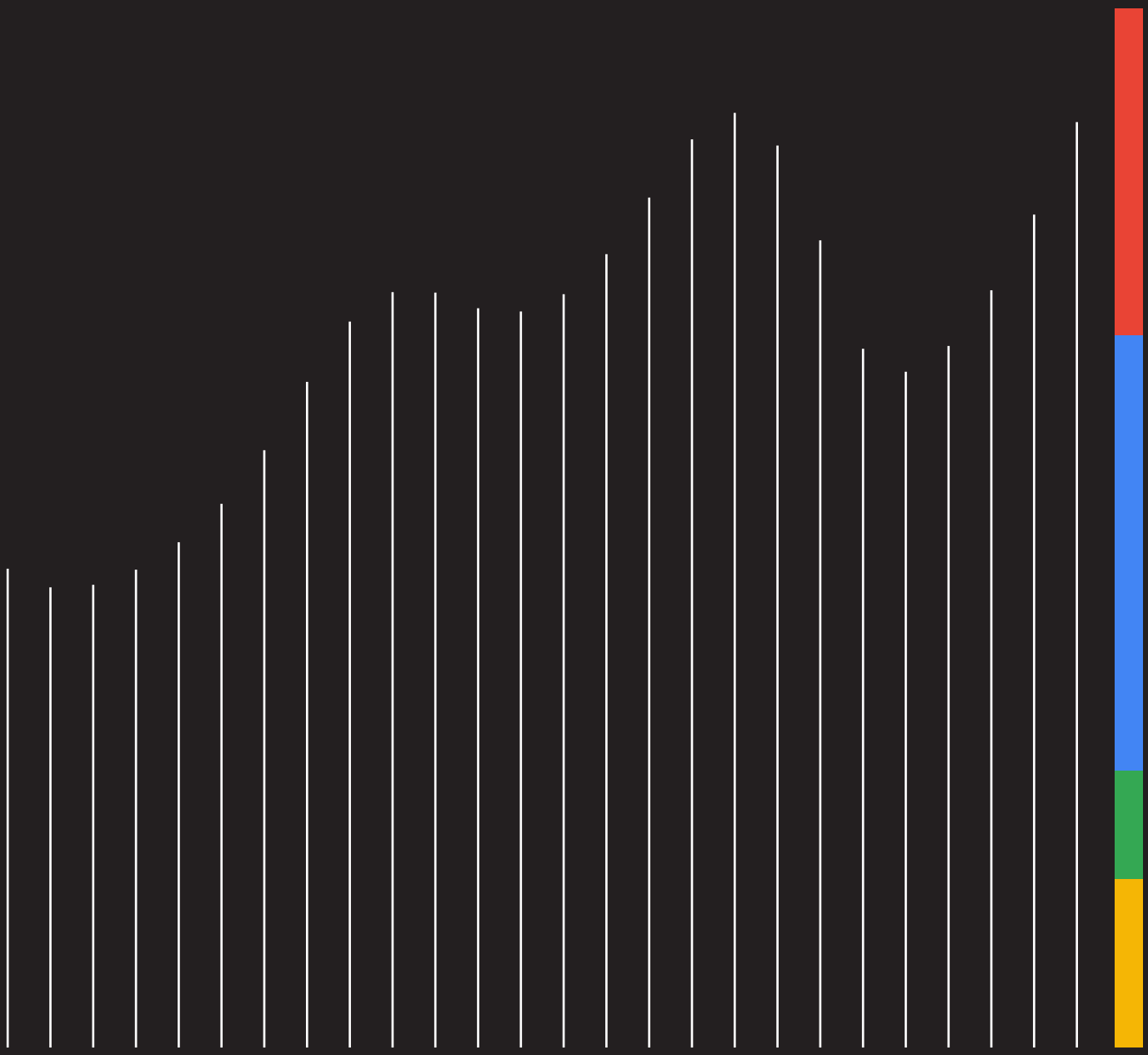
Mandiant

Google Cloud Security

M-Trends

2024 Special Report

Executive Edition



By the Numbers—
The Data of M-Trends

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.

What do I need to know?

- Dwell time is the number of days an attacker is on a system from compromise to detection, and in 2023 the global median dwell time is 10 days, down from 16 days in 2022.
- For ransomware cases, the global median dwell time is 5 days compared to 9 days in the previous year.
- 54% of organizations first learned of a compromise from an external source, while 46% first identified evidence of a compromise internally. 63% of notifications were external in 2022, suggesting organizations are improving at detecting malicious behavior.
- In 70% of ransomware cases, organizations learned of intrusions from external sources. Of those external sources, 76% were adversary notifications and 24% were external partners.
- We most frequently responded to intrusions at financial services organizations (17.3%), business and professional services (13.3%), high tech (12.4%), retail and hospitality (8.6%), healthcare (8.1%), and government (8.1%). Organizations in these industries have access to a variety of sensitive data that is attractive to attackers.
- The most common initial infection vectors were exploits (38%), phishing (17%), prior compromise (15%), and stolen credentials (10%). These numbers are relatively consistent with what organizations faced in 2022.
- In cases where we could determine motivation, 52% of attackers were primarily motivated by financial gain, and 10% principally pursued espionage activities. Financially motivated activity is up from 48% in 2022, which is partially explained by a rise in ransomware and extortion cases in 2023.
- Of the 626 newly tracked malware families in 2023, the top categories include backdoors (33%), downloaders (16%), droppers (15%), credential stealers (7%) and ransomware (5%).

What do we need to do?

- Build and maintain a strong cyber defense capability with proactive threat hunting powered by strong intelligence.
- Engage with red teams to test defenses and identify gaps, and measure the time it takes security teams to identify and respond to compromises.
- Test your ability to detect the latest and most relevant malware, exploits, and initial infection vectors, and conduct regular testing for all employees such as phishing awareness.
- Use tabletop and other exercises to establish protocols, and ensure all employees involved in an incident response are ready to react—especially when it comes to being notified of a compromise externally.
- Practice sound security fundamentals such as vulnerability and exposure management, least privilege, network segmentation, and hardening.

Chinese Espionage Operations Targeting The Visibility Gap

What do I need to know?

- China-nexus (and other) attackers are increasingly targeting edge devices and platforms that traditionally lack endpoint detection and response (EDR) and other security solutions.
- By targeting these systems, as well as leveraging zero-day exploits, attackers can remain on systems for longer periods of time (persistence) and with lower risk of detection due to the gap in visibility.
- Chinese espionage groups will likely continue investing in the acquisition of zero-day exploits and platform-specific tooling to evade detection.
- Chinese espionage groups will continue to deploy custom malware ecosystems that are tailored for the device and operation at hand.

What do we need to do?

- Maintain proper patch management to mitigate the risk of exploitation of known vulnerabilities.
- For zero-day vulnerabilities, a defense-in-depth approach provides better chances of surfacing evidence of malicious activity further in the attack lifecycle.
- If an organization feels it may have been compromised, perform an investigation and conduct hunting activities within networks, including reviewing logs and scanning for indicators of compromise.
- In the event of compromise, perform a thorough and comprehensive investigation that identifies how attackers got into the environment, and how they were maintaining persistence.
- Consider implementation of security controls detailed in architecture hardening guidance provided by security vendors.

Attacker Operations Involving Zero-Days Vary Depending on Motivation

What do I need to know?

- In 2023, we tracked a combined total of 97 unique zero-day vulnerabilities exploited in-the-wild, surpassing the number tracked in 2022 by more than 50%.
- People's Republic of China cyber espionage groups were the most prolific attackers exploiting zero-days in 2023, with a heavy focus on stealth in their zero-day operations.
- Financially motivated attackers continue to embrace zero-days, aiming to infiltrate systems and steal valuable data to turn a profit.
- Espionage groups tend to prioritize stealth and long-term access, and meticulously craft exploits to minimize detection; financially motivated attackers tend to prioritize speed and efficiency, potentially sacrificing stealth for quicker returns and wider exploitation.

What do we need to do?

- A blend of policy, threat intelligence, and active monitoring can serve as an early warning system for attackers leveraging zero-day vulnerabilities.
- Have an existing incident response plan, and broad environmental monitoring to better prepare to assess the potential impact of a vulnerability on your environment.
- Layer network segmentation and logging with advanced EDR solutions for an efficient means through which investigations can be started and brought to a swift close.
- Evaluate security practices and network requirements for vendors prior to deploying hardware or software into the environment to build a quality baseline of what should be considered "normal" use.

Evolution of Phishing Among Shifting Security Controls

What do I need to know?

- Contemporary phishing techniques challenge traditional security paradigms that have focused on user education, email gateway filtering, and MFA.
- To circumvent modern security controls, attackers have begun experimenting with distributing different payload types, including LNK files and newer forms of weaponized Microsoft Office documents.
- Attackers have expanded the scope of their targeting, and are engaging on platforms beyond email such as social media, SMS messaging, and other common communications platforms.
- Attackers exploit trusted relationships and communications through techniques such as conversation hijacking, and by simply masquerading as internal users.

What do we need to do?

- Have a comprehensive detection and threat hunting strategy focused on behavioral indicators across all stages of the intrusion lifecycle.
- Initial discovery of phishing compromises can involve cloud security alerts for risky sign-in events, mailbox rule creation, suspicious MFA device registration, or internal and external users reporting suspicious emails from compromised user accounts.
- Ensure alerts are generated for suspicious activity, and review platform logs that may have recorded messages or URLs transmitted between users that could be proactively analyzed for suspicious content.

How Attackers Leverage AiTM to Overcome MFA

What do I need to know?

- The number of compromises against cloud-based identities configured with multi-factor authentication (MFA) is increasing.
- Attackers are becoming better at overcoming MFA, notably using techniques (web proxy or adversary-in-the-middle (AiTM) phishing pages) that can render MFA implementations ineffective by stealing sensitive login session tokens.
- Many organizations today still rely on security controls that do not offer token theft protection, and there is no simple solution to mitigating token theft and stolen token usage.

What do we need to do?

- Pursue a combination of AiTM-resistant MFA methods and access policies.
- Most cloud authentication services support access policies that can block logons based on organization-defined locations, device management status, or an assessment of risk based on the account's historical logon properties.
- Defenders should monitor for anomalies, such as geographically infeasible or unexpected source IP addresses, and logins originating from data centers.
- Authentication logs will record the IP address associated with phishing infrastructure as the user's source IP address, and IP address and associated User-Agent string will also be recorded when authenticating with a stolen token.

Cloud Intrusion Trends

What do I need to know?

- As enterprises continue to adopt cloud and hybrid cloud/on-premises environments, attackers have followed.
- Attackers of varying motivations are pivoting to cloud environments to target cloud-hosted data, and leverage cloud computing resources in their operations.
- Attackers are targeting weakly implemented identity management practices and credential storage to obtain legitimate credentials and circumvent MFA.

What do we need to do?

- Implement changes to authentication policies to maintain a strong security posture.
- Use commonly accepted phishing-resistant MFA methods such as certificate-based authentication and FIDO2 security keys, and phase out legacy MFA methods such as SMS, phone calls, and time-based one-time passwords.
- Consider implementing additional controls to restrict access to cloud resources to only trusted devices.

Artificial Intelligence in Red (and Purple) Team Operations

What do I need to know?

- One of the cybersecurity areas where gen AI has tremendous potential is in the field of proactive security and red team assessments.
- Mandiant red teams have used gen AI tooling for social engineering; notably to create initial drafts of malicious emails, but also to create landing pages that appear legitimate.
- Mandiant consultants have also leveraged gen AI to assist in the development of custom tooling during red team engagements.
- Mandiant teams have leveraged gen AI to enhance their understanding of various platforms, and subsequently hone in on the security aspects of those platforms.

What do we need to do?

- Leverage red teams to perform approved malicious actions, and help improve the overall security of your environments.

Download the full report.

Google Cloud

For more information, visit **cloud.google.com**.