Mandiant's M-Trends Report Reveals New Insights from Frontline Cyber Investigations

Global median dwell time falls to its lowest point in over a decade; Financial Services is the most targeted sector by attackers

SUNNYVALE, Calif., April 23, 2024 /PRNewswire/ -- Mandiant, part of Google Cloud, today released the findings of its M-Trends 2024 report. Now in its 15th year, this annual report provides expert trend analysis based on Mandiant frontline cyber attack investigations and remediations conducted in 2023. The 2024 report reveals evidence that organizations globally have made meaningful improvements in their defensive capabilities, identifying malicious activity affecting their organization more quickly than in previous years. The report also takes a look at notable threat actors and campaigns, providing a focused look at threat activity by region.

"Attackers regularly adjust their tactics, techniques, and procedures in order to achieve their objectives, which can be challenging for defenders. Despite this, our frontline investigators have learned that organizations have done a better job in 2023 at protecting systems and detecting compromises," said **Jurgen Kutscher, Vice President, Mandiant Consulting at Google Cloud**.

Kutscher continued, "Defenders should be proud, but organizations must remain vigilant. A key theme throughout M-Trends 2024 is that attackers are taking steps to evade detection and remain on systems for longer, and one of the ways they accomplish this is through the use of zero-day vulnerabilities. This further highlights the importance of an effective threat hunt program, as well as the need for comprehensive investigations and remediation in the event of a breach."

Global Median Dwell Time Hits Lowest Point Recorded

While the use of zero-day exploits is on the rise, the M-Trends 2024 report reveals a significant improvement in global cybersecurity posture. The global median dwell time – the time attackers remain undetected within a target environment – has reached its lowest point in over a decade. In 2023, organizations detected intrusions within a median of 10 days, a notable decrease from 16 days in 2022. Shorter dwell times are likely driven by a larger proportion of ransomware incidents in 2023 (23%) versus 2022 (18%). Mandiant also tracked an improvement in internal detection of compromise in 2023 (46%), compared to 37% in 2022. These two trends - shorter dwell times and more internally detected events - suggest that defenders globally have improved detection capabilities.

Dwell Time By Region

A closer examination reveals that median dwell time varies by region. Organizations in the Asia-Pacific (JAPAC) region experienced the most dramatic decrease, reducing their median dwell time to 9 days, compared to 33 days in 2022. This variation could be driven by the quick moving ransomware used in the incidents in the region, as ransomware-related intrusions consumed the highest majority for the investigation type compared to any other region in 2023. Conversely, the EMEA region (Europe, the Middle East and Africa) saw a slight rise in dwell time, increasing from 20 days to 22 days. This small variation could be the result of regional data normalizing following the notable portion of Mandiant's work in Ukraine in 2022.

Targeting By Industry Vertical

The M-Trends 2024 report highlights key trends in industry targeting by cyber attackers. Mandiant most frequently responded to intrusions at financial services organizations (17%) in 2023. Following this sector were business and professional services (13%), high technology (12%), retail and hospitality (9%), and healthcare (8%).

A common thread across the top targeted industries is their possession of a wealth of sensitive information, including proprietary business data, personally identifiable information, protected health information, and financial records. This makes them particularly attractive targets for attackers seeking to exploit this type of sensitive data.

Additional report takeaways include:

- **Increased Focus on Evasion:** In an effort to maintain persistence on networks for as long as possible, attackers are increasingly targeting edge devices, leveraging "living off the land" techniques and exploiting zero day vulnerabilities.
- **Heightened Espionage Efforts by China-Nexus Actors:** China-nexus espionage groups are continuing to prioritize acquiring zero-day exploits and platform-specific tools. They will likely target edge devices and platforms with minimal security solutions due to the ease of compromising them undetected and for a longer period of time.
- **Zero-Day Exploits on the Up-and-Up:** Zero-day exploits are no longer limited to a few, select actors. The trend of increasing availability is expected to continue due to factors like ransomware and data extortion groups utilizing them, continued state-sponsored exploitation, and the rise of commercially available "turnkey" exploit kits. For more on how

threat actors are using zero days, check out Mandiant and Google Threat Analysis Group's first-ever joint report on the topic.

- **Cloud Targeting Aligns with Adoption:** As cloud adoption grows, so does attacker targeting of these environments, including hybrid cloud/on-premise configurations. Organizations are advised to implement stricter controls to limit access to cloud resources by only authorized users.
- **Potential for Red Teaming with Large Language Models (LLMs) and AI:** Like other cybersecurity professionals, Red Teams can leverage LLMs and AI in their work. Use cases could involve Red Teams generating data for model training while AI developers find ways to secure access to trained models. This synergy could significantly enhance Red Team effectiveness and improve organizational preparedness against cyber threats.
- **Evolving Tactics to Bypass MFA:** As multi-factor authentication (MFA) becomes standard practice, attackers are developing methods to circumvent its protections. A concerning trend is the rise of web proxy and adversary-in-the-middle (AiTM) phishing pages that steal login session tokens, effectively bypassing MFA.

M-Trends 2024 Methodology

The metrics reported in M-Trends 2024 are based on Mandiant Consulting investigations of targeted attack activity conducted between January 1, 2023 and December 31, 2023. The intelligence gleaned has been sanitized to protect the identities of targets and their data.

Resources

M-Trends 2024 Report: https://cloud.google.com/security/m-trends
M-Trends 2024 Executive Summary:
https://services.google.com/fh/files/misc/m-trends-2024-executive-edition.pdf
Blog: https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2024
Webinar: https://series.brighttalk.com/series/6462

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 part of Google Cloud.

About Google Cloud

Google Cloud is the new way to the cloud, providing AI, infrastructure, developer, data, security, and collaboration tools built for today and tomorrow. Google Cloud offers a powerful, fully integrated and optimized AI stack with its own planet-scale infrastructure, custom-built chips, generative AI models and development platform, as well as AI-powered applications, to help organizations transform. Customers in more than 200 countries and territories turn to Google Cloud as their trusted technology partner.

SOURCE Mandiant, part of Google Cloud

For further information: mandiant-pr@google.com

Additional assets available online: Photos

https://www.googlecloudpresscorner.com/2024-04-23-Mandiants-M-Trends-Report-Reveals-New-Insights-from-Frontline-Cyber-Investigations