Hackers seek ransoms from Baltimore and communities across the US

June 5 2019, by Richard Forno

Credit: Styves Exantus from Pexels

The people of Baltimore are beginning their fifth week under an electronic siege that has prevented residents from obtaining building permits and business licenses—and even buying or selling homes. A year

after hackers disrupted the city's emergency services dispatch system, city workers throughout the city are unable to, among other things, use their government email accounts or conduct routine city business.

In this attack, a type of malicious software called ransomware has encrypted key files, rendering them unusable until the city pays the unknown attackers 13 bitcoin, or about US$76,280. But even if the city were to pay up, there is no guarantee that its files would all be recovered; many ransomware attacks end with the data lost, whether the ransom is paid or not.

Similar attacks in recent years have crippled the United Kingdom's National Health Service, shipping giant Maersk and local, county and state governments across the U.S. and Canada.

These types of attacks are becoming more frequent and gaining more media attention. Speaking as a career cybersecurity professional, the technical aspects of incidents like this are but one part of a much bigger picture. Every user of technology must consider not only threats and vulnerabilities, but also operational processes, potential points of failure and how they use technology on a daily basis. Thinking ahead, and taking protective steps, can help reduce the effects of cybersecurity incidents on both individuals and organizations.

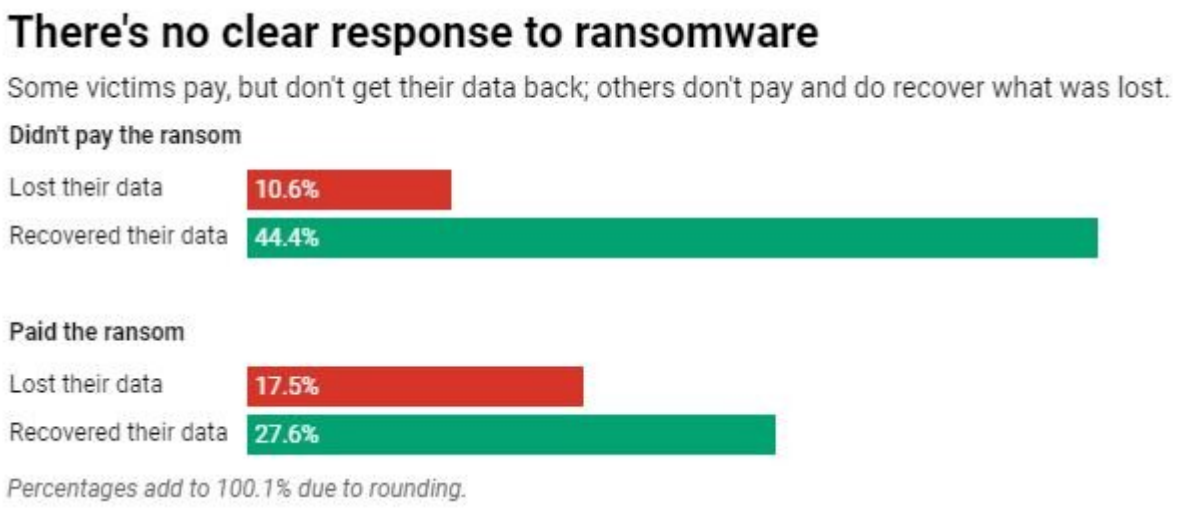
Understanding cyberattack tools

Software designed to attack other computers is nothing new. Nations, private companies, individual researchers and criminals continue developing these types of programs, for a wide range of purposes, including digital warfare and intelligence gathering, as well as extortion by ransomware.

Many malware efforts begin as a normal and crucial function of

cybersecurity: identifying software and hardware vulnerabilities that could be exploited by an attacker. Security researchers then work to close that vulnerability. By contrast, malware developers, criminal or otherwise, will figure out how to get through that opening undetected, to explore and potentially wreak havoc in a target's systems.

Sometimes a single weakness is enough to give an intruder the access they want. But other times attackers will use multiple vulnerabilities in combination to infiltrate a system, take control, steal data and modify or delete information—while trying to hide any evidence of their activity from security programs and personnel. The challenge is so great that artificial intelligence and machine learning systems are now also being incorporated to help with cybersecurity activities.



Credit: The Conversation

There's some question about the role the federal government may have played in this situation, because one of the hacking tools the attackers

reportedly used in Baltimore was developed by the U.S. National Security Agency, which the NSA has denied. However, hacking tools stolen from the NSA in 2017 by the hacker group Shadow Brokers were used to launch similar attacks within months of those tools being posted on the internet. Certainly, those tools should never have been stolen from the NSA—and should have been better protected.

But my views are more complicated than that: As a citizen, I recognize the NSA's mandate to research and develop advanced tools to protect the country and fulfill its national security mission. However, like many cybersecurity professionals, I remain conflicted: When the government discovers a new technology vulnerability but doesn't tell the maker of the affected hardware or software until after it's used to cause havoc or disclosed by a leak, everyone is at risk.

Baltimore's situation

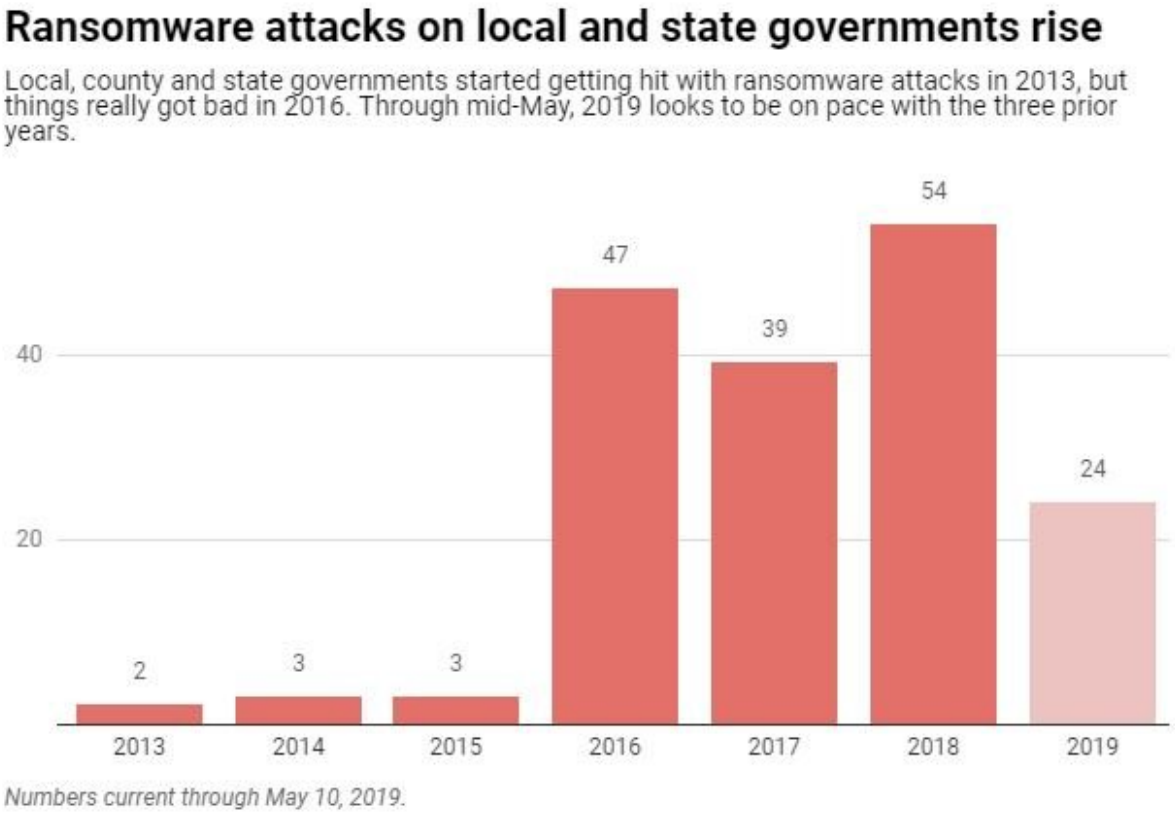
The estimated $18 million cost of recovery in Baltimore is money the city likely doesn't have readily available. Recent research by some of my colleagues at the University of Maryland, Baltimore County, shows that many state and local governments remain woefully underprepared and underfunded to adequately, let alone proactively, deal with cybersecurity's many challenges.

It is concerning that the ransomware attack in Baltimore exploited a vulnerability that has been publicly known about—with an available fix – for over two years. NSA had developed an exploit (code-named EternalBlue) for this discovered security weakness but didn't alert Microsoft about this critical security vulnerability until early 2017—and only after the Shadow Brokers had stolen the NSA's tool to attack it. Soon after, Microsoft issued a software security update to fix this key flaw in its Windows operating system.

Admittedly, it can be very complex to manage software updates for a large organization. But given the media coverage at the time about the unauthorized disclosure of many NSA hacking tools and the vulnerabilities they targeted, it's unclear why Baltimore's information technology staff didn't ensure the city's computers received that particular security update immediately. And while it's not necessarily fair to blame the NSA for the Baltimore incident, it is entirely fair to say that the knowledge and techniques behind the tools of digital warfare are out in the world; we must learn to live with them and adapt accordingly.

Compounding problems

In a global society where people, companies and governments are increasingly dependent on computers, digital weaknesses have the power to seriously disrupt or destroy everyday actions and functions.



Credit: The Conversation

Even trying to develop workarounds when a crisis hits can be challenging. Baltimore city employees who were blocked from using the city's email system tried to set up free Gmail accounts to at least get some work done. But they were initially blocked by Google's automated security systems, which identified them as potentially fraudulent.

Making matters worse, when Baltimore's online services went down, parts of the city's municipal phone system couldn't handle the resulting increase in calls attempting to compensate. This underscores the need to not only focus on technology products themselves but also the policies, procedures and capabilities needed to ensure individuals and/or organizations can remain at least minimally functional when under duress, whether by cyberattack, technology failures or acts of nature.

Protecting yourself, and your livelihood

The first step to fighting a ransomware attack is to regularly back up your data—which also provides protection against hardware failures, theft and other problems. To deal with ransomware, though, it's particularly important to keep a few versions of your backups over time—don't just rewrite the same files on a backup drive over and over.

That's because when you get hit, you'll want to determine when you were infected and restore files from a backup made before that time. Otherwise, you'll just be recovering infected data, and not actually fixing your problem. Yes, you might lose some data, but not everything—and presumably only your most recent work, which you'll probably

remember and recreate easily enough.

And of course, following some of cybersecurity's best practices—even just the basics—can help prevent, or at least minimize, the possibility of ransomware crippling you or your organization. Doing things like running current antivirus software, keeping all software updated, using strong passwords and multifactor authentication, and not blindly trusting random devices or email attachments you encounter are just some of the steps everyone should take to be a good digital citizen.

It's also worth making plans to work around potential failures that might befall your email provider, internet service provider and power company, not to mention the software we rely on. Whether they're attacked or simply fail, their absence can disrupt your life.

In this way, ransomware incidents serve as an important reminder that cybersecurity is not just limited to protecting digital bits and bytes in cyberspace. Rather, it should force everyone to think broadly and holistically about their relationship with technology and the processes that govern its role and use in our lives. And, it should make people consider how they might function without parts of it at both work and home, because it's a matter of when, not if, problems will occur.

Provided by The Conversation