Threat Intelligence Evolution: Strategies for Safeguarding Government and Critical Infrastructure

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Lookout, January 2024

Threats to IT infrastructure and individuals are becoming more sophisticated and harder to identify, especially on mobile devices. Research shows major advanced persistent threat (APT) and nation state actors are now using advanced phishing techniques and multi-factor authentication (MFA) attacks including SIM swapping approaches through mobile to compromise thousands of accounts. Doing so enables threat actors to seamlessly access sensitive data, which can trigger downstream supply chain attacks and have major national security implications.

In a recent roundtable discussion co-hosted by the Advanced Technology Academic Research Center (ATARC) and Lookout, Federal experts discussed the mobile threat landscape and strategies to safeguard data across our nation's critical infrastructure.

Current Threat Landscape

According to Lookout, 60% of mobile devices run on vulnerable operating systems. Anything from an insecure mobile connection to a compromised email can introduce risk to government data. Unfortunately, the practice of mobile security is not prioritized enough to meet the rise in both modern endpoint utilization in our daily lives and malicious activity targeting these endpoints.

Nation state adversaries are seizing this opportunity to use the mobile vector for malicious gain. Some applications, like Pinduoduo, prohibited the removal of their app from user's devices, injected code into and exfiltrated data from third-party applications while beaconing back to China. Analysts have also identified subtle versions of malware installed with applications, but that are later removed during app updates. This allows adversaries to constantly test defenses and gain access to information.

The number of cyber mercenaries, also known as hackers for hire, are on the rise and are becoming harder to catch. Entire chains of vulnerabilities within both apps and operating systems make it increasingly difficult to track vulnerabilities. Because mobile devices contain so many endpoints, adversaries can easily gain access to devices and the data within them. One of the ways they gain access to data is through a technical proxy, such as found in the threat actor PoisionCarp's Moonshine malware. Once the application is on a device, adversaries can broker a connection to the device no matter what network the device is connected to. Known foreign adversarial groups are using these capabilities for surveillance purposes and to target specific individuals to gain access to personal finances.

Adversaries are also becoming more proficient with executing social engineering campaigns, which go beyond email phishing scams. Malicious actors are using social media to build personas and gain the trust of individuals who have access to information. Social media troll farms are also being used to interfere in political opinions, influence public sentiment, and spread misinformation.

Mobile applications are largely unregulated, and roundtable participants agree that mobile carriers should be doing more in regards to SIM swap attacks. Networks possess the ability to authenticate and authorize the SIM cards connecting to their networks, but unfortunately they are not doing this on a regular basis. This is evident in highly successful campaigns by 0ktapus, Scattered Spider, and Lapsus$.

There is also little official guidance on securing mobile devices from the Federal government. In fact, current Federal policies do not provide a definition for what constitutes as a 'mobile device'. This is leaving agencies in the lurch. Despite the lack of formal guidance, technology leaders at the roundtable are hyper aware of the risks associated with mobile, and are making decisions based on what's best for their agency mission.

For some, this means taking on the risk of using certain apps to ensure functionality and productivity. Some agencies receive blowback from end users when new security controls are put in place simply because the controls limit device functionality. Roundtable participants also emphasized the importance of educating end users on making risk-based decisions when choosing applications in the app store, especially since enterprise level security is not currently available.

Securing Mobile Devices

In order to work, social media platforms inherently collect massive amounts of data from the end user. What happens to this data is the real question. For some applications, such as TikTok, it's unclear what safeguards, if any, are in place to protect user's data. Subject to the Chinese National Intelligence Law, these companies are required to cooperate with the Chinese government with state intelligence efforts, essentially giving access to the data collected by Chinese based applications, like TikTok and Temu. This creates major cybersecurity concerns over espionage, data theft and supply chain risk, as well as concerns over U.S. national security and critical infrastructure sectors such as energy, healthcare and transportation systems. Evidence of these exploited vulnerabilities was recently cited in CISA's "People's Republic of China Cyber Threat" report.

Safeguarding Strategies

Securing physical devices is critical, but so is securing data. Panelists point to the zero trust security framework to safeguard devices and data, but agencies struggle to first identify the data that needs protecting. However, roundtable participants note that capabilities do exist to help agencies understand who is accessing their data, and how they're able to access it.

> **"Zero Trust is based on understanding what data needs to be protected. That's our biggest issue."**

Panelists also discuss the varying risk levels of accessing data from different devices. Agencies could make mobile devices a higher security risk, which with the telemetry from other sources tip the confidence score and prevent mobile device users from accessing certain information. However, this becomes more challenging with bring-your-own-device (BYOD). Panelists are resigned to the fact that no matter how many protections are in place, users will find ways around them. The evolution of mobile threat defense (MTD) capabilities was identified as a way to balance end user privacy while providing security on their devices, working with mobile device managers (MDMs) to add a layer of risk-based protection.

The best way to safeguard infrastructure is to educate non-technology participants, such as decision-makers and attorneys, on the complexity of safeguarding infrastructure amidst a rapidly changing environment.

> **"Cybersecurity is a shared responsibility from the CEO to the end user."**

Learn more at https://www.lookout.com/