By Jen Sharp, jensharp.com

Ransomware … WHAT?

Not too long ago, a friend of mine approached me excitedly to tell me about her recent computer struggle and – what she considered—a victory.

“When I started my laptop, there was this message saying there was a threat of virus, and my computer caught it… but I was locked out of everything. The message told me to call the antivirus company to get back into my computer.”

“What? What did you do?” I asked, worried about what was coming next.

“I called them,” she replied. “They got me right back in! They were so helpful and friendly! And it only cost me $99!” I groaned. I explained she had just been taken. I elaborated that this ploy was common, and that the company she called to help her fix the problem was actually the outfit who put the virus on her computer to begin with. She was incredulous and asked, “What?”

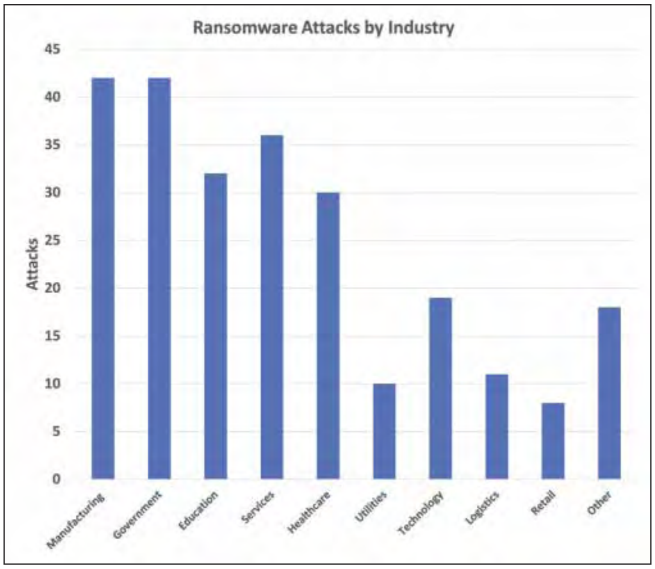
What was that?

My friend experienced a mild version of a form of malware that has been dubbed “ransomware,” for obvious reasons. It works like this: you experience a lock-out or encryption of your data, then receive a message. You cannot get your data or get back into your system unless you pay someone money. The flavor of ransomware my friend experienced is called “Fake Anti-virus,” and is surprisingly a lucrative industry. Using this particular scam, criminals are likely to escape being reported because they appear to be the good guys.

However, ransomware in general has done much larger damage, and municipalities should take notice. In the past, backing up your data was considered one simple step that could mostly single-handedly protect systems from expensive fallout. No longer are solid backup procedures enough. Hackers are getting more and more sophisticated and organized. Sophos reports that 75% of businesses suffering ransomware attacks had security protocols in place that included antivirus and firewall protection. Hence, municipalities need a multi-layered approach to combatting what some have called the inevitable.

What makes it so damaging?

Ransomware has been on the rise in the last five years mainly due to increased internet presence and variety of devices. As the internet allows more access with more anonymity, more criminals, domestic and



Source: BlackFog, State of Ransomware 2020 report

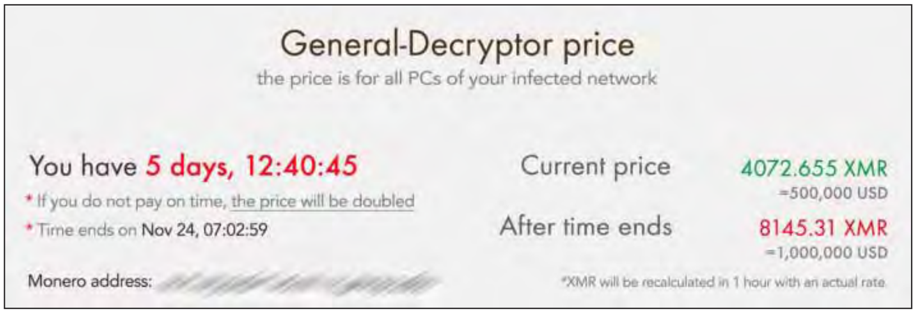
international, are finding their way into our offices, living rooms, and even phones.

However, ransomware still needs someone to open that door. This form of malware sometimes finds a security gap in software, but more often, an unsuspecting individual opens that door by clicking or installing the destructive code. According to Datto, businesses and municipalities suffered losses exceeding $75 billion annually in 2019. Sophos reports that the average single attack costs over $130,000. Instead of targeting pennies in the individual market, full-fledged ransomware companies target high profile victims who are likely to pay out for single large incidents. These targets include schools, hospitals, police departments, small and medium-sized businesses, and yes, water systems and city governments. The damage is significantly greater than the traditional virus because the attacks can quickly shut down entire systems with little or no warning. Government entities are one of the primary industries impacted by ransomware in the past year. While utilities have been targeted less frequently, it can permanently set back financial well-being when an attack hits a system.

What happened in November to KRWA?

For ten days in November just before Thanksgiving 2020, the Kansas Rural Water Association's website and all of the Web Services projects were shut down unexpectedly. Our web host provider, Managed.com, completely turned off their entire system to prevent the spread of a suspected ransomware attack in an abundance of caution. Soon, it was revealed that the company did have one isolated section of their environment infected by REvil, a known Eastern European organization responsible for numerous events over the last few years. Managed.com immediately involved federal law enforcement and international agencies to help respond to the invasion. REvil had demanded $500,000 from the company to restore their system, which would double if not paid within days. As usual, the ransom was to be paid in bitcoin, an untraceable digital currency recently gaining popularity across the world.

Fortunately, Managed.com had a proper plan in place to endure the attack. First, as the FBI recommends, they did not pay the ransom. Paying the ransom encourages more attacks, and sadly – around 22% of the time – victims who



General-Decryptor price

the price is for all PCs of your infected network

You have 5 days, 12:40:45

* If you do not pay on time, the price will be doubled

* Time ends on Nov 24, 07:02:59

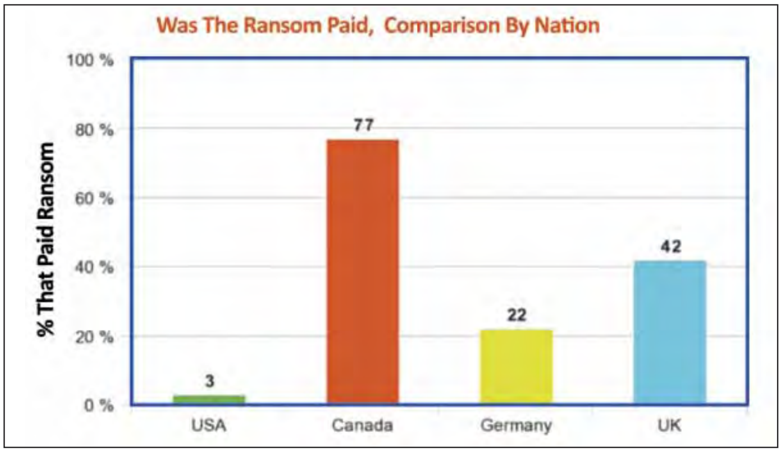
Current price 4072.655 XMR
≈500,000 USD

After time ends 8145.31 XMR
≈1,000,000 USD

Monero address:

*XMR will be recalculated in 1 hour with an actual rate.

Image of the "ransom note" from REvil to Managed.com



Source: PhoenixNAP Global IT Services

pay are not restored access to their system anyway. It turns out, Americans are not inclined to be bullied, as phoenixNAP reports that only three percent (3%) of U.S. companies agreed to pay ransoms, compared to Canadians who paid 77% of the time.

Managed.com was able to detect the infiltration before even receiving the ransom note and took aggressive action by completely shutting off their entire environment to avoid the spread. While inconvenient, the event had no long-term impact, as they were able to restore all of their customers from secured backups. They used the incident to take stock of their security protocols. While given what they knew at the time, they had a reliable process in place, they identified more protocols for even greater protection. These security enhancements, however, will not guarantee another attack. Ransomers continue to evolve and find new ways to infiltrating unprepared entities.

What does it look like right now?

Because of its elusive and evolving nature, identifying ransomware can be tricky. As of today, there have been a few different types:

- Backup targeting – ransomers go after not only current data but also backups of data. Backups should be in multiple copies through various platforms and easily restorable.
- Fake AV – posing as an Antivirus software, ransomers trick individuals into letting them into a system. Install prevention software from only reputable companies you seek out, instead of accepting solicitations for programs.
- File encryption – because it is easy and quick, ransomers use techniques to encrypt the files in your system, but you must pay to decrypt. Certain protection software now includes detection of encryption activity.
- Locker type – ransomers may instead choose to find the one way into a system and lock access. Having a complex structure with multi-factor authentication is a layer of protection for this kind of "in."

As usual, we can learn from others' experiences. And unfortunately, due to the high volume of this criminal activity, there is a lot to learn from various industries. For example, a prominent chip-manufacturing company discovered too late that an undetected breach affected 10,000 machines. The city of Atlanta's entire network was ransomed to the tune of $50,000. Employees were locked

Source: Kapersky Cyber Threats real-time map widget from across the globe https://cybermap.kaspersky.com/widget

What preventative steps can you take?

Prevention starts with an analysis of what is currently working to benefit the ransomers. Statista reports that spam and phishing emails are the most successful way attackers infect their victims, a whopping 67% of causes identified. Another cause contributing 36% that goes hand-in-hand is a lack of understanding on the part of employees as to what constitutes a safe email. Another 30% is attributed to poor password management. The RSA Current State of Cybercrime reminds us that mobile devices are a growing group of susceptible targets. Most attacks (85%) occur on Android devices, and most methods (80%) use apps instead of the phone's browser.

Understanding these vulnerabilities can help you form a multi-layered plan to combat ransomware and protect your system, your customers, and yourself. Fortunately, these tips can be implemented with some education and little to no cost.

- Put your email spam filter on aggressive settings.
- Be very suspicious of anything that even looks like phishing emails – don't click on anything, unless you know the sender and can verify it is directly from them.
- Train and brief all employees about what phishing emails look like: for example, look at the actual email address, not just the "from" title.
- Create longer passwords, better passwords, and passphrases. Change them often, and don't reuse passwords across different platforms. In other words, do not use the same password for everything!
- Make sure all your equipment has firewalls, antivirus and malware software installed and up to date.
- Avoid the obvious risks, like using public WiFi (even on your phone) without a VPN.
- Keep all operating systems up to date and install security patches when they are released.
- When using accounts with other systems, do not create just one "generic" account for all of your employees. Have each user make own account and give them only the permissions they need.
- Of course, have a solid backup system in place. Have multiple copies of important data both on-site and in the cloud on different platforms. Make sure it is relatively easy to restore these backups, both your programs and your data.
- It's annoying, but 2FA (Two-factor authentication) is awesome! This technique requires a user to verify with two separate identifying characteristics, like entering a password but also a code that was texted to you. Opt-in for these extra protections.

For more prevention tips, visit this official advice from the U.S. Government
https://us-cert.cisa.gov/ncas/tips/ST19-001

For more tips on passwords, visit this official advice from the U.S. Government
https://us-cert.cisa.gov/ncas/tips/ST04-002

out. Customers couldn't pay water bills. Although they didn't pay the ransom, the fiasco cost the city $17 million to recover and rebuild its digital infrastructure.

Comparatively, my friend's $99 was a drop in the proverbial bucket. Ransom amounts requested of larger entities vary from $20,000 to $6 million. Attacks have more than doubled in the last two years and are expected to continue growing. Additionally, recent world events spur more creativity in these criminals' minds. Despite the high payout for companies and government, individuals are still a major target. One successful attack in the U.K. began on January 25. It involves a phishing scam pretending to be the country's national health service notifying victims they are eligible for the COVID-19 vaccine. Also, with more workers moving from the office to their living rooms, they are three to four times as likely to unwittingly accept general malware, as their work environments organized protection software may not be activated on personal equipment.

What happens next?

Just as ransomers find new ways to thwart existing security protocols, ethical hackers and creative developers are predicting and implementing avenues to head off future attacks. For example, AI (artificial intelligence) is being used to explore ways for a company to use predictive behavior to make sure you are who you say you are.

Forecasters are expecting cybercrime to cost $6 trillion in 2021. Cyber Security Ventures estimates in 2021 that victims will suffer from ransomware on some level every 11 seconds. It stands to reason, investing a little time and money into better security should be a priority for anyone using online data systems.

What happens next remains to be seen.

Since 1997, Jen Sharp (JenSharp.com) has served business and government across Kansas and the US and even internationally, specializing in Web development, design & programming including e-Learning, ecommerce, content management systems, and other small business solutions.