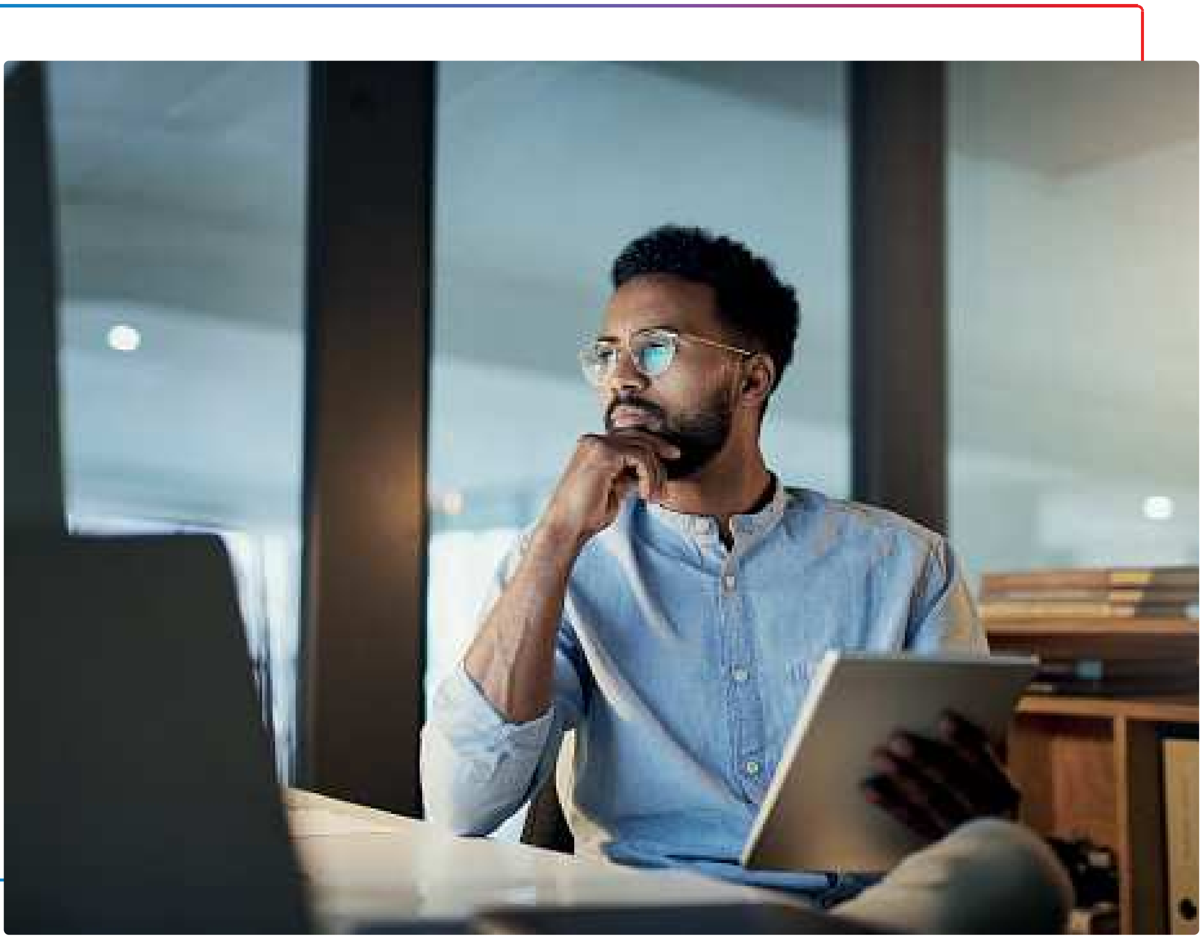
MANDIANT
NOW PART OF Google Cloud

Cyber Snapshot Report
Issue 3



The Defender's Advantage Cyber Snapshot report offers insights into cyber defense topics of growing importance based on Mandiant frontline observations and real-world experiences. In this edition, topics covered include:

The Journey to Passwordless Authentication

Historically, challenge-response authentication using a singular password has been one of the primary mechanisms leveraged by organizations to positively verify an identity for authorization. However, following this model of a singular transaction for authentication, without additional identity verification requirements, could create substantial risk to an organization.

As attackers adopted more sophisticated tactics for compromising identities, new controls and methodologies were introduced to help mitigate risk. The most common control that many organizations have adopted is the requirement for multi-factor authentication (MFA), a concept that combines two or more independent methods to positively verify an identity.

Throughout numerous incident response investigations, Mandiant has observed that while organizations increased their adoption of traditional MFA methods, attackers continued to advanced threat tactics to compromise identities using techniques such as:

bypassing enforced MFA

abusing weaker MFA methods (e.g., SMS, push notifications, phone calls)

enrolling attacker-controlled devices for MFA verification and authentication

This elevated threat shifted the focus of aligning MFA adoption to newer tools with stronger MFA methods, such as number matching, contextual telemetry notifications, and inputting time-based one-time passwords (TOTPs). Additionally, vendors and organizations are further enhancing MFA methods by leveraging either Fast Identity Online 2 (FIDO2) keys / tokens, software / hardware Open Authentication (OATH) tokens, or certificate-based authentication.

Authenticators

To further enhance authentication security, the concept of "authenticators" has started to become integrated as part of identity and access management practices for organizations. Authenticators move away from the singular context of a password, and require multiple components to positively verify an identity. Example authenticators can include a multi-context of a username/password combined with strong MFA methods, certificates, device state context, identity risk calculation, or passwordless methods.

When aligning under the concept of "authenticators," the overall risk of a compromised password is greatly reduced as the singular nature of the password is no longer the first and last line of defense for authentication.

What is Passwordless?

Building off strong MFA methods, passwordless authentication is starting to become part of the "authenticator" equation for many organizations. Passwordless is essentially a method of verifying an identity without the requirement for a knowledge-based secret. Instead, the identity authenticates by using something they have (device) or something they are (biometric). Under the premise of passwordless, the requirement for either possession and/or inherence-based factors increases security by removing the requirement for a "something you know" (password) factor being part of the authentication equation.

Practical and scalable methods of leveraging passwordless authentication can include:

- **Mobile Authenticator Applications** – which can either generate a one-time passcode (OTP)(based upon a synchronized algorithm) or can be used to approve or match a number sequence that is displayed to a user.
- **FIDO2 Hardware Tokens and Keys** – which can interface with a device using either a physical connection, Bluetooth, or near field communication (NFC). With the FIDO2 WebAuthn method specifically, the device-bound hardware token can be used to authenticate to the destination application using a unique cryptographic keypair (stored on the roaming authenticator device) and exchanged using public-key cryptography. FIDO2 Webauthn is an effective method of leveraging passwordless authentication to combat phishing, spoofing, and adversary-in-the-middle (AitM) attacks.
- **Passkeys** – which operate like a FIDO2 token, where a cryptographic keypair is generated and stored locally on a mobile device, and exchanged using public key cryptography with an application that is the target for authentication (which holds the public key). To access a configured passkey, a mobile device will require either biometric identification or a PIN / swipe pattern common with popular mobile devices.
- **Digital Certificates** – which can be used to generate a valid digital "identity" signature in response to an authentication request by using public and private keypairs. On modern devices, the trusted platform module (TPM) can be used as the internal authenticator to store the private cryptographic key, which is used to sign a certificate that will be validated for "passwordless" authentication using a corresponding public key.

- **Biometrics** – which can leverage the unique physical features of a human to validate an identity. Most commonly, biometric authentication will include fingerprint (Touch ID and Fingerprint Unlock as an example) and facial recognition methods (Face ID and Face Unlock as an example), which are inherent to many smartphones, mobile devices, and modern laptops.

Planning for Passwordless as an Authenticator

Legacy applications and infrastructure that do not readily support enhanced authentication methods can present a speed bump for organizations attempting to align under the concept of authenticators. Rather than focusing on integrating the authenticator equation for each individual application, it is now common for organizations to leverage a third-party single sign-on (SSO) solution as the front door for authentication, which will then broker authenticated access to backend applications.

Planning for passwordless as part of the authenticator equation can take time. A high-level overview of considerations include:

Identify:

- Current-state technologies and platforms that function as authoritative identity stores and platforms (IdP).
- Existing identity stores natively support passwordless authentication methods – or will require third-party integration and brokers.
- Identities that exist within an organization, including identity types that could test and verify the passwordless experience.
- Compensating controls and enhanced detections for identity types that don’t support passwordless or strong authentication methods (e.g., programmatic / service accounts).
- The impact to guest / third-party users that may not support passwordless integration.
- Devices that users currently leverage for authentication and access – and verifying if these devices support passwordless methods.
- Applications that can be integrated directly for passwordless, or applications that support SSO integration with a third-party platform that supports passwordless methods.

Developing a plan for:

- Procuring and securely delivering and onboarding devices that will support passwordless authentication.
- Training curriculum to educate users about the passwordless experience.
- Identity store and device configuration modifications to onboard the passwordless integration.
- Testing and validating the passwordless integration with pilot users and scoped applications.
- Initial roll out and onboarding as well as expanding the scope of passwordless throughout the organization.

Another important consideration for passwordless is aligning recovery steps when a device or key is lost or stolen, as these are now core components to the authentication process for an identity. Planning for secure recovery steps must include weighing not only organizational risk, but the pros / cons to the overall user enrollment and self-service experience.

While internal authenticators (e.g., devices with an integrated TPM) can provide the ability to export (store) or sync private keys between devices, this can also introduce a risk if the keys are not secured and stored properly. When using third-party identity providers, recovery keys and phrases can also be considered as a method for recovering a passwordless identity for reconstitution on a new device. When roaming authenticators are used for passwordless authentication, options for identity recovery can include validating messages sent to a mobile device or email address.

Migrating from the concept of singular passwords to passwordless as an authenticator is a journey. Many organizations adopting the concept of authenticators have found that strong MFA is a foundational building block in support of a passwordless roadmap. While the journey requires proper planning, execution, and validation, the security benefits and risk reduction are invaluable, especially as identity is the new security boundary in today’s hybrid operational model.

Minimizing Risk to Obtain Cyber Insurance

U.S. banks identified $1.2 billion in ransomware transactions across 1,489 reports to regulators in 2021–a steep increase from $416 million across 487 reports the previous year.[4]

Ransomware payments more than doubled between 2020-2021[1] forcing insurers to take bigger losses and sending the cybersecurity insurance market on a volatile path that has only recently begun to stabilize. And while the end of 2022 saw an 80% deceleration in cyber insurance rate increases, improving market outlook for 2023[2], most carriers believe cyber risk will continue to rise as ransomware remains a top threat[3]. As a result, organizations can expect increased scrutiny during the underwriting process on their security controls and internal processes and procedures concerning cyber risk. Additionally, there remain troubling exclusions for widespread events (i.e., Log4j) and incidents that can be tracked to the war in Ukraine or nation-state sponsored attack groups. In fact, carriers continue to reduce or even exclude ransomware-related coverages if the organization fails to demonstrate adequate controls in managing this risk.

Over the last 12 months, Mandiant has seen an increase in cyber insurer involvement during incident response engagements. While CISOs are not consistently consulted in policy coverage decisions, we recommend CISOs work hand-in-hand with an organization's risk manager and legal counsel to ensure accuracy in the application process and review policies so they are not caught off-guard during a breach.

Cyber Insurance 101

In the mid-2000s, insurers expanded coverage to reimburse companies for the costs of cyber attacks that directly affected their business[5]. Since then, expanded coverage has become a useful tool for financial risk managers and cybersecurity leaders to mitigate risk and offset costs from data breaches or other security incidents. Policies generally cover cyber risk to the company (first-party risk) and liability from consumers or businesses (third-party liability). Initially, underwriting for cyber insurance focused on the costs associated with data breaches and as such, organizations were required to provide information about the types of records, client data, and regulated data they processed to the underwriters and certifying compliance to regulatory standards like HIPAA and PCI DSS. Ransomware and multifaceted extortion pose an additional risk of business interruption that can cripple a business and generate substantial costs.

[1] Wall Street Journal, Reported Ransomware Incidents, Cost Soard in 2021, Treasury Says, November 4, 2022
[2] Marsh, US Cyber Insurance Market Update Signs of improvement in third quarter of 2022, October 7, 2022
[3] Woodruf Sawyer, 2023 Property & Casualty Looking Ahead Guide, January 10, 2023
[4] Wall Street Journal, Reported Ransomware Incidents, Cost Soard in 2021, Treasury Says, November 4, 2022
[5] The Federal Reserve Bank of Chicago, Chicago Fed Letter, No. 426, 2019 The Growth and Challenges of Cyber Insurance, 2019

TABLE 1: Common Cybersecurity Risk Coverages.

First-Party Coverage	Third-Party Liability
Incident Response and Forensic Fees	Security and Privacy Liability
Notification, Credit and Identity Monitoring	Multimedia/Media Communications Liability
Data Recovery	Regulatory Defense and Penalties
Business Interruption	PCI DSS Liability
Cyber Extortion and Cyber Crime	Telephone Consumer Protection act Defense
Reputational Damage	

*Source: Honigman LLP Attorneys and Counselors, Cyber Insurance 101, May 19, 2021

As a result, insurers have sharpened their pencils to take a deeper look at an organization's technical controls and mitigation activities against interruption and other associated business loss. This translates to a rigorous underwriting process to determine risk and policy pricing. Today, underwriting involves additional questions, interviews, and submitting to external scanning of your environment.

Beth Burgin Waller, Chair of the Cybersecurity and Data Privacy Practice at Woods Rogers, who spends significant time reviewing and negotiating cyber insurance for clients in addition to being incident response counsel, recommends working with your risk management team and legal to prepare for the underwriting process.

Underwriting questionnaires often include black and white questions that don't apply to today's complex multi-cloud, multi-network corporate infrastructures. For example, when answering a question about whether you have multi-factor authentication (MFA) across the enterprise, your underwriters may ask for proof that MFA is present in every part of the enterprise from back-ups, to cloud business applications and the VPN. Your counsel and risk management team can help flag sweeping statements made in the application and assist with supplemental responses that clarify current production controls and any plans for improvement.

Understanding nuance of IR coverage

Burgin Waller highly recommends reviewing the specimen (sample) policy. "As the market stabilizes, cyber policy language is standardizing similar to other insurance policy products," says Burgin Waller. The sample policy may indicate you have business interruption coverage to a certain limit, but without careful examination of the specimen policy, you may have exclusions built into the policy for legacy software, widespread events such as Log4j, or the latest exclusion–acts of war, covering incidents attributed to nation-state threat actors. Burgin Waller suggests paying particular attention to policy sub-limits. In one example, a base-level cyber policy included a sub-limit for incidents initiated via phishing and expected the organization to have supplemental coverage for ransomware. "A careful read of your specimen policy on the front end," says Burgin Waller, "can save you significant headaches during an incident by clarifying what may or may not be covered for your organization in advance of an incident."

Can you expect the incident response provider and associated costs to be covered? Mandiant incident responders encounter three common scenarios:

1) The IR provider is an approved vendor with pre-negotiated rates. This streamlines kicking off the engagements and can make it easier for clients to submit claims.

2) The IR provider is not pre-approved and the insurer will cover $x/hour. The client will have to make up the difference if the IR rate is higher than the covered amount.

3) The IR provider is not pre-approved and the insurer won't provide any coverage if that IR provider is used. This scenario can create the most disruption during a breach event.

It is important to review the specimen policies for coverage of the entire incident response process. Some policies only cover the investigation, and exclude ransomware payouts, general counsel costs, or costs associated with recovery and long-term remediation efforts. Additionally, insurance carriers may not cover a full investigation to determine exactly how an attacker got in and to verify that they didn't leave any backdoors that would make the client vulnerable to reinfection. At that point, it becomes a business decision on whether to move forward with a deep investigation aimed at reducing future risk.

A new approach

Overall the cyber insurance market is maturing such that providers are partnering with their customers to enhance overall cyber resilience. The insurance industry has very advanced risk modeling programs that are being applied to help make organizations safer.

Many insurance partners offer a set of vendors and solutions they have vetted to help their customers navigate the cybersecurity marketplace and reduce risk by employing technologies that have demonstrated effectiveness.

Insurance partners have even identified security controls that can make a positive impact on an organization's cyber risk and related policy costs[6]. Mandiant embraces recommendations from the insurance industry and highlights the following five practices that, properly implemented, can mitigate the impact of or prevent typical attacks:

1. **Multi-factor authentication:** MFA, or two-factor authentication, is a technology that combines two or more independent credentials (e.g., passwords, security tokens, and face or fingerprints) to provide user access. Throughout numerous incident response investigations, Mandiant has observed that while organizations have increased their adoption of traditional MFA methods, attackers continue to advance threat tactics to compromise identities. Implementing strong MFA tools and methods – such as number matching, contextual telemetry notifications, and inputting time-based one-time passwords (TOTPs) – across all externally accessible login portals and for any sensitive internal applications can reduce risks of common adversarial initial access techniques.

2. **Identity and privileged access management:** Identity is the new security boundary in today's hybrid operational model. Mandiant sees the compromise of directory and access management systems in many incident response engagements. These systems are often used by threat actors to escalate privileges. Organizations should ensure users and systems have proper access and that directory and access management systems are properly configured to prevent unauthorized privileged access escalation.

3. **Secured, encrypted, and tested backups:** Mandiant recommends organizations have a tested plan for securing and encrypting backups to facilitate restoration of systems and data in the event of a cyber attack. Backup and external storage solutions can help decrease the likelihood of IP loss and ensure valuable records are protected from loss. Companies are increasingly using cloud service solutions as a way to maintain a copy of their cloud or hybrid networks in case of a cyber attack that would otherwise stall operations.

[6] Marsh, Cyber Insurance Market Overview: Fourth Quarter 2021, December 7, 2021

4. **Cyber incident response planning and testing:** Mandiant views cyber incident response planning and testing as a critical activity involving the review of existing technical controls, network architectures, and first response capabilities. Mandiant suggests developing plans for typical response scenarios and continuously validating cyber defense capabilities to enable rapid containment in the event of an incident.

5. **Retain legal and incident response partners:** An important part of cyber incident response planning is being prepared to engage outside support to protect the company from legal risks and obtain expertise in incident response. Legal counsel–especially those focused on cyber issues–should be able to work seamlessly with forensic responders in the event of an attack to assess legal liability and risks that may arise from the event. External incident response support can significantly reduce the response time, thereby reducing the impact of a breach. An Incident Response Retainer (IRR) allows companies to agree upon terms and conditions for incident response services before a cyber security incident is suspected.

Insurance partners also offer security consulting and services to help navigate the application process. Many brokers and carriers are differentiating their services by extending their consultancy with assessments, cyber hygiene, and processes needed to develop effective defensive capabilities.

Get more help navigating cyber insurance from Mandiant partners, podcasts, webinars and Google Cyber Risk offers.

Security Analyst Case Study: See and Stop Software Supply Chain Compromises

What good looks like when activating your detect and respond functions

Last year, Mandiant reported a significant increase in supply chain compromise–17% of intrusions over the course of 2021 started within the supply chain, up from <1% in 2020[7]. This increase is partially explained by the fact that 86% of the compromise intrusions Mandiant tracked were related to the SolarWinds breach and SUNBURST[8]. However, it also correlates to organizations maintaining technology relationships with an average of 244 vendors[9].

A software supply chain attack is nothing new. In 2017, the world was hit with the attack dubbed NotPetya. The malicious code, disguised as ransomware, exploited the NSA's leaked EternalBlue vulnerability to infiltrate networks and then systematically destroy data. The attackers behind NotPetya breached a financial services software company that was a supplier for the Ukrainian government.

In the same year, the utility CCleaner[10] suffered a breach and hackers were able to replace the legitimate version of the software with a malicious one, which resulted in the compromise of more than 2 million hosts.

In 2020, the aforementioned widespread attack leveraging a SolarWinds component was perpetrated by APT29 (previously UNC2452), a threat actor whose targeting is assessed to be consistent with Russian strategic interests[11]. The breadth of victims impacted by APT29 included government organizations and Fortune 500 companies. Once again, attackers targeted the software supply chain by injecting a backdoor code in the software component Orion, giving them access to the victims' internal environments and enabling them to deploy the SUNBURST malware after the updated code was distributed through a legitimate process.

Attackers have found a way to compromise the building blocks of our digital enterprise. By targeting and successfully compromising a popular package used by software developers, it is then easy to amplify the distribution of malicious code directly to victims themselves at scale. This approach leaves defenders asking if we are confident in our readiness to defend. Organizations worldwide are stretching to maintain visibility on their attack surface, and confidence in their detect and respond functions. Too often organizations are unsure of their ability to quickly see and stop cyber attacks within their software supply chain, in part because they lack properly trained defenders and don't activate–or respond–frequently enough to fine-tune their training and knowledge.

[7] Mandiant, M Trends 2022
[8] Mandiant, M Trends 2022
[9] Mandiant, The Defender's Advantage Cyber Snapshot Issue 2, 2022
[10] Mandiant Threat Intelligence, "CCleaner Supply-Chain Compromise Possibly Linked to Chinese Cyber Espionage Operators:, September 2017
[11] Mandiant, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor", December 2020

Software supply chain compromises are designed to abuse the trust in third-party providers to indirectly gain access to a victim's environment and can be difficult to detect. In the end, the security analyst's trained eyes and investigative process is the deciding factor in identifying and stopping advanced attacks.

> With supply chain attacks, a pre-established trust makes the malicious implant extremely difficult to detect directly. An activated and effective detection and response capability becomes even more critical as a suspicious event detected in the later stages of the same attack lifecycle allows analysts to discover the implant indirectly by rewinding the attackers actions through investigation.
>
> **—Steve Ledzian VP, CTO-APAC, Mandiant**

Analyst Detection and Investigation of a Software Supply Chain Compromise

Starting in mid-October 2021, security analysts in Mandiant's managed detection and response service identified multiple events that appeared to be a poisoning of open-source repositories. The following case describes their detection and investigation process–and the questions they sought to answer–involving packages hosted on Node Package Manager (NPM), the package manager for the Node.js JavaScript platform.

A small team of Mandiant security analysts initially observed multiple alerts indicating that a native Windows utility **CERTUTIL.EXE** was being used to download payloads from a common URL **(hxxps://citationsherbe[.]at/sdd.dll)**. As more analysts in the Security Operations Center (SOC) started picking up similar alerts, the team began to work in coordination towards answers to their investigative questions.

What is it? How did it get downloaded onto the system?

The first investigative questions to be answered are, "What malware is present and what are its capabilities?" and "How did it arrive on the system?" Analysts acquired the payload from initial hosts to determine the functionality and capabilities of the suspicious binary. Triage analysis indicated that the binary was a variant of the DANABOT malware, which targets credentials for theft through communication with an attacker-controlled command and control (C2) server. Using the malware's C2 address, analysts began to further scope the environment by identifying other systems communicating with the attacker infrastructure. This process allows analysts to determine if the same or similar malware may have been deployed on other systems without a corresponding alert. Once the payload is confirmed malware, the analyst team proceeded to contain the compromised hosts remotely or by initiating the incident response team to act.

DANABOT is a backdoor written in Delphi that communicates using a custom binary protocol over TCP. The backdoor implements a plug-in framework that allows it to add capabilities via downloaded plugins. DANABOT's capabilities include full system control using a VNC or RDP plugin, video and screenshot capture, keylogging, arbitrary shell command execution, and file transfer. DANABOT's proxy plugin allows it to redirect or manipulate network traffic associated with targeted websites. This capability is often used to capture credentials or payment data. DANABOT can also extract stored credentials associated with web browsers and FTP clients.

“ua-parser-js” is a lightweight, small footprint package deployed within a web application or server-side application to extract and filter the relevant data needed to parse a User Agent string (i.e., Browser, Engine, OS, CPU, and Device).

How did it get there?

To understand how the malware was deployed, analysts typically rely on data collected by endpoint detection and response (EDR) technologies. By reviewing EDR telemetry, the analysts traced the activity to legitimate commands executed by users to update NPM packages.

Thorough investigation revealed that each of the affected hosts had a similar file written to the **UA-PARSER-JS PACKAGE** directory, which led the analysts to believe it was compromised and distributing malware. The malicious change to the JS Package directory added a preinstall step to the package installation process, which downloaded the malware. In reviewing the compromised script, the analysts found that it also downloaded and deployed coinminers (also called cryptocurrency miners) to the host. Analysts checked the GitHub issues for the package repository and found a question where someone had asked if the package was very recently compromised. According to a GitHub issue raised on October 22, 2021, at approximately 12:15 UTC, the NPM package **“ua-parser-js**", a popular Node.js library that amassed over 7 million downloads per week, was compromised to deliver malware. The threat actor was able to publish three malicious versions of the package by hijacking the author’s NPM account. According to the repository’s Git log, on October 22, between 16:14 UTC and 16:25 UTC, the package author committed a sanitized version of the malicious packages to stop further compromises.

What other activity was performed by this threat actor?

After the hosts were contained, the analysts continued researching to determine the root cause of the attack. Reviewing the git log of the package repository, the analysts found timestamps for when the malicious change was pushed and when the fix was applied a few hours later. Further analysis of attacker TTPs allowed the team to link additional NPM packages, compromised by the same attacker, and scope the extent of the activity performed by the threat actor. The team was able to attribute the activity with reasonable confidence to UNC3379, analyze the malware, document attacker behavior, and develop detection techniques to thwart future activity.

For more information on this software supply chain compromise, review the research blog, No Unaccompanied Miners: Supply Chain Compromises Through Node.js Packages.

Trust analyst instinct, critical thinking and experience

Regardless of the scale of the investigation, time is of the essence. Mandiant relies on our analysts' knowledge, training, and critical thinking in investigation and response. Our team operates like detectives, leveraging the clues, evidence, and forensic artifacts to uncover the story behind each incident. The goal of the investigative process is to answer key questions about the attack to determine:

- Scope of the intrusion
- Whether it is still ongoing
- Earliest date of compromise and cause of the intrusion
- Type and extent of data exposed
- Threat actor Identity and motives

Understanding these facts about the intrusion will guide your containment, eradication, and recovery. Through frontline experience, simulation, and training, Mandiant recommends empowering your analysts to lead investigations and make key decisions around the timing and execution of containment and eradication. "It's common for organizations performing their own incident investigation and response to prematurely jump to remediation," says Eric Scales, Vice President Mandiant. "The more that you understand about the attack, the greater the success in eradication and recovery."

In the case presented here, Mandiant MDR's analyst-led investigation developed key atomic indicators related to the activity, performed triage of the malware deployed to determine the appropriate remediation actions, and, using our in-depth knowledge and research about the threat group, successfully scoped the environments of our customers to discover additional malicious activity related to this campaign that was not detected by their EDR products.

Activating Cyber Defense Around CISA's Cross-Sector Cybersecurity Performance Goals

Nation-state threat actors continue to pursue critical infrastructure technologies. Last year Mandiant reported findings of custom-made tools that enable attackers to scan for, compromise and control certain industrial control systems (ICS) or supervisory control and data acquisition (SCADA) devices once they have established access in an operational technology (OT) network[12]. As industrial and critical infrastructures become increasingly network-connected, this heightened threat sophistication enhances the need for updated cybersecurity guidance for critical infrastructure. The Cybersecurity and Infrastructure Agency (CISA), National Institutes of Standards and Technology (NIST) and the interagency community developed cybersecurity goals consistent across all critical infrastructure sectors.

In October 2022, CISA released the Cross-Sector Cybersecurity Performance Goals (CPGs)[13] as a guide to help organizations identify and prioritize the most important cybersecurity practices. CISA CPGs are meant to be a baseline to address cybersecurity challenges organizations face daily. They aim to make progress on the shared goal of reducing cyber risk to better defend our nation's critical infrastructure such as hospitals, energy suppliers, transportation systems and major manufacturing.

Mandiant embraces CISA CPGs guidelines to create a starting point to reduce risk. The CPGs serve as a first iteration of goals to National Security Memorandum (NSM-5): Improving Cybersecurity for Critical Infrastructure Control Systems. They are an important step, not an all-encompassing cybersecurity program, to get started on the path toward a stronger cybersecurity practice.

[12] Mandiant, INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems, April 13, 2022
[13] Cybersecurity and Infrastructure Security Agency, CPG Cross-Sector Cybersecurity Performance Goals 2022

CPGs are intended to be a floor, not a ceiling, to reduce cyber risk. Key characteristic highlights include:

Mapped subset of cybersecurity practices

Relevant guidelines specific for IT and OT

Prioritized risk reduction practices

Informed by threats observed by CISA and its government and industry partners

Applicable across all CI (critical infrastructure) sectors

The CPGs call out specific actions and items related to OT and ICS as a way to help these organizations better defend their critical infrastructure.

Regardless of the size of an organization, protecting critical infrastructure requires an understanding of relevant cyber threats, rigorous security testing, and threat detection and response conducted across the entire enterprise. The CPGs help organizations think about how to focus investment toward the most impactful security outcomes while taking into account budget, staffing and expertise.
The investment in practices to implement the CPGs will "help meaningfully address serious risks to the safety, health and livelihoods of the American people[14]."

[14] Cybersecurity and Infrastructure Security Agency, CPG Cross-Sector Cybersecurity Performance Goals 2022.

Understanding of Relevant Cyber Threats

The CPGs guide organizations to maintain awareness of relevant threats and leverage attacker tactics, techniques, and procedures (TTPs) to detect ongoing attacks. Understanding relevant cyber threats is paramount in Mandiant's approach to OT security in which we guide customers to enhance threat detection capabilities of both IT and OT networks, with full situational awareness[15]. We believe that defenders and incident responders should focus much more attention on intrusion methods, or TTPs, across the attack lifecycle, most of which are present on what we call "intermediary systems"—predominantly systems that cross the network boundaries of IT and OT or those networked workstations and servers within the OT network that use operating systems and protocols that are similar to (or the same as) those used in IT. Narrowing the focus to intrusion methods is effective because the majority of sophisticated OT attacks leverage these intermediary systems as stepping-stones to their ultimate target.

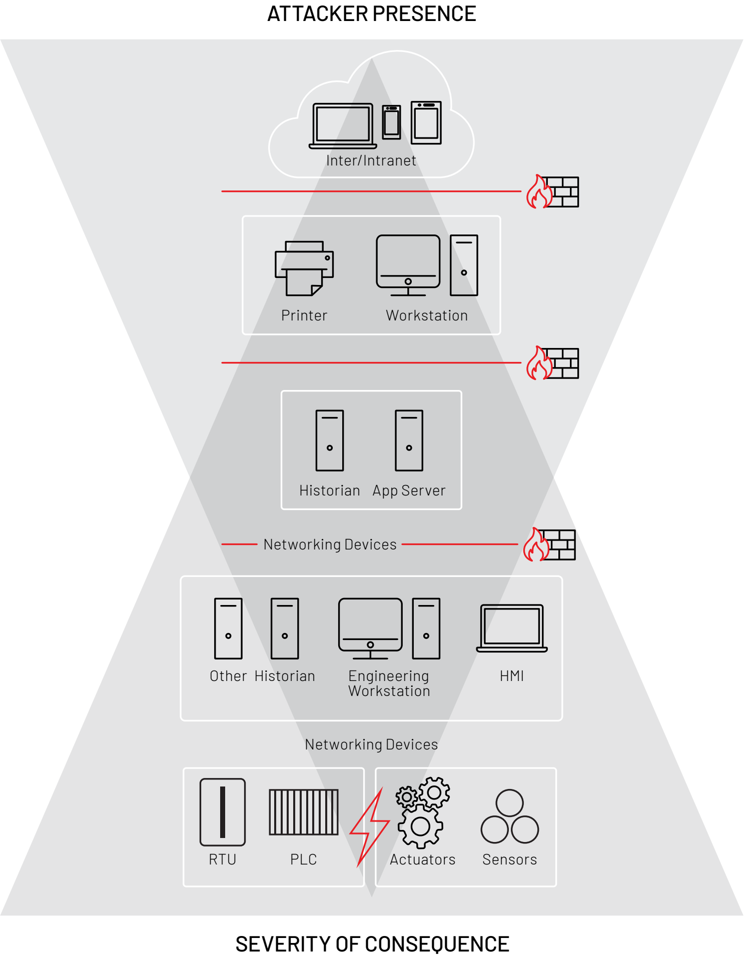


Figure 1. The Funnel of Opportunity for OT Threat Detection.

[15] Mandiant, The Mandiant Approach to Operational Technology Security, December 2019

The greatest opportunity for detecting a targeted OT attacker is in the intersection between the two triangles in Figure 1[16]. It is here that the balance between attacker presence and operational consequence of an intrusion makes it easier and more meaningful for security organizations to identify threat activity. Defenders should understand attacker intrusion methods and leverage that knowledge to hunt for and detect advanced threats. Threat hunting close to the OT DMZ and the Distributed Control System (DCS) can be most efficient as the intrusion's detectable features are still present and the severity of potential consequences of the intrusion is high, but still not critical.

[16] Mandiant, The Mandiant Approach to Operational Technology Security, December 2019

2022

In 2022, Mandiant reported sensitive OT and network documentation being exposed in ransomware extortion attacks[17]. The exposure of sensitive OT data from ransomware-related or any type of data leak provides sophisticated actors with information on targets, specifically about the victim's infrastructure, assets, security weaknesses, and processes. Reconnaissance data of this kind is used by threat actors to create more significant and precise attacks.

TABLE 2: Documentation Exposed in Ransomware Extortion Attacks

Victim (Names Redacted)	Leak Contents
Manufacturer of industrial and passenger trains	Password administration credentials for an OEM, requirements for control architecture and communication channels for European tram vehicle, backups of Siemens TIA Portal PLC project files, etc.
Two oil and gas organizations	In-depth network and process documentation, including diagrams, HMIs, spreadsheets, etc.
Control systems integrator	Engineering documentation from customer projects (Some files were password protected, which we did not attempt to bypass).
Hydroelectric energy producer	Most data was financial and accounting related, however we identified a list of names, emails, user privileges, and some passwords from IT, plant maintenance, and operations employees.
Satellite vehicle tracking service provider	Product diagrams, visualizations, and source code from a proprietary platform used to track automobile fleets via Global Positioning System (GPS).
Renewable energy producer	Legal agreements between the victim and customers stating the conditions for maintenance and supply of renewable energy infrastructure. The contracts stated that the service provider had full access to the third party's SCADA system via public internet IP addresses.

- Enforce robust data handling policies for employees and subcontractors that touch data from all segments of the network to ensure that internal documentation is protected.
- Avoid storing highly sensitive operational data in less-secure networks.
- Place special attention on selecting subcontractors that implement comprehensive security programs to safeguard operational data.
- Victims of ransomware intrusions should assess the value of any leaked data to determine what compensatory controls can help decrease the risk of further intrusions.
- Change any leaked credentials and API keys. Consider changing exposed IP addresses for critical systems and OT jump servers.
- Periodically conduct red team exercises to identify externally exposed and insecure internal information.

[17] Mandiant, 1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information, January 2022

Rigorous Security Testing

One key to confidently improving the security posture of OT networks is safely testing security controls at each layer of the OT network against the most prevalent attacks and malware families targeting critical assets. CISA CPGs recommend regular third-party validation of the effectiveness and coverage of an organization's cyber defenses.

Mandiant advises a tailored program to fit the assessment needs of the organization. A comprehensive testing program for OT is most effective when it is conducted from the attackers perspective, leverages simulation and emulation to alleviate impact to real-time operations, and incorporates an appropriate mix of red team, purple team, penetration testing and network and component security testing. Where proactive testing is not acceptable, due to the operational uptime requirements of production OT environments, Mandiant recommends technical assessments that evaluate the effectiveness of network segmentation, access controls, network monitoring systems, transient device policies, and incident response capabilities. Continuous testing not only evaluates the effectiveness of security controls at a point in time, but also helps to identify complex security issues across integrated networks (IT to OT) before an attacker exploits them. Ongoing validation can also prepare the organization's team to monitor, detect and respond to cyber incidents. From these programs organizations should expect: tactical recommendations for mitigation of critical findings, strategic recommendations for long-term improvement, and identification of gaps in the staff's ability to monitor and respond to OT incidents.

Open Platform Communications servers enable similar and manufacturer-independent data exchange among machines, devices and systems within the industrial environment.

Response and Recovery

In section 7, CISA CPGs outline the need for organizations to maintain, practice and update cyber security incident response plans for relevant threat scenarios. Mandiant's experience on the frontlines of response for high profile OT incidents, such as TRITON and INCONTROLLER and have led to a deeper understanding of the difference between IT and OT incident response and the tools and procedures required to carry out an OT response.

While the goals of remediation and containment (to remove the threat from the environment and restore systems to normal operational conditions) are the same in IT and OT environments, the tools can be vastly different. IT responders routinely use endpoint detection and response technology to aid in investigation, containment and recovery / remediation. These tools are not typically installed on servers or components of OT networks.

Containment in IT is relatively simple and often much less impactful than it can be in complex OT environments. For example, stopping and starting specific functions or even removing an entire system on the IT network is common practice. These actions can be more impactful when taken on an OT component. A comprehensive understanding of the underlying processes must be taken into account before starting or stopping processes or pulling a component offline without impacting operations which can cause significant downtime or potential risk of life safety. Open Platform Communication (OPC) servers, for example, can impact the entire manufacturing line for weeks if haphazardly taken offline. Detailed planning – outside of an active incident response – helps system owners make risk-based decisions based on potential downtime, production loss or life safety risks. The organization's ability to understand the goals and objectives of potential attackers can help guide the system owner into making safer, less risky decisions.

Lastly, OT networks are composed of many vendor-run subnetworks that the organization does not have direct access to. Mandiant recommends response plans and playbooks be developed to incorporate third-party systems and tested in conjunction with those vendors. The importance of having a plan, and practicing it, to resolve cyber security incidents quickly, efficiently, and at scale can not be overstated.

Mandiant maps OT security offerings to the NIST Cybersecurity Framework's Five Functions[18], which CISA CPGs are meant to supplement, matching services to the lifecycle of an organization's cyber security risk management.

[18] NIST, Cybersecurity Framework, The Five Functions, May 2021

		IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Intellligence	Intelligence Subscription	█	█	█		
	Dedicated Intelligence Analyst	█	█	█		
	Vulnerability Assessment Service	█	█			
	Custom Analysis and Blackbox Assessment	█				
Consulting	Healthcheck	▓	▓	▓		
	Security Program Assessment	▓	▓			
	Attack and Penetration Testing	▓	▓	▓		
	Incident Response Planning	▓			▓	▓
	Incident Response				▓	▓
	Security Training	▓	▓			
	Dedicated Consultant	▓	▓	▓	▓	▓
Managed Defense for OT	Jumpstart	▒	▒			
	Ongoing Monitoring		▒	▒	▒	
3rd Party Technology	OT Network Protocol Monitoring	░		░		

Figure 2. Mandiant OT-specific Offerings

Mandiant offers frontline cybersecurity insights with a deep functional knowledge of industrial control systems gained through decades of hands-on work in ICS and OT environments. Mandiant OT experts conduct advanced security testing to help industrial organizations improve mitigation and detection capabilities across end-to-end OT networks. Let us help your organization map CISA CPGs for a more secure OT environment and increased cyber readiness.

Closing Thoughts

This edition of The Defender's Advantage Cyber Snapshot instructs organizations who are charting their journey from traditional passwords and multi-factor authentication (MFA) through to implementing passwordless authentication to build off of strong MFA methods and to consider third-party single sign-on to help broker back-end authentication to all of your devices and applications. We provide tips to those navigating the volatile cyber insurance market suggesting they include counsel and risk management in preparing underwriting applications, carefully review the specimen policy and look to their insurance providers as a partner in overall risk management.

Additionally, we demonstrate how the six critical functions of cyber defense outlined in The Defender's Advantage align with the guidelines provided by the U.S. Cybersecurity and Infrastructure Agency (CISA) in their recent publication of Cross-Sector Cybersecurity Performance Goals (CPGs). These represent cybersecurity practices that critical infrastructure owners and operators can implement to meaningfully reduce risk. We also highlight a case study that exemplifies tactics deployed by an optimized SOC where analysts investigate relevant alerts as a cohesive investigation and rely on the analysts' training, experience, and critical thinking to investigate a supply chain attack.

Knowledge is one of our greatest advantages in the fight against cyber adversaries. The Defender's Advantage Cyber Snapshot is designed to provide just that—insights and intelligence that informs security teams and enables leaders to make smart decisions. The cyber security industry must share information and work together to help keep responders in the fight, and The Defender's Advantage Cyber Snapshot is just one way Mandiant supports the cause.

Learn more at www.mandiant.com

Mandiant

11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com