WHITE PAPER

RANSOMWARE

HOW TO PROTECT YOUR BUSINESS AND CUSTOMERS FROM A DIGITAL PANDEMIC

CYBERSCOUT™

1

ORGANIZATIONS OF ALL SIZES, IN EVERY INDUSTRY, ARE IDEAL TARGETS FOR RANSOMWARE ATTACKS. THE NATURE OF THE ATTACKS MAKES PREVENTIVE MEASURES THE CLEAR PATH TO VALUE AND BUSINESS CONTINUITY.

If your company relies on data to do business, it's a target for a ransomware attack.

Easy to perpetrate and instantly profitable, this increasingly common, sophisticated and costly breed of malware encrypts victims' files and demands ransom for the decryption key. Nasty ransomware strains will threaten to delete data permanently if the ransom isn't paid quickly.

Just how valuable is data to the day-to-day operations of your business? For a quick but relevant answer, consider these questions:

- What would you be willing to pay to unlock encrypted files that contained all your patient appointments, customer account information or other vital information?
- What would it cost your customer relationships if you had to request fresh copies of their data after a ransomware attack?
- How long could your business pay its operating costs without incoming revenue?
- Does your company know the best practices for preventing and recovering from ransomware?

Whatever number you're willing to pay in ransom, it's likely to be significantly more than an investment in preventive measures.

While the pressure's off, design and implement a plan to protect your data. Then, when ransomware strikes, you'll be up and running in a few hours. The details of your plan will depend on your company's unique needs and structure, but it will always include these best practices:

- **Employee training.** Empower them to detect and deny criminals' increasingly effective efforts.
- **Process audit.** Ensure that your recovery plan and response team are prepared to act quickly.
- **Technology recommendations.** Optimize your IT architecture to detect and eliminate as many strains of ransomware as possible.

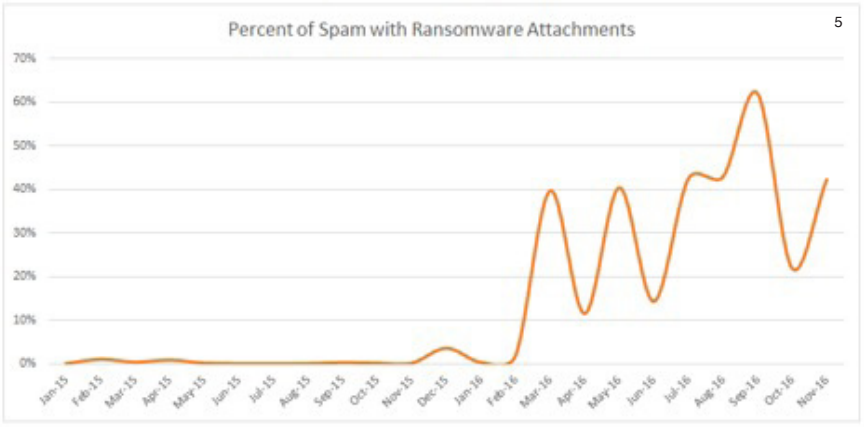
2

RANSOMWARE IS EFFICIENT, LOW-RISK AND EASY TO PERPETRATE. EARLY FORMULATIONS OF RANSOMWARE PROVED PROFITABLE AND ENCOURAGED PERPETRATORS TO INVEST IN MORE SOPHISTICATED INFECTION METHODS.

WHY RANSOMWARE HAS BECOME SO POPULAR AMONG CYBER CRIMINALS

Seemingly out of nowhere, ransomware has exploded into the business world since 2014. It is becoming the preferred revenue-generating mechanism for the Dark Web for several reasons:

- **It's efficient.** Every organization has unique information that is vital to its operations. The inability to access that data, the ensuing disruption to regular revenue-generating operations, and the potential harm to your reputation all add up to one compelling argument to pay the ransom.[1]
- **It's low risk.** Most ransoms are extorted in cryptocurrencies (e.g. Bitcoin), which are impossible to trace. Furthermore, criminals don't need to sell the data on the black market in order to achieve a profit. The value of the decryption key is solely with the victim. Because ransomware requires fewer steps, it reduces criminals' chances of making mistakes that would reveal their identities.[2]
- **It's easy to deliver.** Between 59 percent[3] and 97 percent[4] of ransomware enters through emails with malicious links and malicious attachments.



5

Above all these factors, the primary reason for ransomware's popularity with criminals is the simplest: it's extremely profitable.

1 "Incidents of Ransomware on the Rise," FBI, April 29, 2016, https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise.
2 ibid.
3 "Understanding the Depth of the Global Ransomware Problem," Osterman Research, August, 2016, https://www.malwarebytes.com/surveys/ransomware/.
4 "2016 Q3 Malware Review," PhishMe, https://phishme.com/2016-q3-malware-review/.
5 "Ransomware tops the spam charts in 2016," IBM X-Force, December 9, 2016, https://exchange.xforce.ibmcloud.com/collection/Ransomware-tops-the-spam-charts-in-2016-1332816b2536befc46fb600ab51613da.

3

NOW THAT CRIMINALS HAVE SEEN HOW PROFITABLE RANSOMWARE CAN BE, THEY'RE INVESTING HEAVILY IN MORE SOPHISTICATED STRAINS. THEY'VE EVEN DEVISED A PAY-AS-YOU-GO MODEL FOR PEERS WHO LACK PROGRAMMING RESOURCES.

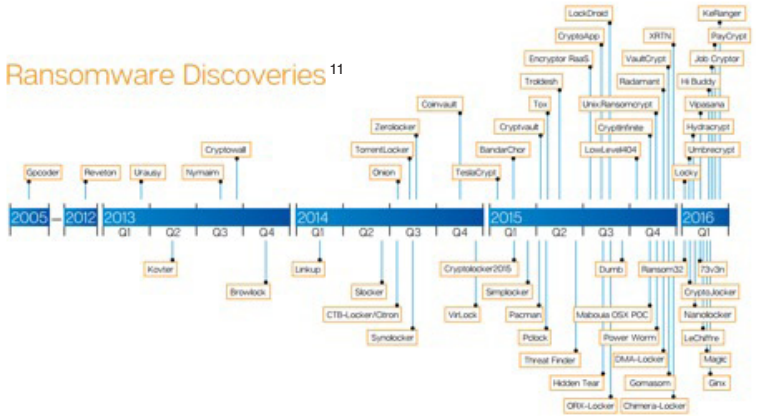
SURVEY OF RANSOMWARE IMPACTS

Ransomware has achieved significant profits for its users during its brief existence.

- Cryptowall, one of the earliest and most successful forms of ransomware, generated at least $325 million in revenue for its creators.[6]
- 35 percent of business executives who have encountered ransomware attacks in the workplace said their companies paid to resolve the attack, with half of those paying more than $10,000 and 20 percent paying more than $40,000.[7]
- In the first quarter of 2016, cyber criminals collected $209 million in successful ransoms. The actual impact was probably bigger, since some victims may have chosen not to report the crime.[8]

Due to the relatively low barrier to enter this "business model" and the potential profits, ransomware attacks against corporate users increased 600 percent between 2014 and 2016.[9]

The variety of ransomware families has increased, too. Between December 2015 and June 2016, Proofpoint observed a 600 percent increase among a representative sample of new ransomware families, noting that the numbers reflected the growing diversity of ransomware.[10]



6 "Cyber Threat Alliance Cracks The Code On CryptoWall Crimeware Associated With $325 Million In Payments," Palo Alto Networks, October 29, 2015, https://www.paloaltonetworks.com/company/press/2015/cyber-threat-alliance-cracks-the-code-on-cryptow

7 "Businesses More likely to Pay Ransomware than Consumers," IBM, December 14, 2016, https://www-03.ibm.com/press/us/en/pressrelease/51230.wss

8 "Cyber-extortion losses skyrocket, says FBI," CNN, April 15, 2016, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/.

9 "Ransomware's history and evolution in facts and figures," Kapersky Lab, June 22, 2016, https://usblog.kaspersky.com/ransomware-blocker-to-cryptor/7327/.

10 "Quarterly Threat Summary APR-JUN 2016," Proofpoint, https://www.proofpoint.com/sites/default/files/proofpoint-quarterly-threat-report-q216.pdf.

11 "Ransomware Infections Grew 14 Percent in Early 2016, April the Worst Month," SoftPedia, May 5, 2016, http://news.softpedia.com/news/ransomware-infections-grew-14-percent-in-early-2016-april-the-worst-month-503743.shtml.

4

APPLY THESE RECOMMENDATIONS TO IMPROVE YOUR CHANCES AGAINST MORE SOPHISTICATED, AGGRESSIVE AND EXPENSIVE RANSOMWARE ATTACKS.

Today, criminals without programming resources can turn to Ransomware-as-a-Service (RaaS) platforms to rent malware ready for infection for a flat fee.[12]

Forbes reported on one RaaS called Stampado: for $39/month, subscribers just need to devise a mechanism to infect victims' computers and servers. Stampado will take care of the rest: detection-evasion, encryption, a 96-hour countdown timer, and the deletion of a random file every six hours until the ransom is paid.[13]

Now for some good news. You have a variety of options to keep your data safe.

HOW TO PROTECT YOUR COMPANY AND CUSTOMERS

Prevention is the best defense. Here's what we recommend:

Back up files regularly

If your data is encrypted, a backup may be the only way to recover it. Decide on the longest stretch of time you are comfortable going without a backup. Then back up your data that frequently. If you don't want to lose more than a day's worth of data, back up every 24 hours.

Secure your backups by ensuring they are not connected to the computers and networks they are backing up. The cloud or a data center works just fine. Note that some ransomware can lock cloud-based backups when the system is configured to back up continuously. Check with your provider about how they mitigate the threat.

In one recent survey of IT professionals, just 42 percent of respondents who had experienced a ransomware attack reported having a completely successful recovery. Common reasons for incomplete recovery included unmonitored and failed backups, loss of accessible backup drives that were also encrypted, and loss of between one and 24 hours of data from the last incremental backup.[14]

Focus on user awareness and training

The majority of ransomware succeeds by tricking users into clicking malicious email attachments and links. Teach employees how to: spot phishing emails; to avoid clicking on banners or links without knowing exactly what they are, where they go, and whom they're from; and to visit only trusted sites.

If you have an internal or client-facing newsletter, share summaries of the latest permutations of ransomware.

Maintain next-generation anti-malware software

In some cases, these applications can catch the ransomware packages on their way in. Ensure that these solutions are set to update automatically and conduct regular scans.

12 "By The Numbers: Ransomware Rising," Trend Micro, June 10, 2016, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/by-the-numbers-ransomware-rising.
13 "Ransomware As A Service Being Offered For $39 On The Dark Net," Forbes.com, July 15, 2016, http://www.forbes.com/sites/kevinmurnane/2016/07/15/ransomware-as-a-service-being-offered-for-39-on-the-dark-net/.
14 "Ransomware by the Numbers: Must-Know Ransomware Statistics 2016," Barkly, 2016, https://blog.barkly.com/ransomware-statistics-2016#0.

5

YOUR PREVENTION MEASURES SHOULD INCLUDE THREE COMPLEMENTARY STRATEGIES: EMPOWERING EMPLOYEES TO DETECT AND DENY ATTEMPTED RANSOMWARE INFECTIONS, AUDITING AND PRACTICING YOUR PLANNED RESPONSE TO A SUCCESSFUL ATTACK, AND OPTIMIZING YOUR INFORMATION TECHNOLOGY ARCHITECTURE TO DETECT AND ELIMINATE RANSOMWARE THREATS AUTOMATICALLY.

Keep all software current

The fewer bugs you have, the harder it becomes to infect your system. Patch all endpoint device operating systems, software and firmware as vulnerabilities are discovered, including Adobe Flash, Java, web browsers, etc. This precaution can be made easier through a centralized patch management system.

Implement protective IT policies

Only allow systems to execute programs known and permitted by security policy.

Prevent programs from executing in common ransomware locations, such as temporary folders supporting popular internet browsers or compression/ decompression programs, including those located in the AppData/LocalAppData folder.

Disable macro scripts from files sent via email. When possible, use Microsoft Office Viewer software to open Office files sent via email instead of the full Office Suite applications.

Categorize and segment data based on its value and utility. For example, sensitive research or business data should not reside on the same server and/or network segment as an email environment.

Configure firewalls to block access to known malicious IP addresses.

Disable Remote Desktop Protocol (RDP) if it is not being used.

Make sure there are no mapped drives a virus can access easily. Some ransomware families like VirLock and Locky are able to access and encrypt shared network drives, spreading the ransomware infection across an entire organization.

Tighten email policy

Strengthen spam filters to prevent phishing emails from reaching end users, to authenticate inbound email to prevent email spoofing, and to filter executable files from reaching end users.

Establish a phishing testing capability. Periodically send fake phishing emails to employees with a safe landing spot. See how many people fall for it. Use the results as teachable moments and gentle reminders.

Plan your response

Make sure your current breach response plan accounts for ransomware. It is possible to shut down and contain an attack if you act as soon as you recognize it.

Make your response plan more than a technical exercise. It isn't the responsibility of network administrators or software engineers to resolve the expensive, sticky issues that follow a technical resolution: notifying clients and staff in accordance with state mandates, interfacing with the media and law enforcement, etc.

Stay informed

Keep up with cyber security news. Alert today is alive tomorrow. Be sure to tell your friends, relatives and colleagues about the latest threats.

6

FOR MORE ON THE DEVELOPMENT OF A DATA BREACH RESPONSE PLAN, **DOWNLOAD OUR FREE WHITE PAPER** "HOW TO NAVIGATE THE FIRST 48 HOURS."

CONCLUSION

You now know how to estimate the potential impact ransomware can wreak on your company. Given its growing success and proven efficacy, you can assume that it isn't going away any time soon.

Fortunately, you can defend yourself. If you follow the guidance we've offered here, you will be in a significantly more resilient position.

We hope you'll share what you've learned with your colleagues, employees and customers. If every business were in a position to avoid paying a ransom, criminals could become discouraged and stop using it.

That change has to start somewhere. Why not with your organization?