# Mandiant Unveils M-Trends 2023 Report, Delivering Critical Threat Intelligence Directly from the Frontlines

*Global median dwell time drops to just over two weeks, reflecting the essential role partnerships and the exchange of information play in building a more resilient cyber security ecosystem*

RESTON, Va., April 18, 2023 /PRNewswire/ -- **Mandiant Inc.**, now part of Google Cloud, today released the findings of its M-Trends 2023 report. Now in its 14th year, this annual report provides timely data and expert analysis on the ever-evolving threat landscape based on Mandiant frontline investigations and remediations of high-impact cyber attacks worldwide. The new report reveals the progress organizations globally have made in strengthening defenses against increasingly sophisticated adversaries.

"M-Trends 2023 makes it clear that, while our industry is getting better at cyber security, we are combating ever evolving and increasingly sophisticated adversaries. Several trends we saw in 2021 continued in 2022, such as an increasing number of new malware families as well as rising cyber espionage from nation-state-backed actors. As a result, organizations must remain diligent and continue to enhance their cyber security posture with modern cyber defense capabilities. Ongoing validation of cyber resilience against these latest threats and testing of overall response capabilities are equally critical." – Jurgen Kutscher, VP, Mandiant Consulting at Google Cloud.

**Global Median Dwell Time Declines to Just Over Two Weeks**

According to the M-Trends 2023 report, the global median dwell time – which is calculated as the median number of days an attacker is present in a target's environment before being detected – continues to drop year-over-year down to 16 days in 2022. This is the shortest median global dwell time from all M-Trends reporting periods, with a median dwell time of 21 days in 2021.

When comparing how threats were detected, Mandiant observed a general increase in the number of organizations that were alerted by an external entity of historic or ongoing compromise. Organizations headquartered in the Americas were notified by an external entity in 55% of incidents, compared to 40% of incidents last year. This is the highest percentage of external notifications the Americas has seen over the past six years. Similarly, organizations in Europe, the Middle East and Africa (EMEA) were alerted of an intrusion by an external entity in 74% of investigations in 2022 compared to 62% in 2021.

Mandiant experts noted a decrease in the percentage of their global investigations involving ransomware between 2021 and 2022. In 2022, 18% of investigations involved ransomware compared to 23% in 2021. This represents the smallest percentage of Mandiant investigations related to ransomware since prior to 2020.

"While we don't have data that suggests there is a single cause for the slight drop in ransomware-related attacks that we observed, there have been multiple shifts in the operating environment that have likely contributed to these lower figures. These factors include, but are not limited to: ongoing government and law enforcement disruption efforts targeting ransomware services and individuals, which at minimum require actors to retool or develop new partnerships; the conflict in Ukraine; actors needing to adjust their initial access operations to a world where macros may often be disabled by default, as well as organizations potentially getting better at detecting and preventing or recovering from ransomware events at faster rates." – Sandra Joyce, VP, Mandiant Intelligence at Google Cloud.

**Cyber Espionage, Malware Families Increase Globally**

Mandiant identified extensive cyber espionage and information operations leading up to and since Russia's invasion of Ukraine on February 24, 2022. Most notably, Mandiant saw activity by UNC2589 and APT28 prior to the invasion of Ukraine, and observed more destructive cyber attacks in Ukraine during the first four months of 2022 than in the previous eight years.

In 2022, Mandiant began tracking 588 new malware families, revealing how adversaries are continuing to expand their toolsets. Of the newly tracked malware families, the top five categories consisted of backdoors (34%), downloaders (14%), droppers (11%), ransomware (7%) and launchers (5%). These categories of malware remain consistent over the years and backdoors continue to represent a little over one third of the newly tracked malware families.

In line with previous years, the most common malware family identified by Mandiant in investigations was BEACON, a multi-function backdoor. In 2022, BEACON was identified in 15% of all intrusions investigated by Mandiant and remains by far the most seen in investigations across regions. It has been used by a wide variety of threat groups tracked by Mandiant including nation state-backed threat groups attributed to China, Russia and Iran, as well as financial threat groups and over 700 UNC groups. This ubiquity is likely due to the common availability of BEACON combined with the malware's high customizability and ease of use, according to the report.

"Mandiant has investigated several intrusions carried out by newer adversaries that are becoming increasingly savvy and effective. They leverage data from underground cybercrime markets, conduct convincing social engineering schemes over voice calls and text messages, and even attempt to bribe employees to obtain access to networks. These groups pose a significant risk to organizations, even those with robust security programs, as these techniques are challenging to defend against. As organizations continue to build their security teams, infrastructure, and capabilities, protecting against these threat actors should be part of their design goals." – Charles Carmakal, CTO, Mandiant Consulting at Google Cloud

**Actioning Intelligence**

The goal of M-Trends is to arm security professionals with insights on the latest attacker activity as seen directly on the frontlines, backed by actionable intelligence to improve organizations' security postures within an evolving threat landscape. To meet this objective, Mandiant provides insight into some of the most prolific threat actors and their expanding tactics, techniques and procedures.

To further support this objective, Mandiant mapped an additional 150 Mandiant techniques to the updated MITRE ATT&CK® framework, bringing the total to 2,300+ Mandiant techniques and subsequent findings associated with the ATT&CK framework. Organizations should prioritize which security measures to implement based on the likelihood of a specific technique being used during an intrusion.

Additional takeaways from M-Trends 2023 Report include:

- **Infection vector:** For the third year in a row, exploits remained the most leveraged initial infection vector used by adversaries at 32%. While this was a decrease from the 37% of intrusions identified in 2021, exploits remained a critical tool for adversaries to use against their targets. Phishing returned as the second most utilized vector, representing 22% of intrusions as compared to 12% in 2021.
- **Target industries impacted:** Response efforts for government-related organizations captured 25% of all investigations, compared to 9% in 2021. This primarily reflects Mandiant's investigative support of cyber threat activity which targeted Ukraine. The next four most targeted industries from 2022 are consistent with what Mandiant experts observed in 2021, with business & professional services, financial, high tech, and healthcare industries being favored by adversaries. These industries remain attractive targets for both financially and espionage motivated actors.
- **Credential theft**: Mandiant investigations uncovered an increased prevalence in both the use of widespread information stealer malware and credential purchasing in 2022 when compared to previous years. In many cases, investigations identified that credentials were likely stolen outside of the organization's environment and then used against the organization, potentially due to reused passwords or use of personal accounts on corporate devices.
- **Data theft:** Mandiant experts identified that in 40% of intrusions in 2022, adversaries prioritized data theft. Mandiant defenders have observed threat actors attempting to steal, or successfully completing data theft operations more often in 2022 compared to previous years.
- **North Korea's Use of Crypto:** Alongside traditional intelligence collection missions and disruptive attacks, in 2022, Democratic People's Republic of Korea operators showed more interest in stealing—and using—cryptocurrency. These operations have been highly lucrative and will likely continue unabated throughout 2023. For more on how North Korean threat actors are using cybercrime as a way to fund their espionage operations, check out Mandiant's APT43 report.

**M-Trends 2023 Methodology:**

The metrics reported in M-Trends 2023 are based on Mandiant Consulting Investigations of targeted attack activity between January 1, 2022 and December 31, 2022. The intelligence gleaned has been sanitized to protect the identities of targets and their data.

**Resources:**

- M-Trends 2023 Report: www.mandiant.com/m-trends
- Blog: www.mandiant.com/resources/blog/m-trends-2023

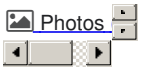
**About Mandiant**
Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now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

**About Google Cloud**
Google Cloud accelerates every organization's ability to digitally transform its business. We deliver enterprise-grade solutions that leverage Google's cutting-edge technology – all on the cleanest cloud in the industry. Customers in more than 200 countries and territories turn to Google Cloud as their trusted partner to enable growth and solve their most critical business problems.

SOURCE Mandiant Inc.

For further information: Mandiant-PR@google.com

---

Additional assets available online: 


https://www.googlecloudpresscorner.com/2023-04-18-Mandiant-Unveils-M-Trends-2023-Report,-Delivering-Critical-Threat-Intelligence-Directly-from-the-Frontlines