Ransomware and Third Parties

A Comprehensive Guide to Protecting Your Organization from This Growing Threat

Table of Contents

About the Authors

Brianna Groves is a Cybersecurity Engineer at CyberGRX who holds various security certifications including: EC-Council's Certified Ethical Hacker (CEH) and CompTIA's Security+. Her interests include red-teaming, malware reverse engineering, and programming.

Aser Garcia is a Data Scientist at CyberGRX and earned a Masters in Applied Mathematics from the University of Colorado Boulder in 2021. His interests include data mining, functional analysis, and reinforcement learning.

Introduction

Ransomware continues to dominate headlines with no sign of slowing down. What started **more than 30 years** ago has become one of the most prevalent and lucrative cyberattacks that does not discriminate by company size, industry, or geography.
In addition, with the growth of the digital ecosystem, ransomware can now work its way not only through the primary target, but affect the third parties that a business may also be working with. Recent attacks on software providers, managed security providers, and credit agencies are perfect examples of the danger ransomware poses to third-party cyber risk management.

> “Ransomware is more than just encrypting data to make it unusable. These days, extortion is all the rage for threat actors as they believe reputational and IP costs are a big motivator for payments. Initial access controls and near real-time detection, alerting, and mitigation are key to staying ahead of these dangerous hacking groups. No traditional ransomware safeguards will help in this situation.”

Dave Stapleton
CyberGRX CISO

Ransomware by the Numbers

At its core, ransomware is an efficient, effective type of malware that when deployed, encrypts files on a victim's computer until a ransom is paid. It is often quick to deploy, with nearly 97 percent of all ransomware infections taking under four hours to successfully infiltrate their target, according to **Microsoft**. The fastest malicious software can take over a company's system in under 45 minutes.

Ransomware is an extremely lucrative business for cyber criminals. It's estimated that ransomware cost businesses globally $20 billion USD in 2020, up from $11.5 billion USD in 2019 (Checkpoint Software Security Report, 2021). In 2020, the average ransom paid by mid-sized organizations was $170,404 USD. However, the average bill for rectifying a ransomware attack, considering downtime, people time, device cost, network cost, lost business opportunity, ransom paid and other expenses was $1.85 million USD (Sophos The State of Ransomware 2021).

And, just because a ransom is paid doesn't mean the organization is free and clear of any detrimental effects from the attack including data loss or corruption, repeat attacks and reputational and revenue loss. A recent study by **Cybereason** titled, "Ransomware: The True Cost to Business," found that 80 percent of victims surveyed who submitted a ransom payment experienced another attack soon after the initial attack and of those, 60 percent still experienced revenue loss and 53 percent suffered damage to their brands. According to **Sophos' report**, "The State of Ransomware 2021," on average, organizations that paid the ransom got back just 65% of the encrypted files, leaving over one-third of their data inaccessible. 29% of respondents reported that 50% or less of their files were restored, and only 8% got all their data back.

45 MIN

The amount of time it takes the fastest malicious software to take over a company's systems

$20 BILLION

cost of ransomware attacks on businesses globally in 2020

$1.85 MILLION

average cost for a ransomware attack (considering downtime, people time, device cost, network cost, lost business opportunity, ransom paid and other expenses)

ONLY 8%

the number of businesses that got all of their files back after paying the ransomware hackers

Extortionware: Ransomware's Bigger (and Meaner) Brother

While ransomware is not a new method of cyberattack, what is new in this story is the evolution from ransomware to extortionware. Typically organizations employ traditional backup processes in an attempt to keep their data safe. This doesn't necessarily stop the bad actors from trying to take over the data, but instead provides a route to recover the data taken hostage without paying the ransom, reducing the profit of those executing the ransomware.

Hackers have innovated, honing their craft into extortionware. With ransomware, the hackers provide a decryption key once the ransom is paid, thereby returning access to the data. Theoretically the attack is complete at that point, and everyone goes on their way, the hackers with fatter wallets and the victim organization flush with hard earned lessons in cybersecurity.

Extortionware takes it a step further, evolving from data encryption to saving the data for use at a later time as a means to extort. Even if an organization pays the ransom, there are no guarantees that all their data will be returned or that the data won't be weaponized against the organization in the future, to extort more money. This carries critical consequences for organizations' operations, reputation, and competitive advantage. This threat cannot be stopped using a traditional data backup process, and it extends beyond an organization's perimeter to their critical third-party ecosystem.

Governments around the world are ramping up efforts to investigate and prosecute perpetrators of cybercrime, often working together to take down multi-national syndicates. But most do not have direct control over the private sector which means they must rely on business leaders and organizations to lead the fight. And fight they have. Many organizations have implemented robust security controls as well as trained their employees on cybersecurity awareness and hygiene to be vigilant against ransomware techniques. But what happens when the ransomware attack takes advantage of a control gap or employee out of your control?

Ransomware & Third Parties

The single biggest global ransomware attack (as of original publish date) targeted an IT Management firm, Kaseya, in July 2021. Shortly after it started, more than 1500 of Kaseya's customers in at least 17 countries were affected. REvil, the Russia-based hacker group, used Kaseya as a means to an end, gaining access to the networks of the affected customers. Given that many of those customers are also managed service providers, the true extent of the ransomware attack is exponentially larger. The hackers reportedly demanded around $45,000 from most of Kaseya's customers, but due to the number of customers affected, the total amount of ransom is estimated to be $70 million. Quite a lucrative haul for a single ransomware campaign.

Cyber attacks on third-party providers are far-reaching and dangerous for the global economy and supply chain. They are also not new, but Target's significant data breach in 2013 brought them into the headlines. The fact that a third-party vendor (in Target's case, an HVAC service provider), became an attack vector for hackers was an eye-opening revelation for both organizations and the bad actors targeting them. While companies shore up their own systems and sleep soundly thinking that their cyber borders are secure, they oftentimes assume that the companies they do business with take the same precautions. And that's the assumption that can potentially make hacker groups around the world very wealthy.

Ponemon reports that enterprises have an average of nearly **6,000 third-party vendors**, with COVID-19 and the rise of Digital Transformation increasing that number exponentially. The pandemic forced companies to transition to a remote workforce, and hackers took full advantage of the increased number of attack vectors with the FBI reporting a 500% increase in the number of cyber attacks in the first months of the shut-down alone.

Businesses don't operate in a vacuum, and very few operate without reliance on another business' service or product even if it's something as simple as an internet provider. And on the flip side, by being a business you are, by definition, a third party. That means that you're a potential target simply by having customers of your own. While you may consider yourself to be a "small fish" that hackers don't care about, the fact of the matter is, hackers don't discriminate based on company size. In fact, in the **2021 Verizon Data Breach Investigations Report**, small (fewer than 1,000 employees) and large (more than 1,000 employees) companies had nearly the same breach occurrence rate in 2020 at 263 to 307, respectively.

In order to fight ransomware, companies need a methodology that combines a wide range of security safeguards with a modern approach to third-party cyber risk management, including threat intelligence and comprehensive data analytic capabilities.

The Concept of Shared Responsibility

Shared responsibility, as it pertains to risk, was birthed as a model to define the line of responsibility between you and your cloud provider to reduce the risk of introducing vulnerabilities into your virtual ecosystems. Traditionally, if you are trusting the storage of your data within an external cloud environment, they adhere to ensuring a certain amount of risk coverage to your service, and your business assumes the rest. But as organizations are progressively interconnecting, this "shared responsibility" model is being being adopted as the basis of risk-management frameworks, analyzing the risk between your own internal controls, as well as your third parties, combining the two analyses into a total risk evaluation.

In a traditional data center model, your organization would be responsible for its own entire operating environment, thus only needing to address risk gaps of single focus around your hardware, software, and even physical building. However, with the growth of as-a-Service technologies, businesses are outsourcing niche solutions to multifarious companies creating a web of interconnected, cross-platform linkages. As a result, there is a build up of a large portfolio of third-party relationships. Additionally, as Digital Transformation is evolving all facets of business, the inherent risk of cyber threats such as ransomware, data breaches and service disruptions is becoming highly advantageous to threat actors. Attacks like ransomware are surging, while businesses in all sectors are failing to address critical security shortcomings within their own environment, as well as the swelling risk to these threats caused by third parties.

Total risk evaluation is a new ideology that can prove overwhelming for many businesses who still struggle with prioritizing security and risk management. And while leveraging third parties can help your business gain significant efficiencies, you must remember that the inherent risk still lies with your organization. Your analysis should not end with a high-level evaluation of a third-party's answers to an assessment. Alternatively, you should determine your highest-risk third-party relationships and use their assessments to understand how effective their security controls are, and implement a third-party risk framework that can flex with the evolving needs of your organization. It has become vital that companies come together, build trust and transparency, and make concerted decisions to mitigate unacceptable risks to a tolerable level.

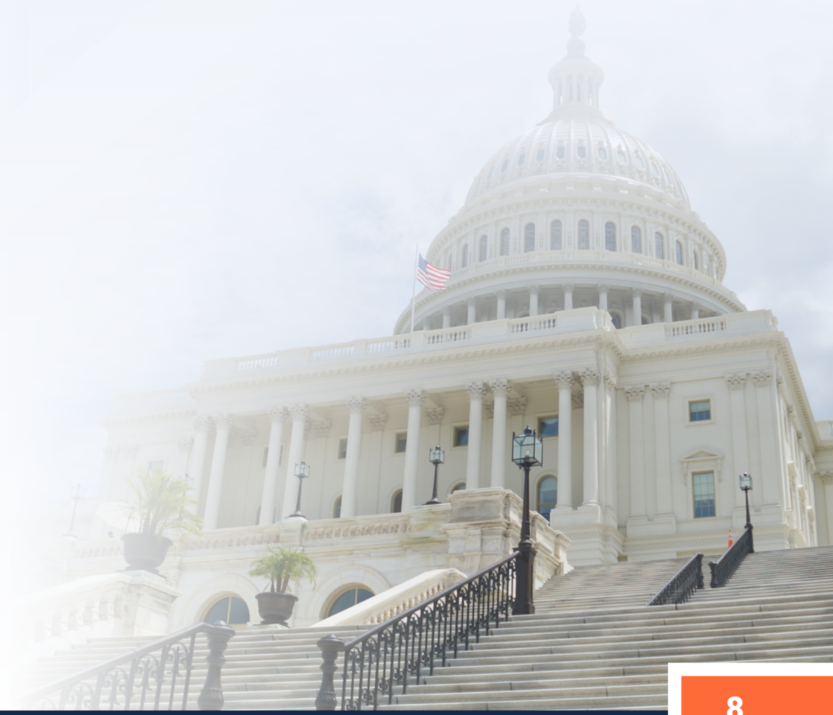
How Does Regulation Contribute?

It's no secret that the recent large-scale ransomware attacks are a call-to-action for greater federal cybersecurity regulations. As it stands, security policies are not mandated and are largely a voluntary mechanism. However, it has become apparent that at-will standards are not getting the job done. According to the report by Cybereason, the frequency with which ransomware attacks are performed has increased to a staggering 11 seconds on average. Ransoms are ranging between $350,000-$1.4 million. Malignant actors are operating with impunity, and many private sector organizations have failed to take the necessary precautions.

As a result, the U.S. may soon begin the work of regulating private companies and mandating higher standards for cybersecurity. Congressional initiatives like the Cybersecurity Act 2012 and Cybersecurity Information Sharing Act 2015 could be the path to structuring these mandatory requirements, and the executive order signed by President Biden in the Spring of 2021 is an indication that more stringent and explicit standards are on the horizon.

While the list of potential remedies is too long and target-specific to exhaustively regulate, there are some baseline themes lurking: Multi-factor Authentication (MFA), software patching, robust segregation of information, mandatory air-gapped system backups, and clearer identity management controls around administrative accounts.

A general posture of security hardening and investment seems prudent in the current climate, and in that regard, there are several steps that can be taken that make good security sense regardless of future mandates. Companies should ensure adequate security policies and staffing, build out robust backup systems and continuity plans, and strengthen not just the technology, but the people using the technology as well.



Mitigation of Ransomware and Extortionware

How do you combat the threat that ransomware poses? While any internet search on the subject will return thousands of results, thinking you are safe just because you add in a few suggested safeguards is a dangerous notion. The current state of ransomware has gotten more complicated with the advent of extortion threats also known as extortionware. This evolution of ransomware finds an organization paying to unlock their data but the data itself is still in the hands of the attacker, to be released publicly in order to damage reputation or proprietary information. In other words, they weaponize your data. Ransomware/extortionware tests security programs on multiple levels, not just the individual security controls designed to combat it.

There are no silver bullet solutions and no tools that make it all go away. Effectively defending against extortionware is a process that must evolve over time. Even with a top notch security program with all the bells and whistles and excellent staff to put security controls in place, you will never be 100% effective against extortionware. Things like backups, least privilege, and patch management are all excellent, but those in isolation aren't comprehensive enough.

So, what is a security team to do?

We'll start by looking at a ransomware kill chain for guidance on how to proceed because most follow the general theme of:

Distribution **Infection** **Staging** **Scanning** **Encryption** **Payday**

Once the files are encrypted and a ransom is demanded, your options become limited. This leaves a window of opportunity for security teams between Distribution and Encryption to Prevent, Detect, and Respond.

To effectively defend against extortionware we must have controls across each of the killchain elements and those controls will be subsets of larger security themes. It might seem to be too late at the Payday phase, but there is still a lot of work to be done by a security team.

Next we'll take a closer look at the different stages of a ransomware attack where you can implement controls in order to protect your system.

Distribution

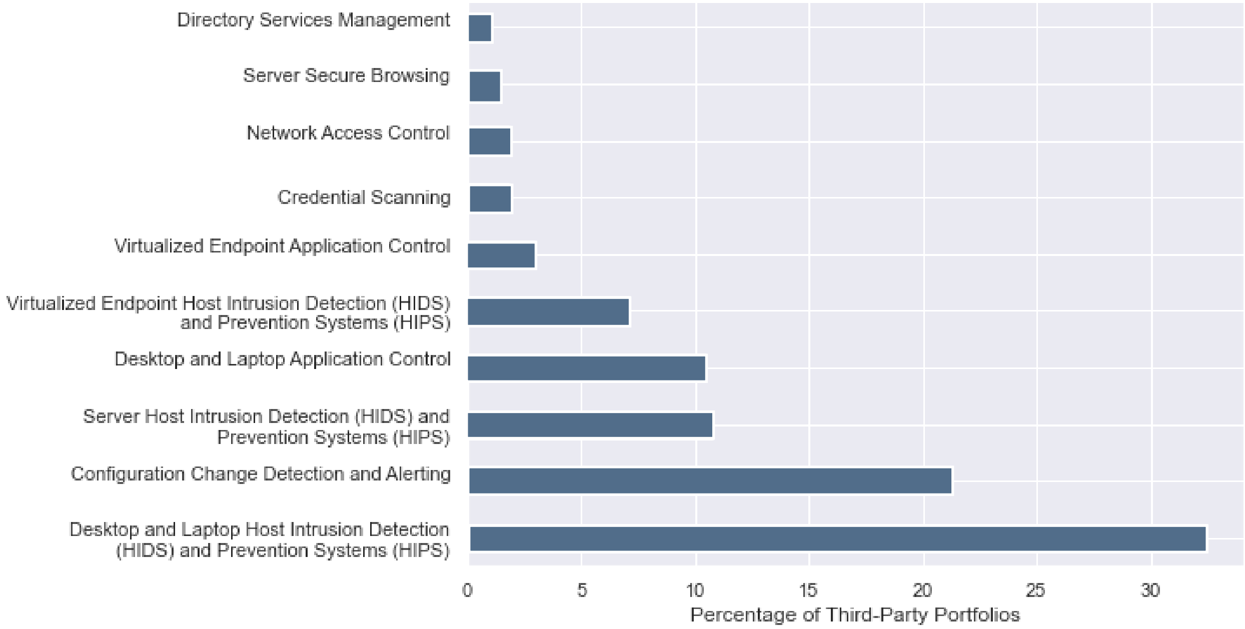
The attacker typically tries to get users to click a link, download a malicious attachment which opens the door to a watering hole attack, even the ability to scan for unpatched/ vulnerable services. Some of the controls that can be put in place at this stage are:

- High-quality email filtering
  - Sandboxing of attachments
  - Identification of URLs
  - Scanning of attachments/URLs
  - Spoofing protection
- Web filtering (at the endpoint)
- Endpoint Detection and Response (EDR)
- Patch management
- User training

User training is one of the most important defenses a security team can employ, and its effectiveness can not be understated.

Any one of these controls can help to stop an attack, but no one control should be completely relied upon to be effective against all attacks. User training is one of the most important defenses a security team can employ, and its effectiveness can not be understated.

Top 10 Commonly Missed Ransomware Controls Among Third-Party Portfolios



Source: CyberGRX Exchange

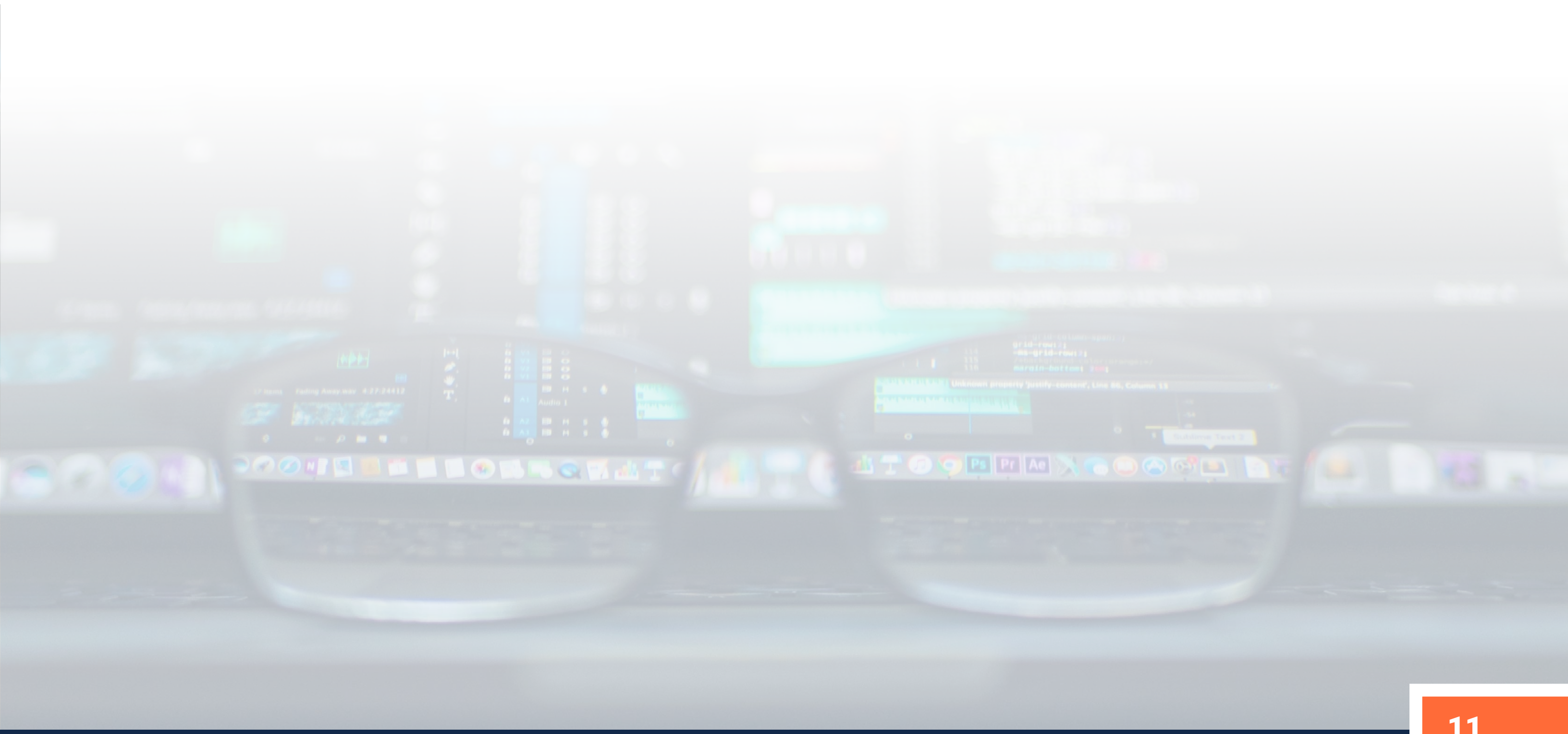
- Detection takes 4 of the top 10 controls related to ransomware mapped by MITRE tactics.
- Within a portfolio of >5 vendors, there is almost a 30% chance that HIDS/HIPS is not implemented.

Infection

At this stage, new processes are being launched and the malware is installed and starts its infection process. Some processes may look legitimate, but they're running from odd locations in the file structure. This is typically when the infection starts communicating with the outside world. At this stage some controls that can help are:

- File Activity Monitoring
- Internet Proxy
- Process Monitoring
- Endpoint Detection and Response (EDR)
- Application Control
- Least Privilege

Not all of these controls on their own will be effective, so a mix of local controls combined with external controls is the way to proceed. It's important to remember that attackers are always looking for ways to obfuscate their attacks, so use tools to help you detect and respond but don't rely too heavily on those tools. We recommend taking the time to research and develop tooling to augment tools that are paid for, and this holds true through most of the killchain.



Staging

If the malware has been able to install, it will try to embed itself in the system, establish persistence, and survive reboots. A process can add an entry to an autorun location like Windows startup or registry keys to achieve persistence after a reboot. The malware will also start taking actions to ensure the victim can't easily remove it, such as deleting shadow copies, changing boot options, and deleting recovery partitions. The malware will also continue to communicate with the outside world and begin to upload data, usually to a newly registered domain or a bare IP. Some controls to consider are:

- File Activity Monitoring
- Internet Proxy
- Process Monitoring
- Least Privilege

Least Privilege is the most effective approach here, as some of the changes the malware will try to make should require administrative rights to the computer in question. But again, don't rely too heavily on any one control.

Scanning

The malware will now begin scanning and looking for content to encrypt both locally and at the network level. At the network level it will look for network drives and cloud accounts such as Box.com, Dropbox, and AWS S3. The most amount of network traffic will be observed in this stage as the malware actively reaches out over the network to enumerate and infect new targets. Some of the controls that can be put in place at this stage are:

- Network Monitoring
- Process Monitoring
- File Activity Monitoring
- Security Analyst Training

This stage presents security teams with the best opportunity to detect the infection and take action. The phase can take seconds if the scans don't reveal a large network or it can take hours to complete if the malware finds a large network to enumerate. This is where having a well-trained security team to identify the infection and have the ability to respond quickly will pay huge dividends.

Encryption

The malware begins to encrypt files and while this may sound like it's too late to successfully defend your systems, there's still time to take action and limit damage. New processes will find files, encrypt them, and delete them from strange locations in the folder structure and there will be a large volume of activity in the folder structure. This is probably where the malware exfiltration of the data will occur if the malware is configured to do so. Unfortunately, the industry has seen an increase in exfiltration in the last few years as there has also been an increase in extortionware. Controls to consider:

- File Activity Monitoring
- Process Monitoring
- Endpoint Detection and Response (EDR)
- Security Orchestration and Automated Response (SOAR)
- Incident Response (IR)
- Network Monitoring

At this point any human intervention will probably be too slow to be effective. SOAR combined with the other controls listed are probably most effective at mitigating the malware infection. Also, you will most likely see the effects of this phase across multiple endpoints in your environment, so your response could be much larger depending on what the malware was able to find in the Scanning phase. A solid Incident Response plan and execution cannot be overstressed. If there is an Incident Response a security team wants to have, this is it: the malware is detected and a response is in progress before it becomes too pervasive.

Payday

Now, you have many potential endpoints all saying the same thing: the contents of this machine are encrypted, send the attacker some form of cryptocurrency to get your files back or face negative consequences. You might be threatened with the release of sensitive data if the demands are not met. Even at this stage all is not lost. Here are some mitigations:

- Secure Backups
- Incident Response (IR)
- Forensics

There is more to think about here than meets the eye initially. Part of your IR plan should have a decision-making paradigm to try and determine whether or not the ransom will be paid if the system restoration from the backup fails. This requires well-trained analysts doing forensics quickly to confirm if data was exfiltrated and how far the attack propagated through your environment.

Another thing to consider is the value of the data that was encrypted and/or exfiltrated. Is it catastrophic to have this data encrypted and unavailable to you? Is the release of the data publicly catastrophic to your business, or others? These discussions should not occur for the first time during an active ransomware attack. Stakeholders, including the C-Suite, Legal team and Board Members, should be well versed in the decisions that need to be made in the case of a ransomware attack.

By analyzing the killchain we can gain insights into controls that are most effective at any given phase. From there we can implement the most effective controls and processes to combat the threats posed from ransomware and extortionware. Remember, no company is 100% protected so ensuring you have a complete and tested security program is truly the best defense against these dangerous threats.

The Timeline of the Kaseya VSA Ransomware Attack

Now that we've reviewed the general killchain of a ransomware attack, let's see how it played out in the case of the nearly month-long Kaseya breach in early July 2021.

Kaseya Breach Timeline

DAY 1

Kaseya's Incident Response (IR) team detected a potential security incident involving its remote computer management tool Kaseya VSA

Kaseya's IR team worked with security experts to determine the **cause of the issue**, alerting law enforcement and other cybersecurity agencies, including the FBI and CISA. They notified all on-premises customers and advised them to shut down their VSA servers while the company themselves shut down their SaaS servers as a precautionary measure.

Kaseya said that they had identified the vulnerability source and fewer than 50 customers were affected, and they began developing a patch as of 10 p.m. ET.

DAY 2

Kaseya publicly confirmed the cyberattack

In addition to recommending on-premises customers keep their VSA servers offline, Kaseya also advised any customers that were experiencing ransomware to avoid clicking on any links. The company announced it was developing a compromise detection tool to help customers assess the status of their systems. The company continued to inform users who were impacted. Kaseya CEO Fred Voccola was interviewed about the attack on the talk show Good Morning America the following day.

DAY 3

Kaseya delayed bringing data centers back online and released a compromise detection tool

Kaseya determined that more time was needed before bringing data centers back online to minimize customer risk. In his interview on Good Morning America, Voccola stated the company was confident they knew how the attack happened and they were remediating it. Kaseya made available the compromise detection tool and the FBI and CISA **issued their own guidance** for impacted MSPs and their customers. REvil members took to the group's "Happy Blog" to brag that more than a million individual devices were infected, and that they would provide a universal decryption key to Kaseya for $70 million in Bitcoin.

DAY 4

Kaseya claimed fewer than 60 customers were compromised, and that the patch was being tested

Kaseya stated that the patch was being tested and would be made available within 24 hours and the company estimated that its SaaS servers would be back online within two days.

Kaseya Breach Timeline

DAY 5

Kaseya added security layers to its SaaS infrastructure

To get its VSA servers back online, Kaseya configured an additional layer of security to its SaaS infrastructure to change the underlying IP address of its VSA servers. An issue was discovered and delayed the release, with Kaseya's teams working through the night to fix the problem. An update on the on-premises patch stated that the patch would be released within 24 hours. At this point the UK's National Cyber Security Centre came into the picture and stated the impact of the attack on UK organizations appeared to be "limited", though it advised customers to follow precautions.

DAY 6

Kaseya apologized for SaaS and on-premises fix delays

Kaseya published a guide for customers to prepare for the patch and apologized for ongoing delays with SaaS and on-premises fix deployment.

DAY 7

US government told Russia it will be held accountable, and Kaseya delayed the patch release again

White House press secretary Jen Psaki said that several top US security officials had contacted Russia about the Kaseya attack to make clear its intentions to hold Russia responsible for the criminal actions. She notified the press that another ransomware-focused meeting between Russia and the US was taking place the following week.

Once again Kaseya pushed back the launch of the on-premises patch while subsequently starting deployment to its SaaS infrastructure. Kaseya released two videos, one from Voccola the CEO and another from CTO Dan Timpson, updating viewers on the situation, progress, and next steps. The company also stated spammers had begun exploiting the incident by sending phishing emails with fake notifications containing malicious links and attachments, stating that it would not be emailing any such updates and people shouldn't click on links or open attachments.

DAY 8

Kaseya updated VSA hardening advice

Kaseya updated its **VSA On-Premise Hardening and Practice Guide** and additional top company officials spoke of the team's continued work towards getting the situation remedied.

DAY 9

Report stated Kaseya was warned of the exploited security flaw

In a video update from Executive Vice President Michael Sanders, he outlined steps companies could take to prepare for the patch launch that was on schedule to be released within the next couple of days. According to **a Bloomberg article**, ex-employees of Kaseya warned executives of critical security flaws in its software on several occasions between 2017 and 2020, which the company subsequently failed to address.

DAY 10

Kaseya released a patch and began the SaaS restoration

On the 10th day of the ransomware attack, Kaseya launched the on-premises patch and began restoring its SaaS infrastructure. Within six hours, the company claimed to have 60% of SaaS customers live with the rest of their customers due to be online in the coming hours. Support teams were working with any customers needing assistance with the patch.

Kaseya Breach Timeline

DAY 11

SaaS restoration was completed

The restoration of Kaseya's SaaS infrastructure was complete in the early morning hours of Day 11, but it was then forced into unplanned maintenance due to performance issues, causing a short downtime.

DAY 12

REvil websites disappeared

All REvil ransomware websites suddenly went offline on the 12th day of the attack, leaving security experts to speculate about potential action by US or Russian governments. Some victims were now unable to pay the ransom demand in order to recover their data.

DAY 13

Kaseya issued patch install check advice to customers

Kaseya put out a statement that read, in part, "When running the Kinstall patch on your VSA, if you chose to reinstall VSA and either unchecked the default option to install the latest patch or reran the Reinstall VSA process a second time without the 'install patch' option selected, it's possible your patch was not re-applied. While these are rare edge cases, we recommend that you verify that the latest patch was installed properly. We have made a tool that enables you to ensure the patch is properly installed."

DAY 15

Victims struggled with REvil's decryption tool and Kaseya released a non-security patch

With REvil's websites still offline and no way to contact the gang for support, some victims struggled to unlock files and systems despite having paid for the decryption tool. Kaseya announced an upcoming non-security-related patch to fix functionality issues caused by enhanced security measures and other bugs.

DAY 16

First updated SaaS patch deployments went live

DAY 18

Remainder of updated SaaS patch deployments went live

DAY 19

New functionality patches released

Kaseya made the updated on-premises patch available and provided additional patch updates to fix functionality issues and bugs.

DAY 20

SaaS functionality updated

Kaseya updated SaaS instances to provide bug fixes and remediate functionality issues that resulted in a 2-to-10-minute interruption in service.

Kaseya Breach Timeline

DAY 21

Kaseya acquired a universal decryption key

Kaseya announced it had obtained a third-party, universal decryption key for ransomware victims. Across the industry, there was a lot of speculation about exactly how Kaseya accessed the decryption tool and whether a ransom payment was made.

DAY 22

Another functional patch and SaaS update was released with Kaseya reportedly requesting a non-disclosure for decryptor

Details of how the decryption key became available remained unclear as Kaseya continued to release patches for on-premises customers to resolve three non-security issues. All SaaS instances were also updated. **According to CNN**, Kaseya requested customers sign a non-disclosure agreement to access the decryptor.

DAY 23

Kaseya declined to comment on whether or not a ransom was paid

There was widespread speculation about how the decryption key was obtained and Kaseya declined to comment on whether it had paid a ransom.

DAY 25

Kaseya eventually said decryption tool is "100% effective," and no ransom was paid

Kaseya **released a statement** saying, "Throughout this past weekend, Kaseya's incident response team and Emsisoft partners continued their work assisting our customers and others with the restoration of their encrypted data. We continue to provide the decryptor to customers that request it, and we encourage all our customers whose data may have been encrypted during the attack to reach out to your contacts at Kaseya. The decryption tool has proven 100% effective at decrypting files that were fully encrypted in the attack."

"While each company must make its own decision on whether to pay the ransom, Kaseya decided after consultation with experts to not negotiate with the criminals who perpetrated this attack and we have not wavered from that commitment. As such, we are confirming in no uncertain terms that Kaseya did not pay a ransom—either directly or indirectly through a third party—to obtain the decryptor."

Conclusion: Best Practices

The war against ransomware rages on, and cyber criminals are getting bolder and more sophisticated. Ensuring you know the cybersecurity posture of your third parties is not only good practice, it's imperative. Your organization may take steps to protect and defend itself against cyber attacks like ransomware, but if your third parties don't and are vulnerable...so are you.

While it may never be possible to stop 100 percent of ransomware or extortionware attacks, there are things you can do to shore up your organization's cyber defenses to decrease the chances of becoming the next news headline due to a cyber attack.

Here are a few of our recommendations:

1. Be diligent with backups. In addition to backing up your systems on a daily basis, make sure you've thoroughly tested your ability to restore everything in the event of a cyber incident.
2. Stay current with patches. Consistently monitor for vulnerabilities and immediately update company systems with patches to keep bad actors from taking advantage of known security flaws to gain access to networks and distribute ransomware.
3. Implement multi-factor authentication (MFA). Many ransomware attacks happen because of human error, for example, clicking on links in emails or reusing passwords. Requiring MFA on accounts across the network can help prevent unauthorized system access because something like a phishing attack may get them a user's account credentials, but it won't provide the second later of security required through MFA.
4. Follow the concept of least privilege. This applies to your internal users as well as the third parties you do business with. Only give users the bare minimum privileges needed to do their jobs and only share with third parties company data that is applicable to the business relationship.
5. Use filters for web and email content. Phishing emails containing malicious URLs are the most common ransomware attack method. Use web and email content filtering controls to block and quarantine threats to remove suspicious links before users can access them.
6. Utilize a comprehensive tool that incorporates threat intelligence for visibility. When it comes to third party cyber risk management, companies need a methodology that combines a wide range of security safeguard including threat intelligence and comprehensive data analytic capabilities. Having complete visibility into the security postures of an entire vendor ecosystem is the key to combating the weaponizing of data.
7. Invest in regular employee training. Providing security awareness training on a regular basis (for example, quarterly) ensures your employees follow good cybersecurity practices and help them detect and react to possible threats they may be exposed to.

If you're looking for an innovative, data-driven approach to third-party cyber risk management, **schedule a demo** or read our **Vendor Risk Management Guide** to learn more.

CyberGRX