The Rise of Ransomware

Can Law Enforcement Just Ignore It?

Some Ignored the Threat and Paid a Price

Evidence Lost, Files Compromised
In January of 2017 the Cockrell Hill Police Department, located southwest of Dallas, had to admit to losing digital evidence from as far back as 2009 after the department's server was compromised with ransomware. All Microsoft Office Suite documents and significant amounts of bodycam video, photos, in-car video and surveillance video were lost. The malware had been introduced onto the network from a spam email that had come from a cloned email address imitating a department-issued email address.

The ransom demand was nearly $4,000 and paying was no guarantee the decryption key would be provided and files preserved. So, the police decided not to pay. As a result, the cops lost eight years of data stored on the server.

No Agency is Immune
This is just one in a series of recently reported ransomware attacks such as the one that hit Washington, D.C.'s CCTV system just eight days before President Trump's inauguration. There ransomware infected 123 of 187 D.C. police network video recorders, leaving 70% of the system inoperable.

Their New Target: Law Enforcement

When it comes to cybersecurity, the biggest threat facing Law Enforcement today is sensitive data, even evidence, being held hostage. The tactic, known as ransomware, has been around a while but has just recently gained traction by evolving into the most profitable type of malware in history. Ransomware is now on track to be a $1B business.

Numerous Law Enforcement agencies, from Detroit to Maine to Louisiana, have already been targeted (see Law Enforcement Held Hostage by Ransomware). And, unfortunately, this success is already spurring others, especially those with a grudge against justice, to launch similar attacks. Add to that a variety of server-side vulnerabilities that your agency may be unaware of and attackers are being presented a unique opportunity to harm your commitment to protect and serve. So it's critical that your agency honestly ask itself: "are we really ready to defend against attempts to shut down our networks, hold our data hostage or use our own IT system against us?"

What is Ransomware?

Ransomware is the name given to a class of malware that, once downloaded, encrypts critical data and demands a ransom for releasing it. Attackers usually attempt to hit as many of your assets as quickly as possible, so the payloads are most often delivered through three methods:

- **Mass phishing** – Emails which rely on unsuspecting users in your agency to activate
- **Malvertising** – Malicious advertising accidently activated by your staff
- **Exploit kits** – Taking advantage of your agency's pre-existing software vulnerabilities, like those found in common applications (Adobe Flash).

Watch: Learn about the biggest cyber threats for 2017

Ransomware specifically targets your user files and avoids damaging any system files, so that you can be notified of what happened. Once the files are encrypted, the malware usually self-deletes and leaves behind a message. This will instruct your agency on how to pay the ransom and regain access to your files. Some variants display a countdown timer, threatening to delete the key/decryption tool if you don't pay before the timer reaches zero or, in other cases, may simply increase the ransom once it hits zero.

But even if your agency does pay the ransom, which is usually done via an online transaction system known as Bitcoin, there is no guarantee that the attackers will send a decryption code, that the files will decrypt intact, or that a second ransomware virus will not be left behind to do even more damage at a later date now that they know how unsecure your network is and that you are willing to pay a ransom.

A New Threat is Targeting Your Agency

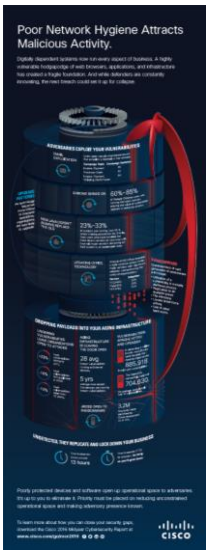
The recent WannaCry Ransomware cyberattack utilized a new self-propagating technique. That is why it was so effective – no need for human interaction to spread. It will attack your agency assets by:

- Utilizing a vulnerability in one of your widely deployed products
- Copying itself to all your drives (local, remote, network and USB)
- Attaching to your files/executables
- Pre-empting your security
- Using back-doors in your system that you don't know about
- Piggybacking on your regular traffic

To battle emerging and existing cyber threats, Cisco has established Talos, an elite threat intelligence organization that provides superior protection for Law Enforcement agencies like yours. We have over 200 full time threat researchers tracking threats across endpoints, networks, cloud environments, web, and email to provide a comprehensive view of cyber threats, their root causes, and the scope of outbreaks.

VIDEO: See how Talos is helping defeat the $60M Angler ransomware threat. Watch Now

They then correlate this data into actionable threat intelligence. The data is automatically fed into Cisco security products, improving their ability to detect new threats. To learn more, check out Cisco Talos.



INFOGRAPHIC: Inviting unwanted malware attacks? View now to find out

The Real Damage? Your Agency's Reputation

There are dozens of ransomware variants that might strike your agency's network, but they can damage something much more important than data; your reputation. Agencies that succumb to attack by either losing years' worth of data and evidence, or by paying a ransom, face a litany of concerns. This can include:

- Loss of confidence from law-abiding and trusting citizens
- Damaged public relations in communities where police actions and authority are already questioned
- Blowback to ongoing investigations, potentially damaging prosecutor cases
- Increased scrutiny that may impact personnel and budgets
- Significant media coverage that can damage relationships with other agencies that have taken years to build.

What if We Pay the Ransom?

Unfortunately, the adversaries behind these threats are taking their malware to an entirely new level of effectiveness by using cryptographically sound file encryption. This technique is quickly gaining popularity, preventing the majority of new ransomware from being easily decrypted. This new twist on ransomware might leave your agency tempted to pay the ransom. But it is important to remember that if you do pay, you are funding development of the next generation of ransomware. That's why it is critical to the security of Law Enforcement agencies across the nation that a cycle of infection-payment-infection be prevented by using industry leading threat-centric cybersecurity. Only then can you properly defend your agency before, during and after attack.

3 Steps to Keep Your Agency Safer

As the next generation of ransomware targets your Law Enforcement agency, it is critical that you deploy a first line of defense that can accomplish three key things:

- Stop opportunities for lateral movement of ransomware within your network
- Eliminate its propagation within and between your assets/devices
- Reduce the amount of time any attacker has to operate inside your network.

Your agency should also adopt best practices for patching vulnerable internet infrastructure and improving password management. Plus regularly monitor browser infections so you can more quickly identify and remediate threats. Your agency can also benefit from network segmentation (splitting your network into sub-networks) to stop, slow and contain self-propagating threats. This includes:

- VLANs and subnets that logically separate access to your data
- Dedicated firewall and gateway segmentation throughout your network
- Host-based firewalls with configured ingress and egress filtering
- Application blacklisting and whitelisting
- Role-based network share permissions (least privilege)
- Proper credential management.

Finally, we suggest your Law Enforcement agency institute a last line of defense: cloud-based backup recovery. Off-site backups are often your only hope for restoring service. Just be sure it is not open to compromise.

Next Steps

To learn more about current and emerging ransomware threats against your Law Enforcement agency and how you can defend against them, check out http://www.cisco.com/go/ransomware and Cisco Cybersecurity for Government.