MANDIANT

The Defender's Advantage Cyber Snapshot

The Defender's Advantage Cyber Snapshot offers insights into cyber defense topics of growing importance based on Mandiant frontline observations and real-world experiences. Topics in this issue include how the attackers see organizations, threats to operational technology, mergers and acquisitions, and major event protection.

Detecting Common Exploit Paths Exposed on the Internet

Data Source

The issue data referenced is directly sourced from Mandiant Advantage Attack Surface Management, spanning 21,092 customer Collections. The data set includes 21,392 issues identified from January 1, 2022, to March 31, 2022, with high or critical severity. Issues are a subset of customer Collections, which contain the asset inventory and associated technologies running on external attack surfaces. Issue severity is assigned based on the potential impact to the affected system. In situations where a CVE is identified, the severity is tied to the Risk Rating from Mandiant Advantage Threat Intelligence.

An issue is a finding discovered on an external asset that warrants further investigation.

From January 1, 2022, to March 31, 2022, Mandiant identified common high and critical severity issues that occurred in medium to large enterprises due to unpatched technologies and configuration drift in internet-facing assets. For these issues, Mandiant highly recommends that security teams establish a process to identify occurrences in their own organization and follow recommended remediation strategies.

High to Critical Issue Categories

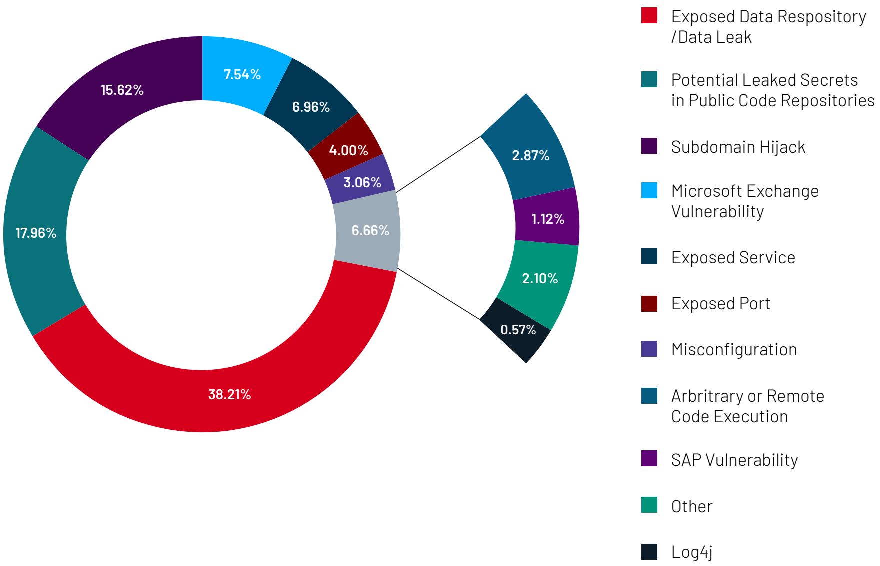


Figure 1. All high to critical-severity issue categories by observed by Mandiant Advantage Attack Surface Management (January 1, 2022 to March 31, 2022).

Issues include vulnerabilities, misconfigurations, indicators of compromise (IOCs) or a data leak of any sort. Mandiant Advantage Attack Surface Management was used to perform reconnaissance in the same manner as an attacker would, scoping internet-facing assets and technologies and scanning Open Source Intelligence (OSINT) sources for areas of weakness to uncover potential paths a threat actor could take to exploit an exposed asset.

Top 5 Issues

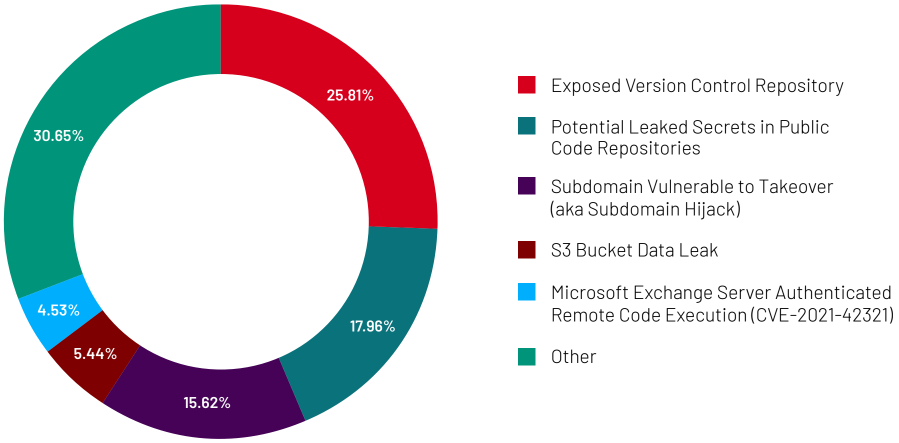


Figure 2. Top five issues observed by Mandiant Advantage Attack Surface Management (January 1, 2022 to March 31, 2022).

Exposed Data Repositories and Data Leaks

Any organization could be impacted by an exposed data repository due to misconfigurations or poor policy implementation. A threat actor takes advantage of this form of exposure by searching for information within the repository.

A quarter (25.81%) of the issues observed were on exposed version control repositories. Typically discovered on public facing webservers, version control repositories can contain sensitive files and source code related to a given organization and/or application. With these repositories exposed, threat actors have an opportunity to look for configuration files, sensitive data or confidential information; all of which can be used to advance a threat actor's attempt to compromise a business.

Organizations can address the exposure by implementing a process to ensure applications pushed to production configurations block access to the repository. When an exposure is found, initiating an investigation into the repository by pulling it down locally and checking for sensitive data and content is recommended.

Exposed S3 buckets (5.44% of sample) are another common issue plaguing organizations. Mandiant has observed two common trends for S3 bucket exposures: A misconfiguration that allows for public access and a bucket policy inadvertently permitting unauthorized access to an authenticated user. In some cases, authenticated users are able to write to the bucket.

Even with sophisticated configuration tools in cloud providers, bucket leaks are still a common issue. If an S3 bucket exposure is discovered, security teams should investigate their level of exposure and adjust the policy to limit access.

Potential Leaked Secrets in Public Code Repositories

Organizations are increasingly using open-source version control such as Github. Mandiant continuously scans public Github repositories, identifying known patterns of confidential and sensitive information. Potential leaked secrets in public code repositories (17.96% of sample) indicate a potential credential leakage or change to the source code that requires immediate attention. Threat actors often use compromised credentials to publish malicious code which could have a devastating impact in open-source communities.

Organizations notified of this type of issue should perform a thorough code review and initiate incident response.

Subdomain Hijacks

Configuring subdomains to point to a third-party service is common practice for almost every organization. However, abandoned subdomains present a subtle but important risk vector. Abandoned subdomains pointing to a provider that allows attacker-supplied configuration and code can be used to compromise session credentials or in phishing campaigns. Strong DNS hygiene can mitigate the risk of a malicious threat actor using an abandoned subdomain on a third-party service for nefarious purposes.

Mandiant observations indicated that discovered subdomains (15.62% of sample) were vulnerable to hijacking. In most cases, the subdomain pointed to a third-party host where it was unclaimed and the third-party provided registration mechanisms that could be used by anyone. A threat actor could therefore claim the subdomain and host untrusted content.

Organizations that receive a high-severity issue notification about a vulnerable subdomain should take the appropriate steps to claim the subdomain through the third-party host.

Microsoft Exchange

Since March 2021, Mandiant has observed targeted attacks and instances of abuse of the Microsoft Exchange Server.[1] As of March 2022, Mandiant continues to see a trend indicating Exchange Servers remain unpatched and vulnerable to CVE-2021-26855, CVE-2021-31206, CVE-2021-34473, CVE-2021-42321 and a small percentage (<0.01%) are vulnerable to a Hafnium-affiliated webshell.

Microsoft Exchange Issues

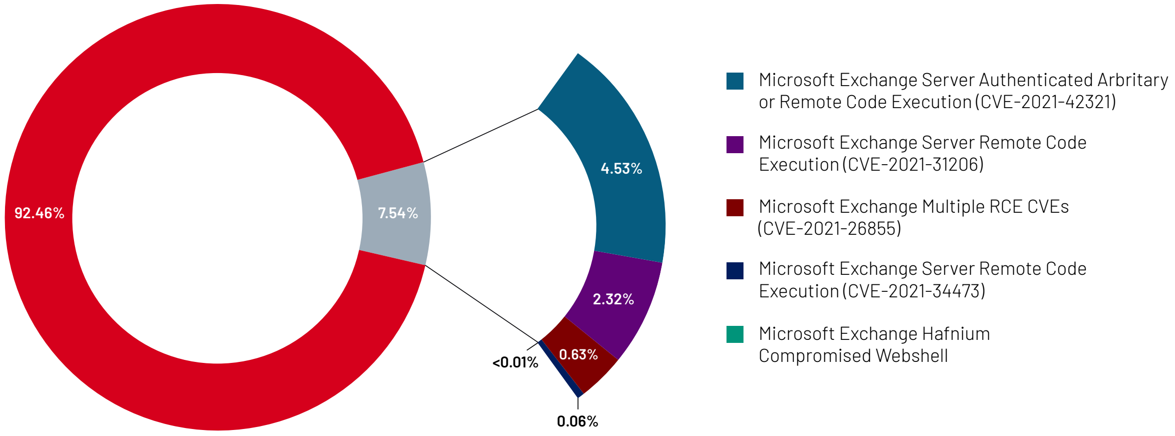


Figure 3. Most prevalent Microsoft Exchange vulnerabilities identified by Mandiant Advantage Attack Surface Management (January 1, 2022 to March 31, 2022).

[1] Mandiant (March 4, 2021). Detection and Response to Exploitation of Microsoft Exchange Zero-Day Vulnerabilities.

The Cybersecurity and Infrastructure Security Agency (CISA) has added several Microsoft Exchange vulnerabilities to its known exploited vulnerabilities catalog and set required remediation dates.[2] Mandiant highly recommends downloading the appropriate security update from Microsoft to patch vulnerabilities and adhere to CISA guidance. For example:

- CVE-2021-26855[3] had a required remediation date of April 16, 2021
- CVE-2021-31206[4] had a required remediation date of November 17, 2021
- CVE-2021-34473[5] had a required remediation date of November 17, 2021
- CVE-2021-42321[6] had a required remediation date of December 1, 2021

Of the Microsoft Exchange vulnerabilities, CVE-2021-42321 is the most prevalent among the Mandiant dataset, accounting for 4.53% of all issues identified. Mandiant considers this a high-risk vulnerability due to the possibility of a threat actor sending a malicious cmdlet augment to a server with an authenticated role.

On March 17, 2022, the Federal Bureau of Investigation (FBI) released a communication advising that CVE-2021-26855 and CVE-2021-34473, among others, are being used to deploy AvosLocker ransomware.[7]

Add External Visibility to Cyber Defense Programs

Understanding the attack surface from the viewpoint of an adversary helps organizations understand what controls need to be tested and crown jewels assessed. Based on Mandiant observations, assets typically overlooked within the attack surface are:

- External-facing database and remote access services
- Developer accounts on sites such as Github or Gitlab
- Staging and QA environments
- External-facing buckets or blob storage within a cloud environment
- Service accounts used for externally facing systems
- More esoteric application software or and network services exposed to the Internet
- Secondary email systems that can be used to deliver payloads w/o content filtering

Establishing a full view of the attack surface allows for cyber threat profile creation, prioritization of updates and config changes, context for penetration testing, and incident response and remediation.

[2] CISA (November 17, 2021). CISA Adds Four Known Exploited Vulnerabilities to Catalog.
[3] Microsoft Security Response Center (March 16, 2021). Microsoft Exchange Server Remote Code Execution Vulnerability: CVE-2021-26855.
[4] Microsoft Security Response Center (July 13, 2021). Microsoft Exchange Server Remote Code Execution Vulnerability: CVE-2021-31206.
[5] Microsoft Security Response Center (July 13, 2021). Microsoft Exchange Server Remote Code Execution Vulnerability: CVE-2021-34473.
[6] Microsoft Security Response Center (December 6, 2021). Microsoft Exchange Server Remote Code Execution Vulnerability: CVE-2021-42321.
[7] FBI IC3 (March 17, 2022). Joint Cybersecurity Advisory: Indicators of Compromise Associated with AvosLocker Ransomware.

Data Collection to Uncover Operational Technology Threats

TRITON is a communication and exploitation framework compiled in Python designed to target OT systems. TRITON was deployed against a Middle East-based critical infrastructure plant's safety instrumented systems in 2017. Mandiant assesses with high confidence the activity was supported by the Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM aka TsNIIKhM, TsNII), a Russian Government-owned technical research institution in Moscow.

INCONTROLLER is a collection of three separate OT tools designed to attack certain industrial control system (ICS) devices. Each tool has tailored capabilities that interact with OPC-UA servers, certain Schneider Electric programable logic controllers (PLCs) and certain Omron devices.

In recent years, Mandiant has observed a significant increase in threat activity with the potential to impact production for industrial and critical infrastructure organizations. This activity has evolved to incorporate opportunistic actors targeting internet-controlled operational technology (OT), high-profile ransomware gangs profiting from obstructing production systems and nation-state sponsored groups developing complex tools with the potential to endanger the physical safety of human populations. As these threats advance, our threat intelligence collection has adapted.

Traditional cyber threat intelligence collection methods on OT systems often rely only on subject matter expertise and qualitative analysis of a few highly impactful cases such as TRITON,[8] INDUSTROYER.V2[9] or more recently, INCONTROLLER.[10] Building large datasets for OT threats has historically been difficult. Contributing factors include, a lack of visibility into production networks, a lack of incentives for organizations to share information and a lack of awareness of the different types of activity that can impact production systems. As we continue to observe actors targeting OT in different ways—ranging from ransomware operators[11] to low sophistication crimes of opportunity[12]—our ability to acquire valuable data increases.

Over the years, Mandiant has uncovered important data related to OT threats hidden in malware repositories, online forums, research and media publications, extortion leaks and other places.

Planning and implementing attacks to modify or disrupt the expected functionality of OT systems requires extensive capabilities to gather information about the target, gain access to IT and OT networks, move across intermediary systems and exploit weaknesses in production systems. By enhancing their visibility into diverse data sources, organizations can identify threat actor activity during the early stages of the attack lifecycle and prevent them reaching production systems.

[8] Mandiant (April 10, 2019). TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping.
[9] Mandiant (April 25, 2022). INDUSTROYER.V2: Old Malware Learns New Tricks.
[10] Mandiant (April 13, 2022). INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems.
[11] Mandiant (July 15, 2020). Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families.
[12] Mandiant (May 25, 2021). Crimes of Opportunity: Increasing Frequency of Low Sophistication Operational Technology Compromises.

Collecting and Filtering OT Data

Mandiant tracks data relevant to OT defenders through a team of researchers working on global intelligence collections, a strong network of information sharing partners, incident response and consulting engagements, threat hunting across a variety of sources and other methods.

Visualization of the OT Threat Landscape

Enriched OT data-driven intelligence based on different sources and filtering methods give Mandiant visibility into different facets of the OT threat landscape.

Financially Motivated Actors Impact Industrial and Critical Infrastructure Organizations

Over the past two years, Mandiant has tracked the evolution of ransomware actors impacting industrial production[13] and expanding access into OT.[14] From April 1, 2021 - March 31, 2022, Mandiant observed many cases where threat actors had deployed ransomware to target industrial and critical infrastructure organizations across sectors that often rely on OT systems to support production.

To systematically analyze this activity, Mandiant collected information from ransomware extortion leaks, tracking nearly 1,400 victims across OT-intensive industries such as water, energy and manufacturing. The data was filtered to uncover the following trends:

- 56% of victims were from manufacturing and construction/engineering industries
- 28% of organizations had over 500 employees
- LockBit and Conti infections were the most prolific, responsible for over 40% of activity
- One out of seven ransomware extortion leaks from this subset were likely to contain sensitive OT documentation[15]

[13] Mandiant (February 24, 2020). Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT.
[14] Mandiant (July 15, 2020). Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families.
[15] Mandiant (January 31, 2022). 1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information.

Percentage of Victims by Primary Industry

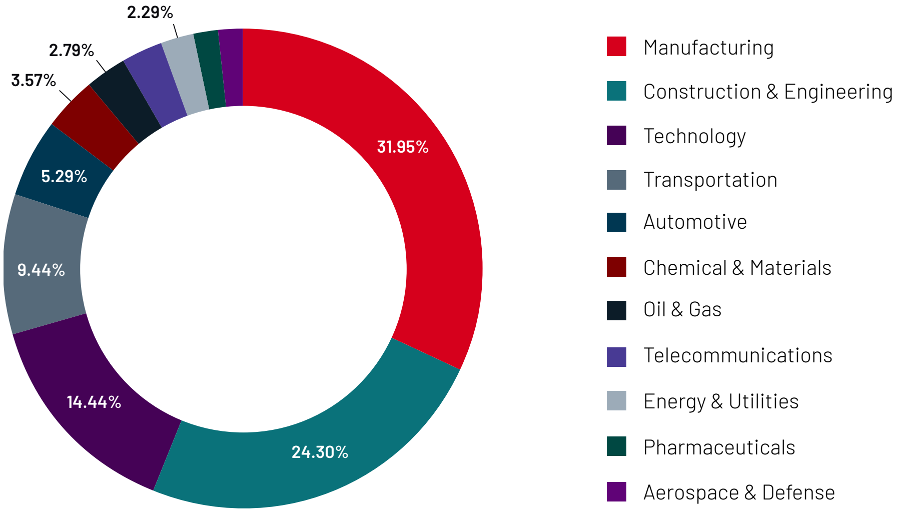


Figure 4. Ransomware victims exposed in extortion leaks from industrial and critical infrastructure sectors (April 1, 2021 – March 31, 2022).

Estimated Company Size of Ransomware Victims

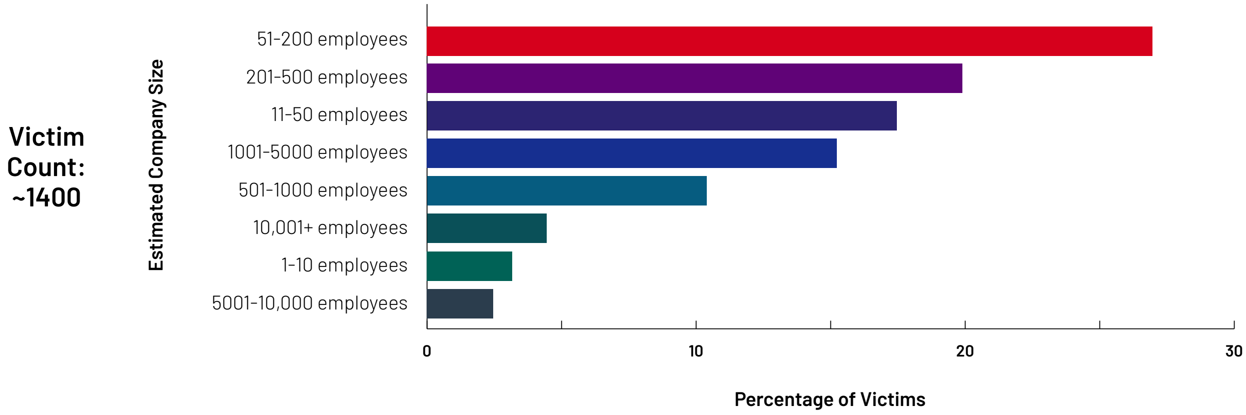


Figure 5. Estimated company size of ransomware victims for industrial and critical infrastructure sectors (April 1, 2021 – March 31, 2022).

Broad Distribution of Malware may Support Initial Access for Future OT Compromises

One common challenge in OT security is to anticipate threat activity as early as possible within the attack lifecycle. Mandiant therefore focuses efforts on filtering threat activity to identify possible indications of interest in compromising OT organizations. Between April 1, 2021 and March 31, 2022, Mandiant collected and analyzed the contents of broadly distributed phishing emails and malicious sites which contained keywords related to industries that commonly employ OT systems. The collection of such data enables better visibility into events that may eventually evolve into more impactful attacks.

In the last year, Mandiant tracked over 1,600 phishing emails with content that included OT-related keywords, such as order, request, rfq, quotation, purchase or invoice. These emails also contained over 2,200 payloads distributing more than 30 types of broadly known malware, including AGENTTESLA, EMOTET, FORMBOOK and GULOADER.

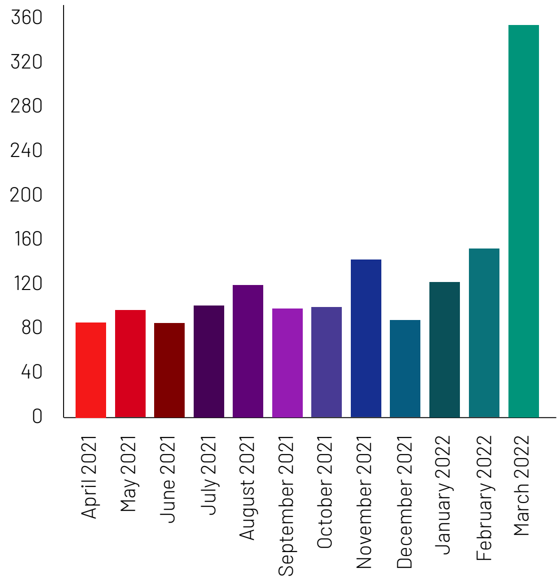


Figure 6. Phishing emails identified containing OT-specific keywords (April 1, 2021 – March 31, 2022).

From April 1, 2021 to March 31, 2022, Mandiant observed over 150 malicious domains with contents related to industrial and critical infrastructure production. Malware such as NANOCORE, FORMBOOK, LOKIBOT and VIDAR were identified in the majority of these websites.

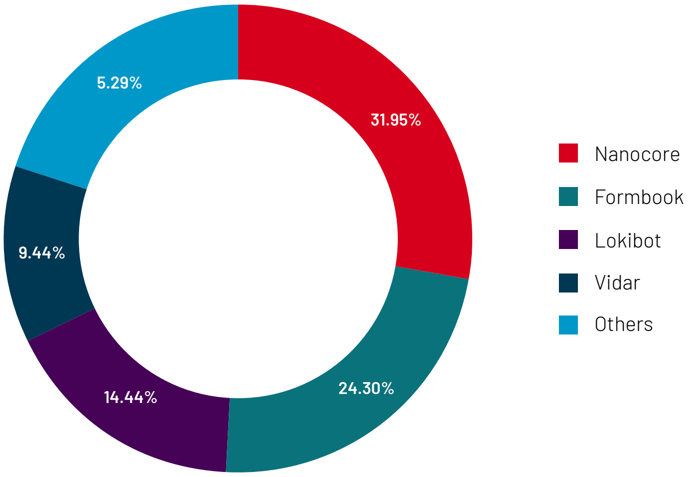


Figure 7. Distribution of malware identified in malicious domains with OT-related content (April 1, 2021 – March 31, 2022).

The Value of Processed Information about OT Vulnerabilities

The first OT vulnerability advisories were released over 10 years ago. Since then, efforts to coordinate the communication of vulnerabilities in OT devices across industry and government entities has improved and Mandiant continues to track a consistent increase in the number of vulnerability disclosures. To better understand this data, Mandiant periodically analyzes trends and collects historical details on exploit modules designed to take advantage of OT vulnerabilities.

From April 1, 2021 through March 31, 2022, Mandiant tracked over 490 advisories related to vulnerabilities in OT or medical devices from over 100 vendors. The advisories contained information about 1,187 unique vulnerabilities and 196 of them received a critical risk score. The most common types of vulnerabilities observed were:

- CWE-787: OUT-OF-BOUNDS WRITE
- CWE-125: OUT-OF-BOUNDS READ
- CWE-20: IMPROPER INPUT VALIDATION
- CWE-79: IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION (CROSS-SITE SCRIPTING)
- CWE-121: STACK-BASED BUFFER OVERFLOW

Mandiant has tracked hundreds of OT-specific exploit modules[16] in popular security platforms. Access to these tools lowers the barrier for different actors to develop skills or custom attack frameworks to target OT. As of April 2022, Mandiant has tracked exploit modules related to more than 530 vulnerabilities and 73% of them were related to zero-day vulnerabilities.

[16] Mandiant (March 23, 2020). Monitoring ICS Cyber Operation Tools and Software Exploit Modules To Anticipate Future Threats.

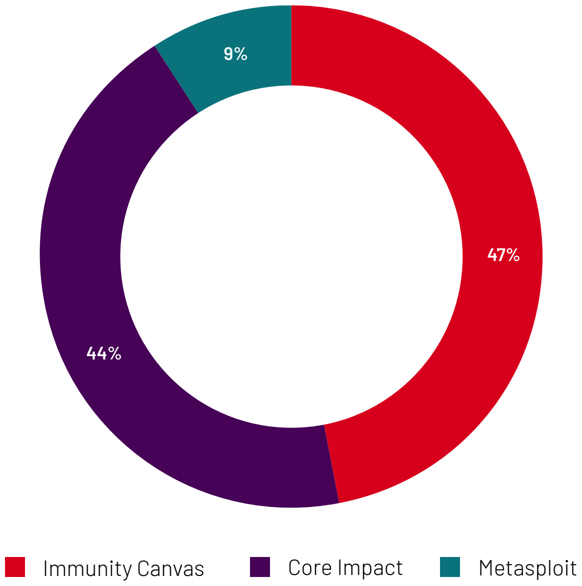


Figure 8. Historical distribution of OT exploit modules by platform until April 2022.

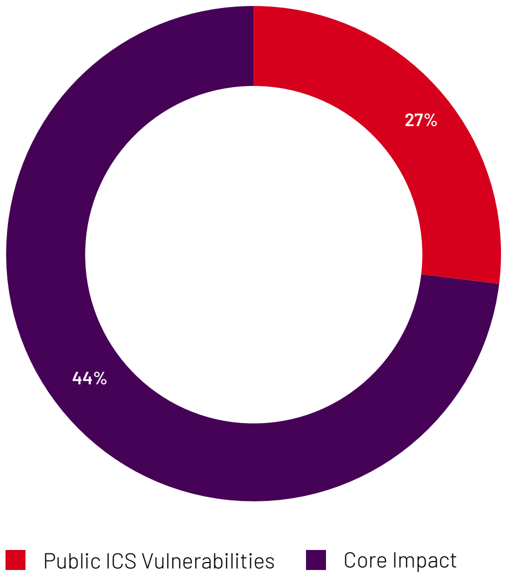


Figure 9. Historical distribution of zero-day vulnerabilities versus known OT vulnerabilities in exploit modules until April 2022.

Summary

Mandiant threat visibility is derived from a variety of sources, including:

- Contextual and technical analysis of impactful events based on data acquired from incident response engagements
- Recommendations for defenders based on an assessment of the security effectiveness of ICS systems against top risks for industrial organizations
- Data collections from our global network of researchers, with close visibility into activity across online forums
- Analysis of threats based on filtering noise from data across large IT-focused Intelligence repositories
- Exploration of the threat landscape and definition of trends based on analysis from data acquired across public, private and Mandiant proprietary datasets

Taken together, building this broad visibility has enabled us to explore different facets of the OT threat landscape to have a holistic view. The different data collection avenues enable us not to hyperfocus only on high profile OT incidents once they happen, but to instead look at threat actor activity much earlier in the attack lifecycle. Our data illustrates that careful filtering and analysis of data from threats in corporate networks can help defenders to prevent future targeting of OT networks and remain one step ahead of the attackers.

Technical Due Diligence for Mergers and Acquisitions

In the 12 months preceding April 2022, Mandiant completed over 240 compromise assessments across nearly one million endpoints. Compromise assessments often inform preacquisition decisions during the due diligence phase of mergers and acquisitions and can also influence integration strategies between companies involved in mergers and acquisitions.

When undertaking an assessment, Mandiant typically evaluates the environment for evidence of current or past compromise and assesses specific technical configurations and controls. Audit methodologies are combined with technical assessments to ensure that any costs required to resolve cyber security gaps or adhere to laws and regulations are identified, reducing the risk of the transaction.

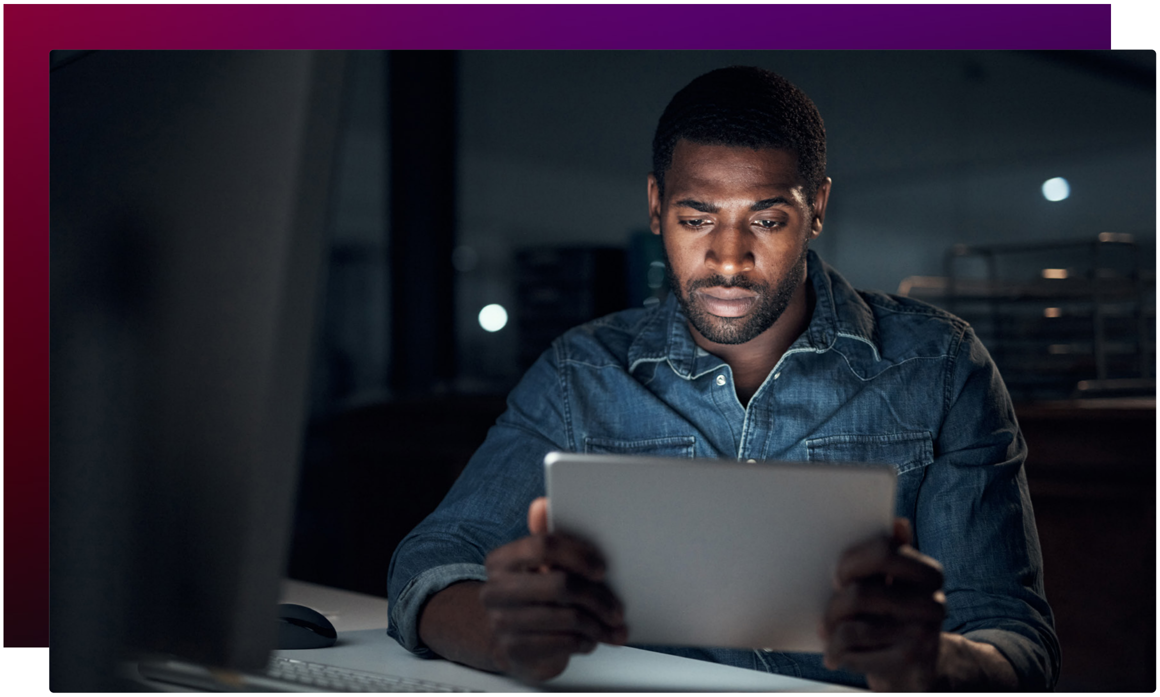
Compromise Assessments Uncover Security Deficiencies

In one case, Mandiant conducted a Compromise Assessment for an organization that was divesting a single business unit (SBU) to be acquired by a third party. Forming part of their due diligence, the third party requested technical analysis of the business unit to determine if there was evidence of ongoing or past compromise or weakness in specific security controls. Findings or deficiencies in either aspect could impact the pace and integration strategy of the SBU by the third party.

Mandiant conducted the assessment in a Windows-centric environment. Subsequent analysis revealed evidence of a previous ransomware event. While the organization was aware of the ransomware incident, Mandiant identified residual binaries and backdoors that remained from an incomplete remediation effort.

Mandiant also located multiple persistent backdoors beaconing to command and control (C2) servers that were unrelated to the ransomware activity. Analysis of the impacted systems indicated a threat actor installed the backdoors from systems in the larger organization and outside the scope of the SBU. However, the organization had a flat network. Mandiant's threat intelligence associated the backdoors with a tracked financial threat actor (FIN11) known to steal data and subsequently deploy ransomware.

By evaluating security controls, Mandiant located security deficiencies in endpoint and domain configurations, system logging, patching and environment hygiene.



Addressing Risks Proactively

If the client had not undertaken the assessment, the acquiring third party may have connected internal networks, potentially exposing their organization to risk from the SBU environment.

The acquiring third party used the assessment outcomes to complete additional incident response analysis of the environment to determine whether any data had been previously exposed. They also modified their integration strategy to deploy new user workstations, migrate data to new servers and accelerate the migration of specific business applications to cloud software as a service (SaaS) solutions. These strategies were intended to reduce risk to the environments and data of both companies. The client was also able to prevent reputational damage and further costs by promptly notifying affected parties of any intellectual property or data theft.

Protecting Societal Events When the Whole World is Watching

Global geopolitical summits, elections and sporting events are some of the most visible international, national and regional events. They also present unique cyber security challenges with respect to critical supportive infrastructure and supply chains. These societal events can last from a single day to multiple weeks or months, necessitating variable capabilities and surge capacity.

Mandiant has developed a recommended, multi-faceted approach to security based on engagements for these types of events. Defending against cyber threats targeting societal events requires active defenses informed by intelligence. The organizations running these events demand strategic security program capabilities and specific technical solutions to harden and enhance their security posture prior to an event and to support operations during the event. Delivering resilient cyber capabilities in a compressed timeframe under intense public attention and scrutiny is a major challenge that requires focus and investment to properly plan and implement.

Strong cyber defenses for major event protection events are based on three phases:

- Prepare, harden and exercise (understand the environment)
- Test, monitor and defend (anticipate threats)
- Respond, contain and remediate (impose costs and survive attacks)

Each phase is informed by intelligence and coupled with tiered framework levels for proactive protection. Initial intelligence collection and observation should provide a baseline of the threat landscape to support future detection capabilities. Intelligence should highlight adversary horizon activities and capabilities throughout major events. This helps continuously inform defenders of activities designed to influence, interfere with or disrupt events. Mandiant intelligence holdings cover a wide range of scenarios, and include details on adversarial tactics, motivations, and evolution over time. This knowledge helps shape framework levels for each phase.

Mandiant relies on two categories of recommendations to strengthen an organization's cyber defenses in parallel with emerging threat conditions.[17] Hardening and readiness recommendations focus on proactive and strategic tasks, while operational recommendations identify what functional changes can be adopted to enhance security posture within each phase.

[17] Mandiant (April 2022). A Tiered Framework for Cyber Threat Levels.

Prepare, Harden and Exercise

This phase takes place before a major event, and its purpose is to proactively protect and harden the security posture. It is intended to align cyber defenses across an organization's environment to best practices and current standards and support review. The threat environment must be properly defined in terms of potential adversarial actions and motivations. This phase is designed to ensure three key outcomes for active cyber defense: baseline, visibility, and validate.

Prepare

- Deploy a managed detection and response capability to monitor and investigate alerts, proactively hunt for attackers and contain and remediate threats.
- Create use cases and alerts for emerging and currently exploited vulnerabilities as well as current and imminent threats based on the threat landscape using up-to-date, real-world intelligence.
- Monitor social media, blogs, forums, news sites and chat apps for threat vectors and misinformation and disinformation campaigns.
- Deploy endpoint and network detection technologies across the entire environment and multi-factor authentication across all accounts and external facing services.
- Apply incident response data and technology processes, collections and requirements to speed containment and remediation.
- Ensure holistic, centralized logging across all platforms, networks and endpoints.
- Coordinate with relevant national agencies to obtain and contribute related intelligence.
- Engage an incident response retainer to pre-manage service level agreements, terms and conditions and funding in the event of a breach.

Harden

- Conduct a compromise assessment to ensure the security and integrity of the environment and data to be protected, informed by most likely and most dangerous adversarial scenarios.
- Identify and harden externally facing assets and pathways into the environment.
- Maintain an inventory of all assets on the domain and network and have those assets regularly scanned for vulnerabilities and hardened.
- Validate effectiveness of controls.

Harden

- Designate a crisis-response team with clear roles and responsibilities to address suspected cyber security incidents; ensure organizational, executive and communications support.
- Test backup procedures to ensure that critical data can be rapidly restored and critical business functions can remain available in the event of an incident.
- Conduct a tabletop exercise aligned to the major event threat landscape to ensure that all participants understand their roles during an incident in accordance with previously developed scenarios.

Test, Monitor and Defend

During this phase, the major event has begun, and increased risk of destructive or disruptive cyber attacks are likely. Elevated active defense readiness postures are recommended. Priorities should include continuous validation of security controls and defense of critical assets. This phase focuses on inhibiting the access an adversary needs to leverage to achieve their goal. Increasing threat hunting operations can increase confidence that an adversary does not maintain access to the organization's network and infrastructure. Mandiant can base all actions in this phase on known and anticipated adversarial activities, using actual attacker malware, tactics, techniques and procedures, and motivating factors. This phase provides three outcomes for active cyber defense: validation, integrity and decision advantage.

Test

- Conduct ad-hoc penetration testing exercises on all externally facing assets.
- Test the internal team's and technology's ability to detect, prevent and respond.
- Test the incident response team's reaction times against real adversarial methods.
- Continuously validate the effectiveness of security controls.

Monitor

- Establish a situation room to centralize operations, intelligence and external organization information and communications.
- Continuously monitor, analyze and report relevant data and analysis from intelligence sources.
- Conduct enhanced hunting and monitoring for indicator-less behaviors; assume attacks are happening and technical controls have missed something.
- Continuously validate security controls effectiveness against active attack behaviors.
- Restrict egress communications on critical systems.

Defend

- Focus on critical asset protection—those assets identified by the target organization and those likely to be identified by an adversary.
- Protect specific high-value infrastructure.
- Restrict network architecture to limit or remove adversary access to critical systems.
- Back up critical assets.

Respond, Contain and Remediate

During the major event, national, international and social media coverage often parallels real-time activity. Extensive intelligence on existing and emerging threat actor tactics, techniques and procedures enables effective and efficient incident response. Incident response services must have the capability to respond, contain and remediate critical security incidents with speed, scale and efficiency. This means using intelligence to establish resilience in a real-world threat environment.

Assessment of impacted systems, applications and information exposure are essential to implementing the appropriate communication, crisis and response plans. Effective incident and breach response extends beyond technical investigation, containment and recovery and includes executive communication and crisis management. Crisis management includes legal, regulatory and public relations considerations. The criticality of resolving incidents quickly and providing continuity is paramount. Doing this requires taking into account a potential adversary's view of the situation. Preparing for an incident from only one side, without invoking real-world experience and known data on threats, solves only half the equation.

De-escalation plans are often more important than escalation plans. All defenders must communicate and conduct themselves thoughtfully, intentionally and openly. Containment and remediation strategies based on attacker actions should be implemented to eliminate attacker access and improve the security posture of the environment to prevent or limit potential damage.

Following the major event, an after-action report should detail successes, challenges and recommendations.

This phase provides three outcomes for active cyber defense: response, recovery and continuity.

The cyber security challenges we face today are too big to tackle alone and the necessary cyber defense operations maturity and capacity require significant, sustained focus and investment. These challenges become even more acute during major events. Protecting such events requires organizations to provide rapid and adaptable cyber defense under unique duress and pressure. A prepared and practiced cyber strategy and playbook helps ensure a favorable outcome for the hosts, participants and other stakeholders.

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

About Mandiant

Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.