

M+E

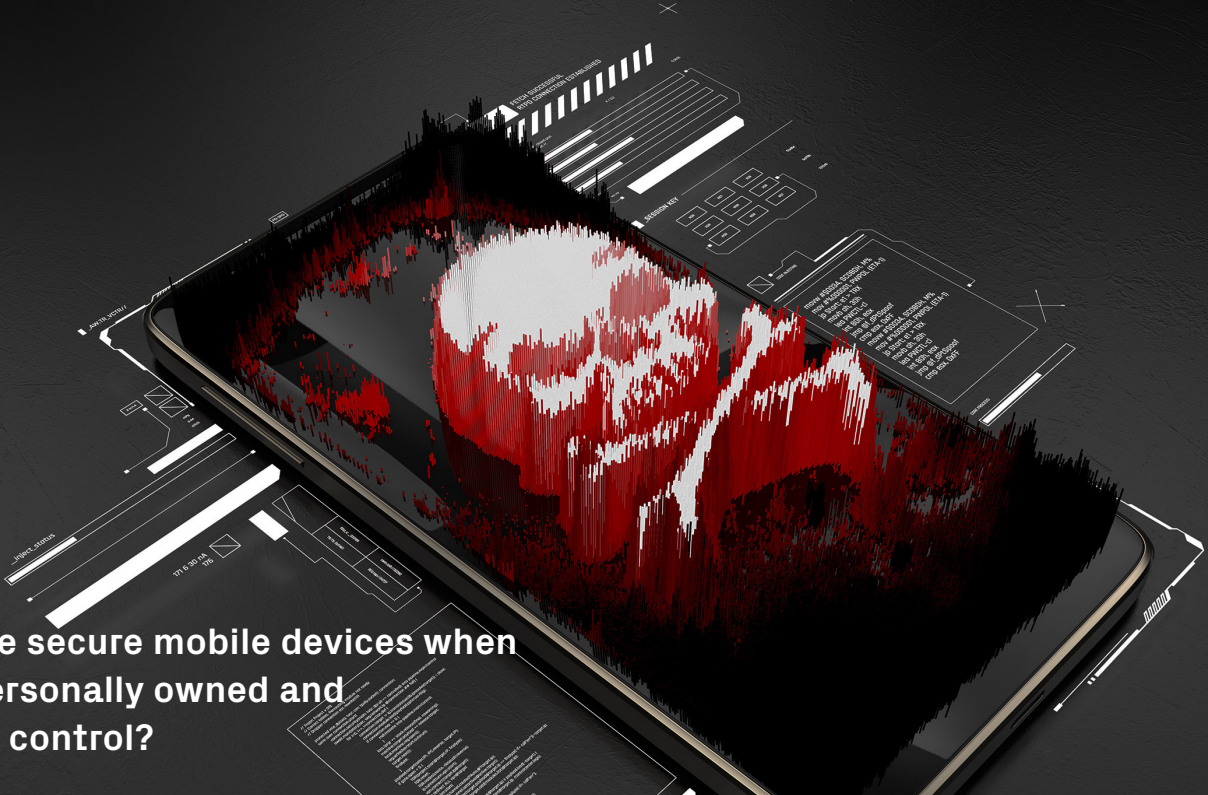
JOURNAL

Charting the Metaverse

The metaverse
will prove
transformative
for M&E.
But only when
the entire
industry gets
on board.

22.01

MOBILE DEVICE EVOLUTION BRINGS EVOLVED THREATS



How do we secure mobile devices when they're personally owned and out of our control?

ABSTRACT: Even putting aside social networking, games, and other common features of even the lowest cost phones, we use them for communication, voice, and text, as our personal organizer, mobile productivity, even to monitor and maintain fitness and health. They are invaluable tools. But with these evolved features come new threats. We look at how to confront them.

By Sean Kalinich, Cybersecurity Architect, Richey May Advisory

MESA Platinum Member

Although not the first smartphone to be launched or mainstream, the iPhone arguably was the first one to capture the consumer, as well as the enterprise, imagination. Looking back at the launch, I still do not believe that anyone really envisioned the widespread adoption, power, and features of today's modern mobile device. Even giants such as Blackberry and Windows Mobile were eclipsed by the potential that the iPhone, and later Android, showed. Now for many, the thought of going through work and personal life without your phone is unimaginable.

Where would most of us be without our phones? Mobile carriers have moved to provide data plans to meet the massive consumption of content that the average user

YOU MIGHT NOT BE ABLE TO PROTECT OR CONTROL the endpoints, yet, but you can protect your environments and data by implementing stricter controls against the evolving attack styles.

needs daily. Bring back gaming and social media and the usage goes through the roof. It would not be an exaggeration to say that most people do not leave their homes without their phone safely in hand. It is a part of their life in an unconscious way.

Although more and more people are gobbling up data and the latest and greatest phones the market can throw out, businesses simply cannot keep up. The days of just issuing a mobile phone and maintaining the plan are pretty much gone. The costs associated with having company issued phones is not truly financially sound for most companies.

This has ushered in the days of the dual-use device. It is personally owned and maintained but is also used to access business accounts and information. It made sense, most people will have a phone that can access this data and they often already have a data plan that will support it as well. Now the problem is not how do you support mobile communication in a business organization; it has become how do you support and secure it?

THE SUPPORT AND SECURITY

In large organizations, the support is little more than a monthly stipend that helps offset the end user cost. It helps, makes the people now using their own personal equipment feel a little better, and all is well. On the security side you have few options. Although you can control the device and perhaps limit the exposure of corporate data with things like AirWatch, Intune, Knox, Apple MDM etc., there is not much that can be done to truly protect the device. The mobile anti-malware space is simply not mature enough to protect endpoints at this stage while mobile malware is evolving by leaps and bounds. Mobile malware is outpacing protection in a way we have not seen since the introduction of ransomware for the PC.

Currently there are roughly three anti-malware apps for mobile devices that can actually provide good protection. McAfee has one, SentinelOne has another, and

Microsoft has the third. Of these three, one is generally available to consumers (McAfee). Yes, there are other vendors on the market, but they are lacking in certain areas in terms of protection features.

Looking over the list of options, most mobile anti-malware apps do not do more than scan files and compare them to a signature file to see if they are overtly malicious. There are no checks for pivots in memory, few checks for calls to command-and-control sites or pivots by downloaders, and none of them have options to check on an applications permission's requests. Of the three that are out there with more advanced protections; Sentinel One's offering is in the early stages having just been released this year and is relatively untested, Microsoft's Mobile offering is tied to their MS365 licensing and is not the simplest thing to set up or even deploy. McAfee's offering tends to be a bit buggy, and we keep seeing features being removed while costs go up.

THE THREATS

Now compare this to the list of malware that security researchers have seen for the mobile device. There are already over 60 identified apps in the Google Play Store and Apple App Store that leverage innocuous looking apps to get by the gate keeper processes. These apps are disguised as everything from games to fitness/workout apps to mobile security and privacy apps. Once an unsuspecting user downloads and installs the app, there is a trigger to alert the user that the app needs some permissions. The permission request often references access to system controlling features like the Accessibility Services inside Android devices. And since users have become desensitized to permission request dialogs, they often just click past the screen and their device is now owned regardless of the anti-malware type in place on the device.



Sean Kalinich is cybersecurity architect for Richey May Advisory and is a strategic and technical security professional focused building and supporting organizations through refining the security culture, identifying changes in the threat landscape, and assisting in building a secure infrastructure (including secure distributed infrastructures). skalinich@richemay.com @decryptedtech

Once the correct permission level is achieved, the app does an inventory, looks for anti-malware and then calls out to its command-and-control servers to execute phase two, the downloading and installation of the actual malware payload. This payload varies between different threat groups, but usually consists of a persistence mechanism, backdoor or remote-control tools as well as keyloggers, or other credential capture tools.

What is clear is that antimalware developers are either not tracking these developments or ignoring them while malware development teams are doing their research, identifying mobile user behavior, and exploiting it. The numbers tell a very clear story, banking malware, with the capabilities listed above, more than 60 apps identified in 2022 alone and with total installations north of one million. One information collection app, at the time of its removal from the Google Play store, had over 46 million installations.

NEW THREAT TACTICS

The stage is set, the tools are built, and the props are ready. Threat group tactics, including initial brokers, are moving away from pounding on the front door. They have identified that in many industries, like the content creation industry, there simply is no front door to pound on. They must look for the people holding the keys to an environment that is not easy to find. In simple terms, they want user accounts and credentials. The best way to do this is target services like MS365 and endpoints (including mobile devices). The tactics here are simple, it is typically going to be via drive-by and phishing (spear or cast net), including vishing and smishing. Identifying a target is exceptionally simple with available tools like Facebook, Instagram, Twitter, LinkedIn, and corporate websites. Spend an hour combing those sites or using Google Dorking and you have a laundry list of targets for your efforts. Craft your phishing email and off you go.

In your typical corporate environment, heavy anti-phishing tools and training can make the effect of this limited, but as we know from incident tracking it still happens repeatedly hundreds of times each year. So, to protect user accounts, corporations implement multi-factor authentication and/or utilize services like Okta, PingOne, Duo etc. Sounds like problem solved right? Well not really, and there is a giant glaring hole in the invisible fence here, it is the mobile device. We know from recent threat intelligence that threat groups are going after personal accounts and devices (Lapsus\$ is an example). We have seen evidence of attempts to thwart and compromise MFA and access brokers like Okta through MFA spamming or simply through users not paying attention when a request comes in. These tactics are effective, but what happens when we combine everything we have talked about?

The APT/threat group targets the individual(s) they have identified via OSINT, they target them with a phishing campaign including smishing to get to the mobile device. The capture of credentials is completed, but they have an MFA barrier to deal with. So, they pivot to malware, like the banking and financial malware we talked about earlier, that abuses core systems like the accessibility services on the mobile device. Now they have the credentials and via the new permissions they can capture and respond to MFA queries

as the accessibility services allow them to capture and respond via internal systems including the potential to replay biometric data stored on the device like a fingerprint. The circle of life is complete. By compromising the mobile device, you can bypass many conditional access policies. If you compromise both the mobile device (phone) and a laptop that is a BYOD device, you are golden. This tactic is not farfetched as we have seen indications that groups are moving in this direction already based on existing and past successful campaigns. The effectiveness of this type of attack is insane, it has massive potential to work against even hardened targets where awareness and tools sets are very capable. In highly distributed environments, like the content creation industry and many small and medium sized businesses, it is a massive threat. One creation partner compromise using the tactics listed above and you have not only put your content at risk, but also have a potential supply chain attack depending on the type of content being delivered.

SHIFTING BATTLEFIELDS

The security battle has shifted from the old siege tactics where attackers throw themselves at the walls. It was always going to do so, but the pandemic pushed up the timeline significantly. Now the fight is to secure the endpoint and the user account. This fight is not just a laptop or home use desktop though. It is also the most exposed device and one with the largest BYOD footprint, the phone and tablet. Until a proper way is found to secure these exposed devices all industries are at risk, right now the targets are banks and fintech, but the content creation industry may also be at an even more elevated risk due to its highly distributed nature and exposure.

This is not to say abandon all hope ye who enter, there are still steps that can and should be taken to offset the risk. Organizations that leverage third parties should always limit any outside access to content/data storage. Malware scans of consumption content (video, audio, and static images) as well as vulnerability and malware scans of any code-based content should be performed during and after transfer of the content. Additionally, implementing least privilege style access and controls are always a good option. Requiring the use of trusted IP ranges and/or a VPN connection to storage and/or tools can help as well. Lastly enable the monitoring of sign-ins for risk based on time, type of access and what is done in the environment. Then you can combine these efforts with policies that block user access if there is a violation of any of them. It is always better to annoy one person (or company) than risk the impact of an incident. You may also need to change current partner agreements to include having protection for mobile devices like phones and tablets.

In a highly distributed work environments, like the content creation industry, you will need to communicate these changes in advance so that your partners are aware, but do not shy away from enforcing them. You might not be able to protect or control the endpoints, yet, but you can protect your environments and data by implementing stricter controls against the evolving attack styles. ■

Who Hollywood Calls When They're Hacked

We assess risk across your holistic tech stack and customize solutions to keep your assets safe.

Our deep industry knowledge means we are uniquely capable of anticipating your needs to achieve your strategic objectives. We are intimately familiar with IT operations and software development standards. Our broad spectrum of services means we can leverage the expertise of credentialed data privacy, cybersecurity and experts focused on business and IT risk, helping you thoroughly understand your risks and develop the appropriate mitigation efforts to reduce risk and maximize investments in people, process and technology improvements.

Roundtables for an opportunity to engage with your industry peers to exchange ideas and best practices in a facilitated, confidential, group discussion.

REGISTER HERE:

<https://us02web.zoom.us/meeting/register/tZ0lf-uvqTspHdJLugzr44P-A6VZat4mDxhl>

Contact us for a holistic tech stack that works across your entire enterprise.



Christian Calson

Business Development Director,
Media & Entertainment

Christian@richeymay.com
310.945.6284



info@richeymay.com



www.richeymay.com



Denver HQ | Charlotte | Los Angeles
Salt Lake City | Grand Cayman

