MAPPING THE RANSOMWARE LANDSCAPE

Understanding the Scope and Sophistication of the Threat

EXECUTIVE SUMMARY

When a cyber threat grows in magnitude by 35 times in one year, every organization should pay heed. This is exactly what happened with ransomware. Hacktivists targeted organizations around the world representing myriad industry segments and businesses of virtually every size. Traditional security approaches are not sufficient to thwart ransomware attacks. Advanced models using next-generation firewalls, layered security, and proactive threat intelligence are a requisite.

Ransomware-as-a-service and affiliate models have lowered the entry bar for cybercriminals. And monetary technologies like bitcoin make it virtually impossible for law enforcement authorities to track ransom payments. With the exponential growth in ransom paid to ransomware hacktivists, the prospect that this will continue—and at a faster rate—in coming years is great. Recognizing the growing threat, banks are stocking up on bitcoin so that their customers (and themselves) can quickly pay cybercriminals to unlock hacked data.

The financial impact to organizations is much larger than just the ransom being paid to cybercriminals. Downtime translates into thousands and often hundreds of thousands of dollars in lost revenue and productivity. Organizations across multiple industry sectors can attest to these implications.

SCOPE OF THE THREAT

Data is at the heart of most organizations today—from small businesses to large enterprises. Digitization of more and more company assets, in addition to the growing importance of the cloud, puts data in the crosshairs of cybercriminals. It is becoming a much bigger problem today, with data growing at a rate of more than double every two years.[1]

Recognizing the value of data, cybercriminals are increasingly turning to ransomware as a means of monetization. They infiltrate IT systems and access data through various hacks, encrypting, locking, and exfiltrating files. Unable to access information that is critical to their businesses, hacked organizations are forced to pay for the information to be released by the cybercriminals. The sophistication of many of these efforts has evolved to the point where cybercriminals provide their victims with live customer support that walks them through the processes to remit payment as well as regain access to their data and IT systems.

RANSOMWARE ATTACKS SKYROCKET

So how serious is the threat of ransomware? Last year, ransomware attacks more than doubled.[2] Upwards of 4,000 ransomware attacks happen daily, infecting an average of between 30,000 and 50,000 devices monthly.[3] And the potential for additional growth is huge. Even with this rate of increase, ransomware only comprises two percent of total malware attacks today.[4]

The financial repercussions of ransomware skyrocketed as well. Consider the following. In 2015, a total of $24 million in ransom was paid out; in 2016, that number shot up to more than $850 million.[5] The amount being demanded by cybercriminals is following a parallel path: the average demand for every attack jumped from $294 in 2015 to $679 in 2016.[6]

But the biggest impact of ransomware is not in the ransoms being paid. Sixty-three percent of organizations that experienced a ransomware attack in the past year indicate it led to business-threatening downtime. Another 48 percent report it resulted in the loss of data or hardware. And for those organizations that pay a ransom in exchange for being able to recover their data (42 percent admit they paid the ransom), one in four never recovered the data.[7] This is why the FBI recommends that victims not pay ransoms.

JUST THE TIP OF THE ICEBERG

Yet these numbers are likely not a true representation of the extent of the problem. Ransomware attacks are vastly underreported, with fewer than one in four incidents being reported. Over half of businesses admit they experienced a ransomware attack sometime during the past year.[8] Thirty-four percent of them lost money, and 20 percent were forced to shut down their business! When these factoids are factored into consideration, the financial impact is alarming. But it gets worse: 3.5 percent indicated lives were put at risk as a result of the effects of the ransomware attack.[9]

For organizations thinking they are too small to be a target for ransomware attacks from cybercriminals, think again! Often lacking a dedicated in-house IT expert and managing IT systems lacking the necessary controls, small businesses aren't immune to ransomware attacks. Indeed, operating without the proper data protections in place to defend against, prepare for, and recover from ransomware, these businesses are quickly becoming a prime ransomware target for cybercriminals. A recent report finds that downtime from ransomware costs small businesses around $8,500 an hour. This adds up to losses exceeding $75 billion annually.[10]

Ransomware infected **30K** to **50K** devices monthly

$850M

was paid out to **Ransomware attacks** in 2016

Ransomware is underreported. Fewer than **1 in 4** report the attack

63%

of organizations experienced **business-threatening** downtime

34% of companies lost money

BUSINESS IMPACT OF RANSOMWARE

The cost in system downtime and the inability to access information due to ransomware attacks equates to billions of dollars today, a number that could rise into the tens of billions as ransomware hacktivists go after IoT devices.

DOXXING

Cybercriminals are an innovative bunch. Rather than threatening to delete locked data, some cybercriminals are beginning to threaten to release it (aka "doxxing"). For organizations that deal with private and sensitive customer data, like financial services, hospitals, law firms, and others, this can have deleterious consequences. In addition to the impact to brand reputation, regulations such as the Health Information Portability and Accountability Act require customer notifications and other painstaking activities that can quickly tally into hundreds of thousands—or even millions—of dollars.

STORING UP BITCOIN FOR A "RANSOM" DAY

The impact of ransomware reaches beyond those organizations that are hacked. Take banking as an example. As the potential impact resulting from lost data or the inability to access data is measured in minutes or even seconds, businesses cannot wait several days for cybercriminals to grant them access to their hacked data. Therefore, banks are storing up bitcoin—as it typically takes three to five days to get it in stock—so that their customers can pay cybercriminals immediately.[11]

HOW RANSOMWARE HAPPENS

DISTRIBUTION OF RANSOMWARE

So, how does ransomware happen? Let's begin by addressing how it is distributed. Any digital means can be used: email, website attachments, business applications, social media, and USB drivers, among other digital delivery mechanisms. Emails remain the number one delivery vector, with cybercriminals preferring to use links first and attachments second.

- Email Links, 31%
- Email Attachments, 28%
- Website Attachments, 24%
- Unknown Sources, 9%
- Social Media, 4%
- Business Applications, 1%

In the case of email, phishing emails are sent as delivery notifications or fake requests for software updates. Once a user clicks on the link or the attachment, there is often (but less so recently) a transparent download of additional malicious components that then encrypt files with RSA 2,048-bit private-key encryption, leaving it nearly impossible for the user to decrypt the files. In other instances, ransomware is embedded as a file on a website, which when downloaded and installed, activates the attack.

DIFFERENT TYPES OF RANSOMWARE

Ransomware attacks come in different forms. This past year has seen a substantial evolution in ransomware attacks. Traditional ransomware goes after your data, locking files until the ransom is paid. But with the rapid growth in Internet of Things (IoT) devices, a new strain of ransomware emerged. It doesn't go after an organization's data, but rather it targets control systems (e.g., vehicles, manufacturing assembly lines, power systems) and shuts them down until the ransom is paid.

Let's take a quick look at some of the most prevalent types of ransomware that exist today:

- **Off-the-Shelf Ransomware.** Some ransomware exists as off-the-shelf software that cybercriminals can purchase from darknet marketplaces and install on their own nefarious servers. The hacking and encryption of data and systems are managed directly by the software running on the servers of the cybercriminal. Examples of off-the-shelf ransomware include Stampado and Cerber.
- **Ransomware as a Service.** CryptoLocker is perhaps the most well-known ransomware-as-a-service model. Since its servers were taken down, CTB-Locker emerged as the most common ransomware-as-a-service attack method. Another ransomware as a service that is rapidly growing is Tox, a kit that cybercriminals can download. The result produces a dedicated executable file that can be installed or distributed by the cybercriminal, with 20 percent of gross ransoms being paid to Tox in bitcoin.
- **Ransomware Affiliate Programs.** Cybercriminals who sign up as an affiliate get access to a ransomware-as-a-service model and can distribute it to their own selection of targets, often garnering as much as 70 percent of the profits.[12]

- **Attacks on IoT Devices.** Ransomware infiltrates IoT devices that control systems critical to a business. It shuts down those systems until a ransom is paid to unlock them. With some of these IoT devices controlling mission- and life-critical systems, the damage resulting from not unlocking them in time can be substantial or even catastrophic.[13]

Ransomware families and variants exploded in 2016, growing tenfold. FortiGuard Labs saw multiple new variants every day throughout 2016. Interestingly, in addition to polymorphic code, ransomware often uses metamorphic code to change its digital identity while operating the same way. This rapid growth and constant evolution makes it even more difficult for organizations that rely on traditional signature-based antivirus solutions to keep pace. By the time one strain has been identified and blacklisted, cybercriminals have already moved to a new variation. It thus makes sense that nearly three-quarters of organizations that experienced ransomware attacks in 2016 suffered one or more infections.[14]

Virtually every operating system is targeted by ransomware today. Attacks also extend to the cloud and mobile devices. For example, Android ransomware attacks more than quadrupled over the period of a year starting in April 2015.[15]

TYPICAL RANSOMWARE WORKFLOW

With the majority of ransomware attacks occurring via spear phishing, where an email, purportedly from a known individual or company, targets an individual. Historically, ransomware delivery predominantly used spear phishing. In those instances, the email includes an infected link or an attachment. These email links or attachments are easily changed, enabling cybercriminals to prepare fresh sites in bulk or attachments limited to simple code for downloading additional components at a later time, enabling them to bypass email filters and land in the end-user's inbox.

In other instances, a user visits an infected website or business application from which the ransomware is launched. Often the ransomware is configured to launch and download the larger malicious payload without the user even clicking on anything. Finally, in growing instances, an infected IoT device is used to control—normally shut down—mission- or life-critical systems.

Assuming the ransomware successfully launches, the following is the typical workflow sequence:

1. Once the user clicks on the infected link or attachment, the ransomware launches through a PowerShell or other extension.
2. The infected device communicates with the cybercriminal's server (often through indirect means such as Google Apps) for instructions. This often includes the download of new payloads, which subsequently encrypts files on the individual's device.
3. Once this is completed (sometimes in a matter of less than one minute), a ransom note is delivered with a demand for bitcoin in exchange for a decryption key.
4. At the same time, the ransomware seeks to move laterally across the company's network to infiltrate other systems.

A recent strategy of ransomware hacktivists is to target and compromise vulnerable business servers.[18] This enables them to identify and target hosts, multiplying the number of potential infected servers and devices on a network. This compresses the attack timeframe, making the attack more viral than those that start with an end-user. This evolution could translate into victims paying more for decryption keys and an elongation of the time to recover the encrypted data.

SAAS-BASED INFECTIONS

When asked to indicate which SaaS-based applications they have seen infected by ransomware, IT professionals in a recent survey indicate:

- Dropbox, 70%
- Microsoft Office 365, 29%
- Google Apps, 12%
- Box, 6%
- Salesforce, 3%

EVOLUTION OF RANSOMWARE[16]

Top Ransomware Families in 2016

1. Locky
2. CryptoWall
3. CryptXXX
4. Bitman
5. Onion (CTB-Locker)

Top Ransomware Families in 2015

1. CryptoWall
2. Blocker
3. Onion (CTB-Locker)
4. Snocry
5. Bitman

97% of phishing emails now deliver ransomware.[17]

NO IMMUNITY

Organizations that believe they're immune from a ransomware attack because they have all of the basic security measures in place need to think again. In a poll of hosted solutions providers, most had a base layer of security defense in place.[19]

- Antivirus & Anti-malware Software, 93%
- Email and Spam Filters, 77%
- Patched/Updated Apps, 58%
- Ad and Pop-up Blockers, 21%

GOING VIRAL

Ransomware is viral, spreading across networks 63 percent of the time. In the remainder of instances, it remains isolated to a single system.[20]

REAL-LIFE ATTACKS

Nearly every industry sector and organization size is affected by ransomware. Manufacturing tops the list when it comes to percentage of total ransomware per industry (16 percent). The utilities and energy sector is a close second (15.4 percent), with technology, professional services, retail, healthcare, financial services, and legal with a substantial share. Several reports tag professional services as an area where there has been the fastest growth in ransomware attacks.

The following is an examination of the implications ransomware is having in some of these leading industry segments. The examination will call out specific examples where businesses have been hacked, not only paying the price of ransom but suffering serious financial and operational impact.

HEALTHCARE

Healthcare is a sector where there is much cause for concern regarding ransomware. This makes a lot of sense, considering that many IT systems and data in healthcare are connected to patient care. Any system downtime or inability to access information could put lives at risk. Even if the ransomware attack doesn't affect system and data used for patient care, the loss of patient records can incur tangible fines and time remediating the damage.

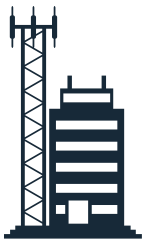
With doxxing, whereby cybercriminals threaten to release rather than delete private information, becoming a tactic ransomware cybercriminals employ, the repercussions are even more serious. Add ransomware attacks on IoT devices used to deliver patient care, and the implications become life-threatening.

The attacks are not going to slow down in the coming year; ransomware attacks on healthcare organizations are expected to double in the next year. Compared to other industry segments, personal health information is 50 times more valuable on the darknet than financial information. Stolen health records can garner as much as $60 per record.[21] Examples of healthcare organizations being hit with ransomware are myriad. Consider these three examples:

Hacktivists gained access to a MongoDB database containing protected health information for 200,000 patients of the *Emery Brain Health Center.* The database was wiped clean and replaced with a ransom demand for $180,000 in bitcoin for its safe return.

Hollywood Presbyterian Medical Center in Hollywood, California, declared a state of internal emergency after its systems were infected with Locky ransomware. Physicians and other caregivers were locked out of electronic health records, forcing staff to use pen and paper for logging patient data, and fax—instead of email—for communicating with each other. The hacktivist demanded 40 bitcoin (or about $17,000) in exchange for a key to decrypt the locked files, which the hospital paid.

But cybercriminals do not always grant victims access to their information. In the case of the *Kansas Heart Hospital in Wichita, Kansas*, the hospital paid the initial ransom, but the hacktivists did not fully unlock the files and demanded more money to do so. It was at that juncture that the hospital elected to decline the additional ransom.



UTILITIES AND ENERGY

The utilities and energy sector experiences as many cyberattacks as any other industry. The industrial control systems (ICS) used to manage and run the critical infrastructure for utilities and energy companies present cybercriminals with new opportunities—and this includes ransomware hacktivists.

Fortunately, in the case of the *Lansing Board of Water & Light* that serves the city of Lansing, Michigan, its ICS was not affected by a spear-phishing ransomware attack that forced the utility to shut down its computer server and phone lines for a week. Likely the result of an employee opening an email containing an infected file, the ransomware quickly locked the utility from its email, accounting system, printers, and other technologies. Only after a week of remediation was the utility able to bring its systems back online.

MANUFACTURING

Manufacturing is fast becoming a high-value target for ransomware hacktivists. Manufacturers are at higher risk than other industry segments, as they are not under the same regulatory and compliance constraints as other industries like financial services.

In addition to IT systems containing intellectual property and proprietary information, manufacturers place a high premium on efficient processes and operations. An interruption can incur downtime that translates into less financial profitability. Time is money for a manufacturer. Thus, manufacturers can see greater value in paying a ransom to get their systems up and running as quickly as possible.

Last year, of the recorded 8.63 million ransomware attacks on manufacturers, over three-quarters were on those with 1,000 employees or more. The Necurs botnet was the most prevalent ransomware delivery vehicle in manufacturing, comprising 41 percent of all attacks. Conficker is a distant second at 17.7 percent.[23]

A concrete manufacturer experienced over a week of operational downtime after one of its employees clicked on an email attachment infected with CryptoWall ransomware. It propagated throughout the company's network and encrypted accounting data and files critical to several production systems. It was discovered at the beginning of the business day when a worker was unable to access production files to initiate manufacturing. Even though the company paid the ransom after two days, some of its accounting files were not unlocked. Without backups of that data, the company had to undertake a lengthy accounting recovery project.

EDUCATION

News headlines about ransomware attacks typically focus on breaches in healthcare, financial services, and other industry sectors. But education ranks high on the list of organizations being targeted with ransomware. Why? Educational institutions possess social security numbers, medical records, financial data, and intellectual property of faculty, staff, and students, making them lucrative targets. Add that cybersecurity preparedness is among the last among industry segments for K-12 schools and post-secondary schools, it makes full sense why cybercriminals are targeting them.

The *University of Calgary* experienced a ransomware attack that locked its email server. The university paid a $16,000 ransom in exchange for a key to unlock the encrypted server files. Fortunately, the IT staff isolated the infiltration before other systems were affected.

Los Angeles Valley College paid nearly $28,000 in bitcoin after a ransomware attack locked hundreds of thousands of files on its computer network, email, and voicemail systems. The infection was identified on December 30, 2016, and the college elected to pay the ransom on January 4, 2017, a day after classes started for the winter semester.

Ransomware in education is a global issue. *Queen's University in Belfast, Ireland*, knows. Three ransomware attacks successfully infiltrated its network last year. In one instance, Queen's University paid a ransom of approximately $600 after hacktivists infected a Windows XP server containing documents and images.

FINANCIAL SERVICES AND BANKING

The breadth of information financial services and banks store about their customers makes them prime targets for ransomware attacks. Financial services firms and banks agree: 55 percent list ransomware as the biggest cyberattack threat vector. Nearly one-third of them also say they have lost between $100,000 and $500,000 due to ransomware attacks.[24]

Credit unions and small banks are seeing significant jumps in ransomware hacktivism. They experienced 54 percent of total incidents in financial services and banking in 2015, compared to 81 percent in 2016.[25] This is largely due to the fact they traditionally have smaller cybersecurity budgets than larger counterparts.

GOVERNMENT

Nearly 10 percent of organizations impacted by a ransomware attack are in the public sector. With critical information contained on their systems, government agencies offer cybercriminals an alluring target.

The state of Ohio issued a warning to local municipalities last year, noting that ransomware attacks are on a steep incline and that local municipalities need to heed those threats by instituting the right technologies and processes.

Multiple local Ohio municipalities were hit with ransomware during the past year. More than 170,000 voting records in *Henry County* were compromised, with the hacktivist threatening to release them unless a ransom was paid. No ransom was remitted, and the records have not yet been released to date.

The computer systems for the *Morrow County Ohio Court* were infected with ransomware. The county elected not to pay the bitcoin ransom, and the files were destroyed by the cybercriminals. Unfortunately, the backup systems for the court system were not up to date, and Morrow County possessed only hard copy files for backup. To restore the files from the hard copies cost the county upwards of $30,000 in staff cost.

Cybercriminals are even targeting law enforcement. The computer systems used by the *Lincoln County Sheriff's Office in Maine* were infected with ransomware. After attempting several times to recover the information, the law enforcement agency elected to pay approximately $300 in bitcoin to the hacktivist for the information.

TAKEAWAYS

With cybercriminals reaping a thirty-fivefold increase in their earnings from ransomware attacks in 2016, the frequency and sophistication of the attacks will most assuredly increase in velocity and scope. Organizations will do well to heed the following takeaways as ransomware evolves and mutates into an ever-increasing threat to organizations of virtually every shape and size:

1. **Stop Known Threats.** Seek out a cybersecurity solution that stops known ransomware threats across all attack vectors. This requires a layered security model that includes network, endpoint, application, and data center controls powered by proactive global threat intelligence.
2. **Detect New Threats.** As existing ransomware is constantly morphing and new ransomware is being released, it is important to institute the right sandbox and other advanced detection techniques to pinpoint the variants across those same vectors.
3. **Mitigate the Unseen.** Real-time actionable intelligence must be shared between the different security layers (and generally vendor products) and even extended to the broader cybersecurity community outside of your organization such as Computer Emergency Response Teams (CERTs), Information Sharing and Analysis Centers (ISACs), and industry coalitions like the Cyber Threat Alliance. This rapid sharing is the best way to respond quickly to attacks and break the kill chain before it mutates or spreads to other systems or organizations.
4. **Prepare for the Unexpected.** Segmentation of network security helps protect against ransomware wormlike behavior such as that of SamSam and ZCryptor. Data backup and recovery is just as important. Organizations that have recent data backups are able to spurn demands for a ransom and quickly and easily recover their systems.
5. **Back Up Critical Systems and Data.** Although it can be a time-consuming process to restore an encrypted system, as well as an interruption to business operations and a drain on productivity, restoring a backup is a far better option than being held hostage with no guarantee that your ransom payment will result in your data and systems being unlocked and restored. In this case, you need the right technology, processes, and even business partner to ensure your data backups meet business requirements and their recovery can be done expeditiously.

[1] "The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things," IDC, April 2014.

[2] "Non-Malware Attacks and Ransomware Take Center Stage in 2016," Carbon Black Threat Report, 2016.

[3] Minal Khatri, "Ransomware Statistics – Growth of Ransomware in 2016," Systweak, August 25, 2016.

[4] "Non-Malware Attacks."

[5] Ibid.

[6] Khatri, "Ransomware Statistics."

[7] "State of the Channel Ransomware Report 2016," Datto, 2016.

[8] Angela Moscaritolo, "Ransomware Hit 40 Percent of Businesses in the Last Year," PC Magazine, August 3, 2016.

[9] Ibid.

[10] "Non-Malware Attacks."

[11] Adam Chandler, "How Ransomware Became a Billion-Dollar Nightmare for Businesses," The Atlantic, September 3, 2016.

[12] Vincent Weafer, "Franchising Ransomware," DARKReading.com, July 1, 2015.

[13] Ben Dickson, "What Makes IoT Ransomware a Different and More Dangerous Threat?" TechCrunch, October 2, 2016.

[14] "The Complete Guide to Ransomware," Barkly, accessed January 30, 2017.

[15] "Khatri, "Ransomware Statistics."

[16] "Non-Malware Attacks."

[17] "2016 Q3 Malware Review," PhishMe, October 2016.

[18] "Ransomware Getting More Targeted, Expensive," KrebonSecurity.com, September 20, 2016.

[19] "State of the Channel Ransomware Report."

[20] Ibid.

[21] Jennifer Schlesinger, "Dark Web Is Fertile Ground for Stolen Medical Records," CNBC, March 11, 2016.

[22] Erin Dietsche, "12 Healthcare Ransomware Attacks of 2016," Health IT & CIO Review, December 29, 2016.

[23] Bill McGee, "Move Over Healthcare, Ransomware Has Manufacturing in Its Sights," Fortinet Blog, June 6, 2016.

[24] G. Mark Hardy, "From the Trenches: 2016 Survey on Security and Risk in the Financial Sector," SANS Institute, October 2016.

[25] "Cyber Attacks on Financial Firms Up; Ransomware Attacks Way Up," Insurance Journal, July 22, 2016.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

Feb 09, 2017