The hijacking of smartphone cameras and microphones

For nation-states and threat actors alike, remotely and stealthily hijacking the smartphone cameras and microphones of a targeted individual can yield valuable insights about an organization of interest. Given the failure of existing security measures to reliably detect or stop advanced spyware and the invasive audio/video collection that results, security-conscious organizations must look beyond software-based solutions to protect their most important 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-arms 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 spyware.

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

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

2008 – DROPOUTJEEP development
One year after the release of the iPhone, the NSA catalogs a planned exploit[1] for the device capable of microphone activation and camera capture via close access methods, with stated plans to develop a remote installation capability.

2012 – RCSAndroid in the wild
A commercial malware suite[2] 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.

2013 – AndroRAT binder
On the underground market, a binder[3] begins to be sold for what is perhaps the first remote access Trojan (RAT) for Android capable of using a device's camera and microphone, giving users a way of repackaging legitimate apps with the RAT.

2016 – Targeted Pegasus attack
Ahmed Mansoor, an internationally recognized human rights activist, is targeted[4] with what is likely the first known attack using malware capable of employing an iPhone's cameras and microphones.

The goal: data in vicinity

For malicious actors, smartphone surveillance has opened up a new target for attack that we at Privoro call *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 concerning a planned military offensive or a commercial product launch, this captured information can be leveraged by hackers in a number of ways:

- **Awareness:** At a minimum, the information can be used to develop an understanding of an organization's projects, strategies and inner workings.
- **Attack:** The information may be used to further attacks (physical or cyber) against the organization and even for blackmail.
- **Financial gain:** In some cases, the information can be sold on the black market or used 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 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.

Methods of attack

Spyware remotely infects a targeted smartphone using one of three known methods: social engineering, zero-click attack or IMSI catcher (fake cell tower).

Social engineering

With social engineering, the target is lured into opening a malicious link, downloading a malicious file or installing a malicious app, generally with the operator masquerading as another person or organization. Commonly, the operator will deliver a malicious link over SMS or another messaging platform, and the link will exploit browser vulnerabilities to install spyware on the victim's device.

Zero-click attack

A zero-click attack bypasses the need for social engineering entirely, letting operators take over a smartphone in real time without any interaction with the target. With fewer clues provided to the target and a higher probability of successful infection, zero-click attacks have become the preferred method of nation-state hackers and spyware vendors.

Zero-click attacks often target apps that provide messaging or voice calling because these services are designed to receive and parse data from untrusted sources. Attackers generally use specially formed data, such as a hidden text message or image file, to inject code that compromises the device.

IMSI catcher (fake cell tower)

An IMSI catcher, also known as a fake cell tower, is a portable device used to simulate a cell tower. Once connected to a targeted smartphone, an IMSI catcher essentially performs a man-in-the-middle (MITM) attack, situating itself between the smartphone and its cellular network. Though mainly used for identifying devices within an area and extracting certain types of cellular data from connected devices, some IMSI catchers can deliver spyware to a targeted phone.

NOTABLE INCIDENTS OF SMARTPHONE SURVEILLANCE

Jamal Khashoggi's assassination (October 2018)

Using commercial spyware, the Saudi government hacked the smartphone of Omar Abdulaziz[5], a friend of journalist Jamal Khashoggi. According to a lawsuit filed by Abdulaziz against spyware dealer NSO Group, the Saudi government was able to access Abdulaziz's conversations with Khashoggi and the information captured from these conversations ultimately contributed to the journalist's murder.

The Jeff Bezos hack (November 2018)

Jeff Bezos, then CEO of Amazon, had his iPhone X hacked[6] in 2018. An investigation into the hack found that his phone had most likely been infected after receiving a WhatsApp message from the account of Mohammad bin Salman, the crown prince of Saudi Arabia. The message allegedly included a video file containing a piece of code that enabled the sender to extract information from Bezos's phone over a period of several months.

China's surveillance of Uyghurs (November 2018)

Starting in 2014, the Chinese government has orchestrated a high-tech campaign of oppression against the Uyghur people in the province of Xinjiang, relying in part on targeted hacking campaigns. One particular campaign[7] that lasted between November 2018 and January 2019 employed malicious websites targeted to the religious group to infect the iPhones of visitors with spyware.

The Pegasus Project (July 2021)

The Pegasus Project[8] was a global investigative reporting effort that revealed the scale of surveillance operations from customers of NSO Group's Pegasus spyware, based on a leaked list of over 50,000 phone numbers believed to belong to individuals identified as "persons of interest" by the company's clients. Notably, the reporting showed that several heads of state and government had been targeted.

The smartphone surveillance economy

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 commercial spyware vendors, exploit brokers, defense contractors, cyber-mercenaries and enterprising hackers. Spyware vendors like FinFisher, Circles and NSO Group have gained much of the attention in this arena, given the popularity of their products, the sophistication of their exploits and the many controversies around improper usage of their tools by customers. However, individual solutions for smartphone surveillance may also be custom-built for a client or created to sell on the dark web.

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.

Protecting against smartphone surveillance

Until recently, organizations seeking to protect themselves from the threat of hijacked cameras and microphones have had a limited menu of less-than-ideal options.

One option is to rely on the phone's operating system and/or third-party security software to detect and stop advanced spyware and any attempts to remotely activate the device's cameras and microphones. As we've seen with recent high-profile attacks, spyware vendors seem to be working at a permanent advantage over phone makers, leveraging sophisticated and highly valuable exploit chains for a period of time until phone makers have a chance to discover the vulnerability and implement a workable patch. For security-conscious organizations, this is simply an unacceptable risk.

Other, more draconian options include removing the cameras and microphones from smartphones and banning the devices from work areas altogether. While obviously effective from a security standpoint, these options ignore the realities of the modern workforce and their expectations around using smartphones to complete tasks, collaborate and connect with the outside world.

At Privoro, we've developed stronger approaches to protecting important information from leaking out in the form of captured conversations and rich visuals.

Privoro has partnered with Samsung to develop a hardware-to-hardware integration between SafeCase ONX™ security devices and Galaxy phones (starting with S23) that provides secure, chip-level control of the phone's cameras and microphones. This low-level, two-system architecture means that even if the phone is infected with spyware, the spyware cannot turn on cameras and microphones if the user has explicitly disabled them using ONX.

SAFECASE ONX
FOR GALAXY S23

Privoro also offers products that physically block the phone's cameras and employ audio masking to scramble sounds from the phone's environment before they're picked up by the device's microphones. In effect, any captured audio and imagery is rendered meaningless to the attacker. This functionality is available via SafeCase CRBN™, which allows full use of the phone as these protections are used, as well as Vault™, our Faraday case.

With our approaches, organizations and users can take full advantage of smartphones while at the same time mitigating the potential for these devices to be used as spying devices turned against their users.

Sources

1. Ippolito, Nina, "The NSA Had Access to Your iPhone's Camera and Microphone," Mic, January 1, 2014.

2. Brandom, Russell, "New spy tool lets cops bug your phone remotely," The Verge, June 24, 2014.

3. Marshall, Patrick, "AndroRAT signals commercialization of mobile malware," GCN, July 19, 2013.

4. Marczak, Bill, and John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender," The Citizen Lab, August 24, 2016.

5. Morris, Loveday, "Khashoggi friend sues Israeli firm over hacking he says contributed to the journalist's murder," The Washington Post, December 3, 2018.

6. Zetter, Kim, "Here Is the Technical Report Suggesting Saudi Arabia's Prince Hacked Jeff Bezos' Phone," Vice, January 22, 2020.

7. O'Neill, Patrick Howell, "How China turned a prize-winning iPhone hack against the Uyghurs," MIT Technology Review, May 6, 2021.

8. Priest, Dana, Craig Timberg, et al., "Private Israeli spyware used to hack cellphones of journalists, activists worldwide," The Washington Post, July 18, 2021.