MANDIANT
NOW PART OF Google Cloud

Issue 5

Cyber Snapshot Report

Google Cloud

The Defender's Advantage Cyber Snapshot report provides insights into cyber defense topics of growing importance based on Mandiant frontline observations and real-world experiences.

Contents

Understand Why (and How) Attackers Bypass Your Application's Defenses 3

Case study setup 4

Unique application feature leads to vulnerability 5

Missing validation leads to potential breach 7

Selecting the right assessment 8

Proactive Cybersecurity: 6 Critical Tasks to Mitigate Risk 9

Understanding the attack surface 9

Ensure endpoint security solutions have near-full coverage 10

Restrict network-based protocols and services 11

Implement strong MFA methods 11

Enhance logging, monitoring, and detections 12

Enhance incident response strategy and processes 12

Strengthening Cyber Defense Through Intelligence-led Threat Hunting 13

Threat intelligence is the foundation for threat hunting 14

Six best practice characteristics of effective threat hunting 14

A powerful tool 15

The Evolving Insider Threat Landscape: Mindset, Opportunities, and Circumstances 16

Changing mindset 17

Changing opportunities 17

Changing circumstances 18

Adaptation 19

Maritime: A Supply Chain Target 20

Digital transformation effects on maritime cybersecurity 21

Maritime industry threat landscape 22

What to expect in the future 23

What organizations can do 23

Understand Why (and How) Attackers Bypass Your Application's Defenses

There is a constant mismatch between the types of security assessments organizations request versus the evaluations they actually need. For example, organizations frequently pursue unauthenticated web application assessments, with the belief of a cost-effective approach that will also provide comprehensive testing of their critical applications. However, the majority of web-based vulnerabilities are discovered within the application's complex inner-workings including its access control barriers, data control models, and tiered architecture, those of which an unauthenticated assessment does not include or have the capability to identify. Herein lies the need for a formal, comprehensive web application assessment, to establish a security baseline for the application from front to back.

Mandiant uses eight phases to review a web application from top to bottom:

1. Discovery
2. Configuration management
3. Authentication
4. Authorization
5. Session management
6. Data validation
7. Error handling
8. Data protection

This comprehensive evaluation is a fully authenticated engagement and, therefore, requires user account credentials at each major role level. If the application is multi-tenant, then multiple tenants should be provisioned for the assessment. While comprehensive assessments possess longer testing time, and more complexity to set up, they are exponentially more effective at securing web applications.

In this article, we'll walk through a recent client assessment performed by Mandiant to show its impact on the organization's risk profile and how a comprehensive assessment delivers more value than an unauthenticated version.

Case study setup

A retail organization asked Mandiant to perform an evaluation of their mission-critical digital marketing application that enabled management of their core web presence. Through the engagement scoping process, Mandiant determined an effective course of action was a comprehensive application assessment.

The client provisioned a multi-tenant testing environment, complete with user accounts for each major role in the digital marketing application. These two elements are crucial in order to perform rigorous authorization controls testing, such as:

- Vertical privilege escalation
- Horizontal privilege escalation
- Cross-tenant authorization controls
- Page-level authorization controls
- Feature-level authorization controls
- Data-level authorization controls

Mandiant performs assessments with an "application-first" approach, to understand the application in its original context, the way an average user would interact with it before attempting to find vulnerabilities.

From an unauthenticated, Internet-based perspective, this digital marketing application possessed a login form, a forgotten password flow (Figure 1), and a few static pages (i.e., contact us, privacy policy, etc.)—however there were no self-registration capabilities.

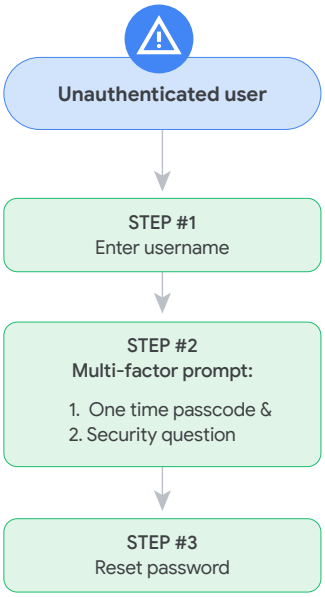


Figure 1. Forgotten password flow

Mandiant began authenticated testing as a standard user to explore the inner-workings of this application. Standard users possessed limited functionality—they could read values in the application, but did not have capabilities to create, update, or even delete data. The attack surface was very small, with data-level authorization controls seemingly locked down.

Mandiant took note of one application feature in particular where a standard user could create and delete data—internal messaging that enabled users to communicate with both support users and administrators. Typically, this was used to fix an application issue or request further access by allowing users to search for tenant and administrative support by their usernames and in turn send a message. Mandiant observed that the messaging endpoint translated the usernames into a secure, globally unique identifier (GUID), to ensure the destination usernames were not transmitted in cleartext.

Unique application feature leads to vulnerability

As Mandiant continued with the engagement, our experts noted that the messaging endpoint was unique in nature by using the previously mentioned GUIDs to reference its users. Whereas the other application features referenced its users by their usernames, the messaging endpoint did not. Typically, development teams seek consistency in their feature design patterns, therefore this inconsistency in the reference pattern indicated an unusual occurrence connected to the related GUIDs. As a result, Mandiant consultants turned to their Burp Suite's proxy history to search one of the returned GUIDs and discovered the forgotten password for the messaging endpoint utilized the same GUIDs, as shown in Figure 2.

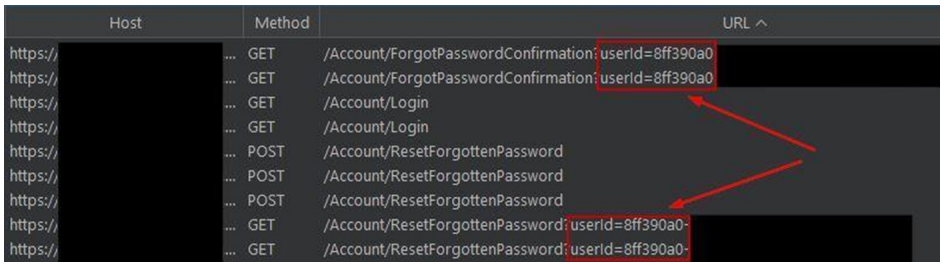


Figure 2. Proxy history

During the forgotten password process, as seen in Figure 1, the user must first enter a username. If an attacker can identify a valid username, the next step is to answer the MFA challenge, which translates the username into a GUID (Figure 3). The final step, in which the password is changed, uses the GUID to update the user's password (Figure 4). In summary, if an attacker can find a user's GUID, their ability to change a user's password significantly increases (Figure 5).

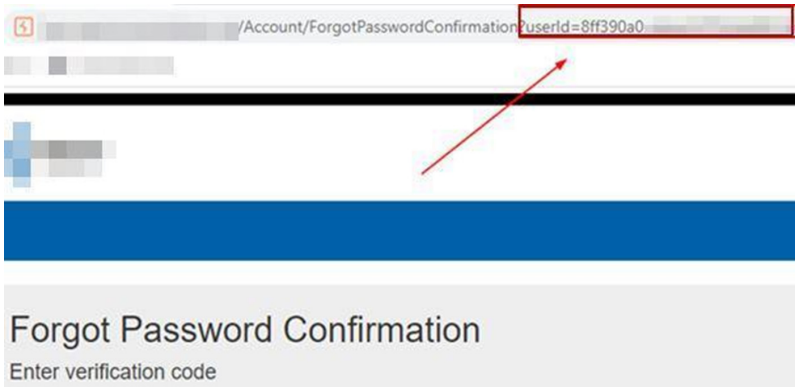


Figure 3. MFA challenge discloses user GUID

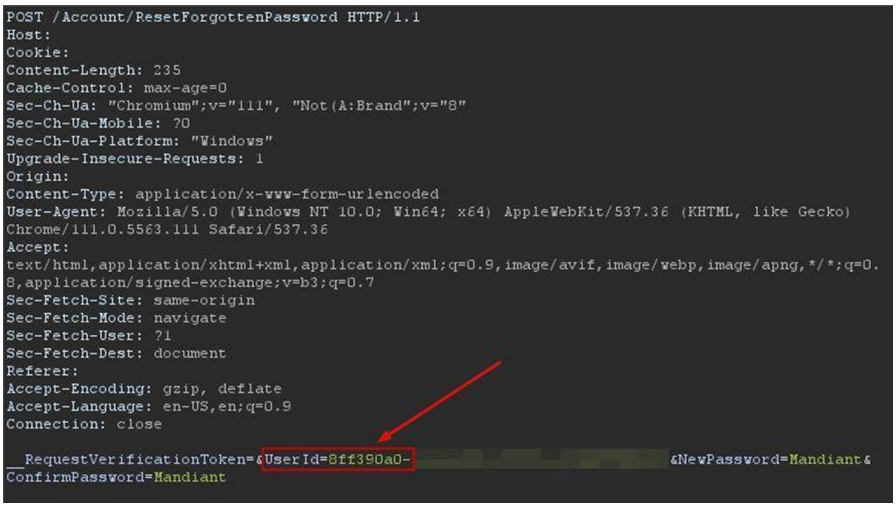


Figure 4. Password change uses GUID

Looking closer at the forgotten password process, Mandiant consultants found additional issues related to a misconfiguration that left the forgotten password process stateless. The application server had no mechanism to enforce a strict flow through the three-step process, enabling Mandiant consultants to skip the MFA challenge entirely. This also resulted in the three-step forgotten password process being reduced to only one-step (Figure 5)—if a user's GUID was identified, their password could be changed.

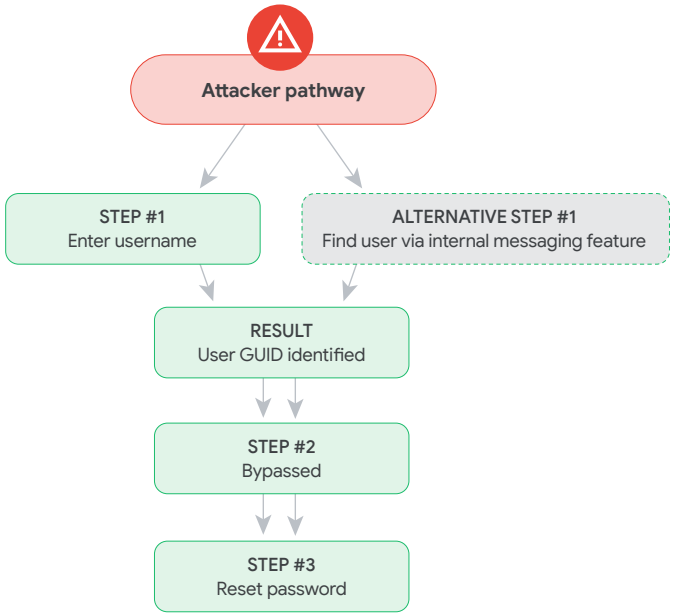


Figure 5. Attacker pathway to reset password

Ultimately, Mandiant identified an attack path allowing for the compromise of every user account in the application, but this was only possible in the time allotted because user accounts were provisioned to examine the application's full functionality and features. Without a comprehensive application assessment, this critical vulnerability would have taken longer to find or would have been likely missed altogether through a different assessment type.

Missing validation leads to potential breach

Leveraging this vulnerability, Mandiant compromised a super administrator's account (with the client's permission). The organization did not provision a super administrator account for the assessment, but to demonstrate the full impact of the attack path, they agreed for Mandiant to continue the attack within a testing environment. Mandiant examined the features to which the super administrator had access.

The super administrator possessed access to a feature that allowed a new single-sign-on (SSO) connector to be defined for the digital marketing application. To establish this connector, the super administrator was required to upload a Java ARchive (JAR) file that contained details of the connector. Mandiant consultants downloaded the JAR file, inspected its contents, and in turn noticed the application server did not perform validation of the uploaded file.

After a few adjustments to the JAR connector code, Mandiant successfully ran system-level commands on the underlying system—achieving remote code execution.

Effectively, this attack-chain demonstrated that an unauthenticated, Internet-based attacker could compromise any user in this mission-critical application, gain access to a super administrator's console, and breach the organization's cyber defenses through a remote code execution exploit.

Selecting the right assessment

Web applications have several safeguards in today's modern landscape:

- Firewalls
- Secure code delivery and review of third-party libraries
- Bug bounty communities looking for vulnerabilities
- AI-powered programming assistants

Many of these safeguards are designed to compensate for the deficiencies found in an application's code. If an attacker is able to breach the cyber defenses, then the application is ripe for abuse.

This threat is not only applicable to traditional applications, commonly known as Web2. Next generation applications, also known as Web3, like smart contracts, decentralized applications, and applications leveraging AI, are also susceptible to application-layer attacks. Authentication, authorization, data validation, and sensitive data protection categories are not relegated to one particular technology or application language, instead, they transcend the boundaries of technological generations. The recommended assessment employed to properly evaluate these applications must take into account the holistic view of technical and logical controls, not simply the singular view offered by an unauthenticated assessment.

Unauthenticated assessments are but one arrow in a quiver of assessment options. If an organization has never performed a web assessment of their application before, Mandiant highly recommends beginning with a comprehensive assessment to establish a baseline of the application's security posture. From there, the client can pursue more iterative web assessments that focus on new features, developments, or coding improvements, with a comprehensive assessment performed for major version releases.

Ultimately, when selecting the right assessment to fit your overall objective, it's crucial to consider the true cost of a breach to that application and how it will impact the organization, its users, and its data.

Proactive Cybersecurity: 6 Critical Tasks to Mitigate Risk

The summer of 2023 was dubbed by the cybersecurity community as the "hot zero-day summer," not only based on the sheer number of vulnerabilities found by both ethical security researchers and threat actors, but also due to the widespread exploitation of significant vulnerabilities throughout the season.

Through Mandiant's extensive experience responding to some of the world's most impactful cyber threats–including zero-day threats—we have compiled a list of critical tasks that organizations can implement to help mitigate the impact of the next widespread cybersecurity event.

These recommendations are not exhaustive, and should not be implemented in a sequential or linear fashion. Instead, organizations should prioritize security initiatives based on the type of risk, level of effort required, and capabilities of their security team.

1. Understanding the attack surface of an organization

One of the primary tasks for an organization to mitigate risk is taking inventory of the public-facing assets that form its external attack surface. Once an inventory has been collected, the organization should perform daily vulnerability scanning and thorough configuration review of these assets to reduce vulnerabilities and misconfigurations that are likely to be exploited by threat actors.

Automated solutions for external attack surface management can aid in the discovery and evaluation of their internet-facing assets and cloud resources, as well as help identify vulnerabilities and misconfigurations.

2. Ensure endpoint security solutions have near-full coverage across an organization

An important goal for organizations is to strive for near-full coverage of endpoint detection solutions. Endpoint security tools monitor systems for suspicious activity, malware families, backdoors, and commodity-based threats—and send alerts once these threats are identified. Another key feature of an endpoint security solution is the ability to isolate a system from the environment and allow for live response forensics when a threat is detected. It is vital for organizations to review the deployment of endpoint security tools, most notably on external or public-facing systems.

Mandiant recommends documenting specific aspects of endpoint security tool deployment, including:

- Deployment scope: Identify which devices the tools are deployed to. Ensure there are no visibility gaps based on the operating system type (e.g., ChromeOS, Linux, Unix, etc.)
- Software version: Know what version of the software is installed.
- Deployment mechanism: Understand how the tools were deployed and if the deployment requires manual intervention on particular systems.
- Signature/Indicators of Compromise (IOCs) update frequency: Familiarize yourself with how often the tools are updated with new signatures and IOCs.
- Administrative access and configuration: Document who has access to the tools and how they are configured.
- Configuration and alerting mechanisms for identified malware infections and detections: Realize how malware infections and detections are configured and alerted on. Learn if the alerts generate an internal chat or email notification.
- Detection settings: Be aware of the tools configured for detection and the types of alerts generated by the tool to the organization's SIEM/SOAR.
- Visibility and notification channels for high-fidelity alerts: Know which visibility and notification channels exist for high-fidelity alerts.

Organizations should also be able to identify and mitigate the following:

- Systems without the endpoint solution: Realize which systems do not have the endpoint security solution installed.
- Disabled endpoint agent services: Identify which endpoint agent services have been shut down or disabled.
- Improperly configured endpoint solutions: Understand which endpoint security solutions are not configured to properly remove or block threats.

By documenting all aspects of endpoint security tool deployment, organizations can remediate gaps and continue monitoring their endpoint security to ultimately improve threat visibility and response.

3. Restrict network-based protocols and services for external facing systems

To reduce exposure and limit the attack surface, organizations should restrict network-based protocols and services for external facing systems. Mandiant recommends limiting the number of ports and protocols to only those essential and necessary for the system or application. Organizations should also place the system or application behind a Layer-7 firewall or a Web Application Firewall (WAF), which can offer protection against web-based threats and DDoS attacks.

Further, organizations should isolate and segment external facing systems from the main corporate network. A deny-list approach should be adopted for unnecessary east-west communication originating from these systems. Special attention should be given to blocking common ports (e.g., RDP, SSH, SMB, WMI, etc.) and services that attackers could use to laterally move from the external system to the corporate network.

4. Implement strong MFA methods across all external facing systems

Not all user or system accounts are created equal, and the same goes for multi-factor authentication (MFA) methods. MFA has long been considered the strongest way to protect identities, and it still is. However, as organizational defenses have strengthened, threat actor techniques for compromising identities have also adapted.

Mandiant has investigated numerous attacks of which the threat actor compromised a weaker MFA method, such as SMS text, voice calls, or push notifications via an authenticator application. Both SMS and voice calls are unencrypted, putting them at high risk for being intercepted. It is also possible to maliciously transfer a phone number to an attacker's SIM, allowing them to receive legitimate authentication requests, as we have seen with UNC3944.

If the organization prefers to maintain push notifications as its form of MFA, Mandiant recommends for the authentication platform to provide additional contextual information about the MFA request, to help inform the approval or denial decision. Some examples of additional contextual information include, but are not limited to:

- Show the application name requesting the MFA
- Feature the geographical location where the request originated from
- Require number matching on the authentication application to validate the request

Mandiant recommends enforcing an even stronger form of MFA authentication for all user accounts, especially privileged accounts, such as hardware tokens or FIDO2 Security Keys. Additional security considerations for privileged accounts is to require the privileged user to input MFA verification for each session, regardless if the request is coming from a trusted location or corporate VPN.

To learn more about the deployment and management of MFA solutions, review the following white papers by Mandiant:

- The Journey to Passwordless Authentication
- 6 Tips for Implementing Privileged Asset Management

5. Enhance logging, monitoring, and detections on external facing systems

Organizations should enhance logging and detection capabilities on external facing systems and cloud resources. For applications or systems that support transaction-level or object-level logging, it should be activated for all critical and public resources.

Centralizing all logs should be a priority, most notably for external facing systems. For organizations with hybrid environments (on-premises and cloud-based resources), all logs should be centrally managed and correlated to track user activity across that environment.

6. Enhance incident response strategy and processes

To support an organization's cyber defense and risk management program, it is natural to begin with operational capabilities. By understanding and aligning the most important systems and data (e.g., crown jewels) with incident response plans, playbooks, and governance documentation, organizations are better positioned to respond to incidents rapidly and effectively.

Organizations must have a clear and well-defined cybersecurity strategy that follows industry best practice. This strategy should empower the identification, evaluation, and remediation of security threats effectively. These capabilities should also include channels for transparent and effective reporting of cyber risk metrics and measurements to relevant executives and business stakeholders, including those that may have financial, operational, or reputational repercussions. Lastly, it is vital to regularly review and update the security response strategies to ensure their effectiveness against the current and evolving threat landscape.

In an ever-changing world where cybersecurity threats continue to grow, staying proactive remains crucial. The 2023 “hot zero-day summer” serves as a potent reminder of the constant vigilance needed in today's cyber threat landscape. Mandiant's insights and recommendations aim to empower organizations with the knowledge and tools they need to navigate these challenging times.

Strengthening Cyber Defense Through Intelligence-led Threat Hunting

As threat actors continue to alter their techniques while blending in with the noise of routine IT operations, proactive threat hunting is becoming more than a nice-to-have capability for most security operations teams. Over the past year, Mandiant has tracked state-based threat actors who are steadily evolving their tactics to become more agile, stealthy, and complex.

The volume and velocity of security data generated by organizations continues to mount, making it challenging for many security operations teams to comb through in hopes of identifying suspicious behavior. In fact, most organizations were notified of breaches by external entities in 63% of incidents, an increase from previous years, according to Mandiant's 2023 M-Trends Report.

Threat hunting teams that leverage threat intelligence and the experience of skilled security professionals to develop and test hypotheses for tracking previously unknown malicious activity, can not only aid security teams in finding hidden attackers, but can also help:

- Identify and investigate known suspicious activity that may indicate a data breach or other security incident,
- Reduce the cost of a historical or ongoing data breach by uncovering the incidents and responding to them more quickly, and
- Improve the overall security posture of an organization by increasing understanding of the operating environment and baseline knowledge of "good" behavior to make detection of anomalies more apparent.

Threat intelligence is the foundation for threat hunting

The objective of threat hunting is not searching for Indicators of Compromise (IOCs). By definition, IOCs are known. When looking for the unknown, threat hunt teams develop hypotheses guided by internal and external cyber threat intelligence, combined with knowledge of an organization's environment and critical assets. Threat hunters look at a wider aperture of information, such as how a specific attack plays into known advanced persistent threats (APTs) and uncategorized group clusters (UNCs), so they can hunt for raw indicators and other activity from the attack group.

For example, APT29, the Russia-based espionage group, uses phishing techniques to conduct its operations, according to Google TAG and Mandiant threat intelligence teams. In many cases, this threat actor will compromise websites to later distribute malicious payloads in ZIP/ISO format, which contain the payloads necessary for the intrusion to continue. Detecting both the download of ZIP/ISO files and their manipulation, is an effective step used by threat hunters to analyze the initial phases of infection carried out by this group.

Intelligence is crucial to the success of a threat hunting program because it offers enhanced awareness of evolving threats, helps prioritize responses, provides context for IOCs, enables proactive detection and customized rules, supports incident response, facilitates continuous learning, encourages collaboration, reduces risks, and ultimately leads to cost-effective cybersecurity. Intelligence equips threat hunters with the knowledge and tools needed to stay ahead of cyber threats in a complex digital landscape, enhancing overall security.

Six best practice characteristics of effective threat hunting

Aggregated threat intelligence: Hunt teams need a hub for threat intelligence that aggregates data from various sources, including antivirus vendors, cybersecurity researchers, and user contributions. Aggregating a wealth of information allows threat hunters to access up-to-date IOCs, malware signatures, and behavioral patterns—making it easier to identify and track threats.

Historical data analysis: To hone their hypothesis, hunters need current and historical intelligence data. They can access past scan results for files, URLs, IPs, and domains that will enable retroactive threat analysis. This capability is invaluable for understanding the evolution of a threat, tracking its origins, and identifying changing patterns of attack over time.

Contextual information: Hunt teams need contextual information regarding detected threats, such as file metadata, domain information, and behavioral analysis. This helps threat hunters better understand the nature and impact of a threat, ultimately assisting in the development of effective mitigation strategies.

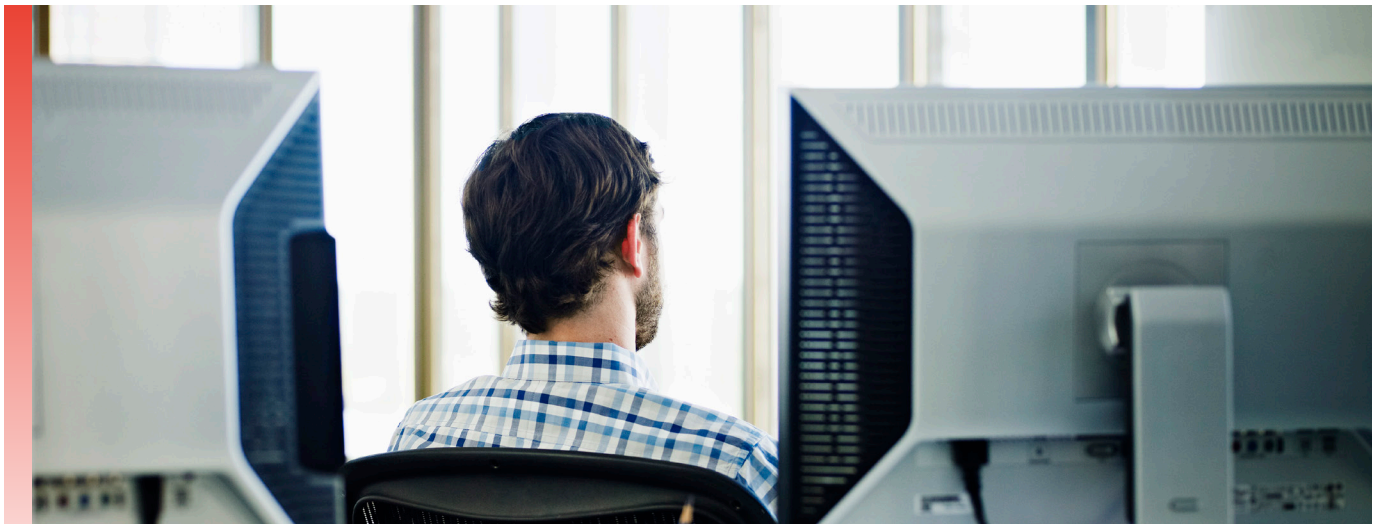
Custom YARA rules: For advanced threat hunters, cyber threat intelligence platforms support the use of custom YARA rules. This feature enables users to create and upload their own rules for detecting specific threat patterns, resulting in enhanced platform flexibility and adaptability.

Internal testing: Just as MITRE evaluations are known in the cybersecurity industry for vendors to check whether their products have visibility and capability to detect real APT attacks, many organizations carry out the same internal tests to verify that their products comply with desired requirements, including a trained threat hunting team that can respond to a future incident.

Managing false positives: Detection engineers also play a fundamental role in threat hunting. Many times threat hunters need detections to begin a hunt investigation, and the results of a threat hunting mission should be used for future detection improvement. However, false positives play a big role. Effectively managing and minimizing false positives is crucial in threat hunting because it allows threat hunters to create accurate and efficient detection rules. This ensures their efforts are focused on genuine threats, in turn saving precious time and security operations resources.

A powerful tool

Threat hunters require powerful tools to stay ahead of malicious actors. Cyber threat intelligence platforms offer a comprehensive set of features and benefits that make it an indispensable asset for threat hunting. By providing access to evolving adversary behaviors and motives, historical data, and collaborative capabilities, threat intelligence empowers cybersecurity professionals to identify, analyze, and mitigate threats effectively—ultimately bolstering the security posture of organizations and individuals alike.



The Evolving Insider Threat Landscape: Mindset, Opportunities, and Circumstances

Successful cyber attacks are often conducted through an organization's employees or insiders. With authenticated access, insiders have intimate knowledge of the organization, including the people, processes, and technologies applied. Mandiant has observed a shift in the motivations and behaviors of insider threats. This shift is occurring across all sectors, industries, and geographic regions. This latest iteration of insider emerges as a chameleon, marked by their adaptability and unpredictability. Additionally, operations have evolved from directly stealing data to potentially monetizing access by selling credentials to third parties. Outsourcing to a third party adds layers of obfuscation, ultimately complicating detection. In some cases, insiders may not even need direct access to critical information. Instead, they might simply become conduits, executing scripts or deploying malware at the behest of external threat actors.

Adding to this complexity, the modern insider threat is technologically agile. With multiple devices at the fingertips of insiders, each potentially offering entry and exit points to organizational networks, tracking malicious insider activities can seem near impossible. The sheer volume of data and routine authorized actions conducted daily, can drown out illicit activities, rendering them nearly indistinguishable amidst the flood of alerts.

Therefore, to enhance an organization's cyber defense against the latest insider threats, it's crucial to have a deeper understanding of the evolution and current mindset of insider threats. For a more precise understanding, Mandiant categorizes this transformation into three essential arenas: changing mindset, changing opportunities, and changing circumstances.

Changing mindset

Changing mindset refers to the motivations and intentions of insiders. Motivations refer to why an insider takes a specific action and the intentions of an insider refer to the outcome that the insider seeks to achieve.

Robert Hanssen epitomized the “old insider threat mindset.” Fueled by narcissism and greed, the old insider threat’s main drive was self-importance, while their intention was to trade secrets for personal validation and money. In corporate settings, economic espionage was about bartering information for advancement opportunities (a new position, new company, etc.) and economic gains. This mindset was characterized by selling information for personal gain (money and validation).

Edward Snowden introduced the world to the "leaker mindset” and the "public good ideology." This shift is noteworthy, as it underscores a change from *selling* information to *disclosing* information publicly and seeking widespread validation. Although narcissism and financial gain might occasionally factor in, the primary motivation for these individuals is ideology. Leakers prioritize the "greater good" over organizational loyalty. While their declared aim might be to address perceived injustices, many often strive for self-aggrandizement.

Enter the "enabler." Surpassing the dichotomies of narcissism and idealism, their primary drive is greed. For them, access is the new currency, not the information it might unlock. This evolution marks a shift from selling information for self-importance to selling access solely for financial gain. This is a primary difference between the narcissist and idealist in that former focus on the information itself as the valued item. In the case of the enabler, the access itself is the value that is traded.

Changing opportunities

Opportunities refer to the ways and means available for insiders to collaborate or communicate with outsiders to execute their harmful insider threat actions (leaking to the media, transferring IP to a competitor, selling access to a foreign power or criminal enterprise). Ways and means can be further understood in the context of solicitation and acceptance of that information.

Historically, both solicitation and acceptance by third-party outsiders was covert. The modus operandi for insiders to collaborate with outsiders traditionally required secretive, "cloak and dagger" techniques. Physical meetings, like covert garage rendezvous with reporters, involved considerable risk due to direct interactions and the tangible exchange of assets.

Tactics, Techniques, and Procedures

Dark web ecosystem: The dark web has become a hotbed for illicit activities. Within its encrypted confines, a thriving ecosystem exists, linking potential insiders with nefarious entities. Specialized forums and chat rooms are dedicated to discussions, tactics, and strategies related to insider threats, enabling smooth solicitation.

Targeted recruitment: Specific entities are dedicated to headhunting potential insiders based on their roles, access privileges, and even vulnerabilities, like financial distress or dissatisfaction. Using psychological profiling, they identify individuals who can be swayed and then approach them with tailored propositions.

Advertisement platforms: Think of this as the "Craigslist" of the dark web, where insiders anonymously post about their access levels, the type of data they can extract, or the systems they can compromise. These platforms are equipped with a reputation system, allowing buyers to rate insiders based on the success of their past "transactions". This not only lends credibility to the sellers but also gives prospective buyers a sense of security.

Cryptocurrency payments:
The widespread acceptance of cryptocurrencies has made financial transactions more clandestine. Insiders usually demand payments in cryptocurrencies like Bitcoin or Monero to ensure their activities remain untraceable. This method further emboldens them, knowing that their financial footprints are concealed.

Platforms like WikiLeaks and SecureDrop heralded an era of overt solicitation and acceptance. This was marked by a more impersonal communication between the insider and outsider, as well as dedicated channels, using internet portals to upload digital assets. This lowered the risk for the insider, but still required exchanging information. The watershed moment occurred when mainstream publications began detailing methods on how to leak sensitive information without detection, signaling a changed environment.

Mandiant has observed that insider threats are now moving into the targeted recruiting and advertising phase. The landscape is now riddled with criminal enterprises specifically recruiting insiders or "innies" as they're called on dark web platforms. In fact, the targeted recruitment and number of insiders advertising their access and their willingness to sell that access—has increased 300% in the last 12 months. These transactions, often executed on the dark web, prioritize selling access over information. This threat is marked by the ever-increasing anonymous and highly secure dark web channels that offer greater anonymity, lower risk, and don't require the exchange of information, since what is being sold is access. Moreover, the insider may not have elevated access, but offers their general access to the network for running a script that allows an external attacker to gain access.

Changing circumstances

Circumstances refer to the workplace conditions pertaining to how insiders are granted access, and create, use, and interact with organizational assets.

Given the remote work shift notwithstanding, organizations continue to grant excessive access. Astonishingly, half of all employees possess access beyond their job's requirement, with a significant portion of them retaining access even after leaving the organization.

The proliferation of personal devices, cloud storage, and unmanaged corporate devices has provided insiders with multiple gateways into an organization's environment. The blend of remote work, combined with complex hybrid cloud environments, means sensitive data traverses various platforms and devices, perpetually at risk.

Tactics, Techniques, and Procedures (continued)

Bespoke malware: Sometimes, external attackers provide insiders with customized malware or tools to aid in their endeavors. These are designed based on the specific systems the organization uses. Once the insider deploys them, they can bypass security measures, siphon data, or even create backdoors for future access.

Escrow services: To build trust between insiders and their "clients", certain dark web platforms offer escrow services. The buyer deposits the agreed-upon amount into an escrow account. Once the insider delivers the promised access or information, the funds are released. This mechanism ensures neither party can easily scam the other.

Training and guidance: Some sophisticated entities go the extra mile by providing potential insiders with tutorials, guidance, and even real-time support to execute their operations. This could range from simple advice on how to avoid raising suspicions to step-by-step instructions on deploying tools or extracting data.

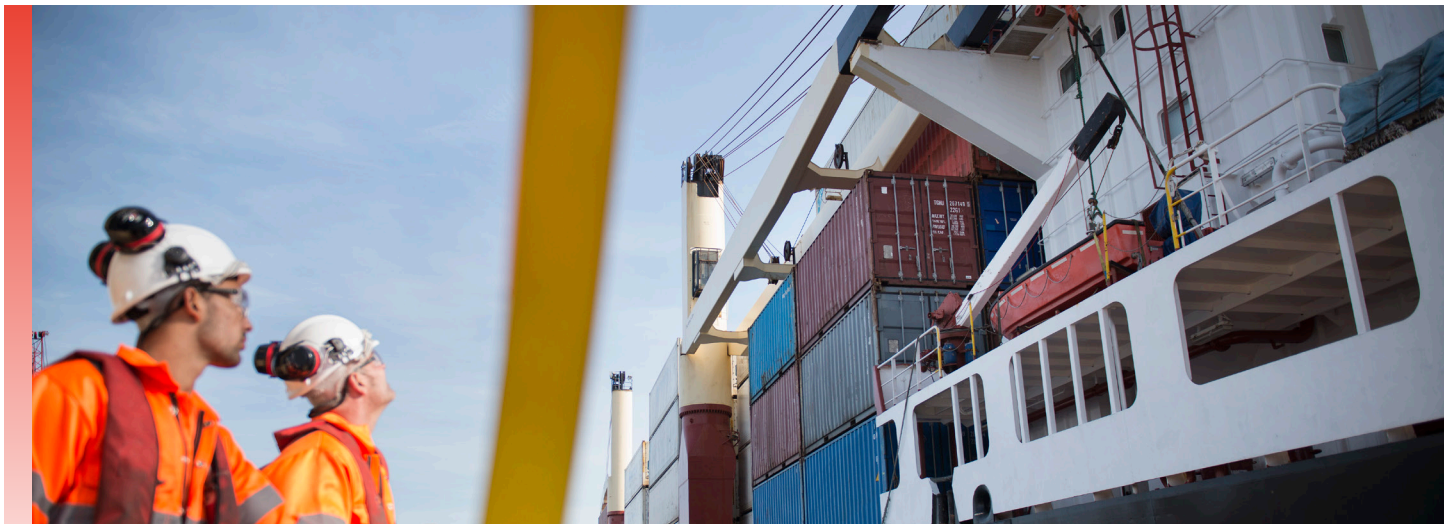
Evolving tactics: It's not solely about selling existing access anymore. Some insiders now collaborate with external hackers to intentionally escalate their privileges within the organization. They exploit vulnerabilities to gain deeper access, which can then be sold at a premium.

Organizations also struggle to maintain oversight across insider interactions. Monitoring device logs is progressing, but a comprehensive analysis of insiders' behavioral dynamics remains a daunting challenge due to the volume and disparate nature of the information. This information can be digital (structured and unstructured), personnel (HR data), and physical (access logs). This information is most often the domain of multiple functions across an organization, with different systems and data requirements—all which make aggregating and analyzing this information a complex task.

Organizations often lack a basic framework, specifically to manage insider risks. A formal insider risk management program focused on aligning cross-functional components, will provide the necessary framework for managing insider risk. With the continuous evolution of insider tactics, traditional safety nets are proving insufficient and in turn formal insider risk programs are required.

Adaptation

Insider threats, with their shifting motives, increased opportunities, and evolving circumstances, present a multi-faceted challenge. Addressing these challenges requires a holistic approach that encompasses advanced technology, revised organizational policies, and continual vigilance. In summary, the modern-day landscape of insider threats has become a web of advanced tactics, specialized platforms, and sophisticated strategies that organizations must take into consideration when adapting their insider risk programs for effectiveness and success.



Maritime: A Supply Chain Target

In today's interconnected world, global economies are heavily reliant on a functioning supply chain. A predictable and reliable maritime transportation system is essential for supporting modern just-in-time production strategies. Even a slight disruption to this ecosystem can have a cascading effect, impacting a wide range of industries that depend on maritime trade operating as planned, making this sector a prime target for threat actors.

This year, a staggering 14% of the maritime industry has reported paying ransomware operators to unlock critical systems. While ransomware-related threat activity is not new to this sector, the sharp increase in payments is a clear indication that both espionage and criminal groups are keenly aware of the importance of the maritime industry to not only individual nations or regions, but also the global supply chain as a whole.

Mandiant has observed a range of threat actor activity from nation-state and financially motivated groups targeted at the maritime industry. Mandiant estimates the potential for widespread disruption in the event of a successful breach is significant. Given the critical role that maritime transportation plays in the global economy, it is essential for organizations in this sector to take steps to mitigate the risk of an attack.

Digital transformation effects on maritime cybersecurity

Heightened cyber threats come at a time when the maritime industry is undergoing a digital transformation driven by the need for ever-greater efficiency and optimization. The move to digitalization is expanding the threat surface for the entire maritime ecosystem, and includes key systems such as:

- Chart digitalization
- OEM access to onboard systems (maintenance and monitoring solutions)
- Crew/guest internet (welfare) access
- Integrated bridge systems
- Integrated platform systems
- Digital cargo management systems
- Systems supporting perishable goods (refrigeration)
- Ballast water management systems
- Port movement systems
- Integrated tugs
- Shoreside IT support (includes full remote access)

As the digital transformation accelerates, there remains massive challenges around legacy systems, visibility into operational systems, and identification of assets. This can make it difficult for security teams to identify relevant vulnerabilities and track how they apply to a range of often different onboard/port environments.

Cybersecurity within the maritime industry is significantly underfunded—particularly when budgets are competing against other areas such as on-board safety issues, crew wages and condition demands. Though there have been a number of maritime breaches and cyber incidents, cyber is still a relatively new risk element for this industry and possesses larger liability risk during wide-scale economic impact events. For this reason, insurance companies have been wary and slow to offer ample policies, stating they do not have sufficient data to map the risks of breaches and cyber incidents. Cyber insurance policies that do exist often refuse to define the terms of coverage clearly, containing ambiguous provisions around key terms like "maliciousness" and excluding "war risks," while typical insurance policies, like Hull & Machinery policies, are now explicitly excluding risks related to cybersecurity.

Maritime industry threat landscape

Espionage and nation-state threats

Nation-state-aligned threat actors have recognized the significance of the maritime domain as a target that can yield both economic and military effects. Ports, particularly in the West, are often effectively shared spaces between private industries and military facilities. As the dynamics of geopolitics change around the world, the maritime ecosystem remains a vulnerable target to highly capable nation-aligned or nation-state threat actors.

Mandiant has observed information that Iranian-linked threat actors have demonstrated an interest in a variety of onboard ship systems, including satellite communications systems and ballast management systems. While this information does not suggest successful targeting of these systems, it does demonstrate a specific interest at a high level.

Nation-state actors have also used electronic warfare capabilities to impact maritime services. This has included the jamming of global positioning services (GPS) in specific geographical areas. The targeting of positioning services can impact a bridge crew's ability to safely navigate. With the reliance on electronic charts and smaller crew sizes, there is an increased risk to safe navigation.

The use of maritime services to push information operations has also been a tactic by nation-state adversaries. This has included the spoofing of services such as AIS. While this type of activity is easily disproved with open-source data, it demonstrates a willingness to manipulate the service and data when needed.

The maritime sector is a critical infrastructure that is essential to the global economy and military operations. Nation-state-aligned threat actors are aware of the significance of this sector and are actively targeting it. Maritime organizations must be aware of the threats posed by these actors and take steps to mitigate the risk of cyber attacks.

Financially motivated threat actors

Financially motivated criminal actors have targeted various elements of the maritime sector, including major ports, shoreside support services, and ferry operators. These attacks often result in media attention and disrupt local economies. Criminals steal sensitive data and extort victims, and target port cargo management systems to facilitate illegal activities.

Ransomware actors have also targeted shoreside infrastructure, disrupting shipping operations. This has included attacks on large cargo ports and smaller inland ports. In some cases, port management has declared "force majeure," forcing vessels to find alternative ports.

The NotPetya attack of 2017 is a prime example of the potential impact of nation-state cyber attacks on the maritime sector. The attack, which was linked to a unit within the Russian military intelligence apparatus (GRU), resulted in billions of pounds of costs to victims and had a wide-scale economic impact around the world. This included major shipping organizations, which were unable to process containers and other goods at just-in-time speeds.

When targeting ports, attackers often target specific systems that have a significant impact on operations. One such system is the terminal operating system (TOS), which manages a range of subsystems within the port, including cranes, cargo storage, and onward movement or processing. Denying access to this system severely impacts the ability to control and operate port terminal operations.

Other shoreside entities targeted have included maritime-specific services, such as IT or communications support and software-as-a-service (SaaS) organizations that provide electronic charts. The targeting of these organizations has an operational impact on vessels, forcing operators to move to alternative services or operating methodologies.

What to expect in the future

The maritime industry will likely continue to be targeted by a range of threat actors with differing objectives. Targets will likely span the entire industry, including owners, operators, charterers, insurers, ports, and onward supply chain organizations. The complex owner-operator-insurer model complicates response and investigation activities, potentially hindering timely response to a cyber incident.

A cyber event affecting the maritime industry could have a direct and serious impact on global trade. As geopolitical tensions rise, and the vulnerabilities of the maritime ecosystem remain, the industry becomes increasingly vulnerable. Such an event would significantly test the resilience of global trade and the levels to which nations can cooperate, particularly those reliant on chokepoints, transit routes, and key ports.

An increased number of threat actors may become maritime-aware. As this awareness increases, attacks will likely become harder to detect and more impactful. The maritime industry must be aware of the evolving threat landscape and take steps to mitigate the risk of cyber attacks.

What organizations can do

There are many white papers and guidance-related documentation available advising maritime organizations on the basics of establishing a relevant cyber security program (often associated with the 2021 IMO regulation on cyber security risk management). Below are some areas of focus that often prove particularly effective:

- **Improve access to and understanding of threat intelligence:** The industry as a whole needs to significantly uplift threat intelligence capabilities. Without knowing threats likely to target an organization, it is very difficult to appropriately position cyber defense.
- **Intelligence-led risk management:** By understanding the specifics around threats posed to an environment, an organization can tailor risk management. This includes activities such as the prioritization of patching based on known threat actor TTPs vs systems in use, and prioritization in terms of investment/headcount/technology uplift.
- **Threat modeling:** By identifying business/operationally critical systems, compensating controls and then mapping these against threat actor TTPs, organizations can identify gaps in capability and defense in depth. This can then be documented both visually and in written technical detail for a variety of audiences.

- **Third party/vendor management:** As described above, the threat to the industry (as with many industries) from the range of suppliers is vast and has the potential to be highly impactful. Best efforts to mitigate this risk should be focused around third party/vendor management. It's important to ensure appropriate contractual language is in place, as proactive security assessments play a role in the procurement process and ongoing documentation to help monitor accounts and provide connectivity.
- **Response planning:** Development of a cyber incident response plan is key. This should detail the types of attacks likely to be faced, roles and responsibilities (including delegated authority to act), and details on communications plans and associated escalation responsibilities.
- **Business continuity:** Maritime organizations have systems and plans dedicated to safety and other critical controls. A similar effort should be made with regards to business continuity associated with cyber incidents. Examples include:
  - Ensuring that there are sufficient skills and materials in place to adopt the use of paper charts and handheld navigation aids if there is an incident.
  - Validating that both the ship and port maintain operational secondary communications systems if primary systems are taken offline, including ensuring an out-of-band communications system is available for responders to use if primary systems become compromised.
- **Exercise:** Organizations should conduct cyber incident-based exercises. Using realistic threat-driven scenarios allows for the testing of existing plans and processes. This should cover incidents that impact both corporate environments and also OT/ICS environments onboard and in port facilities.
- **Industry sharing:** Pan-industry information and intelligence sharing should be improved. While maritime focused ISACs exist, the level of intelligence sharing does not match that of other industries. The sharing of information and intelligence across the industry is a highly effective way of mitigating incidents that may spread, impacting multiple organizations.