RANSOMWARE RESOURCE GUIDE FOR LAW ENFORCEMENT

Part One: Ransomware Explained and Why You are a Target

What is ransomware?

Ransomware is a type of malicious software that locks your electronic device and prevents you from accessing your data unless a fee is paid. Ransomware usually comes in two forms. The first type of ransomware is known as "locker ransomware." Just like it sounds, locker ransomware locks (also known as "encrypts") your electronic device's complete hard drive, which essentially locks you out of your entire system. The second type of ransomware is called "crypto ransomware" and only locks certain important files on your electronic device like spreadsheets, word documents, or photos.

Ransomware can be set to:

- Automatically delete files
- Travel your network infecting other machines
- Hide out in your backups
- Publish files to the Internet
- Provide your data to a competitor who will pay the fee; and more

Just like it sounds, ransomware provides users with a "take it or leave it" decision: either pay the fee and recover your important data, or don't pay the ransom and permanently lose your information. In fact, ransomware is built to automatically delete computer files in the event that a ransom is not paid, which leaves victims with only a small amount of time to try to fix the problem through alternate means. Further, even if you pay the ransom, there is no guarantee you will be allowed to have access to your files again.

As evidenced by recent high-profile ransomware attacks against the cities of Atlanta and Baltimore, government entities are increasingly being targeted by cybercriminals. Atlanta's ransomware incident has cost the city $2.6 million dollars to fix. The attack is thought to be the most extensive government ransomware attack to date and caused city systems such as utility bill payment and court information portals to remain offline for several days. In Baltimore, cybercriminals used ransomware to lock up portions of the city's 9-1-1 dispatching system, forcing the city to manually handle emergency calls for a seventeen hour period.

How is ransomware distributed?

Cybercriminals most often use phishing emails or exploit kits to place ransomware on your electronic device.

In a phishing email, cybercriminals use "bait" that is usually in the form of what appears to be either a legitimate website link or valid attachment such as a word document or spreadsheet. However, the links or attachments actually deliver malicious software that infects your electronic

device with ransomware. Plus, since the "bait" is usually sent via email, it is difficult for security software to filter out potentially harmful messages.

An exploit kit is an automated malicious tool that searches for security vulnerabilities in electronic devices that not have been updated (also known as "patched."). After the exploit kit locates the security weakness, the cybercriminal can then deliver ransomware to the device.

Why are law enforcement agencies a target?

Law enforcement agencies are targets for ransomware attacks because of cybercriminals' desire for profit, retaliation, and notoriety.

- Profit. Cybercrime is a profitable business and there is a large market for information that is held on law enforcement computer systems such as case files and personnel records. Most often, ransomware attackers will require payments to be made in some sort of digital currency. The most popular digital currency is Bitcoin and as of early June 2018, the value of one Bitcoin was over $7,600.00. Thus, receiving even only a single Bitcoin is a sufficient reward for cybercriminals to continue ransomware attacks.

- Retaliation. Cybercriminals could attempt to deliver ransomware to a law enforcement agency's systems as retaliation for day-to-day law enforcement work such as investigations or verdicts that result in criminal convictions. At the same time, witnesses or suspects connected to controversial cases could target law enforcement agencies. Finally, disgruntled former or current employees may turn to ransomware as a way to retaliate against their prior or present employers as well.

- Notoriety. Successfully executing a ransomware attack against a law enforcement entity can provide individuals or groups with notoriety and credibility in the cybercriminal community. Moreover, news media coverage and social media mentions are very enticing to cybercriminals.

Part Two: How to Protect Yourself and Your Agency

The ransomware threat is continually evolving and as a result, law enforcement entities must be proactive and continually work on your cyber defense. However, there are several simple ways to help protect you and your agency from ransomware attacks:

- Educate Your Personnel - Make your coworkers aware of the ransomware threat: How often does law enforcement tell the public to report suspicious activity. End users are the primary source for an easy entry to your systems and data; your users knowing what to look for and how to react to well-crafted emails will provide a layer of defense.

  Human behavior can be the weakest link in your efforts to improve your agency's cyber security posture. Therefore, educating employees can go a long way to secure your agency against ransomware attacks. Examples include:

  - Provide information and create awareness to keep up with the latest ransomware trends.
  - Require regular cybersecurity trainings for your agency.
  - Train employees to identify and report suspicious and questionable links.
  - Implement a plan with IT and ensure employees understand the plan.

- Proactive measures are the best defense:

  - Regular user training for your staff reinforcing good digital habits, and current threats.
  - Leverage SPAM filters that sort out suspicious content
  - Actively scan email for malicious content
  - Leverage a firewall to block known bad hosts
  - Patch systems to prevent "known" vulnerabilities that leave your systems open
  - Deploy end point protection for all devices accessing your network (desktop, laptop, tablet. Cellular, etc.)
  - Only give users the minimum level of permissions on the system needed to do their work
  - Disable macros
  - Only allow applications to be installed by authorized technology personnel
  - Actively monitor network traffic and file access

- Have a back-up strategy: Backing up your data and device configurations is still the single most important defense against ransomware. Back-ups need to be checked regularly and need to have a well thought-out cycle to ensure a clean back can be used with an acceptable loss of data, should the infection get into the back-up system.

- Keep your operating system and software programs are updated: Develop a patching and maintenance strategy to keep your systems protected from common vulnerabilities that would allow your systems to be exploited.

    - Inventory hardware and software, don't forget the supporting applications like Java, .NET Framework, etc. that need to be patched as well.
    - Work with your technology staff and vendors to ensure updates don't disrupt critical system functions.
    - Schedule regular maintenance windows to keep systems safeguarded.

- Utilize up-to-date end point protection software. This application will be installed on all desktops, laptops, tablets, servers, etc. on your network to scan for and protect from malware and unauthorized intrusions. This applications should be set to stay current with the vendor's rules and definitions that protect your systems.
- Before clicking, verify links found in emails, text messages, or multimedia messages.
- Limit employee access to information. You will want to make sure all persons at your office have individual user accounts that they use whenever they log in and out of your network. At the same time, employees should only have access to the information that they need to perform their day-to-day duties.
- Never share account information or passwords.
- Create an incident response plan. An incident response (also known as "IR") plan is a written document that explains the steps you will take in the aftermath of a cyberattack. The purpose of an IR plan is to allow you to handle the situation in a fashion that limits damage and cuts down the costs and time period needed to recover. Your IR plan should include items like persons' roles in the event of an attack, a communications strategy, the IT experts you are going to call, etc.
    - One of the calls you need to make is to the OHLEG HelpDesk enabling us to take certain precautions to protect OHLEG and the other Law Enforcement users.

Part Three: What to do if You are Infected with Ransomware

Have an established response plan, every organization and situation will be different. There is no one size fits all solution but the core processes to consider are:

1. Preparation - have a rehearsed plan so key personnel know what to do. Keep the plan up to date as systems and personnel change.
2. Detection and analysis – something gives rise for concern, determine specifics of the incident and the type of malware
3. Containment, eradication and recovery

a. Isolate the infected computer or computers immediately. Infected computers should be disconnected from your network as soon as possible to prevent the ransomware attack to spreading to other parts of the network or your shared drives.

b. Isolate or power-off affected devices that have not been fully taken over by ransomware. This may allow more time to recover your information, contain damage that has already occurred, and prevent damage from getting worse.

c. Immediately secure your backups by taking them offline. Remove any physical backups that are connected to your devices and make sure that any cloud backups are isolated from your system. Also, make sure that any backups do not contain malware before you reconnect them to your system.

d. Change passwords. Change all of your account and network passwords once the infected device or devices have been removed from your network. Furthermore, once the ransomware is removed from your device, change all of your device passwords as well.

e. Contact the FBI or U.S. Secret Service immediately upon discovering a ransomware attack and ask for help.

f. Contact the OHLEG Help Desk to notify of the attack

4. Post-incident – Evaluate the effectiveness of the plan and response to correct any deficiencies.

Additionally, the Attorney General's CyberOhio Initiative offers free presentations for law enforcement officers to learn more about cybersecurity. Email cyberohio@ohioattorneygeneral.gov or call (614) 466-8831and ask to speak to either Greg Tapocsi or Nick Smith to learn more.