Cyber Risk Monitor

MAY 2021

by Luke Tenery and Ross Rustici

Message from Luke Tenery

Welcome to the premier issue of our monthly Cyber Risk Monitor, designed to provide actionable, relevant, and timely analysis of the most important cyber risk and intelligence trends.

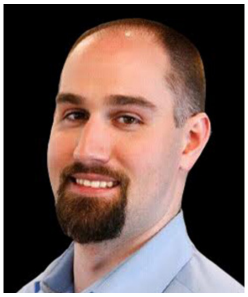
In each Monitor, we'll highlight the significant issue(s) of the previous month and key action items and/or areas to monitor. We'll also outline changes in reconnaissance and targeting, initial intrusion vectors and changes to on-network activity perpetrated by threat actors.

On behalf of StoneTurn's Cybersecurity team, we look forward to helping our readers make more informed risk decisions and welcome your feedback on this Monitor and future topics.

May's Intelligence Trends:

- Supply chain intrusions result in more third-party breaches as threat actors move to access enablement operations.
- Several new vulnerabilities drive a renewed emphasis on automated exploitation.
- Poor user account hygiene provides easy, hard to detect, malicious access.
- Ransomware extortion now leverages embarrassing executive data.

Luke Tenery
Partner, StoneTurn
ltenery@stoneturn.com
+1 312 775 1210



Ross Rustici
Managing Director, StoneTurn
rrustici@stoneturn.com
+1 617 570 3716

One-To-Many Hacks Threaten Supply Chains
Read more >>>

Automated Exploitation Targets More Vulnerabilities
Read more >>>

Common IT and Security Procedures Undermine Defenses
Read more >>>

Ransomware Extortion Gets Personal
Read more >>>

One-To-Many Hacks Threaten Supply Chains

Key Delta

Supply chain intrusions are not new, nor are the most recent identified intrusions the most impactful to date. Taken together and coming on the heels of SolarWinds, there appears to be an alarming new trend toward the increased use of the one-to-many hack. However, once the news cycle is put in perspective, what we are observing is actually a steady, systematic increase in an activity that is over a decade old.

In April, the most significant supply chain compromise in terms of reach and impact was Codecov. An online software testing platform that can be integrated with GitHub projects, Codecov has over 29,000 enterprises using its software. The supply chain intrusion went undetected for at least two months and allowed the threat actors to steal customer credentials such as tokens, API keys, and anything stored as an environment variable. This breach, along with Passwordstate and Accellion, as well as the attempted compromise of the PHP programming language used by 80% of all websites in the last two months, reaffirms that threat actors continue to conduct enablement operations around large third-party vendors.

Threat actors, whether they are nation state-backed or financially motivated, are constantly looking for economies of scale. Supply chain intrusions provide that in two ways. First, the threat actors are able to target less secure networks that have inherent trust with larger, more important targets. Second, a successful compromise allows a threat actor to selectively exploit follow-on victims. This reduces the cost of targeting each individual entity, allowing in some cases the threat actor to bypass the first seven tactics in the ATT&CK framework. This reduces both the time required to achieve their objective and the number of actions taken on a particular network, decreasing the likelihood of detection.

This is precisely the logic that drove NotPetya in 2016 and Stuxnet in 2009; destructive malware was pushed to end victims via a supply chain compromise. The supply chain compromise has been a favorite of nation-state actors for over a decade and we are now seeing this technique trickle down to more advanced cyber criminals precisely because of its efficacy.

Lastly, the growing complexity of the modern business world is unrivaled. The number of third-party dependencies required to run digital infrastructure, produce a tangible product or, maintain process oversight is both an economic imperative as well as a poorly mitigated risk. Threat actors will continue to exploit these relationships and vulnerabilities. Organizations in both the public and private sectors must focus on the levels of inherent trust granted to their suppliers and partners and craft acceptable loss strategies that focus on assumed breach models.

The risk cannot be eliminated with technology but, rather, through well-crafted policies and implemented architectures that reduce the impact of any one vendor compromise. Additionally, for those third parties that are truly mission-critical or must have elevated access, strategies must focus on reducing the time to detection of compromise through enhanced monitoring, intelligence and analysis of patterns of legitimate behavior for anomaly detection.

Automated Exploitation Targets More Vulnerabilities

Reconnaissance and Targeting

With the recent vulnerabilities in email services and VPNs allowing for remote code execution, threat actors have recently increased their automated targeting and exploitation. Like brute force attempts, mass phishing campaigns, or watering holes, this automated scanning activity eliminates the need for threat actors to conduct extensive reconnaissance or targeting. They can set up limited infrastructure and just wait for compromised hosts to unknowingly provide data about what network and access the successful exploitation gave them. This allows the threat actor to choose the most lucrative targets for focused follow-on attacks, while also reducing the clarity defenders have around the scope and intention of any particular campaign.

This is primarily an N-Day problem, which gives defenders an opportunity to combat it and reduce the likelihood of automated exploitation. Those who have found Zero-Day vulnerabilities in Internet-connected devices will not make noise by setting up automated scanners proactively. Instead, when a crisis hits, there will be a "race" between those exploiting as many devices as possible and those patching the vulnerability. This means corporations must focus on two main remediation capabilities. First, Internet-connected devices and services must have a short patch cycle. Services such as VPNs should always be patched as soon as possible. Second, policies such as least privilege must be leveraged around these types of services and devices. Limiting the ability of a threat actor to move laterally from these network beachheads will greatly reduce the impact of a breach.

Common IT and Security Procedures Undermine Defenses

Initial Intrusions

Between large password dumps, failure to properly decommission user accounts, inconsistent application of MFA, and the re-use of accounts and passwords between admin and local accounts, network security is being forced to change what it prioritizes and focuses on. While threat actors are still leveraging exploits for initial access, the underground economy around legitimate accounts continues to grow. The complexity of modern environments, especially when it comes to the rapid digital transformation that occurred in the last year, has created a unique opportunity for threat actors to pivot their operations to leverage legitimate access and services.

This combination of tactics, techniques and procedures (TTPs) complicates network security and incident response because teams rely on technical indicators of compromise rather than behavior analytics. Just as we have seen a seismic shift in the amount of fileless malicious code that has been deployed in the last five years, we are seeing a similar trend, especially among financially motivated threat actors, to leverage legitimate accounts and access rather than leaving fingerprints through traditional exploitation.

This trend is only possible because there are inherent and systemic weaknesses between how IT and Security operate in the majority of businesses. The tension between usability and security, user experience and network maintenance often puts security teams at a disadvantage. As the threat continues to evolve by leveraging legitimate application-level access, more focus needs to be placed on how IT and Security programs can collaborate to reduce risk exposure and find malicious use in the noise of normal activity.

Ransomware Extortion Gets Personal

On-Network Activity

Last year, largely as a result of better incident response practices and more companies adopting data recovery plans, ransomware groups started to shift tactics to double extortion schemes. The groups not only encrypted files in the targeted networks but also stole email and sensitive business information. The threat was to leave the network encrypted, locking authorized users out, and if the ransom was not paid, to release the exfiltrated information shaming the company and potentially exposing it to additional liabilities.

In addition, in the last month we have seen more groups attempt to leverage embarrassing information about senior executives to increase the pressure to pay the ransom, including: inappropriate images on corporate systems, information about adultery and other correspondence that would cause significant reputational harm.

Coercing powerful individuals into having a personal stake in paying hush money is not new. There are several scams targeting personal email addresses directly using the same pressure tactics. The convergence of personal targeting in corporate intrusions, however, is a new wrinkle – though it is unlikely to be widely adopted or successful in corporate attacks. After all, either the information is unknown and simply alluding to its existence brings sufficient shame and potential consequences or, it is known information, in which case it creates no leverage for the threat actor.

Instead, this type of additional, targeted ransoming is likely to be made as a smaller demand, directly to the compromised individual. This would allow the threat actors to gain multiple payments from a single attack and would likely create different risk scenarios for the individual and the corporation.

Practice Area

Cybersecurity

Increased opportunities for cyber threat actors worldwide. Increased regulatory pressure on data security. Widespread transformation to cloud-enabled and unsecured digital technologies. Ongoing merger, acquisition and integration activity that exposes or creates vulnerabilities in critical operations. An increasing imperative for technology leaders to deliver value and assurance across the enterprise.

Today's business leaders must strike a critical balance when it comes to cybersecurity—undertake appropriate risks to move the organization forward without compromising the robust security framework and supporting internal controls that make sustainable results possible.

StoneTurn brings a multidisciplinary team of security leaders, cyber technology, risk and investigative experts to help clients across the threat and risk continuum—from prevention to detection, mitigation through to remediation and transformation. Whatever the context, we work collaboratively with you to restore trust, expedite resiliency and proactively secure business-critical information. Rely on insights from our experienced, pragmatic professionals to help simplify complex cybersecurity, data privacy and data protection challenges.

Turn to us when:

- Rapid and holistic, incident response, cyber investigation, and/or a threat intelligence is required to restore stakeholder trust and protect the enterprise
- You need assistance to strategically manage complex cyber risk issues that drive the business forward
- Regulatory issues or inquiries require independent cybersecurity or privacy expertise
- Financial or other fraud reveals vulnerabilities in your technology operations
- A merger, acquisition, integration or transformative issue is on the horizon
- Situational risks dictate the need for enhanced security protections from economic crime, bribery or corruption
- Remediation is required to address long-standing control issues that resulted in a cyber incident
- Developing a strategy and vision for future state of secure technology operations to maximize opportunities

StoneTurn.com

StoneTurn

Learn more about StoneTurn's Cybersecurity practice.

About the Authors

Luke Tenery, a Partner with StoneTurn, brings nearly 20 years of experience helping leading organizations mitigate complex cybersecurity, data privacy and data protection risks. He applies extensive expertise in cyber investigations, threat intelligence, incident response, and information risk management to assist clients across the threat and risk continuum—from prevention to detection, mitigation through to remediation and transformation.

Ross Rustici, a Managing Director with StoneTurn, has over a decade of experience advising governments and global corporations on cybersecurity matters, as well as building security and intelligence programs for clients. Over the course of his career, Ross has architected a variety of cyber threat solutions to reduce risk and secure organizations. Specifically, Ross has built customer engagement and content delivery frameworks for intelligence services, while orchestrating end-to-end alignment of product, sales, customer success, and services. Additionally, he has developed analytic standards, structures, and road maps to create new and value-driven business units in the security space.

Leaving no stone unturned.

StoneTurn, a global advisory firm, assists companies, their counsel and government agencies on regulatory, risk and compliance issues, investigations and business disputes. We serve our clients from offices across the U.S., U.K. and in Germany, Brazil and South Africa, assisted by a network of senior advisers around the world.

StoneTurn.com

StoneTurn