artist rather than to its customer.

The U.S. Department of Justice released a best practices document on the subject of responding to a cybersecurity attack. It was drafted with smaller, less-resourced organizations in mind and includes a Cyber Incident Preparedness Checklist at the end. Generally speaking, this document advises creating specific concrete procedures including, at a minimum:

- Who has lead responsibility for different elements of an organization's cyber incident response, from decisions about public communications, to information technology access, to implementation of security measures, to resolving legal questions;
- How to contact critical personnel at any time;
- How to proceed if critical personnel is unreachable and who will serve as back-up;
- What mission-critical data, networks, or services should be prioritized for the greatest protection;
- How to preserve data related to the intrusion in a forensically sound manner;
- What criteria will be used to ascertain whether data owners, customers, or partner companies should be notified if their data or data affecting their networks is stolen; and
- Procedures for notifying law enforcement and/or computer incident-reporting organizations.[7]

An example of an incident-reporting organization focused on the financial services sector is the Financial Services Information Sharing and Analysis Center (FS-ISAC). Membership in the FS-ISAC gives firms access to risk alerts and can help firms develop cybersecurity knowledge and best practices. The FS-ISAC website is available at www.fsisac.com.

Further, having a pre-existing relationship with someone at the FBI or the U.S. Secret Service, which are the principle federal agencies responsible for conducting criminal cybersecurity investigations, will speed up making such a report and potentially result in information sharing on a local level. The FBI conducts outreach to likely targets through its InfraGard chapters and Cyber Task Forces in its 56 field offices, and the Secret Service conducts outreach through its Electronic Crimes Task Forces.

---

[7] To review the full, 13-page report, see http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf.

Ohio InfraGard Chapters:

- Central Ohio Members Alliance - http://cmhinfragard.org/
- Cincinnati Members Alliance - http://infragardcincinnati.org
- Dayton Members Alliance - http://infragard.dayton.oh.us/
- Northern Ohio Members Alliance - http://nocinfragard.org/
- Toledo Members Alliance - http://www.toledoinfragard.org/

In addition to maintaining an actionable incident response plan, you should regularly test and update the plan. Testing the plan can locate deficiencies and/or potential breaches. Testing also provides the firm and the employees a level of comfort in knowing what steps to take when an incident occurs.

An incident response plan is an important element, but only an element, of a comprehensive cybersecurity program. Creating, implementing, and testing an incident response plan is no substitute for identifying the personally identifiable information and other private information you have, implementing safeguards to protect it, and implementing policies and procedures to ensure that these safeguards are incorporated into a firm's culture of compliance. However, thinking through how to react before an attack occurs will dramatically improve your ability to respond quickly and appropriately to an attack.