MANDIANT
NOW PART OF Google Cloud

M-Trends 2023 Special Report

Executive Summary

The 14th edition of the M-Trends 2023 report is available at www.mandiant.com/m-trends

By the Numbers—The Data of M-Trends

The information provided is based on Mandiant Consulting investigations conducted between January 1, 2022, and December 31, 2022.

What do I need to know?

- Globally, attacks are being detected faster, with improvements seen in the Americas and EMEA regions, but not in the APAC region.
- Security vendors and other external sources are notifying organizations of compromises more often than internal security teams are finding them; however, when internal teams detect attacks it is faster than when notified by external notification.
- To gain access to organizations, attackers are leveraging what works best in different regions: exploits in the Americas, phishing in EMEA, and prior compromises in APAC.

Ask your CISO

- How do we measure our detection and response time, and what is our median time from detection to response and remediation?
- Are we prepared to detect and respond to the most common malware, exploits, and initial infection vectors such as phishing?
- What is our protocol when we are notified by a third-party that we are potentially compromised?
- How are we positioned to ensure exploit mitigation for systems with known vulnerabilities?

Invasion of Ukraine

What do I need to know?

- Mandiant identified extensive cyber espionage, disruptive and destructive cyber attacks, and information operations leading up to and since Russia's invasion of Ukraine on February 24, 2022.
- Russian operations have impacted industrial control systems and critical infrastructure, and in some cases were enabled due to campaigns conducted and access gained before the invasion.
- Russia's invasion of Ukraine has demonstrated the potential overlap of cyber operations and kinetic warfare as a new de facto standard.

Ask your CISO

- Have we taken steps to harden our systems against destructive and disruptive attacks?
- What were the results of the most recent test of our backup and continuity of operations plan?
- Should we be using threat intelligence to combat information operations?

North Korea's Financial Operations

What do I need to know?

- Alongside traditional intelligence collection missions and disruptive attacks, in 2022, Democratic People's Republic of Korea (DPRK) operators showed more interest in stealing—and using—cryptocurrency.
- These operations have been highly lucrative and will likely continue unabated throughout 2023.

Ask your CISO

- How prepared are we to deal with the financial threats most relevant to our organization?

Shifting Focus and Uncommon Techniques

What do I need to know?

- Attackers with less technical skills are causing huge impacts to organizations.
- These operations have resulted in data theft, stolen intellectual property, and significant reputational damage.
- These attackers seem motivated by notoriety more so than money or espionage, have demonstrated resourcefulness, and are willing to use bribes and even bullying or threatening to achieve their goals.

Ask your CISO

- How are we minimizing the risk of social engineering and other similar threats from reaching our employees?
- What programs do we have to protect our employees, especially executives and highly visible employees, from these types of attacks?
- How would we react if proprietary information or client PII was stolen and used as extortion against us?
- Do we have a procedure to rapidly acquire cryptocurrency in response to an extortion threat?

Cloud Focus—Red Team Case Study

What do I need to know?

- Red team engagements help organizations evaluate their security program's capabilities against real-world attack scenarios, and improve their security postures.
- Mandiant showed a utility company how attackers can gain access to critical cloud and operational technology environment resources.

Ask your CISO

- Do we have full visibility into exactly how our organization is using the cloud?
- Are we regularly checking for misconfigurations that attackers can exploit?
- Are we testing our cloud architecture deployments?

Campaigns and Global Events

What do I need to know?

- To better protect customers throughout 2022, Mandiant's Campaigns and Global Events Team investigated Russian espionage activity, ransomware, and significant vulnerabilities such as Log4Shell.
- Mandiant shares valuable intelligence and indicators to help our clients and the community protect themselves from these campaigns.

Ask your CISO

- What are we doing to track and patch vulnerabilities in our network?
- How are we using current threat intelligence to inform decisions?

APT42—Notable Graduations

What do I need to know?

- APT42 is an Iran-nexus threat group that conducts espionage using sophisticated phishing and social engineering attacks.
- APT42 activity poses a threat to foreign policy officials, commentators, and journalists working on Iran-related projects, particularly those in the United States, the United Kingdom, and Israel.

Ask your CISO

- What can our security, IT and business teams be doing to protect all employees?
- How are we minimizing the risk of social engineering threats from reaching our employees?
- How do we make our employees aware of phishing and other social engineering attempts?

Learn more at www.mandiant.com/m-trends

Mandiant

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

About Mandiant

Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT
NOW PART OF Google Cloud