Tucker Eklund (tce2113@columbia.edu)
Mr. Gibbons
Cyber-Threat Intelligence
13 August 2025

2025 M-Trends Report

Issue Presented- To provide a summary of Google Security's Mandiant M-Trends 2025 Report

Short Answer- The M-Trends 2025 Report details how advanced, highly opportunistic threats in cyberspace exploit recurring vulnerabilities and newer technologies, changing the course of security initiatives and challenges.

Background- Through Mandiant's annual M-Trends report, findings relating to security education, recent attacker tactics or threats, remediation effort support, and further developments in security transformation initiatives are shared with the larger cybersecurity community. The important knowledge in the report is shared to highlight Mandiant's dedication to serving those vital to the defense of various organizations.

Discussion- Here's a summary of some of the key points in the M-Trends Report:

- **Iranian threat landscape:** Since Middle Eastern tensions have recently been escalating, Mandiant reports heightened escalation of the scale of Iran-nexus threat actor operations. They, including nationalist-hacktivist organizations, have launched continuous operations using more than twenty proprietary malware families against relevant strategic and operational targets, with a more focused lens on Israeli targets. Iranian state actors use a variety of approaches to enlarge their capabilities, including upping a custom arsenal of malware in full-scale operations. The detection of these malicious attacks has been limited by developed measures to evade detection, including more use of cloud infrastructure and more traditional evasion tools. Social engineering schemes have also been utilized to effectively complete strategic and national objectives.
- **Insider threats from the Democratic People's Republic of Korea:** Due to widespread sanctions from the West against the DPRK since 2003 that intensified in 2016, financial motivations for funding the nation's national interests have fueled much of their campaigns. Funds have been sourced from the sale of illegal firearms and deadly weapons, front companies in global regions, or frequent outright theft. In 2016, hundreds of millions of dollars (USD) were stolen through false SWIFT transactions and in 2024, cryptocurrency had become more of a primary target. For Western companies, threats have risen from North Koreans posing as remote IT contractors for hire. Employment of these "contractors" has plagued high-tech companies, with these agents funneling capital gained from their salaries back home to support national interests. In particular, lots of these operations have made use of other 3rd party accomplices and stolen identities as well. Beyond finance, threats from the DPRK can include greater risks of espionage, business disruption, user data theft, and other criminal means of extortion.
- **Infostealer Malware:** This class of malware broadly includes capabilities of theft and collection of sensitive or private user data such as cookies, crypto-currency wallets, and important credentials. Mandiant's research has found greater exploitation of user credentials in 2024 than in previous years. This rise can be attributed to these infostealers from large-scale cybercrime communities and organizations. These are not new threats by any means, moreso the renewed focus on infostealers shows how there could be a pretty large change in how cybercriminals use and monetize stolen data.
- **Cryptocurrency and Web3 Threats resulting from growing blockchain technology:** In a very diverse set of operations, from financing terrorism to money laundering, malicious actors have involved decentralized next-generation technology. Mandiant has highlighted a recent uptrend in targeting cryptocurrency for the past couple of years. It has offered significant advantages to many dangerous organizations, like fast adoption, increased cybersecurity strength and security posture, as well as the inherent difficulty in disrupting these campaigns. The emergent Web3 technology really isn't all that new, though it still presents complex challenges to organizations adopting them or having to deal with them regardless. In the finance industry, blockchains have been implemented into many platforms, which has created new products and caused an expansion upon existing regulations. With further adoption into commercial industries, cybercriminals present an additional need for security and protection of digital assets.
- **Data Repository Threats:** Although great resources are used in increasing perimeter-defenses against outsider threats, unsecured data repositories are being targeted, mostly from a lack of rudimentary security hygiene. Commonly, sensitive data relating to user credentials, finances, or intellectual property is found within these repositories. This creates a highly exploitable malicious attack pathway, making it necessary to put more resources into an internal data-centric security approach rather than focusing on perimeters. Furthermore, more barriers placed between perimeter and interior defenses would not only limit access from foreign threats, but would also create additional opportunities for security teams to detect misuse and for incident response teams to quickly understand security failures.

Conclusion- Evolving cyber threats have blended foreign state-run campaigns with other criminal tactics. As seen with the DPRK and Iran leveraging their developed skills in advanced malware and social engineering, infostealers, crypto-exploitation, and data repository breaches, Mandiant has to maintain specific focus on a couple of goals. That includes continuous monitoring, defensive adaptations, and cross-sector collaboration, all being necessary to counter ever-changing risks in the landscape.

Recommendations- None, for educational purposes and the establishment of new security standards only.