Growing Risk of Data Sabotage:
Protecting Law Enforcement Agencies

By Michael Gregg, M.B.A.

7/13/2016

While cybersecurity becomes more important for law enforcement organizations across the country, one specific threat—the data-sabotage attack—should be prioritized above all others. Recently, several local agencies experienced one type of assault known as “ransomware.”[1] In these attacks, cybercriminals lock agencies’ files and other types of data behind almost unbreakable walls of encryption, rendering them entirely inaccessible and unusable. Recent strikes targeted police and sheriff’s departments in Massachusetts, Maine, Illinois, and Tennessee.[2] In all of these incidents, the criminals had financial motivations—the targeted agencies paid ransoms to the perpetrators, and the files were decrypted.[3]

What if these hackers were not motivated by money?[4] What if they refused to decrypt the data, and police departments never could access it again?[5] What would happen if the files included autopsy reports, witness statements, or crime scene photographs?[6] Law enforcement professionals must prepare for these possibilities. Changes in society and criminal culture have created an environment that could promote more vicious data-sabotage attacks in the future.

Mr. Gregg is a consultant and the founder and CEO of a cybersecurity company in Houston, Texas.

Recognizing the Goal

Two categories of data sabotage exist—the “crypto,” or encryption attack exemplified best by ransomware, and the “wiper” assault, which does not lock up files, but deletes them and destroys the computers and servers where they reside.[7] The number of ransomware viruses (e.g., CryptoLocker, CryptoWall, TeslaCrypt, and AlphaCrypt) continues to grow.[8]

Security vendors have ascertained ways to mitigate some types of ransomware; however, certain versions remain impenetrable and are not removable without destroying the data that was held hostage.[9] Cybercriminals with monetary goals primarily hold responsibility for these attacks. Several law enforcement organizations across the United States paid ransoms to get their files back.[10]

The wiper is designed to excise documents and data and cripple the computers and servers that store them.[11] This type of attack recently struck several major U.S. corporations and affected businesses around the world, including energy conglomerates, gas companies, banks, and television stations.[12] Wiper assaults typically result from politically sponsored hacking groups.

Understanding the Threat

Ransomware and wipers have existed for years, so why do they pose a greater threat to law

Ransomware and wipers have existed for years, so why do they pose a greater threat to law enforcement now? There are several important changes occurring within society and amidst the criminal economy. When viewed independently these cause concern; however, when considered as part of a larger entity, law enforcement can understand the severity of the threat.

- The black market for cybercrime, where criminals purchase hacking tools—referred to as “crimeware”—is highly organized.[13]
- Black markets also sell ransomware and wiper malware.[14]
- There is an increase in hacker-for-hire services, with a number of Internet sites offering to connect people with hackers who can handle sensitive jobs, ranging from hacking a spouse’s social media password to erasing a criminal record.[15]
- Antagonism is growing between law enforcement and local communities, with current policing methods facing increased scrutiny.
- Online activism progressively is becoming more a part of police protests, with “hacktivists”—online activists and hackers focused on social or political causes —threatening to release sensitive information about officers or departments.[16]
- Crimeware surpassed user errors and insider abuse as the top cyberthreat for law enforcement agencies, courts, and other government bodies. It was 2.4 times higher in 2015 than in 2014, while other categories decreased.[17]

“

...one specific threat should be prioritized above all others—the data sabotage attack.

Close quotes

These trends indicate that hacking tools are becoming substantially more powerful and sophisticated. Almost anyone can access them, and citizens frequently view attacks on police as justifiable.

The main reason ransomware attacks on police departments have not been detrimental is because the hackers were motivated by money—once they were paid, they moved on. Law enforcement professionals should be concerned when a perpetrator who is not compelled by money, but instead wants to cause as much damage as possible, launches this type of assault. Data sabotage, whether a wiper or encryption virus, fits the motivation of hacktivists and criminals who want to thwart a law enforcement investigation or disrupt an agency.

There are no technological obstacles to launching these assaults. Law enforcement departments are fortunate because they have not been targets of widely destructive cyberattacks. However, cultural changes increase the likelihood that such strikes could occur in the future. Agencies must prepare for the worst-case scenario.

Infecting Agencies

In the vast majority of cases, a malware infection stems from an employee opening a malicious e-mail—a “phishing” attempt—and clicking on an embedded link or downloading an attachment.[18] However, this is not the only way for ransomware, wipers, and other dangerous malware to infiltrate law enforcement organizations.

Increasingly, criminals corrupt legitimate websites with malicious code that hacks a computer as soon as someone visits a webpage on it.[19] If a perpetrator already infected an agency’s system with a “trojan,” which provides a backdoor to the network, the malefactor can use this to install ransomware or wipers the same way an individual runs updates on the computer.[20]

“

Security vendors have ascertained ways to mitigate some types of ransomware....

Close quotes

Preventing Attacks

There is no room for error when dealing with a data-sabotage attack because of the potential for catastrophic damage. The best protection is a layered defense.

First, agencies must establish formidable perimeter security, including a strong firewall and a robust antivirus or malware-exposure program with built-in phishing detection. They should schedule both the firewall and antivirus to update automatically and ensure all other software is current. Organizations also can use e-mail “whitelisting” to prevent employees from receiving e-mails from anyone except trusted contacts. In addition, they can install application-whitelisting software on computers, which will prevent unwanted programs from running on the network. Individuals should apply “password managers,” which securely store access codes for all of their accounts. This encourages use of strong, unique passwords. Another way to boost the perimeter defense is to replace some of the department’s standard computers with “thin clients.” These do not store data or programs locally on the computer; instead, everything is done by connecting to the server or using cloud-based tools. This dramatically reduces the risk of an attack.

Second, organizations must establish a strong backup defense in case attackers sneak past the perimeter. The best way to do this is to ensure that employees have their own dedicated storage on regularly backed-up servers. Data caching must occur routinely, at least once a day; however, individuals should not leave these devices on the network at all times because malware also could infect them. Network segmentation prevents an infection from spreading laterally across the entire agency.[21] Departments should not allow any one employee to have excessive access to critical data or networks.

Finally, if possible, agencies should set up intrusion-detection and -prevention systems (IDS/IPS) and exfiltration monitoring. These

Finally, if possible, agencies should set up intrusion-detection and -prevention systems (IDS/IPS) and exfiltration monitoring. These tools continually scan the network for any unusual activity indicating a system breach by a hacker.

Considering the Worst-Case Scenario

If a ransomware or wiper attack occurs, the entire network must be shut down immediately.[22] No one should attempt to restart the network until a cyber-incident response team—either government or private—assesses the situation. It is imperative to have an emergency-contact sheet and incident-response plan prepared beforehand.

In cases with a ransom demand, agencies must consider the pros and cons before deciding to negotiate. Cybercriminals may or may not release the data or target the same agency again.[23] Usually, the offenders give back the files once the ransom is paid. They operate these schemes like businesspersons and do not want a negative reputation. These individuals want people to pay them, and with a reputation diminished by not following through on a decryption promise, fewer people will pay. If the information is such that the department wants to make a ransom attempt, it is important for them to consult with an IT-security professional who can work to prevent any secondary infections.

“

In the vast majority of cases, a malware infection stems from an employee opening a malicious e-mail....

Close quotes

Conclusion

Law enforcement agencies face a growing number of cyberthreats from a variety of criminal groups, but the most critical risk is the data-sabotage attack. Currently, this threat occurs most often in ransomware assaults by cybercriminals out to make money. Due to the changing criminal environment and current society, these attacks could become more malicious and destructive in the future. Because these cyberattacks could undermine investigations and disrupt operations, it is important for law enforcement administrators to prioritize this threat when developing their IT-security programs. It is impossible to prevent every attack; however, by creating a layered defense that focuses equally on prevention and postinfection damage control, departments can protect their most critical operations and assets from serious harm.

For additional information the author may be contacted at mikeg@thesolutionfirm.com*.*

Endnotes

[1] Alyssa Newcomb, “Ransomware: How Hackers are Shaking Down Police Departments,” *ABC News.com,* April 13, 2015*,* accessed October 13, 2015, *http://abcnews.go.com/Technology/hackers-shaking-police-departments-ransom/story?id=30278202*.

[2] Christopher Burns, “How Local Maine Police Departments Let Their Cyber-Guard Down and Paid Criminals,” *Bangor Daily News,* April 24, 2015, accessed October 13, 2015, *http://bangordailynews.com/2015/04/24/the-point/how-local-maine-police-departments-let-their-cyber-guard-down-and-paid-criminals/*.

[3] Ibid.

[4] Adam Ghassemi, “Sheriff’s Office Forced to Pay Ransom for Their Own Case Files,” *News Channel 5,* November 12, 2014, accessed October 13, 2015, *http://www.scrippsmedia.com/newschannel5/news/Sheriffs-Office-Forced-To-Pay-Ransom-For-Their-Own-Case-Files-282493831.html*.

[5] Ibid.

[6] Ibid.

[7] Jim Finkle, “Exclusive: FBI Warns of ‘Destructive’ Malware in Wake of Sony Attack,” *Reuters,* December 2, 2014, accessed October 13, 2015, *http://www.reuters.com/article/2014/12/02/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202*.

[8] Jeremy Kirk, “CryptoWall Ransomware Variant Gets New Defenses,” *Computerworld,* January 8, 2015, accessed October 13, 2015, *http://www.computerworld.com/article/2865303/cryptowall-ransomware-variant-gets-new-defenses.html;* and Brian Donohue, “Angler Exploit Kit Pushing New, Unnamed Ransomware,” *Threatpost,* May 12, 2015, accessed October 13, 2015, *https://threatpost.com/angler-exploit-kit-pushing-new-unnamed-ransomware/112751*.

[9] Michael Mimoso, “New Utility Decrypts Data Lost to TeslaCrypt Ransomware,” *Threatpost,* April 27, 2015, accessed October 13, 2015, *https://threatpost.com/new-utility-decrypts-data-lost-to-teslacrypt-ransomware/112440/*.

[10] Hiawatha Bray, “When Hackers Cripple Data, Police Departments Pay Ransom,” *Boston Globe,* April 6, 2015, accessed October 13, 2015, *http://www.bostonglobe.com/business/2015/04/06/tewksbury-police-pay-bitcoin-ransom-hackers/PkcE1GBTOfU52p31F9FM5L/story.html*.

[11] Sean Gallagher, “Inside the ‘Wiper’ Malware That Brought Sony Pictures to Its Knees,” ARS *Technica,* December 3, 2014,

[11] Sean Gallagher, "Inside the 'Wiper' Malware That Brought Sony Pictures to Its Knees," *ARS Technica,* December 3, 2014, accessed October 13, 2015, *http://arstechnica.com/security/2014/12/inside-the-wiper-malware-that-brought-sony-pictures-to-its-knees/*.

[12] Ben Elgin and Michael Riley, "Now at the Sands Casino: An Iranian Hacker in Every Server," *Bloomberg Business*, December 11, 2014, accessed October 13, 2015, *http://www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas;* and John Leyden, "Experts Finger Disk-Wiping Badness Used in S. Korea Megahack: The Long, Dark Teatime of the Seoul," *The Register,* March 22, 2013, accessed October 13, 2015, *http://www.theregister.co.uk/2013/03/22/sk_megahack/*.

[13] Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Santa Monica, CA: RAND Corporation, March 25, 2014), accessed October 13, 2015, *http://www.rand.org/content/dam/rand/pubs/ research_reports/RR600/RR610/RAND_RR610.pdf* .

[14] Steve Weisman, "Ransomware is Threatening Your Computer," *USA Today,* January 11, 2015, accessed October 13, 2015, *http://www.usatoday.com/story/money/personalfinance/2015/01/11/computer-hacker-ransomware-malware-sony/21397777/;* and Sheera Frenkel, "Sony Hackers Used Widely Available Malware, Cybersecurity Experts Say," *BuzzFeed News,* December 18, 2014, accessed October 13, 2015, *http://www.buzzfeed.com/sheerafrenkel/sony-hackers-used-widely-available-malware-cybersecurity-exp#.reE46naZA*.

[15] Robert McGarvey, "Hackers for Hire: The 2015 Way to Snoop on Lovers, Even Scores, Even Erase Government Records," *Main Street,* February 13, 2015, accessed October 13, 2015, *https://www.mainstreet.com/article/ hackers-for-hire-the-2015-way-to-snoop-on-lovers-even-scores-even-erase-government-records*.

[16] Federal Bureau of Investigation, Internet Crime Complaint Center, *Hacktivists Threaten to Target Law Enforcement Personnel and Public Officials,* April 21, 2015, accessed October 13, 2015, *http://www.ic3.gov/media/ 2015/150421.aspx*.

[17] *Verizon 2014 Data Breach Investigations Report* (Basking Ridge, NJ: Verizon Enterprise Solutions, April 2014), accessed October 13, 2015, *http://www.verizonenterprise.com/DBIR/2014/reports/rp-Verizon-DBIR-2014_en_xg.pdf;* and *Verizon 2015 Data Breach Investigations Report* (Basking Ridge, NJ: Verizon Enterprise Solutions, April 2015), accessed October 13, 2015, *http://www.verizonenterprise.com/DBIR/2015/reports/rp-Verizon-DBIR-2014_en_xg.pdf*.

[18] Jonathan Hassell, "Cryptolocker: How to Avoid Getting Infected and What to Do If You Are," *Computerworld,* October 25, 2013, accessed October 13, 2015, *http://www.computerworld.com/article/2485214/ microsoft-windows/cryptolocker-how-to-avoid-getting-infected-and-what-to-do-if-you-are.html*.

[19] Lucian Constantin, "Ransomware Authors Streamline Attacks, Infections Rise," *PC World,* February 10, 2015, accessed October 13, 2015, *http://www.pcworld.com/article/2882532/ransomware-authors-streamline-attacks-infections-rise.html;* Rene Millman, "Ransomware Risk From Over 140 Million Websites Researcher Warns," *SC Magazine,* September 7, 2015, accessed October 13, 2015, *http://www.scmagazineuk.com/ransomware-risk-from-over-140-million-websites-researcher-warns/article/437202/;* and Invincea, *Ransomware: Malware That Kidnaps Your Data to Extort Money From You* (Fairfax, VA: Invincea Inc., June 2014), accessed October 13, 2015, *http://www.invincea.com/wp-content/uploads/2014/06/Invincea_Ransomware_whitepaper_061614.pdf*.

[20] Ellen Messmer, "CryptoLocker Gang Casts Tentacles into Botnet Crime World," *Network World,* November 22, 2013, accessed October 13, 2015, *http://www.networkworld.com/article/2172166/malware-cybercrime/cryptolocker -gang-casts-tentacles-into-botnet-crime-world.html;* Danielle Walker, "Windows Trojan Packs Punch, Downloads Ransomware 'Cribit,'" *SC Magazine,* March 26, 2014, accessed October 13, 2015, *http://www.scmagazine.com/ windows-trojan-packs-punch-downloads-ransomware-cribit/article/339958/;* and Gregg Keizer, "Massive Botnet Takedown Stops Spread of Cryptolocker Ransomware," *Computerworld,* June 5, 2014, accessed October 13, 2015, *http://www.computerworld.com/article/2490343/malware-vulnerabilities/massive-botnet-takedown-stops-spread-of-cryptolocker-ransomware.html*.

[21] Jaikumar Vijayan, "Target Breach Happened Because of a Basic Network Segmentation Error," *Computerworld,* February 6, 2014, accessed October 13, 2015, *http://www.computerworld.com/article/2487425/ cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html*.

[22] Lauren Orsini, "How to Fight CryptoLocker and Evade Its Ransomware Demands," *ReadWrite,* November 8, 2013, accessed October 13, 2015, *http://readwrite.com/2013/11/08/cryptolocker-prevent-remove-eradicate*.

[23] Tracy Kitten, "Ransomware: The Right Response," *BankInfoSecurity: The Fraud Blog,* April 2, 2015, accessed October 13, 2015, *http://www.bankinfosecurity.com/blogs/ransomware-p-1838/op-1*.

Close