FORTINET

WHITE PAPER

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 attention. This is exactly what happened with ransomware. Hacktivists have targeted organizations from many different industry segments, as well as businesses of virtually every size. Piecemeal approaches to security are not sufficient to thwart ransomware attacks. Integrated models using next-generation firewalls, layered security, and proactive threat intelligence are critical when mounting a defense against cyberattacks.

Ransomware-as-a-Service (RaaS) and other kit-like tools have lowered the entry bar for cyber criminals enabling even novice attackers to be successful against scattered security infrastructures. 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 their customers can quickly pay cyber criminals to unlock hacked data.

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

From 2018 to 2019, the number of ransomware detections rose by 365%.[1]

Over the past year, the number of new ransomware variants increased by 46%.[2]

Scope of the Threat

From small and midsize businesses (SMBs) to large enterprises, data is at the heart of most organizations today. However, digitization of more and more company assets, in addition to the growing push to the cloud, puts data in the crosshairs of cyber criminals. While 90% of the world's data was created in the last two years, in that same time span, data breaches were up 54%.[3]

Recognizing the value of data, cyber criminals 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 cyber criminals. The sophistication of many of these efforts has evolved to the point where cyber criminals 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

How serious is the threat of ransomware? Ransomware attacks more than doubled last year, with hackers modifying attack methods for more lucrative payouts.[4] Yet at the same time, only one in three organizations say they are confident they can track and remediate attacks.[5]

The financial repercussions of ransomware skyrocketed as well. Ransomware is expected to have a global impact of $20 billion by 2021.[6] Ransomware demands commonly reach six-figure sums, and because the transfer is often made by bitcoin, it is relatively simple for cyber criminals to launder it without it being traced.[7]

The indirect costs are those of business interruption that are associated with a ransomware attack. In the public sector, 42% of organizations have suffered a ransomware incident in the last 12 months, with 73% of those experiencing two or more days of downtime as a result.[8]

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. A new report reveals that cyber crime may be widely underreported. Over half of respondents said they believe most enterprises underreport cyber crime, even when required.[9]

Last year, more than 70 U.S. state and local governments were hit with ransomware attacks.[10]

For organizations thinking they are too small to be a target for ransomware attacks from cyber criminals, it's simply no longer the case. Often lacking a dedicated in-house IT expert and managing IT systems lacking the necessary controls, small businesses aren't immune to ransomware attacks. Discouraged by the strong security controls of larger organizations, attackers are looking more downstream for easier targets, charging less for recovery in line with small business revenues but making up in volume. 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 cyber criminals. For SMBs, the average cost of downtime comes out at $141,000, a more than 200% increase from the previous year's average.[11]

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 Internet-of-Things (IoT) devices.

Doxxing

Cyber criminals are an innovative bunch. Rather than threatening to delete locked data, some cyber criminals 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 Insurance Portability and Accountability Act (HIPAA) 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 cyber criminals to grant them access to their hacked data.

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 cyber criminals 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 2048-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 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 cyber criminals 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 cyber criminal. 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 (RaaS) model. Since its servers were taken down, CTB-Locker emerged as the most common RaaS attack method. Another RaaS that is rapidly growing is Tox, a kit that cyber criminals can download. The result produces a dedicated executable file that can be installed or distributed by the cyber criminal, with 20% of gross ransoms being paid to Tox in bitcoin.
- **Ransomware Affiliate Programs.** The RaaS model uses affiliate hackers with a proven track record to spread the malware.
- **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.

Top SaaS-based infections:[12]

- Dropbox, 64%
- Microsoft Office, 47%
- G Suite, 18%
- Box, 6%
- Salesforce, 2%

Top causes of ransomware infections:[13]

- Spam or phishing emails, 76%
- Lack of cybersecurity training, 36%
- Weak passwords, 30%

Top ransomware in 2019:[14]

- CryptoLocker, 66%
- WannaCry, 49%
- CryptoWall, 34%
- Locky, 24%

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, cyber criminals have already moved to a new variation. The Ryuk and Sodinokibi ransomware families, for example, both contributed to an increase in the ransom amounts demanded by attackers in Q1 of 2020.[15]

Virtually every operating system is targeted by ransomware today. Attacks also extend to the cloud and mobile devices. The cloud has been left largely untouched by ransomware thus far, so it's a new market opportunity for hackers.[16]

Another recent strategy of ransomware hacktivists is to target and compromise vulnerable business servers. By targeting servers, hackers can identify and target hosts, multiplying the number of potential infected servers and devices on a network. This compresses the attack time frame, 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.

Real-life Attacks

Nearly every industry sector and organization size is affected by ransomware. During 2019, ransomware attacks affected 113 government agencies, municipalities and state governments, 764 healthcare providers, and 89 universities, colleges, and school districts with up to 1,233 individual schools potentially impacted.[17]

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

Ransomware attacks dominated healthcare headlines during the latter part of 2019, increasing by 350% in Q4, with attacks on IT vendors disrupting services on hundreds of dental and nursing facilities, while many hospitals, health systems, and other covered entities reported business disruptions from these targeted attacks.[18]

There are many examples from recent years, including how hacktivists gained access to a MongoDB database containing protected health information for 200,000 patients of a major health center. The database was wiped clean and replaced with a ransom demand for $180,000 in bitcoin for its safe return.

Another major 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.

The cybersecurity market will reach $300 billion by 2024.[19]

Email

More than nine in 10 malware infections were delivered to victims via email last year. The most commonly used file types for concealing malware were:[20]

- Microsoft Office documents, 45%
- Windows apps, 26%

Privacy

Nine in 10 respondents in a survey of over 2,000 security professionals believe their personal data is available to criminals at any time, no matter how careful they are.[21]

But cyber criminals do not always grant victims access to their information. In the case of a hospital system in 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 cyber criminals with new opportunities—and this includes ransomware hacktivists.

Fortunately, in the case of one utility company overseeing electric for a large city in the midwest of the United States, 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.

In another recent event, a ransomware attack shut down a natural gas compressor station for two full days, causing significant loss of productivity and revenue. The disruption represents a growing threat to the domestic energy sector, with more sophisticated attacks beginning to target the ICS.

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.

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.

Last year, ransomware strain LockerGoga hit a series of industrial and manufacturing firms with catastrophic consequences. Security researchers say that the recently discovered strain of the malware is particularly disruptive, shutting down computers entirely, locking out their users, and rendering it difficult for victims to even pay the ransom.[22]

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 cyber criminals are targeting them.

A university in Canada 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.

A college in Los Angeles 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. Three ransomware attacks successfully infiltrated a university in Ireland's network last year. In one instance, the 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. Phishing and ransomware attacks are the most reported types of cyberattacks on financial services firms.[23] The most common cause of an incident, perhaps reflecting the interconnected nature of IT infrastructure, was described as a "third-party failure" which accounted for 21% of reports. Hardware and software issues were blamed for 19% of incidents, and change management for 18%.[24]

Credit unions and small banks are seeing significant jumps in ransomware hacktivism. Ransomware attacks skyrocketed in the first quarter of last year, which was a 105% increase in the number of ransomware attack notifications against clients compared to Q1 of the prior year.[25]

Government

With critical information contained on their systems, government agencies offer cyber criminals 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 an Ohio county were infected with ransomware. The county elected not to pay the bitcoin ransom, and the files were destroyed by the cyber criminals. 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.

Cyber criminals even target law enforcement. The computer systems used by a 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

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] Lucian Constantin, "More targeted, sophisticated and costly: Why ransomware might be your biggest threat," CSO, February 10, 2020.

[2] "Ransomware Facts, Trends & Statistics for 2020," Safety Detectives, April 22, 2020.

[3] Nick Parkin, "Businesses will need to be more data savvy in 2020 to reap rewards of big data," ITProPortal, January 9, 2020.

[4] Jessica Davis, "Ransomware Attacks Double in 2019, Brute-Force Attempts Increase," HealthITSecurity, September 3, 2019.

[5] "New Study Reveals Cybercrime May Be Widely Underreported – Even When Laws Mandate Disclosure," Financial Post, June 3, 2019.

[6] "Ransomware Facts, Trends & Statistics for 2020," Safety Detectives, April 22, 2020.

[7] Danny Palmer, "Ransomware is now the biggest online menace you need to worry about—here's why," ZDNet, April 22, 2020.

[8] Yotam Gutman, "What is the True Cost of a Ransomware Attack? 6 Factors to Consider," SentinelOne, January 8, 2020.

[9] "2019 State of Cybersecurity," ISACA, 2019.

[10] Alfred Ng, "Ransomware froze more cities in 2019. next year is a toss-up," CNET, December 5, 2019.

[11] Yotam Gutman, "What is the True Cost of a Ransomware Attack? 6 Factors to Consider," SentinelOne, January 8, 2020.

[12] "Ransomware Facts, Trends & Statistics for 2020," Safety Detectives, April 22, 2020.

[13] "Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2019," Statista, 2020.

[14] "Ransomware Facts, Trends & Statistics for 2020," Safety Detectives, April 22, 2020.

[15] David Bisson, "Increase in Ransomware Demand Amounts Driven by Ryuk, Sodinokibi," Tripwire, May 4, 2020.

[16] Corey Nachreiner, "Why Ransomware Will Soon Target the Cloud," Dark Reading, February 11, 2020.

[17] "The State of Ransomware in the US: Report and Statistics 2019," EMSISOFT, December 12, 2019.

[18] Jessica Davis, "Ransomware Attacks on Healthcare Providers Rose 350% in Q4 2019," HealthITSecurity, March 9, 2020.

[19] Casey Crane, "80 Eye-Opening Cyber Security Statistics for 2019," The SSL Store, April 10, 2019.

[20] "2019 Data Breach Investigations Report" Verizon, 2019.

[21] "Privacy in an open world: How much do Americans care about online privacy?" Nixplay, June 6, 2019.

[22] Andy Greenberg, "A Guide to LockerGoga, the Ransomware Crippling Industrial Firms," WIRED, March 25, 2019.

[23] Steve Ranger, "Phishing, ransomware are top cyberattacks on financial services firms," ZDNet, July 1, 2019.

[24] Ibid.

[25] Gene Fredriksen, "Ransomware—A growing credit union threat and the unified solution," CUInsight, October 9, 2019.

FORTINET

www.fortinet.com

May 29, 2020 8:34 PM

679688-0-0-EN