THE HIJACKING OF SMARTPHONE CAMERAS AND MICROPHONES

PRIVORO®

Smartphone cameras and microphones act as the eyes and ears of the digital age, capable of capturing the smallest audio and visual details in high-definition clarity. Unfortunately, threat actors have demonstrated the ability to hijack these smartphone components, using them to gain valuable insights about targeted government agencies and enterprises. Given the failure of existing security measures to detect or stop this new breed of attack, organizations must look beyond software-based solutions to protect their most valuable data.

THE NEW SURVEILLANCE BATTLEFIELD

The adoption of smartphones began to take off in 2007, and it didn't take long for intelligence agencies, cyber-arm s dealers and threat actors to see the enormous surveillance potential of always-connected, ever-present devices containing integrated cameras and microphones. As early as 2012, if not before, surveillants achieved the ability to remotely hijack smartphone cameras and microphones through multi-stage malware suites. These tools provide the ability to capture audio, photos or videos for exfiltration and even perform live surveillance, all without alerting the user or leaving a trace.

In contrast to physical surveillance or the placement of bugs and hidden cameras, smartphone surveillance offers a number of key benefits for surveillants:

- **Obfuscation:** Malware makes it easy to hide both the presence and identity of those doing the spying.
- **Ubiquity:** Smartphones constantly accompany targets wherever they go, from their homes to their workplaces.
- **Reusability**: The same piece of malware can get used repeatedly for a large number of targets and attack vectors.

THE HISTORY OF SMARTPHONE SURVEILLANCE

DROPOUTJEEP development
One year after the release of the iPhone, the NSA catalogs a planned exploit for the device capable of microphone activation and camera capture via close access methods, with stated plans to develop a remote installation capability.

RCSAndroid in the wild
A commercial malware suite for Android that is capable of recording audio (using the smartphone's microphone) and capturing photos (using the front and rear cameras) begins to appear in the wild.

AndroRAT binder
On the underground market, a binder begins to be sold for what is perhaps the first remote access Trojan (RAT) for Android capable of using a device's camera and micro-phone, giving users a way of repackaging legitimate apps with the RAT.

Targeted Pegasus attack
Ahmed Mansoor, an internationally recognized human rights activist, is targeted with what is likely the first known attack that uses malware capable of employing an iPhone's camera and micro-phone.

THE FOUR TYPES OF SMARTPHONE DATA

DATA AT REST
Data physically stored in the smartphone's memory.

DATA IN TRANSIT
Data transmitted to or from the smartphone.

DATA IN USE
Data actively utilized by the smartphone's processes.

DATA IN VICINITY
Data created in the presence of the smartphone.

THE GOAL: DATA IN VICINITY

For malicious actors, smartphone surveillance has opened up a new target for attack known as data in vicinity. Unlike data stored on or transmitted by the smartphone, data in vicinity occurs in the environment surrounding the device. This includes any audio that can be picked up by the device's microphones and any visual data that can be seen through the device's cameras.

Data in vicinity represents a potential goldmine of unfiltered information about an organization. This is because some valuable details are only discussed or displayed ephemerally, never meant to be captured in any digital format. Other times, sensitive information is brought up long before being jotted down in a document or email. Whether details about a military offensive or a product launch, this information can be leveraged by hackers in a number of ways:

- To develop an understanding of an organization's inner workings
- To further attacks against the organization
- To be sold on the black market
- To be distributed to competitors
- For blackmail
- For insider trading

EXAMPLES OF DATA IN VICINITY

Audio data:

- Meeting discussions and presentations
- Professional and personal conversations
- Processes and activities
- Environmental noise

Visual data:

- Colleagues, associates, friends and family
- Computer screens
- Products in development
- Whiteboard notes

THE MECHANICS OF TARGETED SURVEILLANCE

While there's been an evolution in the tools known to be used by threat actors for hijacking smartphone cameras and microphones, most targeted forms of surveillance malware follow a similar pattern of infection.

Step 1: Social engineering
To begin, a hacker uses social engineering techniques to lure the targeted victim, often by masquerading as a fictional person. Communication usually occurs over SMS or social media. The victim is enticed to click a link for a malicious website fronting as a legitimate website, and then uses the site to download a malicious app or update.

Step 2: Malware
During installation or execution, malware – often of the Trojan horse variety – infects the smartphone behind the scenes, unknown to the victim. The delivery of malware often occurs in later stages in order to encourage the victim to accept the elevated permissions required for the malware to access the smartphone's camera and microphones.

Step 3: Remote control
Once given full control of cameras and microphones, the hacker can exfiltrate captured audio recordings, photos and videos back to a server for collection and analysis. Depending on the type of tool used, the hacker can specify the parameters for capture – like user actions, device location and time intervals – and even perform live surveillance.

NOTABLE INCIDENTS OF SMARTPHONE SURVEILLANCE

Pegasus
- Discovery: August 2016
- Platform: iOS
- Creator: A cyber-arms dealer
- Initial targets: Activists and journalists
- Attack vector: Malicious websites
- Notable feature: Remote jailbreak exploit

ViperRAT
- Discovery: February 2017
- Platform: Android
- Creator: A threat group (suspected)
- Initial targets: Israel Defense Forces
- Attack vector: Malicious websites/apps
- Notable feature: On-demand surveillance

Skygofree
- Discovery: October 2017
- Platform: Android
- Creator: A cybersecurity solutions provider (suspected)
- Initial targets: Individuals in Italy
- Attack vector: Malicious websites/updates
- Notable feature: Geofencing for triggering audio recordings

Desert Scorpion
- Discovery: April 2018
- Platform: Android
- Creator: A threat group (suspected)
- Initial targets: Individuals in the Middle East
- Attack vector: A legitimate app with a second-stage payload
- Notable feature: Hosted on Google Play

THE SMARTPHONE SURVEILLANCE ECONOMY

While it's largely unclear who may be responsible for any given instance of smartphone surveillance or the goal behind such an attack, much more is known about the larger landscape. Smartphone surveillance has its own unique economy with a diverse mix of participants and motivations. Players range from malicious actors to trusted governmental agencies, and many exist within the gray area in the middle.

Intelligence agencies
Intelligence agencies have long been at the forefront of surveillance, for both domestic and foreign targets. It's safe to assume that all intelligence agencies – and the threat actors working on their behalf – are dedicated to hacking mobile devices. Some foreign intelligence services have even disrupted smartphone supply chains, building in control of devices before they reach end users. Tellingly, the Pentagon has banned the use of smartphones within spaces containing classified information, with the exception of government-issued devices that have had the cameras and microphones disabled through painstaking hardware modifications.

Likely targets for surveillance include:

- Military groups (for battle strategies, troop movements, etc.)
- Other intelligence agencies (for classified information, sources, etc.)
- High-level individuals (for private affairs, criminal activity, etc.)
- Enterprises (for trade secrets, financial information, etc.)

Cyber-arms dealers
The cyber-arms market includes defense contractors, cyber-mercenaries and enterprising hackers. Individual tools for smartphone surveillance are custom-built for a client, developed as a ready-made solution or created to sell on the dark web. Some exploits may take advantage of unpublished zero-days and other unpatched vulnerabilities. The clientele of these cyber-arms is typically undisclosed, but include reputable governmental actors like intelligence agencies, law enforcement and prosecutors, as well as nefarious actors like hostile nation-states and threat groups.

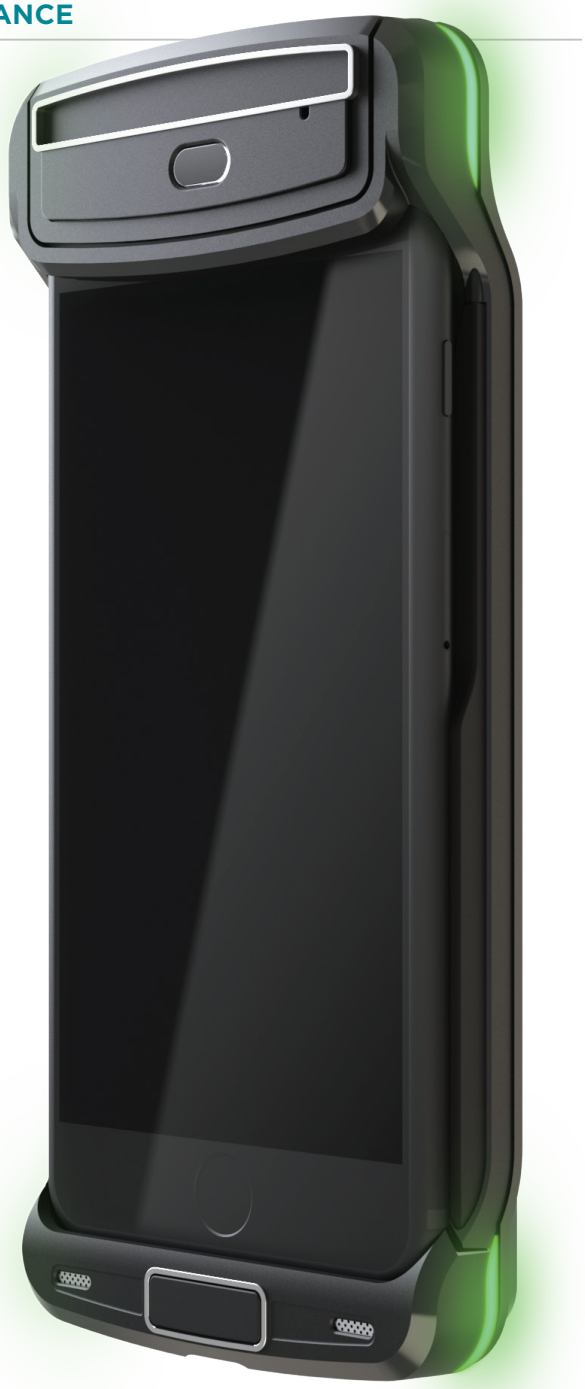
Cybercriminals
Cybercriminals may be motivated by a variety of reasons, including economic, political, social or personal. In addition to developing their own malware capabilities, hackers often use existing malware families and exploits – open-source, proprietary, or commercial – to carry out their goals. Tools – including those stolen or leaked from cyber-arms dealers – are widely shared underground.

Technology companies
Though not actively surveilling users, digital assistants and certain apps function through elevated camera and/or microphone permissions. Virtual assistants like Siri and Google Assistant, for example, are designed to always listen, waiting for wake words that prompt them into action. While such services are still unexplored territory for hackers, it's conceivable that malware can piggyback on these services to intercept conversations and other audio.

PROTECTING AGAINST SMARTPHONE SURVEILLANCE

Organizations seeking to protect themselves from the threat of hijacked cameras and microphones have had limited options. One option is to simply ban smartphones from spaces where sensitive information is being discussed; while effective, this option is incongruent with smartphone-centric work cultures and can damage morale. Another option is to suggest that users physically cover their cameras (using a sticker or sliding cover) and plug their microphones (using a modified pair of earbuds or a special audio jack plug); this option – in addition to suffering from a lack of enforcement capabilities and a clunky user experience – fails to protect against the hijacking of the smartphone's other microphones.

Privoro provides a different approach to defending against smartphone surveillance. The SafeCase, a first-of-its-kind smartphone case, surrounds a user's mobile device to provide physical counter-surveillance protections for every camera and microphone. The case masks audio transmissions with true random noise that's specific to each of the device's microphones (the iPhone has four), ensuring that any discussion is indecipherable during analysis. The cameras are blocked with a simple barrier. Protections are verifiable by both users and administrators, giving organizations a way to ensure that their most valuable conversations and visual details are protected from intruders.



PRIVORO®

© 2018 PPIP LLC. All rights reserved. PRIVORO and the PRIVORO DOG LOGO are trademarks of PPIP LLC, registered in the U.S. and other countries. PVOCONJ008V02