thirdpartytrust | BITSIGHT

Zero Day 101

Everything to know about Zero Day attacks and remediation

Contents

About Zero Days

Lessons from past Zero Days

How to prevent and remediate Zero Days

Zero Days and Your Organization's Security

[Log4j and SolarWinds brought the danger of zero day vulnerabilities to the front pages. While these critical flaws have been put under the microscope, many open-source apps, and not to mention enterprise applications and APIs, are targets of zero day attacks every day.]

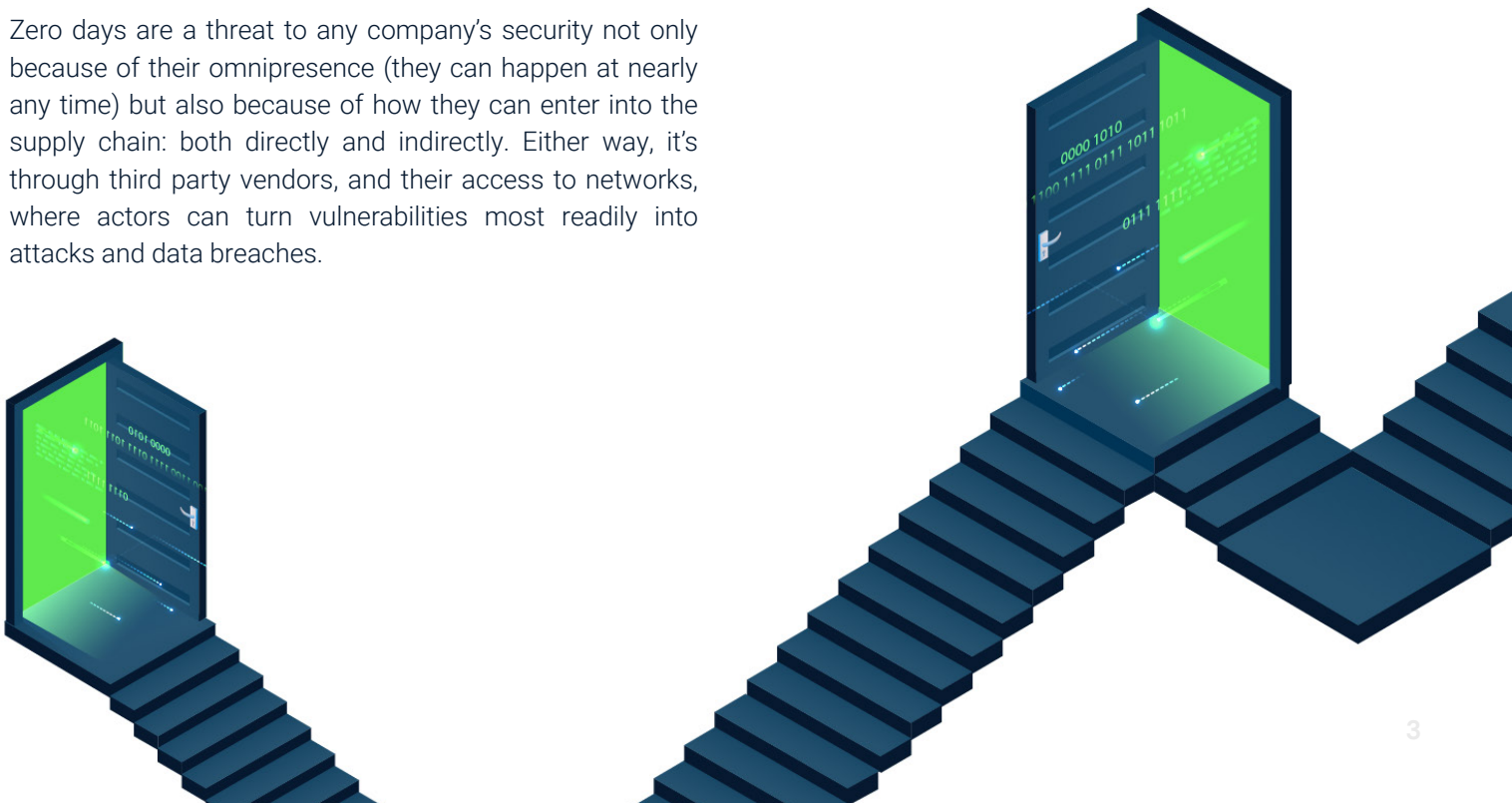
In fact, 67% of malware attacks in Q3 2021 used zero day exploits in order to succeed, according to a WatchGuard report. This means cybercriminals often (and increasingly) leverage software vulnerabilities before manufacturers have the chance to patch them.

Headline-grabbing attacks and associated headlines are both a wakeup call and a reminder that remediating zero days is going to be an ongoing concern for security teams in the foreseeable future.

Zero days are a threat to any company's security not only because of their omnipresence (they can happen at nearly any time) but also because of how they can enter into the supply chain: both directly and indirectly. Either way, it's through third party vendors, and their access to networks, where actors can turn vulnerabilities most readily into attacks and data breaches.

This is why vendor risk assessments and continuous monitoring (as part of a comprehensive third party risk management program) are increasingly discussed as a solution to help reduce the risk of zero days in a supply chain. With this as a perspective, this guide covers the essentials about zero day vulnerabilities, zero day exploits, and zero day attacks, via definitions, case studies, and research. By reading it, you and your organization will be better prepared to prevent and/or respond to any zero days that may come your way.

ThirdPartyTrust and BitSight have teamed up to combine research, statistical analysis, and expert insight into the topic. Zero days will continue to make the news, but this guide is built to serve as foundational reading for everyone on your team for years to come.



What Is a Zero Day?

Presented by ThirdPartyTrust

What Is a Zero Day?

A zero day (also referred to as 0day or 0-day) is a software vulnerability that is either unknown to its developer or is known but has no patch to fix it. The name comes from the fact that the vendor has "zero days" to fix it before it is actively exploited.

Until the vulnerability is mitigated, attackers can use it to compromise data or additional systems, including operating systems, web browsers, office applications, open-source components, hardware, firmware, or Internet of Things (IoT) devices.

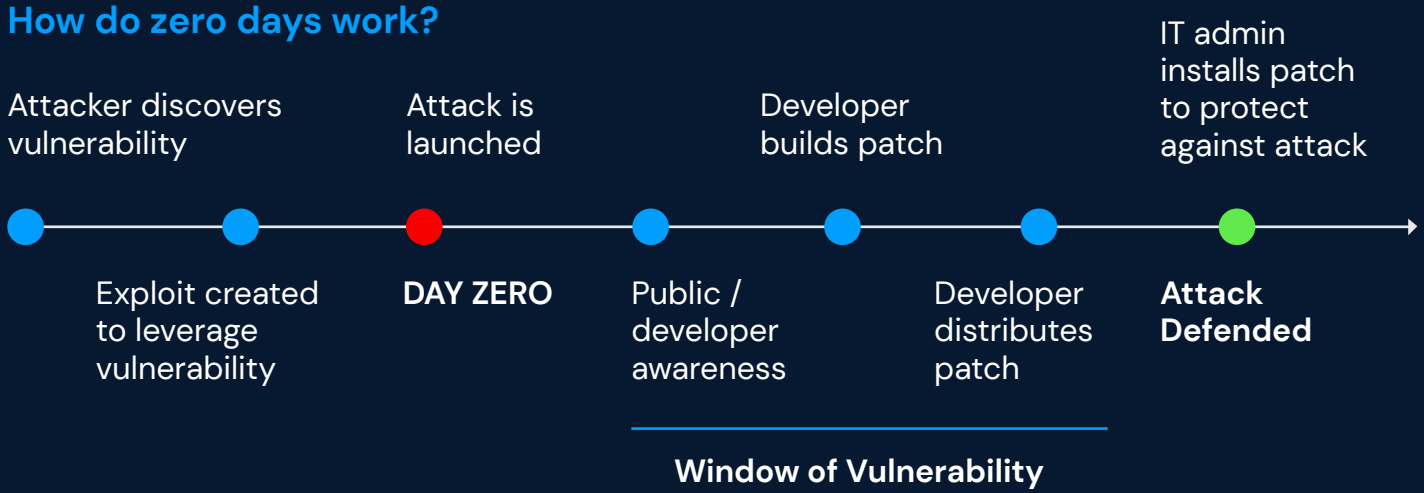
Zero days can follow a path from vulnerability to attack, but rarely conform to a universal approach. It's important to know the three most common phases of zero days in a cybersecurity context:

A zero day **vulnerability** is a software flaw that attackers discover before the vendor does. Because no patch exists yet, attacks exploiting it are likely to succeed.

A zero day **exploit** is the code that allows attackers to leverage the vulnerable piece of software to compromise systems or networks.

A zero day **attack** is the use of a zero day exploit to disrupt, cause damage to, or steal data from a vulnerable system.

How do zero days work?



What Is a Zero Day?

Vulnerability exploitations often result in data breaches, where data is compromised, stolen, and exfiltrated from a system without the knowledge or authorization of its owner. When a zero day exploit is used, this is what is widely called a zero day attack. The most famous recent cases of attacks include the log4j vulnerability first discovered in late 2021, and SolarWinds Orion in 2020.

The list, of course, goes on and on, from the Google Chrome breach of early 2021 and Zoom vulnerability of 2020 to the many exploits of Windows software and systems over the past decade. It's no coincidence that most readers have heard of these companies before; attackers typically use zero day exploits against large companies where the most damage (and the most reward) can be found.

Preparing for the next zero day

Zero day vulnerability detection can be a normal part of due diligence in any security system. However, even if a patch is rolled out, unless it is adopted uniformly across an organization and its third party supply chain, vulnerabilities will persist, and exploits can quickly become attacks.

As part of normal due diligence, continuous monitoring, and ongoing reassessment processes, businesses need to make sure that their vendors are enforcing standards that keep their business(es) safe. Should a zero day vulnerability appear, organizations must ask their vendors if they're vulnerable, how they are planning to respond, and/or request additional assurances through a standardized third party risk management process. These measures are discussed in more detail throughout this guide.

The zero day threat in numbers

67%
of malware attacks used zero day exploits in 2021 [1]

80%
of public exploits are published before CVEs [2]

11%
of vulnerabilities have a critical score [3]

22K
vulnerabilities were published in 2021 [4]

60
days is the mean time to remediation [5]

$1M+
is the average price tag of a functional zero day exploit [6]

1 WatchGuard Internet Security Report – Q3 2021 | 2 Palo Alto State of Exploit Development | 3 CVE Details | 4 NVD database | 5 Edgescan | 6 Zerodium program

Analysis of the

SolarWinds Orion Breach

Presented by BitSight

Analysis of the SolarWinds Orion Breach

The cyberattack targeting SolarWinds, a provider of network and system monitoring software, in 2020 was one of the most significant attacks against a critical supply chain partner, with significant implications for national security.

The attackers compromised a software provider in order to gain access to the trusted update channel. Any organization using specific versions of the SolarWinds Orion Network Configuration Manager (aka SolarWinds Orion) product was presumed to be at risk.

This incident was as significant then as it is now because Orion is highly prevalent in the business ecosystem. To illustrate this, after analyzing more than 260,000 organizations across 24 sectors, BitSight found that:

Orion is observed most frequently within the Technology sector, Government, and among large organizations with more than 10,000 employees.

At least 14% of Fortune 1000 companies were utilizing Orion just after the attack.

Orion was observed most frequently among companies headquartered in the U.S.

The following research is presented as a case study for what organizations can learn to prevent similar cyberattacks in the future.

SolarWinds Breach Summary

Attackers targeted the SolarWinds Orion product and inserted malware into the software update function, allowing them to access multiple targets who rely on the Orion software -- including U.S. government agencies.

According to SolarWinds, at the time of the attack nearly 18,000 of its customers may have been at risk. On Dec. 13 2020, the U.S. Department of Homeland Security issued an emergency order calling for federal agencies to immediately disconnect SolarWinds Orion, further recommending that all organizations assess their exposure.

By running specific versions of Orion software, organizations were potentially at risk of malicious actors infiltrating their organization through the remote update feature.

Even if an organization was not using Orion, business partners, third party vendors, and suppliers who used it posed risk to the business.

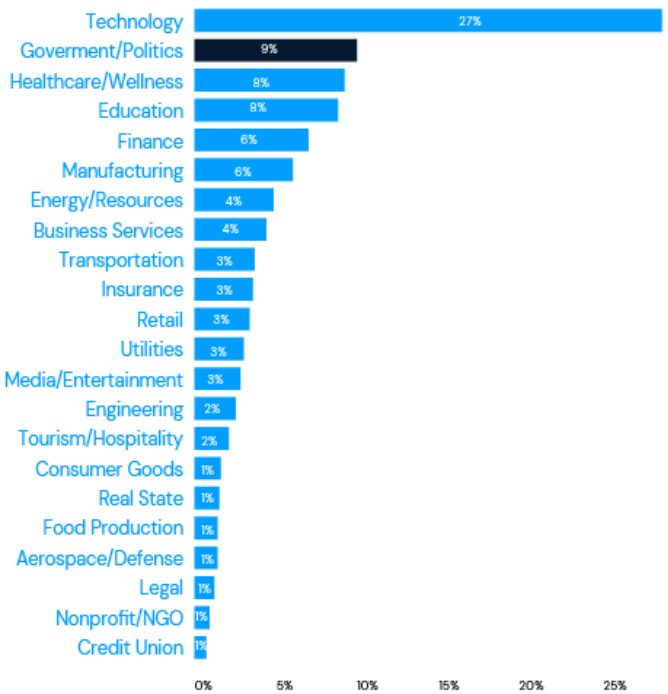
BitSight Findings on the SolarWinds Breach

BitSight observed that **27% of Orion cases affected Technology companies, followed by Government (9%), Healthcare (8%), and Education (8%).**

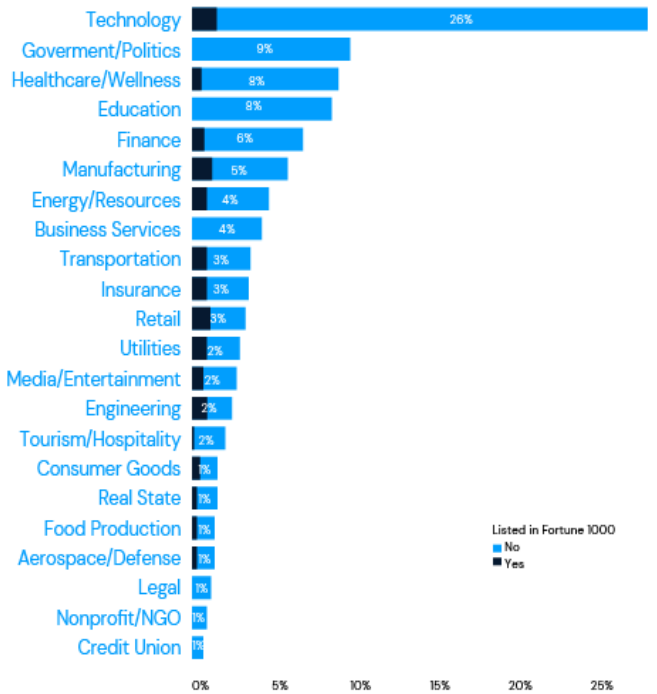
Another reason why this breach shook the business community is that Orion is commonly used among Fortune 1000 organizations, with at least 14% of them using the software, predominantly in the Technology sector.

Fortune 1000 - Percentage of Companies with SolarWinds Orion Seen By Bitsight

Distribution of Solar Winds Orion by Sector



Distribution of Solar Winds Orion by Sector with Fortune 1000



As a result of the implications for so many well-known U.S. companies, SolarWinds is still a household name today when discussing zero day attacks. It stands as an unfortunate reminder of how third parties in particular can expose businesses to risk.

Deloitte's 2020 Global Extended Enterprise Risk Management Survey (interestingly published before the SolarWinds breach) found that companies are exposed to between $50million and $1billion USD in fallout via a third party incident. Likewise, 85% of companies were unable to manage their entire third party risk spectrum. Had SolarWinds, and the many companies who work with them, been able to count themselves among the 15% with complete visibility into their third parties, the outcome in 2020 could have been much different.

Log4j

The threat of zero days in open-source software

Presented by ThirdPartyTrust

Log4j: The threat of zero days in open-source software

Log4j was 2021's last reminder of the impact zero day vulnerabilities can have on entire supply chains. In the final weeks of the year it was discovered that the coding vulnerability could allow attackers to seize control of nearly everything from industrial control systems to web servers and consumer electronics. Until the patch was released, every organization and vendor using the open source Apache logging library known as Log4j was vulnerable.

Shortly after the exploit was made public, the Department of Homeland Security ordered federal agencies to "urgently eliminate" the security flaw, impacting an unknowable number of entities, and called it "one of the most critical cyber vulnerabilities ever encountered."

The Log4J utility is one of the most widely used tools by developers to get reports of their code's health or performance. In other words, it's used for debugging or fixing issues that show up in the code developers are writing.

The vulnerability allowed easy-to-exploit remote code execution (RCE), which attackers could use to insert text into log messages that load the code from a remote server. It's difficult to know how many sites were affected by the Log4j vulnerability, as it's so widely adopted. Major tech players, including Amazon Web Services, Microsoft, Cisco, Google Cloud, and IBM have all found that at least some of their services were vulnerable.

Learning from Log4Shell remediation

The steps organizations needed to take after Log4Shell can be extrapolated to any new vulnerability with the same characteristics.

Scanning

There are a number of Log4j scanners available to help organizations test if they are vulnerable—at least in a way that could be remotely exploited by attackers. At the U.S. Department of Homeland Security, CISA hosts a Log4J scanner in its Github repository and there are several other resources available both for online scanning and file system scanning. However, these scanners alone are not enough to ensure complete identification.

Many Log4j scanners available today rely on HTTP. That is because many HTTP speaking servers, like web servers, use the Log4J library. Scanning, in this context, is the act of running a tool that tries to identify vulnerable web servers, by generating different kinds of payloads and using them in the HTTP request and/or headers in order to trigger the vulnerability.

One of the advantages of this approach is that it roughly mimics what the attackers are doing to get the maximum amount of low hanging fruit, as fast as possible. However, there are many remotely reachable services that depend on Log4J and not all of them speak HTTP. Similar to SQL injection, valid Log4j attack vectors might appear anywhere user controllable input is not filtered, ranging from a simple input field to files, to more esoteric ones, like access point names or QR codes.

Scanners will soon evolve, as more and more HTTP servers get patched and attackers seek new ways to trigger the vulnerability elsewhere. However, at the time of writing, the current crop of Log4j scanners can provide a false sense of security.

Understand Exposure

It is not possible to protect assets if you don't know they exist. So, the first step to solve this issue is to understand the organization's exposure to Log4Shell. This involves knowing which software runs where.

This, by itself, can be a huge task. If you don't have a detailed software inventory, now is a good time to start. A complete and updated software inventory enables one to quickly check against a known vulnerable software list and start patching immediately.

To exhaustively identify the presence of software which uses a vulnerable version of Log4J on a system, it is also important to scan the filesystem. Several tools exist that can scan a filesystem for JAR files and even patch Log4J on the fly.

Lastly, and only if the risk is acceptable, the Internet facing side (and intranet), should be scanned.

Update and Patch

As the organization's vulnerable software is being identified, updating and patching should begin immediately, prioritizing Internet facing and/or easily reached assets. Now is a good time to review your organization patching cadence and its update policy and processes. Follow what your vendors recommend about the vulnerability, as some might offer an update right away while others provide guidance on how to mitigate the issue while an update is not yet published.

Detect and Mitigate

While understanding the exposure and updating is underway, there are some immediate steps you can take to detect and mitigate incoming attacks.

Log files should be analyzed for evidence of the Log4Shell attack signature. However, be aware that his vulnerability is prone to heavy obfuscation and simple string matching can be easily defeated.

Another way to immediately act and circumvent the lack of updates or patches for a particular piece of software is with rules on your WAF or packet filtering firewall, if available. This might be particularly useful in case of legacy systems that cannot be updated in a timely fashion.

Keep in mind that WAF filtering should not be considered sufficient defense, but it can thwart many attacks.

As is evident in the aforementioned remediations, Log4j continues to wreak (potential) havoc well into 2022, providing yet another example of how a vulnerability can affect a company's security via its supply chain.

Observations Into the

Hafnium Attacks

Presented by BitSight

Observations Into the Hafnium Attacks

On March 2, 2021, Microsoft announced that it had detected multiple zero day exploits being used to attack on-premises versions of Microsoft Exchange Server. Threat actors attributed to a Chinese APT Group, dubbed "Hafnium" by Microsoft, exploited four Exchange server zero day vulnerabilities.

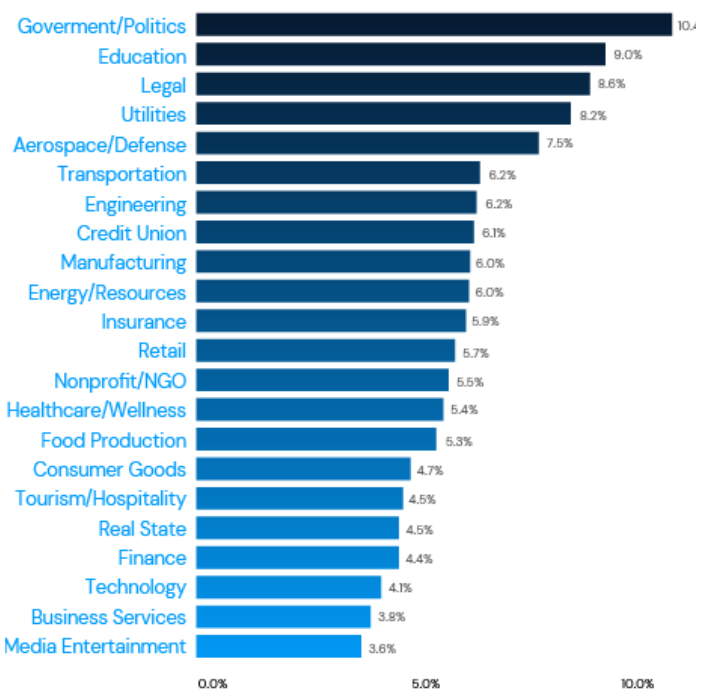
According to Microsoft, in the attacks observed, cybersecurity threat actors used this vulnerability to access on-premises Exchange servers, which enabled access to email accounts, and installed additional malware to facilitate long-term access to victim environments.

After Microsoft's announcement, the Department of Homeland Security issued an emergency alert for federal agencies to take emergency actions to combat these cybersecurity threats.

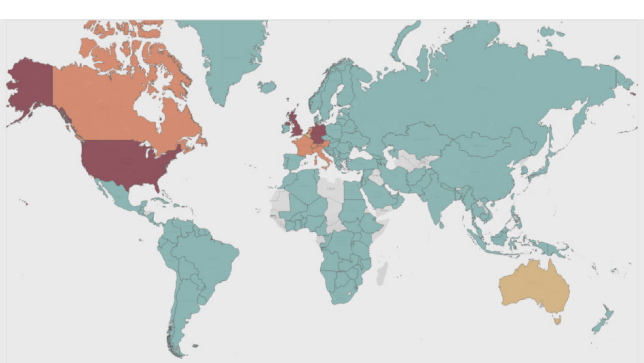
BitSight observed at least 30,000 global organizations potentially vulnerable to exploitation. After examining the prevalence of organizations running Microsoft Exchange Server by sector, BitSight found that the Government sector had the highest prevalence of Microsoft Exchange among all sectors, followed by the Education and Legal sectors:

Percentage of Impacted Entities In Sector

The following chart shows the amount of entities potentially impacted by these Exchange vulnerabilities by sector.



BitSight also examined the prevalence of potentially vulnerable organizations running Microsoft Exchange Server by country, finding that the highest concentration of organizations was within the **United States (29%), Germany (13%), UK (8.5%), Canada (5%), France (5%), Netherlands (4%), Italy (4%), Switzerland (4%), Austria (3.5%) and Australia (3%).**



This was a notable attack because MS Exchange is an extremely popular software and the fact that a state-sponsored actor might have been involved presented significant cybersecurity threat risk.

Significance of the Attack

The Hafnium attack was particularly unusual because it was one of the rare situations where bad actors had performed mass exploitation on near-zero day threat vectors, particularly those that allowed for RCEs. Many organizations were -- and are still -- still vulnerable to exploitation.

BitSight's global analysis showed that despite repeated warnings from Microsoft and government agencies, many organizations were slow to patch vulnerable Microsoft Exchange Servers and remain at risk of threat vector exploitation. A month after the attack, BitSight still found that:

Nearly 1 in 3 companies who use Microsoft Exchange were currently running vulnerable versions.

Nearly 1 in 3 exposed Microsoft Exchange servers were vulnerable to threat vectors.

More than 5% of global government entities were running vulnerable versions of Exchange.

More than 340 U.S. government entities at the state, local, and Federal level -- including multiple U.S. Federal agencies -- were running vulnerable versions of Microsoft Exchange.

More than 5% of global utilities were running vulnerable versions of Exchange.

More than 3% of global aerospace/defense companies were running vulnerable versions of Exchange.

Despite recent warnings to patch threat vectors in their systems, BitSight observed a very high rate of confirmed vulnerable versions of Exchange currently running across the globe. In other words, despite the publicity, warnings, and guidance of patches, many organizations were slow to act in response.

Observations and Lessons

The above numbers demonstrate that when attacks like Hafnium occur there are remediation laggards. The laggard group is similarly represented by large and small organizations. Instead of size or resources, we can speculate that it is an organization's commitment (or not) to daily security performance excellence within their own organization and across their digital supply chain that marks them as more likely to be a laggard or not.

Organizations, large and small, who are slow to patch represent the soft spot within digital supply chains, and can represent a third-party threat within the digital vendor ecosystem.

This highlights the need for security and third-party risk leaders to rethink enterprise risk to encompass their third parties.

Looking back on prior events such as SolarWinds, NotPetya, BlueKeep, WannaCry, and now Hafnium, the question truly is what are the key lessons learned from these events. The following lessons are a start:

Lessons learned

For CISOs

- ☑ Hafnium was a massive attack. Visibility across the extended enterprise is critical.
- ☑ Ask the right questions and focus on remediation. Checking for patches alone is not enough, as patched systems may still have been exploited. CISO's must ask if systems are patched and the exploit remediated.

For Vendor Risk leaders

- ☑ Vendor Risk Management programs should adapt their own version of Zero Trust.
  - Subjective attestations are not reliable. Therefore, programs should implement their own version of "never trust, always verify"
  - Revisit the definition of critical vendors who require continuous monitoring

For Business leaders

- ☑ Regulatory cyber risk due diligence standards are evolving. Regulators expect data owners to preemptively test existing security measures within the organization and perform ongoing monitoring of its supply chain.
- ☑ Hyper-connected organizations benefit by raising the bar on mutual accountability over security performance.
  - Cyber supply chain risk is a "we are they" problem. Better security performance, stronger vendor risk management programs, higher assessment standards all result in better mutual assured resilience.

Kaseya

Lessons Learned on Digital Supply Chain Threats

Presented by ThirdPartyTrust

Kaseya: Lessons Learned on Digital Supply Chain Threats

The cybersecurity community was shaken in July 2021 after a massive supply chain ransomware attack hit managed service providers (MSPs) who use the Kaseya Virtual System Administrator (VSA). Attackers encrypted data at more than 1,000 companies and initially demanded $70 million ransom to retrieve the files.

After reporting the vulnerability in their on-premise remote monitoring and management solution, Kaseya quickly took SaaS services offline and warned customers not to run its software until a patch was available and manually installed.

Kaseya spokesperson Dana Liedholm confirmed that the incident involved multiple vulnerabilities in the company's products, as opposed to a single zero day exploit, and called it a "sophisticated weaponized attack with ransomware."

News outlets reported that more than 70 managed service providers were impacted, resulting in more than 350 further impacted organizations. Kaseya's CEO pointed out that only between 50-60 of the company's 37,000 customers were compromised, but since 70% were managed service providers, the attack surface was expanded to their entire customer bases.

It is believed that the threat actor was REvil/Sodinokibi, a ransomware-as-a-service (RaaS) affiliate. Automation allowed attackers to move from exploitation of vulnerable servers to installing ransomware on downstream companies faster than most defenders could react.

The attack succeeded in a couple of hours, so companies would have to run frequent monitoring and alerts to have caught the changes in their network. This means enterprises had very little to no time to detect and block the attacks.

Ten days later, after taking extra security measures to address all vulnerabilities, Kaseya released the patch to VSA on-premises customers and completed the restoration of services.

Among the affected organizations was the Swedish grocery chain Coop, which had to close several hundreds of stores on Saturday because of the ransomware attack, according to Reuters. As it turned out, its cash registers are run by Visma Esscom, which manages servers for a number of Swedish businesses and in turn uses Kaseya.

Who owns the risk?

In a report from the Associated Press, Kaseya CEO Fred Voccola said that when an investigation is complete, it would show that not just Kaseya but also third party software were breached by the attackers.

This raises a critical question: who is accountable for supply chain data breaches?

Even when a third party vendor is compromised and, as a result, another organization is affected, end users usually blame the company to which they trusted their data, and not their third party vendors.

It is a business responsibility to assess and secure all levels of information sharing with a third party vendor as part of a third party risk management (TPRM) program.

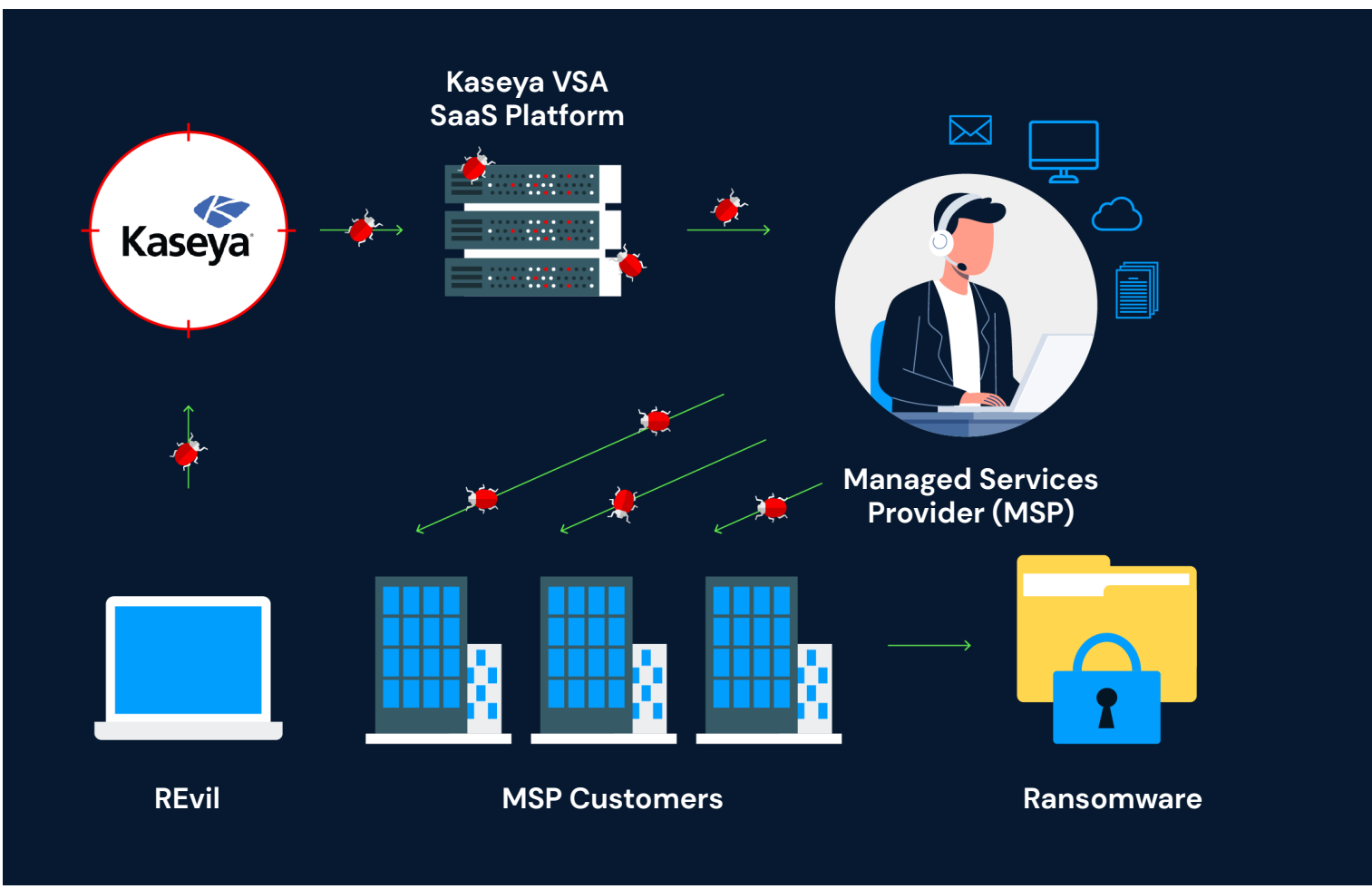
The Kaseya attack underscores the danger that weaknesses in business supply chains pose to organizations. Remote monitoring and management (RMM) providers are ideal targets for supply chain attacks, as they're used by managed service providers who act as entry points to their client networks.

One lesson learned from this case is the importance of continuous monitoring: in less than two hours, attackers spread throughout a network of interconnected businesses and only a real-time continuous monitoring tool could have detected that movement.

A second lesson is the importance of assessing and monitoring the relationship with third party vendors with access to critical data or systems. Organizations can have hundreds or thousands of suppliers digitally connected, and the risks are rarely quantified, as supply chain cybersecurity is often a relegated part of the strategy.

However, monitoring vendor risks and conducting a third party risk management strategy can be simplified given the right toolset.

In the world of cybersecurity, prevention goes a long way to avoid ending up in the headlines for the wrong reasons.



From Months to Minutes

Can New Regulations Accelerate the Cyber Incident Disclosure Process?

Presented by BitSight

Can New Regulations Accelerate the Cyber Incident Disclosure Process?

In the wake of numerous high profile cyber incidents, including ransomware and attacks impacting critical infrastructure, policymakers continue to consider new cyber incident disclosure laws to improve cybersecurity. On March 15, 2022, President Biden signed legislation requiring critical infrastructure organizations to disclose "substantial" cyber incidents to the Federal government within 72 hours. The Securities and Exchange Commission (SEC) is also considering new regulations requiring disclosure of "material" cyber incidents within 96 hours.

Are organizations prepared to meet these new cyber incident disclosure requirements?

BitSight analyzed more than 12,000 publicly disclosed cybersecurity incidents from 2019-2022 to assess the current state of cyber incident disclosure. We examined how organization size and incident severity affects the timeliness of incident discovery and disclosure.

This research suggests that compliance with these new obligations will be difficult to achieve, because cyber incident discovery and disclosure is a long, slow process.

In a world that requires speed and rapid response, data suggests that the time between incident occurrence, discovery, and disclosure is quite slow. Cyber incidents are typically discovered and disclosed after weeks and months, rather than hours and days.

It takes the average organization 105 days to discover and disclose an incident from the date it occurred; of that time, organizations typically don't discover an incident until 46 days after it has occurred, and they don't disclose an incident until 59 days after discovery. This is well beyond the 72-96 hour disclosure requirements envisioned by policymakers. Larger organizations are faster at discovering and disclosing incidents than smaller organizations, but they are still slow.

Time to disclosure per severity of incident

Organizations can do more to improve their cybersecurity posture and reduce the likelihood that they will experience a significant or material cyber incident. Timely remediation of vulnerabilities, reducing attack surface exposure, and implementing sound cybersecurity hygiene all measurably reduce the likelihood of experiencing cyber incidents, including zero day attacks.

As in previous examples mentioned in this ebook (e.g. Hafnium attacks), even when organizations are quick to identify vulnerabilities, laggards will persist in acting to remediate them. It's for this reason alone that vigilance and speed are crucial to preparing for future zero day attacks.

This BitSight resource has been amended. The full and original version can be found at: https://www.BitSight.com/blog/months-minutes-can-new-regulations-accelerate-cyber-incident-disclosure-process

Tips and Best Practices to

Prevent Zero Days

Presented by ThirdPartyTrust

Tips and Best Practices to prevent Zero Days

Software is written by humans, and humans are fallible. Developers create software every day, but unbeknownst to them, it may contain vulnerabilities. This makes zero day attacks inevitable, as attackers often spot those vulnerabilities before the developers detect and act on them.

The biggest take-away for any organization with this type of concern is understanding where vulnerabilities (and exploits) are most likely to occur. While cybercriminals often target the big companies hit by attacks in major headlines, it's often the much smaller third party vendors within their supply chains that present the biggest opportunity for bad actors to exploit a network.

So how can you minimize risk in your organization and across your vendor supply chain?

Zero day protection measures include:

1. Keeping all software and operating systems up to date, installing patches as soon as they become available. Security patches often cover newly identified vulnerabilities.
2. Enforcing security standards as part of your vendor risk assessments and updating your requirements if needed after a zero day is discovered.
3. Performing continuous monitoring and reassessment of your vendors as opposed to point-in-time calendar evaluations.
4. Using a layered defense strategy, combining antivirus, firewall, and other security solutions, with security mechanisms like zero trust or MFA.
5. Educating users on cybersecurity best practices, especially amid flexible work arrangements; many zero day attacks capitalize on human error.

What To Do If Your Organization

is Affected by a Zero Day

The first thing you need to do when a new zero day is reported is to assess the prevalence of the vulnerability in your organization and within your supply chain. In other words, determine if your organization or your vendors are utilizing vulnerable versions of the software in question.

As part of your due diligence and ongoing reassessment processes, you need to make sure that your vendors are enforcing standards that keep your business safe. Should a zero day vulnerability appear, you need to be able to promptly:

Identify vulnerable third party vendors in your supply chain

Ask them how they are planning to react and mitigate the vulnerability

Update your requirements and request additional assurances

All of these actions need to be conducted with a centralized, standardized third party risk management process, as opposed to chasing vendors via email and using spreadsheets to assess their security level.

If (or when) a zero day happens, immediately report potential exposure to senior executives and the board, using clear, concise language to effectively communicate risk.

Below are some practical steps to follow for zero day vulnerability remediation:

1

Patch your systems

Vendors and makers usually act fast to issue a patch once the zero day vulnerability is discovered. Install it as soon as it becomes available.

2

Assess risk exposure

Identify vulnerable third party vendors in your supply chain and check if your own organization is vulnerable.

3

Update your requirements

Ask your third parties for additional security requirements and assurances, and add them to your upcoming vendor contracts if needed.

4

Show your posture

If you are a vendor to other organizations, share an update of your security posture to let them know you already took the necessary steps.

5

Track, report, and conclude

Vulnerability management includes identifying, analyzing, remediating, and reporting phases; make sure everything is documented.


How
ThirdPartyTrust
and BitSight Can
Help

ThirdPartyTrust and BitSight combine vendor management and continuous monitoring for a complete view of third party security across your entire supply chain. The result is complete visibility into an organization's third party ecosystem, with end-to-end coverage of the supply chain.

ThirdPartyTrust is a third party risk management (TPRM) automation platform where enterprises and vendors connect to complete risk assessments, exchange security documentation, track, and monitor risk, increasing efficiency and eliminating repetitive tasks in vendor management programs.

BitSight is a provider and standard in security ratings, providing an objective, continuous, data-driven view into organizational security performance. Using an approach similar to credit ratings for financial risk, BitSight customers are able to gain insight into the security posture of third parties as well as into their own organizations.

Best of all, ThirdPartyTrust and BitSight integrate seamlessly into one another, offering complementary and comprehensive security coverage. The integration of both solutions enables organizations to manage their vendor risk program from start to finish with faster vendor validation, broader scale, and more integrated continuous monitoring solutions.

Benefits include:

Streamlining and automating the security questionnaire process

Identifying issues like zero days and acting proactively on your third party cyber risk

Getting an objective security rating for every vendor and comparing it to industry averages across a number of security vectors

With flexible fit-for-purpose features, the tools adapt to help you stay ahead of zero days or unexpected vulnerabilities like Log4j, SolarWinds, Kaseya, and more.

The ability to continuously monitor your vendors' security posture will raise timely alerts when an indicator goes beyond your security standards. In addition, a comprehensive and categorized third party inventory will make it easier to understand where to focus your attention when a zero day occurs.

When it comes to zero day response, the ability to rapidly create and distribute a simple questionnaire among your vendors to assess exposure and manage potential threats can make the difference between business as usual and business continuity issues.

If one of your vendors is vulnerable, you can use the ThirdPartyTrust TPRM platform to immediately ask them for additional requirements and assurances, and easily track them.

You can also update their category or change their classification (i.e. more or less critical, more or less impactful for the business). A variety of BitSight licenses are available directly within the ThirdPartyTrust platform (likewise you can use BitSight on its own), so you never have to choose between solutions. Everything is in one view, with solutions at your fingertips.

ThirdPartyTrust is a third party risk management tool for companies and vendors to perform assessments, automate TPRM workflows, and share security documents. Our platform allows both sides to connect in a single place to take risk assessments out of email and spreadsheets, and accelerates the security questionnaire review process through automation and centralized communication.

BITSIGHT

BitSight provides trusted data and insights that enable risk-based decision making for the world's insurers, investors, enterprises, and governments. BitSight pioneered the security ratings industry in 2011, creating the world's first cybersecurity ratings platform. Today, the BitSight rating is known around the world as a trusted analytic to help organizations understand and manage cyber risk.

Additional Resources

Ransomware in the Technology Sector: Key Findings To Protect Your Organization

GET THE GUIDE

Preparing for and Preventing Zero Days in Your Supply Chain

WATCH ON DEMAND

To learn more about our third party risk management automation tool, visit

www.thirdpartytrust.com