RANSOMWARE:

DON'T LET YOUR DATA BE HELD HOSTAGE

RCN BUSINESS

Executive Summary

Ransomware is one of the hottest white-collar crimes of the 21st century[1]. Incidences are skyrocketing and cybercriminals have set their sights on more vulnerable small- and medium-sized businesses, as they usually have less resources to ward off an attack and are more likely to pay a ransom to retrieve encrypted files. Unlike other types of malware that simply destroys data, ransomware is different in that there is an out: the criminals want to get paid and you may be able to recover your data. But is that the best course of action?

This White Paper is intended to educate SMBs about ransomware attacks and to provide simple action steps that every business can take to avoid falling victim in the first place, as well as recommendations for recovering if an attack should occur.

LESS THAN SIX DEGREES OF SEPARATION

We all know the game *6 Degrees of Kevin Bacon* in which virtually any Hollywood actor can be linked to Bacon in a network of six or fewer connections. Well, there's another networking game out there called *ransomware* and the consequences for your connections will most certainly **not** be good. In today's uber-connected world, just about everyone knows someone who has been the victim of a ransomware attack; whether that someone is you, a coworker, a friend or family member. If you don't, chances are you will soon.

In fact, a Ponemon Institute study of 600 US and UK companies, *State of Cybersecurity in Small and Medium-Sized Businesses (SMB)*, found more than half of responding firms experienced a ransomware attack in 2017[2]. Another 2017 UK government survey found that 46% of all businesses were targeted, with more than two-thirds being SMBs[3]. Security software giant Symantec reports that 60% of small businesses fail within six months of a ransomware attack. So, the question of having your data held hostage is most likely a matter of *when,* not *if,* and how to minimize the damage. For those that have experienced it, the question is how to stop it from recurring because the criminals will try again.

What is Ransomware?

Ransomware is malicious software that seizes control of a computer or network, usually through a web browser or email. It encrypts data into an unreadable form and holds it hostage until the victim makes a payment to the cybercriminals behind the attack in exchange for a decryption key[4]. Some attacks may infect entire networks, others may leave some vital systems operational – either to prove the attacker's ability to disrupt business further or to leave a communication channel open through which to pay the ransom. Some attacks target customer records including credit and debit card information, others seek company intellectual property, employee or financial data.

Ransomware can get into a network simply by a user opening an infected email or through flaws in website design. Security loopholes allow legitimate sites to be compromised, redirecting website visitors to spoofed URLs. Unsuspecting visitors and email recipients then infect their systems with invisible scripts that begin encrypting files when a user clicks on a banner ad or opens the email, for example. Once installed on a host, the code quickly spiders to any networked drive or peripheral device and brings entire operations to a standstill. Cloud services are not immune either. When hackers access a cloud service provider they can launch a ransomware attack using Microsoft Office macros, Java Script exploits and backdoors that will directly affect every customer using that service[4].

Usually within seconds – and certainly the next time your device is powered on – a message like the one shown here pops up on the screen and your heart skips a beat. Your network credentials are gone, passwords exposed, and/or all your file extensions have been changed to an unrecognizable string rendering your data and PC useless. And everyone in your address book is about to get infected. Too late. The damage is done. The clock is ticking and the price is going up by the minute.

The truth is, your personal information may have already been compromised in some of the larger recent cyberattacks and you might not even know it. We've all heard the nightmare stories about the data of hundreds of millions of social media users, hotel guests, airline passengers and bank customers being stolen. In these events, you may have been a secondary victim and the breach was resolved without your involvement. But these days it doesn't take a multinational corporation to attract the attention of a cybercriminal. In fact, **individuals and SMBs are far more vulnerable than enterprises with robust IT departments.**

Cybercriminals like the path of least resistance and smaller businesses typically have fewer security resources in place to defend against an attack[3]. Many SMBs think they're under the radar, but one unguarded network port can allow ransomware to quickly spread across entire supply chains and infect multiple networks. SMB employees and casual web surfers with less networking savvy are more likely to fall for phishing scams and accidentally click infected links. Innocent actions with damaging results.

Your takeaway should be that everyone is vulnerable, but also know that falling victim is as preventable as linking Kevin Bacon to your favorite star in six steps or less. Let's now focus on causes and effects and some recommended *befores* and *afters* for dealing with a ransomware attack.

RANSOMWARE: CAUSES, COST & OUTCOMES

What causes ransomware? In a word, *greed*. There are some not-so-nice people out there who prefer to spend their days extorting businesses rather than putting their considerable cyber skills to work at an honest job. They are 21st century digital pickpockets. And like a pickpocket victim, you don't have to do anything to become a target other than be in the wrong place at the wrong time with your wallet (or, in this case, network) unprotected. In fact, 90% of reported ransomware attacks are the result of unintentional employee errors, with malware enticing unwitting end users to click on a link or open an email[5]. The remainder is comprised of angry employees or ex-employees who deliberately seek to sabotage the business, or attacks at a specifically identified high-profile enterprise in hopes of a big payday[2].

When it happens, don't get mad at employees or blame yourself; cybercriminals are very good at what they do. Great care is taken to emulate legitimate websites and business communications. Elaborate phishing schemes are devised. Technology is constantly evolving and the criminals are usually one step ahead of the good guys. The Internet of Things (IoT) and Bring Your Own Device (BYOD) policies mean there are more unprotected network entry points than ever[4]. Security professionals often don't know what to look for until it's too late (called a *Zero Day Threat*). Whereas some ransomware injects its code and wreaks havoc immediately, other types worm through a network collecting credentials and encrypting multiple systems and then lie dormant until the attacker is ready to spring the trap[6]. Either way, it comes as a surprise to the victim.

But cybercriminals have one thing in common with legitimate businesses: they want to get paid for their efforts. One of today's most popular ransom demands is for payment through Bitcoin. Virtually untraceable, Bitcoin provides a safe digital currency for criminals, but many businesses are unprepared to pay through this channel. Other means of payment include GooglePlay, iTunes, or Amazon gift cards – vehicles that allow for activation codes to be released online so the criminals can anonymously redeem the cash value. To prove their "trustworthiness," the attackers may send one file back decrypted to demonstrate they are capable of restoring data as promised to entice you to pay the ransom as quickly as possible. At the end of the day, cybercriminals want your money, not your data.

Assessing the Damage

There is no way to put a fixed number on the cost of a ransomware attack, although some sources put the estimate at hundreds of thousands of dollars per incident at a major enterprise. In addition to hard costs – the income lost due to a stoppage in business operations and possibly the expense of replacing damaged computing hardware, infected drives, etc. – companies must deal with potential compliance fines and legal fees if customer privacy was breached. Further, one event may result in multiple fines if more than one type of security standard was violated. There are also virtual costs – permanent loss of data and the time it takes to rebuild databases and restore infected systems. Then there are soft costs – soiling of the company's reputation among customers, the potential loss of future business, and diminished trust among supply chain partners[5]. And finally, the cost of paying the actual ransom demand (should you decide to go that route). Suffice it to say, every dollar spent on prevention is worth not having to experience an attack.

Alternatives & Outcomes

Let's assume your company has been hit with a ransomware attack. Your computer is frozen, all data is inaccessible, your phone is chirping with messages from employees and customers demanding answers while the ransomware clock is ticking. What do you do?

First, immediately disconnect the device(s) from the network. Not just the hardwired connection, but also deactivate any wireless or Bluetooth connectivity. Do **not** turn off power to the device; more on that in a bit.

Next, take a deep breath and consider your options[7,9]:

1. **Wipe your system clean and restore the data from a recent backup prior to the attack.** This should always be your first option as the business should have data backup policies and capabilities in place. This will be your "whew" moment as you dodge the bullet and praise your company for being prepared and allowing you to basically ignore (after reporting) the incident. (If not, may we suggest downloading the white paper *IT Disaster Recovery Planning: Essential to Business Survival*, to learn how to put a plan in place to minimize financial impact, reduce downtime and speed the return to normal operations after an outage no matter the cause.)

2. **Try to decrypt the system yourself.** There are many ciphers available on the web and if you know where to look and have the expertise, you might find a key to unlock your data without paying the ransom. But that could be time consuming and the clock is still ticking….

3. **Take the hit and start over.** Maybe you can't find the decryption tool, you didn't have much data to lose, or it can be easily reconstructed. Wipe the system and start rekeying. But keep in mind that 60% of businesses hit by a cyberattack do not recover if they did not have proper backup capabilities beforehand.

4. **Pay the ransom.** Evaluate the cost of the business interruption. If your business is bleeding money by the second or you do not have backup systems in place and the data is irreplaceable, this may be your best/last-ditch option. While there is a high probability of recovering your data – remember, cybercriminals want to get paid – there are no guarantees usable data will be returned, and it increases the likelihood of recurrence once the attackers know you are open to paying ransom[5].

RANSOMWARE ATTACK: *BEFORES & AFTERS*

The best defense is prevention. Security architects have accepted today's reality that virtually all devices will eventually become compromised or will be the target of an attempted hacking. Making any other assumption is a fatal mistake[10]. Therefore, the focus has shifted to strengthening IT defenses, employee education and implementing early detection technologies.

How do you detect something with zero notice when you don't know what form it will take? The answer lies in "heuristic analysis" which uses code patterns and behavioral anomalies to detect a potential threat and isolate the file before it does any damage[6]. Other businesses are moving to a *zero-trust security model* where everyone is a suspect and must prove their credentials every time before access to a system is granted[10].

Consider these actions 1) to reduce the chances of falling victim to a ransomware attack or 2) to implement after an attack in order to minimize the damage[4,5,6,7,8,9]:

Before: Minimize your exposure

- Install firewall management and security/malware detection software with real-time network scanning and keep it up to date.
- Implement rigorous and strict data backup procedures.
- Consider cloud resources or outsourcing data backup and threat detection to security service providers.
- Emphasize good password hygiene and the use of complex sequences.
- Train employees to recognize phishing scams and malware traps, such as:
  - Look for misspelled words and poor grammar in emails.
  - Check the URL for the origin of the site domain. Does it seem obscure?
  - Check the "From" line to see if the addressee is spoofed in emails.
  - If you receive a questionable email regarding a credit or debit card, do not call the support number provided in the email. When in doubt, call the number on the back of the card.
  - Never reply to very old emails sent by your company that get an unsolicited response.

After: Lock it down

- Immediately disconnect all infected devices from the network but DO NOT TURN OFF THE POWER. Shutting down the device may do more damage to data and/or destroy potential evidence. Disconnect wired and wireless ports; turn off any NFC or Bluetooth channels to isolate the device.
- If you have access to local or remote data backup systems, wipe the device and restore it to a point before the attack. If your company does not have a backup policy, create one!
- Do not insert a USB drive to try to copy the data, you will only infect the USB drive.
- DO NOT CONTACT THE ATTACKERS (unless you intend to pay the ransom).
- Immediately alert your company IT department or service provider and begin implementation of the company's IT Disaster Recovery Plan, which may include the following steps:
  - Identify the type and source of the ransomware. Evaluate the threat severity level to the business.
  - Review and select your option for dealing with the incident. Can a decryption tool be found?

RCN BUSINESS

Before: Minimize your exposure (cont.)

- Do not open macro-enabled files unless they are from a trusted source.
- Be wary of email notifications from shippers that include a code to enter to reschedule a package delivery.
- Getting a zipped file and the associated password to open it in the same email is a red flag. Legitimate businesses will send a zipped file and the password in two separate transmissions.

- Test your employees. Periodically send out a fake phishing scam and see if anyone clicks the bait. If so, time for further training.
- Establish an out-of-loop emergency contact system with other key members for safe communications during an outage.
- Update user network credentials and permissions, especially after dismissing a disgruntled employee.
- Have an incident response procedure in place. When an employee's device is targeted, they should know whom to call and next steps.
- Hire a Data Protection Officer (DPO) whose primary responsibility is to identify and exterminate threats before they cause damage.

After: Lock it down (cont.)

- Notify all supply chain members.
- Notify the proper authorities/law enforcement and your legal team.
- Notify your customers via alternative communication means that you are aware of the issue and addressing the situation.

- Afterwards, update your firewall management and security/malware detection software (it obviously needs it) or install it if you haven't already.
- Consider a third party or cloud service for assistance with data backup and threat detection.
- Implement the employee education and prevention steps listed in the "before" column to make sure it doesn't happen again.

Click here to download the White Paper, ***IT Disaster Recovery Planning: Essential to Business Survival***

In conclusion, the best offense is a good defense. With a little preparation and education, you can prevent your data from being held hostage. While there are no guarantees – technology is constantly evolving and identifying new strains of malware is a moving target – the cost of prevention pales in comparison to the price you might pay in the event of an attack. Don't wait until it's too late. Put the necessary steps in place today and you'll be glad you did tomorrow.

SOURCES & ACKNOWLEGEMENTS

[1] *Ransomware: Now a Billion Dollar a Year Crime and Growing*, nbcnews.com by Herb Weisbaum, January 9, 2017

[2] *2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB)*, Ponemon Institute, September 2017

[3] *https://techerati.com/features-hub/opinions/the-blase-attitude-of-smes-towards-cybersecurity-must-end/* by David Kay, January 25, 2019

[4] *https://www.eletimes.com/ransomware-how-to-prevent-a-ransomware-attack-what-all-you-need-to-know* by ELE Times, December 28, 2018

[5] *https://www.nojitter.com/security/developing-your-2019-cyber-security-checklist* by Gary Audin, January 4, 2019

[6] *https://www.pcmag.com/article/365993/how-it-can-defend-against-ransomware* by Wayne Rash, January 16, 2019

[7] *https://www.forbes.com/sites/forbestechcouncil/2018/12/27/battling-ransomware-how-to-respond-to-a-ransomware-incident/#1f1d1c9164dc* by Michelle Drolet, December 27, 2018

[8] *https://www.forbes.com/sites/forbestechcouncil/2019/01/14/battling-ransomware-how-to-prevent-a-ransomware-incident/#47aaf74e2ac2* by Michelle Drolet, January 14, 2019

[9] *http://www.mondaq.com/unitedstates/x/770102/Security/Ransomware+Recommendations+for+Preparation+and+Response* by Christopher E. Ballod, Frank Gillman and Sean Hoar, January 10, 2019

[10] *https://www.nojitter.com/why-you-should-embrace-zero-trust-networking* by Sorell Slaymaker, August 09, 2018

©2019 RCN Telecom Services, LLC. All Rights Reserved. | www.rcn.com/business