RANSOMWARE
Overview and Lessons Learned from Recent Hackings

Rise in Ransomware Attacks

Recently, news of ransomware attacks has dominated national headlines. Private companies, local governments, and law enforcement agencies have all been victims of such attacks.

From the Colonial Pipelines hacking[1] to the attack on the Metropolitan DC Police Department, ransomware continues to be a relevant and pressing danger. In the wake of these cyber-attacks, "the U.S. Department of Justice is elevating investigations of ransomware attacks to a similar priority as terrorism." [2] This new DOJ guidance highlights the national security threat that ransomware poses to the nation.

What is Ransomware?

According to the Department of Justice, ransomware is "a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted."

Source: https://www.justice.gov/criminal-ccips/file/872766/download

Law enforcement agencies, big and small, continue to be a large target for ransomware attacks. These attacks have become more threatening over the years as "criminal hackers are increasingly using brazen methods to increase pressure on law enforcement agencies to pay ransoms, including leaking or threatening to leak highly sensitive and potentially life-threatening information."[3] Ransomware attacks pose a serious hinderance to public safety and have "taken down 911 systems, prevented officers from

[1] https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices

[2] https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/

[3] https://apnews.com/article/ransomware-gangs-hacking-police-cybercrime-pipeline-3a38c27c4fafe0c39461fb71bf91a42a

checking suspects' criminal histories during traffic stops and blocked access to investigative files or video, impeding investigations. In some cases, prosecutors have had to drop criminal cases."[4]

Recorded Future, a security firm that tracks ransomware attacks, reported that there were an estimated 65,000 successful ransomware attacks last year, or one attack every eight minutes.[5] According to Allan Liska, an intelligence analyst at Recorded Future, "'Ransomware attacks are only going to get worse and more pervasive into people's lives, and they're not disappearing anytime soon… There's a line of cybercriminals waiting to conduct these ransomware attacks. Anytime one goes down, you just see another group pop up.'"[6]

Overview of Recent Hackings

Unfortunately, local government agencies and police departments have served as popular targets for ransomware attacks. In April 2021, the Metropolitan Police Department (MPD) was hit with the ransomware, Babuk, which is a tricky strain of ransomware since it is "buggy and causes data loss."[7] As a result, many organizations may be unlikely to successfully recover all of their stolen data even if they do give into the cybercriminals' demands.[8] The attackers notified MPD that they had stolen more than 250 GB of data and threatened to publish the materials if they did not pay the stated ransom amount. [9] MPD refused to pay the ransom and, as a result, the Babuk group released thousands of MPD's sensitive documents on the dark web, many of which included "police officer disciplinary files and intelligence reports that include feeds from other agencies, including the FBI and Secret Service." [10] According to experts, this attack on MPD is the "worst known ransomware attack ever to hit a U.S. police department."[11]

Unfortunately, large departments are not the only target for ransomware attacks. The Presque Isle Police Department, a small department in Maine, was hit in April 2021 by an unidentified cybergang associated with Avaddon Ransomware.[12] The Avaddon-related gang reported they had the department's files, which included "victim statements, personal data of employees, reports of criminal cases, data from officers' computers, confidential data, records and certificates."[13] The cybergang published over 200 GBs of data on the dark web after the department did not comply with the gang's ransom request.[14]

[4] https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/05/14/hackers-threaten-to-release-police-records-knock-911-offline

[5] https://www.nytimes.com/2021/06/03/us/politics/ransomware-cybersecurity-infrastructure.html

[6] Ibid.

[7] https://www.cnn.com/2021/04/27/politics/dc-police-department-ransomware-attack/index.html

[8] Ibid.

[9] Ibid.

[10] https://apnews.com/article/police-technology-government-and-politics-1aedfcf42a8dc2b004ef610d0b57edb9

[11] Ibid.

[12] https://bangordailynews.com/2021/04/27/news/aroostook/presque-isle-police-server-hacked-by-ransomware/

[13] Ibid.

[14] https://bangordailynews.com/2021/06/10/news/aroostook/hackers-dump-presque-isle-police-department-files-on-dark-web/

In the winter of 2021, the 63-officer police department of Azusa, California was infiltrated by the hacking group, DoppelPaymer. As a result of refusing to pay the ransom, hundreds of sensitive files, including criminal case files and payroll data, were posted online. [15] Despite this attack occurring in early 2021, the department kept quiet about the attack until May, causing pushback from the community over their decision to stay silent for so long. The community was concerned about the privacy of residents and employees since the materials released may have included sensitive information, such as social security numbers; driver's license numbers; medical information; and financial account information.[16]

Lessons Learned

Protecting Against Ransomware Attacks

Despite the rising threat of ransomware attacks and the increasing sophistication of cybercriminals, there are actions law enforcement agencies can take to protect themselves.

Tips from the FBI for Avoiding Ransomware

- Keep operating systems, software, and applications current and up to date.
- Make sure anti-virus and anti-malware solutions are set to automatically update and run regular scans.
- Back up data regularly and double-check that those backups were completed.
- Secure your backups. Make sure they are not connected to the computers and networks they are backing up.
- Create a continuity plan in case your business or organization is the victim of a ransomware attack.

Source: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

The first step agencies should take to prevent a ransomware attack is to **educate personnel** on safe internet and email practices through **awareness trainings**. Cybercriminals often infiltrate agencies by tricking a user to provide their password information or getting them to click on a phishing email, which

[15] https://www.latimes.com/california/story/2021-05-31/azusa-ransomware-hack-sensitive-police-documents-online
[16] Ibid.

allows the cybercriminal to infect the system and conduct their ransomware attack.[17] Educating personnel on smart internet practices, and alerting them to potential scams, will help prevent ransomware attacks.

Responding to Ransomware Attacks

Despite preventative measures, ransomware attacks may still be successful, so it is essential that agencies have an incident response and business continuity plan in place. A **business continuity plan** allows an agency to maintain its essential functions, even while under attack. To prepare for a potential attack, agencies should "maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures."[18]

If an agency does become a victim of a cyberattack, there are steps to take to **immediately mitigate** and control the impact of the attack on the agency. Once an agency suspects they have become a victim of a ransomware attack, they should:

- "Isolate the infected computer immediately. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or share drives.
- Isolate or power-off affected devices that have not yet been completely corrupted. This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.
- Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware.
- If available, collect and secure partial portions of the ransomed data that might exist.
- If possible, change all online account passwords and network passwords after removing the system from the network. Furthermore, change all system passwords once the malware is removed from the system."[19]
- Contact their local FBI field office to request assistance, or submit a tip online.
- File a report with the FBI's Internet Crime Complaint Center (IC3).

Agencies should also try and **be as transparent as possible** with the community about the cyberattack. Sharing information in a timely manner allows them to get ahead of the narrative, calm fears, answer questions, and strengthen relationships of trust with community members.

Additionally, it is up to each department to consider whether they should pay the ransom. The Department of Justice **does not encourage paying a ransom**, and asks victims to considering the following risks:

- "Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.

[17] https://www.justice.gov/criminal-ccips/file/872771/download
[18] Ibid.
[19] Ibid.

- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model."[20]

Additional Resources

Check out these sources for additional information on protecting your agency from, and responding to, a ransomware attack:

- *How to Protect Your Networks from Ransomware*, Department of Justice
- *Ransomware and cyberattacks are not going away anytime soon—here is how to protect your agency*, National Police Foundation
- *Ransomware Playbook*, Cyber Readiness Institute
- *Ransomware: What It Is and What To Do About It*, Department of Justice
- *Scams and Safety – Ransomware*, FBI
- *5 tactics to protect your police agency from ransomware*, Police1

Resources for Creating a Business Continuity Plan:

- *Responding to Ransomware (a Playbook): An open-source template for ransomware response planning*, Counteractive Security
- *9-step ransomware incident response plan*, H-11 Digital Forensics
- *Ransomware: Remove Response Paralysis with a Comprehensive Incident Response Plan*, Marsh

Conclusion

Ransomware attacks are on the rise and pose a threat to national security. However, departments can mitigate this threat by proactively securing their networks through three vital steps:

(1) Implementing staff training and awareness campaigns.
(2) Establishing operating system and software safety protocol.
(3) Developing a continuity of operations plan to control the impact if a cyberattack is successful.

By Hyla Jacobson, Police Executive Research Forum

Police Executive
Research Forum

[20] Ibid.