Attack Archetype

Mobile Device Compromise

Internews
# Table of Contents

- Mobile Device Compromise ................................................. 4
- Types of Attack .............................................................. 4
- Targeted Individuals and Organizations ............................... 5
- Social, Political, and Economic Context ............................... 5
- Community Context .......................................................... 6
- Attack Impact ................................................................. 6
- Process of the Attack .......................................................... 7
- Prevention ..................................................................... 7
Mobile Device Compromise

This type of attack targets mobile phones or tablets. It can be carried out remotely in an identical manner to a standard spear-phishing attack, where the victim clicks a link. In these instances, the link may be delivered via an SMS (smishing attack) or via another service or messaging app. In a parallel to a standard malware attack, the victim may install the malicious app themselves either from an app store or from side loading an app on their own.

Beyond these types of remote attacks, if the adversary has physical access to the device, they may install a software or hardware implant directly. This scenario can happen if the victim has been detained by police or military and the device has been confiscated for any period of time. Essentially, times when the device is out of the possession of the victim can be the moment when hardware or software on the device are compromised.

Types of Attack

The two main ways to categorize a mobile device compromise is whether the attack was carried out remotely or with physical access to the device. With regards to remote attacks, other than the attack targeting a mobile device rather than a desktop or laptop computer, the primary differentiation is that the method of delivery of the spear-phish is via a short message rather than the more traditional email based attack. These can be delivered via SMS as well as a social media app or a messenger app. In the latter cases, most of these services and apps have privacy features that can restrict who can send messages to the mobile device based
likely to target organizations outside of the critical infrastructure sectors. The most frequently targeted sector has been non-governmental organizations (NGOs), such as advocacy groups, human rights organizations, nonprofit organizations, and think tanks focused on public policy, international affairs, or security.”

Social, Political, and Economic Context

The context around a particular mobile device compromise can be used to determine the adversary-victim relationship. According to the Diamond Model of intrusion analysis, this relationship is the social-political axis of the diamond. There are two main components of an attack that this context can help inform. The first is the motivating factors behind the attack. There may be an event that has occurred within the region or area within which the victim operates. Additionally, the adversary may be seeking to suppress information or silence speech about a particular event. Alternatively, the goal may be to steal information from the victim to be used at a later point in time for intimidation, harassment, doxxing, or influence operations. Separated somewhat from motivating factors, the second component of an attack that context can help inform is the topic used in the lure itself, if the method of delivery is via a link in a message. If there is a persistent, long-term adversary relationship with the victim, an event can be used to make the text of a message more enticing.

Targeted Individuals and Organizations

Mobile device compromise attacks typically affect one or more individuals from nearly any type of organization, but according to the 2020 Microsoft Digital Defense Report, “nation state activity is significantly more

---

1 https://blog.checkpoint.com/2019/03/13/mobile-supply-chain-attacks-are-more-than-just-an-annoyance/


**Community Context**

Careful attention to and communication about mobile device compromises can help prevent further attacks once one has been identified. If one organization or individual within a community is targeted by a particular attack, other related individuals or organizations may be targeted by the same adversary at the same time or shortly afterwards. For example, campaigns in the real world are often observed to target multiple individuals or organizations with similar roles. If the journalistic focus, or beat, of journalists from different organizations is the same, those different individuals may be targeted by a single malware campaign from one adversary. Similarly, if the focus of a set of civil society organizations are the same or similar, it follows that they are often targeted by the same set of adversaries using the same techniques all in a single campaign. It’s critical for organizations and individuals within spheres of civil society to communicate amongst one another about attacks that are occurring. This can include sharing of malicious links and locations where a particular malicious app was downloaded or installed from. This can help detect and identify new attacks and prepare targets to be ready when one arrives.

In the case of physical device access and subsequent tampering with the hardware or software of the device, sharing with peers in the community where, when, and how it happened can help others avoid or at least prepare for that same situation.

**Attack Impact**

The impact of a mobile device compromise can be severe if undetected. Malicious app capabilities with the goal of avoiding detection can allow an adversary to maintain access to the victim’s mobile device for long periods of time. Over the course of this, the adversary can download files and data from the device, monitor the victim’s actions, and take screenshots, among many other potential actions.

Some of the most worrisome impacts of an attack can include, but are not limited to, the following:

- Web inject changes what the victim sees when they visit a legitimate website.
- Files and data are downloaded from the victim’s mobile device.
- Contact lists can be accessed or modified.
- Malicious messages can be sent to contacts using the victim’s device.
- Victim’s files or data are modified by the adversary.
- Audio and video from the microphone and camera on the victim’s device are recorded surreptitiously.
Process of the Attack

The most dangerous and invasive of the types of mobile device compromise described above is where the adversary has had physical access to the device. There are very sophisticated malware implants that can be used on a mobile device, but these are not strictly needed to carry out a successful attack. There is an entire category of malware called stalkerware or spouseware which is essentially commercial, over the counter software. This software is definitely in a grey area morally, but is widely available and legal.

An attack of this type that leverages stalkerware along with physical access to the device may progress something like this:

- The victim is stopped at a border crossing when returning to their home country.
- The border guards demand to examine the Android mobile device.
- They require that the victim unlock the device.
- The device is then taken to a separate room out of view of the victim.
- The device is put into developer mode
- A malicious APK is side loaded on the device.
- The device is returned to the victim.
- The victim is allowed to continue on their journey.
- In the background, on the device, images from the device’s camera storage are downloaded by the adversary.


Prevention

Because this type of attack is a special case of spear-phishing or malware attack, the same prevention methods and security controls used for those types of attacks can be used here. In addition to these standard types of prevention, because a mobile device compromise can involve physical access to a device, additional prevention measures can be appropriate. First and foremost, always use a PIN, password, passcode, or other device authentication method. This can prevent access when the mobile device is not on the owner’s person. Mitigating the damage when this type of compromise occurs is also important. One thing to make sure of is that the device is backed up in case it must be wiped due to tampering. Another is to install an app or configure a device feature that can wipe the device remotely. This and other mobile device security controls can be found here and here.
