Ransomware 101 – What Emergency Communications Leadership Needs to Know!

By D. Jeremy DeMar, MA, CPE, ENP
APCO Cybersecurity Committee

January 4, 2020 (updated April 29, 2021, finalized June 10, 2021)

Nationally, attacks by cybercriminals continue to wreak havoc on connected systems. In 2020 alone, "ransomware attacks – which encrypt and disable computer systems while demanding a ransom – affected 113 federal, state, and municipal governments, 560 health facilities and 1,681 schools, colleges, and universities." (Techxplore.com, 2021) Ransomware, which is a type of malware (short for malicious software), is only one of several types of malware that by design, can infiltrate and infect a user's computer system or mobile device.

McAfee, a leading cybersecurity company, defines ransomware in the following way:

"Ransomware is malware that employs encryption to hold a victim's information at ransom. A user's critical data is encrypted so that they cannot access personal files and a ransom is demanded to provide access to the files." (McAfee, 2019)

Understanding how ransomware works is important but as the old saying goes, and ounce of prevention is worth a pound of cure. Knowing how to protect your public safety answering point (PSAP)/emergency communications center (ECC) from a ransomware attack is vital. Threat/attack "vectors", the routes malicious attacks may take to get past your defenses and infect your network (Barracuda, 2016) are an excellent starting point for anyone wanting to educate themselves on methods of transmission.

While there are a variety of ransomware types, the most common threat vectors are e-mail phishing campaigns (a form of social engineering), remote desktop protocol (RDP) vulnerabilities, and software vulnerabilities. (CISA.gov, 2020)

Considered by many cybersecurity professionals to be one of the easiest ways to access a private network, social engineering exploits network protections by extracting relevant username and password information directly from the user. Phishing, the most common social engineering attack method, exploits a user's trust of a specific individual or organization to extract confidential information or encourage the download of an attached file. Developers of these malicious messages will use well known company names and recognizable logos to coerce a user into interacting with delivered correspondence. Phishing attacks do not target a specific individual or entity; instead, as the term suggests, a wide "phishing" net is cast into the water of the internet, seeking to arbitrarily capture prey. Spear phishing (targeted), vishing (phone based), and smishing (text message based) are some other common social engineering attack methods.

Remote Desktop Protocol, or 'RDP', allows a user to remotely access a computer workstation from just about anywhere, provided an internet connection is available. Some might suggest the threat of RDP intrusion as a means of introducing ransomware into our nation's 9-1-1 system is minimal, believing the system to be effectively closed to outside access. Many proprietary 9-1-1 systems, be they client server or cloud based, still require periodic connections to the internet to

be effectively updated and maintained. These ‘openings’, even if not frequently occurring, make 9-1-1 systems every bit as vulnerable to this style of attack.

Speaking of updates, did you know that unpatched software applications provide an excellent gateway for malware to enter a computer network? Malware, which is software intended to disable or destroy critical network systems, often finds its way into a secure network via an exploit package. An action as simple as a user clicking a link in a spammed e-mail (social engineering) or clicking a nefarious online advertisement within a website is all that is necessary to expose critical systems to a ransomware infection.

Prevention efforts are bolstered when those who have authorized access to critical systems remain situationally aware. Users must be kept up to date on the latest in intrusion techniques, and more importantly, understand how convincing and legitimate the attempts may appear. An excellent example of this would be the ransomware package known as Reveton. The Federal Bureau of Investigation (FBI) provides the following description of the Reveton scam:

“Reveton is a computer virus that is installed on a computer when a user visits a compromised website. Once installed, the computer locks up while displaying a warning that the FBI or the Department of Justice has identified the computer as being involved in criminal activity. The bogus message instructs the user to pay a “fine” using a prepaid money card service, which will unlock the computer. Users are threatened with criminal prosecution if they fail to make the payment.” – FBI.gov, 2012

The use of an official logo, accusations of criminal activity, and threats of legal action might be enough to convince even the most careful system user to click a nefarious link and expose a network to a ransomware attack.

In the first few months of the COVID-19 pandemic, work deemed non-essential effectively came to a halt as millions of Americans were asked to remain at home with their families. When it became clear the duration of widespread non-essential work closures would continue indefinitely, many businesses began transitioning to a telecommuting or remote work model. At the height of the pandemic, 44% of employees were working from home five days or more per week, in sharp contrast to the 17% of employees telecommuting pre-pandemic. (Mlitz, 2021)

The dramatic shift from traditional brick and mortar office work to a telework setting was not limited solely to the private sector. In response to the pandemic, the City of Alexandria, Virginia deployed a home-based 9-1-1 service (Careless, 2020), becoming the very first PSAP in the nation to do so. This option allowed personnel to remotely field 9-1-1 calls for service and enter information into the center’s computer aided dispatch system. While this effort was without question a progressive and necessary step for the 9-1-1 profession, its implementation does underscore the need for additional cybersecurity research and awareness as it pertains to remotely connected public safety systems.

So how do we best protect our PSAP/ECC and those needing legitimate access to critical public safety systems? An internet search on the question yields a variety of results, most of which appear to be reactive in nature. While enterprise-wide cyber hygiene is important, since most

methods discussed in this work suggest user error is the primary cause of ransomware transmission, keeping your personnel informed and educated is one key element of prevention.

Cybersecurity awareness should be part of your monthly and/or annual training regimen. As new attack methods are constantly being developed, PSAP/ECC leadership should work closely with IT staff to stay up to date on the latest threat vectors. If no dedicated IT staff exists, the communications leader must keep herself/himself aware of current attack trends and update and advise center staff accordingly. Topic specific training programs, like APCO's Cybersecurity Fundamentals for the ECC, provide a comprehensive overview of current Cybersecurity concerns in the emergency communications space, touching on areas like Cyber Hygiene, the anatomy of a Cyber Attack, and of course, a deeper dive into ransomware. Other options include CISA's Cyber Skills Training and FEMA's Independent Study Programs.

References

https://www.emsworld.com/article/1225293/reach-me-home-alexandria-va-pioneers-remote-9-1-1-call-taking

https://techxplore.com/news/2021-01-ransomware-heavy-toll.html

https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html

https://us-cert.cisa.gov/ncas/tips/ST04-014

https://www.statista.com/statistics/1122987/change-in-remote-work-trends-after-covid-in-usa/

https://www.cisa.gov/sites/default/files/2021-01/NCIJTF%20Ransomware_Fact_Sheet.pdf

https://blog.barracuda.com/2016/11/17/threat-vectors-what-are-they-and-why-do-you-need-to-know-them/

https://www.paloaltonetworks.com/cyberpedia/what-is-an-exploit-kit

https://archives.fbi.gov/archives/knoxville/press-releases/2012/internet-scam-warning-reveton-ransomware

https://www.statista.com/statistics/1122987/change-in-remote-work-trends-after-covid-in-usa/

https://smallbiztrends.com/2020/06/work-from-home-permanently-survey.html

https://blog.emsisoft.com/en/36601/how-to-secure-rdp-from-ransomware-attackers/

http://www.unifiedguru.com/how-ransomware-is-evolving-as-a-threat-to-organizations/