Washington D.C. Cyber Threat Landscape

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Zimperium in October 2023

In the last few years, the prevalence and intensity of mobile cyber threats has increased. Mobile security is now at the forefront of conversation as federal agencies work to secure mobile devices and networks from threats. The Advanced Technology Academic Research Center (ATARC) and Zimperium hosted a roundtable for federal experts to discuss the rapidly expanding mobile cyber threat landscape.

Background

The cyber landscape has shifted and expanded exponentially over the past few decades.. According to Zimperium, there are two fundamental trends driving the mobile cyber threat landscape. The first is the pervasiveness of mobile devices in society. Everyone has at least one mobile device, and, in many cases, more than one. The second aspect is the way mobile devices are being used. Mobile devices are driving how we communicate and access information, and they are certainly a driving force in the economy.

Due to the prevalence of mobile devices and our reliance on them, threat actors are targeting mobile devices much more frequently. Compared to a few years ago, mobile devices now contain the same information as a laptop or desktop computer, which not only expands the attack surface but also makes mobile devices a prime entry point.

> **"There is no such thing as peace or war. Our adversaries are using their capabilities we would typically associate with war during peace time."**

Agencies are continuously pivoting, learning, and collaborating to ensure devices and networks remain protected from adversaries and threat actors. As such, federal guidelines have been released around mobile security, including:

- **OMB 23-13** - This memorandum banned TikTok and ByteDance apps and services on government devices.
- **OMB 22-01** - This memorandum refers to Executive Order 14028 directing agencies to adopt robust Endpoint Detection and Response (EDR) solutions. This memo acknowledged and included mobile devices as an endpoint.
- **NIST SP800-124r2** - NIST published Guidelines for Managing the Security of Mobile Devices in the Enterprises, which includes endpoint management and mobility management recommendations and best practices.
    - **4.2.3 Mobile Threat Defense** - This section highlights the need to identify risk and threats across vectors in a way that acknowledges them on devices.
    - **4.2.4 Mobile App Vetting** - This section discusses best practices with vetting mobile applications.

Challenges with Mobility

Panelists openly discussed some of the biggest mobile challenges facing their agencies:

- Protecting against smishing and phishing attempts
- Balancing user expectations with proper security
- Offering the latest technology to end users
- Communicating security needs to leadership

Because mobile devices are an integral part of daily life, panelists note that most people are unaware of how easy it is to pick up malware and spyware on mobile devices. In many cases, people with affected mobile devices are unaware they've been compromised.

"We've trained people to trust these devices, because they are useful tools. A hammer, like any tool, can build something, but it can also destroy something."

Easy Entry Point for Malware & Spyware

Attackers are becoming more sophisticated with their methods, but phishing schemes on mobile devices are the biggest driver. One panelist referred to a recent study which indicated that the generation most susceptible to phishing or smishing are Millennials and Gen Z. Because younger generations are digital natives, they're more likely to trust technology and tend to not be as cautious when taking action online.

Malware downloaded from third-party app stores is also a major challenge with mobile devices because these third-party stores have fewer, if any, security checks before an app is listed in the store. Currently, the threats from third-party app stores occur on Android systems; however, Apple will begin to see these issues once they begin supporting third-party apps stores in 2024.

But malware attacks aren't always delivered via complex delivery systems. They can occur simply by clicking on a link in a seemingly innocuous email or text, connecting to an open network at a coffee shop, or scanning a QR code at a restaurant. What people are less aware of are the consequences of these routine, seemingly innocent actions. Once on a device, malware can take complete control of a phone and camera, take contacts and credit card numbers, send text messages and emails, and record passwords. Malware is also capable of turning a phone into bugs in order to listen into private conversations. Once threat actors gain access, malware, including spyware, can quickly spread through entire networks.

Using personal devices to conduct government business is another issue agencies must pay attention to because there is significant risk to organizations if a personal phone is compromised. There's also risk beyond just compromised phones and malicious intent. For example, agencies should have insight into the mobile apps on those devices and should question what data is collected, the purpose of collecting data, who collects the data, and where the data is being stored.

People will go out of their way to bypass security measures, which is a reality IT must contend with. The solution from a technical perspective is to put up guardrails, but a balance must be struck between security and usability.

Leveraging Technology to Stay Ahead of Attacks

While there should be preventative measures in place with the creation of management profiles and standards, agencies should also utilize technology tools to help identify risk and automate interventions when necessary.

Some roundtable participants consider AI and machine learning as mere tools that will make threats more prevalent and sophisticated. As such, agencies should consider using these tools to take a more aggressive posture against threat actors and adversaries. For one panelist, quantum computing is the more challenging threat facing the federal government.

When quantum computing becomes mainstream, the government will likely lose its encryption ability. Since World War II, encryption has been used to encode things no one else can see. There is a potential within the next decade that adversaries will be able to use quantum computing to interfere with traditional means of encryption. As such, technologists must identify the next level of encryption in preparation of this reality.

Agencies should talk more about taking advantage of tools capable of staying ahead of threats and less about the technical elements of AI, machine learning, and quantum computing. In an ideal world, adversaries would confront something unanticipated if they penetrated government networks. Staying imaginative, innovative, and ahead of technology is the goal of technologists in government.

Resources & Leadership Buy-In

Mobile security is still a relatively new subject. Even veteran technologists are unfamiliar with mobile security protocols and innovative solutions. Many continue to rely on the strategic marketing tactics of large mobile suppliers that tout the safety and security of mobile devices.
Even then, the lack of visibility into the supply chain is a challenge facing the government today.

As threats to mobile infrastructure continue to increase, gaining the buy-in from senior leaders is critically important to ensure agencies are adequately prepared for zero-day attacks. IT leaders should attempt to help senior leadership visualize and contextualize cyber threats so they better understand the consequences of inaction and underfunding. Communicating effectively to decision makers is as important as technical competence.

IT leaders must continually ask forward-thinking questions about where the next vulnerability could be. Imagining where vulnerabilities are in an organization can help identify gaps, anticipate where adversaries might attack, and help prepare the organization from emerging threats. Painting a complete picture of potential scenarios is a way to help contextualize the importance of cyber security to senior leaders.