Chinese EagleMsgSpy Spyware Found Exploiting Mobile Devices Since 2017

The Hacker News ⋮ 6-8 minutes

Cybersecurity researchers have discovered a novel surveillance program that's suspected to be used by Chinese police departments as a lawful intercept tool to gather a wide range of information from mobile devices.

The Android tool, codenamed EagleMsgSpy by Lookout, has been operational since at least 2017, with artifacts uploaded to the VirusTotal malware scanning platform as recently as September 25, 2024.

"The surveillanceware consists of two parts: an installer APK, and a surveillance client that runs headlessly on the device when installed," Kristina Balaam, senior staff threat intelligence researcher at Lookout, said in a technical report shared with The Hacker News.

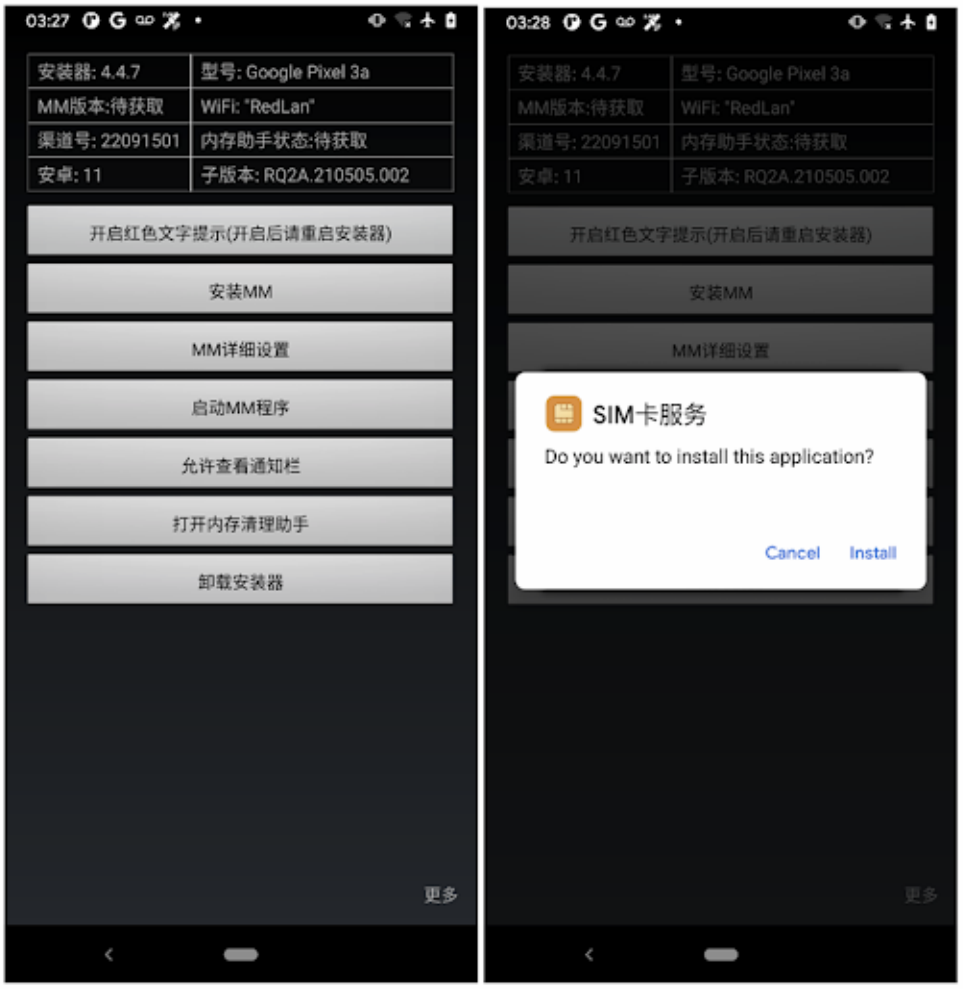
"EagleMsgSpy collects extensive data from the user: third-party chat messages, screen recording and screenshot capture, audio recordings, call logs, device contacts, SMS messages, location data, [and] network activity."

EagleMsgSpy has been described by its developers as a "comprehensive mobile phone judicial monitoring product" that can obtain "real-time mobile phone information of suspects through network control without the suspect's knowledge, monitor all mobile phone activities of criminals, and summarize them."

The cybersecurity company attributed the surveillance program to a Chinese company called Wuhan Chinasoft Token Information Technology Co., Ltd. (aka Wuhan Zhongruan Tongzheng Information Technology Co., Ltd and Wuhan ZRTZ Information Technology Co, Ltd.), citing infrastructure overlap and references within the source code.

Lookout said the company's internal documents it obtained from open directories on attacker-controlled infrastructure hint at the possibility of an iOS component, although such artifacts are yet to be uncovered in the wild.

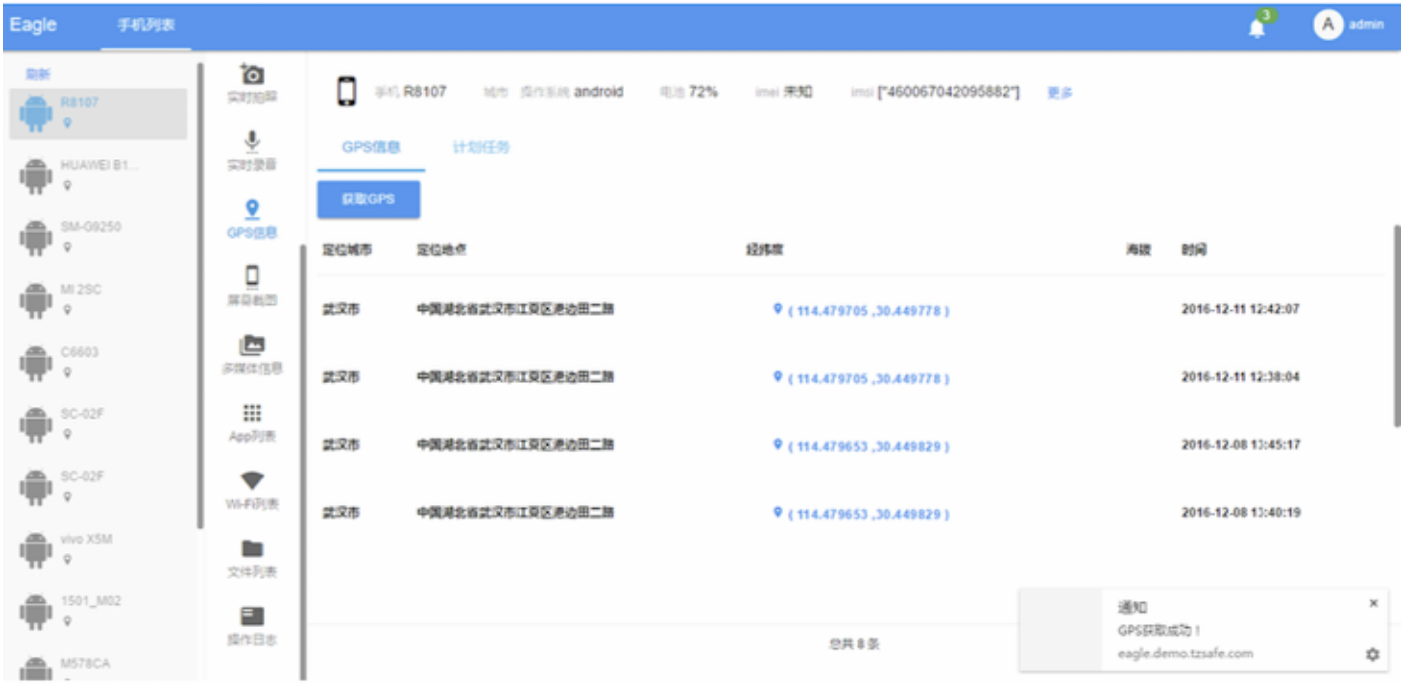
What's notable about EagleMsgSpy is the fact that it appears to require physical access to a target device in order to activate the information gathering operation. This is accomplished by deploying an installer module that's then responsible for delivering the core payload, otherwise referred to as MM or eagle_mm.



The surveillance client, for its part, can be acquired through various methods, such as QR codes or via a physical device that installs it on the phone when connected to USB. It's believed that the actively maintained tool is used by multiple customers of the software vendor, given that it requires them to provide as input a "channel," which corresponds to an account.

EagleMsgSpy's Android version is designed to intercept incoming messages, collect data from QQ, Telegram, Viber, WhatsApp, and WeChat, initiate screen recording using the Media Projection API, and capture screenshots and audio recordings.

It's also equipped to gather call logs, contact lists, GPS coordinates, details about network and Wi-Fi connections, files in external storage, bookmarks from the device browser, and a list of installed applications on the devices. The amassed data is subsequently compressed into password-protected archive files and exfiltrated to a command-and-control (C2) server.



Unlike early variants of EagleMsgSpy that employed few obfuscation techniques, the recent counterparts use an open-source application protection tool called ApkToolPlus to conceal some of the code. The surveillance module communicates with the C2 through WebSockets using the STOMP protocol to provide status updates and receive further instructions.

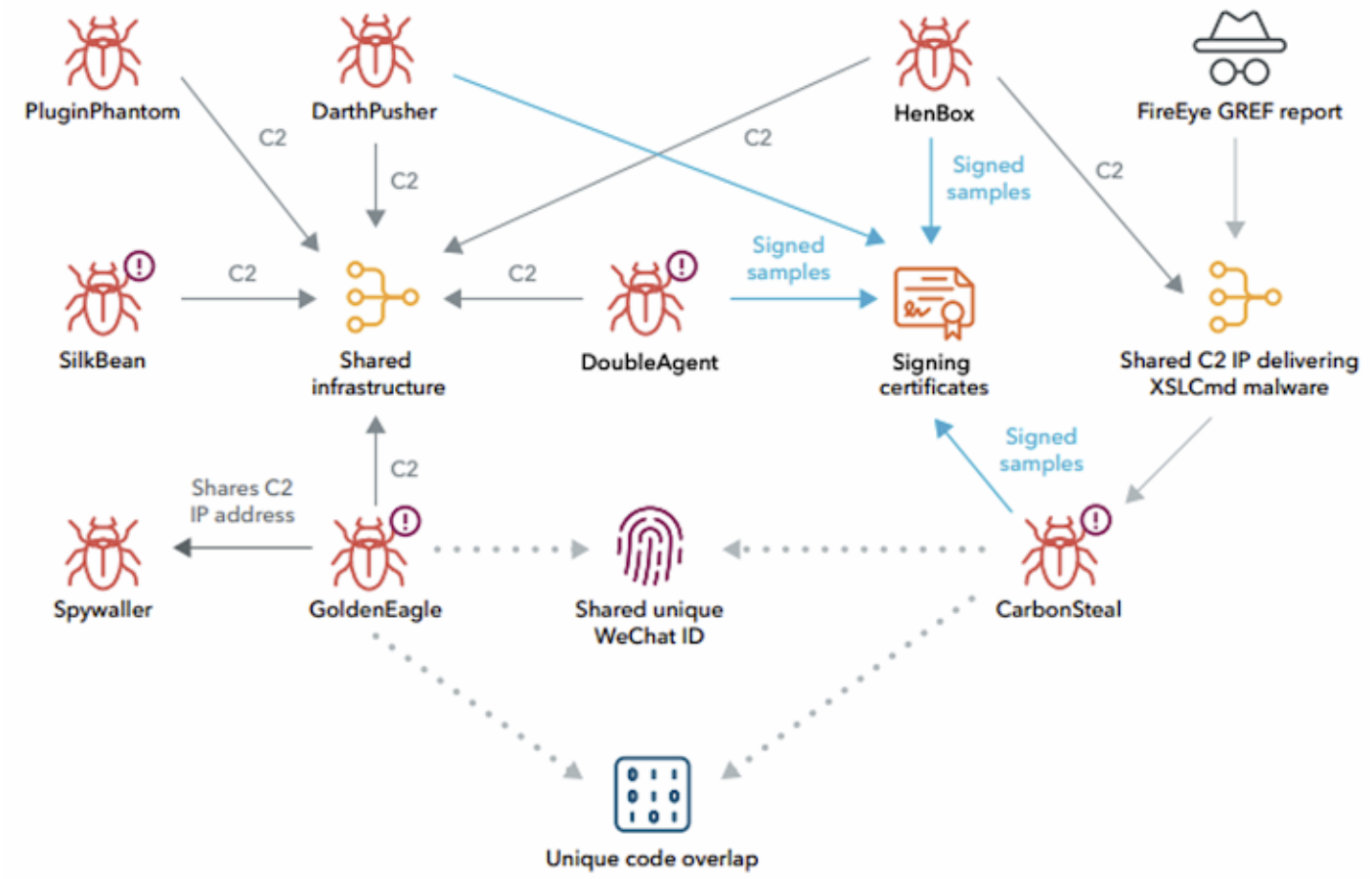
"EagleMsgSpy C2 servers host an administrative panel requiring user authentication," Balaam said. "This administrative panel is implemented using the AngularJS framework, with appropriately configured routing and authentication preventing unauthorized access to the extensive admin API."

It's this panel source code that contains functions such as "getListIOS()" to distinguish between device platforms, alluding to the existence of an iOS version of the surveillance tool.

Lookout's investigation has found that the panel allows customers, likely law enforcement agencies located in Mainland China, to trigger data collection in real-time from the infected devices. Another link that points to China is a hardcoded Wuhan-based phone number specified in several EagleMsgSpy samples.

The Hacker News also identified multiple patent applications filed by Wuhan ZRTZ Information Technology Co, Ltd. that delve into the various methods which can be used to "collect and analyze client data such as data of certain types like call record of the suspect's mobile phone, short messages, an address book, instant chat software (QQ, WeChat, Momo, etc.) and so forth, and generate a relationship diagram between the suspect and others."

Another patent details an "automatic evidence-collecting method and system," indicating that the company behind EagleMsgSpy is primarily focused on developing products that have law enforcement use cases.



"It's possible that the company incorporated the methodologies described in their patent applications – especially in cases in which they claim to have developed unique methods of creating relationship diagrams between victim datasets," Balaam told The Hacker News. "However, we don't have insight into how the company processed data server-side that was exfiltrated from victim devices."

What's more, Lookout said it identified two IP addresses tied to EagleMsgSpy C2 SSL certificates (202.107.80[.]34 and 119.36.193[.]210) that have been used by other China-linked surveillance tools such as PluginPhantom and CarbonSteal, both of which have been used to target Tibetan and Uyghur communities in the past.

"The malware is placed on victim devices and configured through access to the unlocked victim device," the company said. "Once installed, the headless payload runs in the background, hiding its activities from the user of the device and collects extensive data from the user. Public [calls for proposals] for similar systems indicate that this surveillance tool or analogous systems are in use by many public security bureaus in China."

Found this article interesting? Follow us on Twitter and LinkedIn to read more exclusive content we post.