MANDIANT

MANDIANT ADVANTAGE
WHITE PAPER

Uncover Operational Technology Threats with Data Collection

The content in this document was originally published in The Defender's Advantage Cyber Snapshot.

MANDIANT

The Defender's Advantage Cyber Snapshot

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,[1] INDUSTROYER.V2[2] or more recently, INCONTROLLER.[3] 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[4] to low sophistication crimes of opportunity[5]—our ability to acquire valuable data increases.

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.

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.

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.

[1] Mandiant (April 10, 2019). TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping.
[2] Mandiant (April 25, 2022). INDUSTROYER.V2: Old Malware Learns New Tricks.
[3] Mandiant (April 13, 2022). INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems.
[4] 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.
[5] Mandiant (May 25, 2021). Crimes of Opportunity: Increasing Frequency of Low Sophistication Operational Technology Compromises.

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[6] and expanding access into OT.[7] 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[8]

Percentage of Victims by Primary Industry

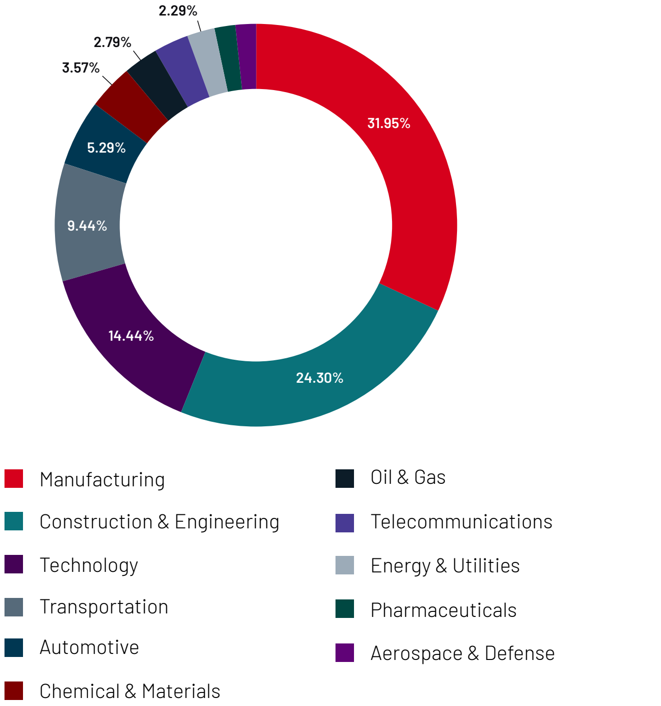

FIGURE 1. Ransomware victims exposed in extortion leaks from industrial and critical infrastructure sectors (April 1, 2021 – March 31, 2022).

Estimated Company Size of Ransomware Victims

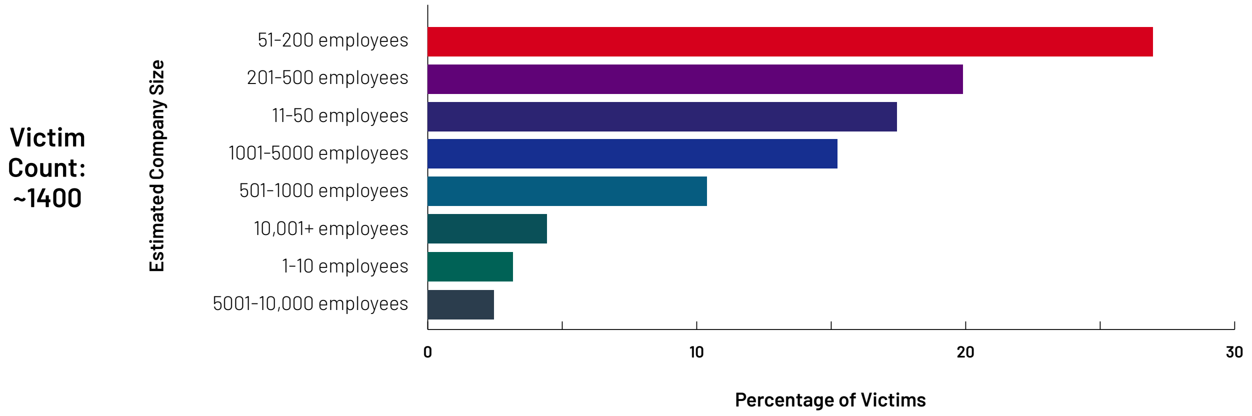

FIGURE 2. Estimated company size of ransomware victims for industrial and critical infrastructure sectors (April 1, 2021 – March 31, 2022).

[6] Mandiant (February 24, 2020). Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT.
[7] 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.
[8] Mandiant (January 31, 2022). 1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information.

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.

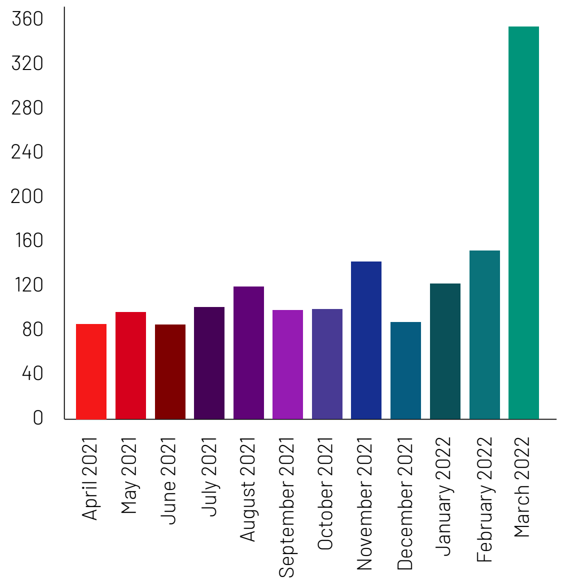

FIGURE 3. Phishing emails identified containing OT-specific keywords (April 1, 2021 – March 31, 2022).

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.

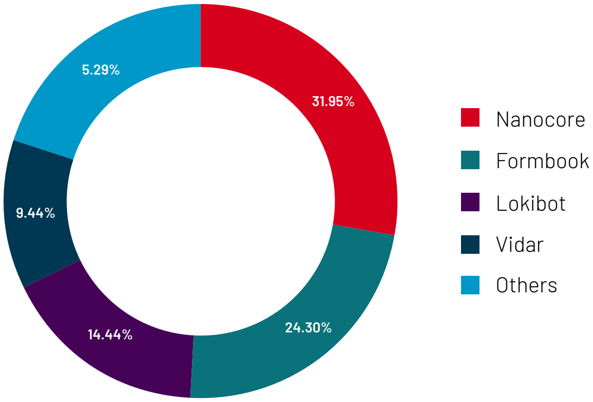

FIGURE 4. Distribution of malware identified in malicious domains with OT-related content (April 1, 2021 – March 31, 2022).

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[9] 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.

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

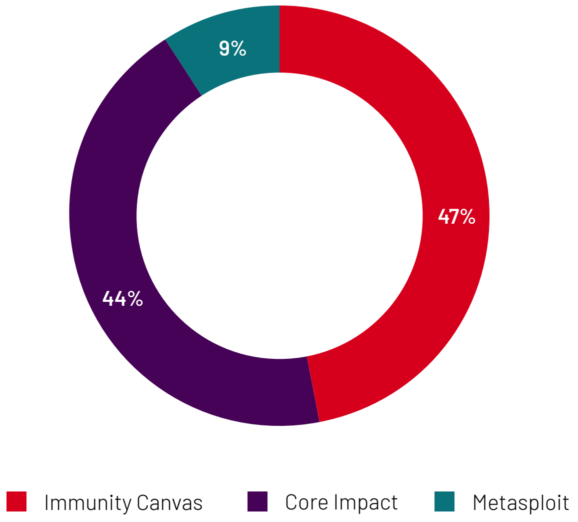

FIGURE 5. Historical distribution of OT exploit modules by platform until April 2022.

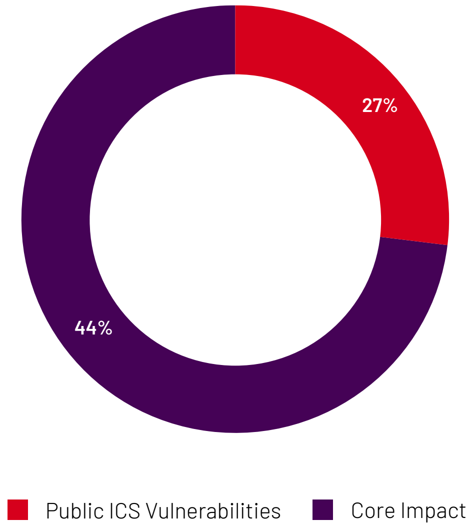

FIGURE 6. Historical distribution of zero-day vulnerabilities versus known OT vulnerabilities in exploit modules until April 2022.

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.

Read more articles from The Defender's Advantage Cyber Snapshot.

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.

MANDIANT®
YOUR CYBERSECURITY ADVANTAGE