'Luckycat' APT Campaign Building Android Malware

By Kelly Jackson Higgins

Published: 2012-07-30 · Archived: 2026-04-05 19:18:10 UTC

DEF CON 20 -- Las Vegas, NV -- Windows long has been the favorite target of cyberespionage actors, but newly discovered evidence shows they are also setting their sites on mobile platforms, namely the Android.

The attackers behind the recent Luckycat advanced persistent threat (APT)-type attack campaign are in the process of developing malware aimed at the Android, a researcher with Trend Micro said in a presentation here last week. Luckycat, an attack campaign with ties to Chinese hackers that targets Indian and Japanese military research institutions and the Tibetan community, last year also began targeting Mac OS X users.

Trend Micro researchers found two Android apps in the early phase of development that can communicate with Luckycat's command-and-control (C&C) server. The malware is currently capable of gathering information on the mobile device and uploading and downloading files as directed by the C&C server. Some of the features, including remote shell, are still under construction, and it's unclear just how the attackers plan to infect victims with the mobile malware, according to Trend Micro.

"We don't know if it has been used or is spreading widely. It might be a proof-of-concept, and it was also possibly already used -- when there's only one infected victim, we may not see it," says Raimund Genes, CTO at Trend Micro.

The Luckycat Android malware also has the classic APT element, a remote access Trojan (RAT). "So it's a typical spy tool -- for the Android. This is the first evidence of targeted attacks not only on Windows and Mac OS X, but on Android" as well, Genes says.

The Luckycat Android APT malware is a file infector, so it works on all Android platforms, Genes says. "You don't need root access to hijack every SMS and change messages before [the victim] reads them, or to get online banking [credentials]," he says. "You don't need root access to switch on the mike ... it all depends on what the attacker wants to do. You could hide an advanced threat in the OS."

[Trojans, botnets, adware, and more are jumping from theoretical to practical. See 6 Discoveries That Prove Mobile Malware's Mettle.]

It's possible the attackers will use SMS messages or email with malicious URLs that download the app onto the targeted Android, according to Trend Micro. "This can be accomplished via social engineering lures designed to lead targets into downloading and installing the app. The attackers can combine these methods with a drive-by exploit that silently installs the malicious app in the target’s device," Trend Micro said in a report on the findings.

Bottom line: Cyberspies are going after BYOD devices, as well, in their quest to gain a foothold into the targeted organization, Genes says. Trend Micro's mobile app analysis has shifted with this trend as well: "Initially, we only

looked at malicious apps, but now we look at power consumption and privacy -- what the app is leaking out," he says. "It's amazing what these apps are leaking out."

Trend Micro's researchers specifically found two identical apps called "testService" on the Luckycat C&C server. "These only differed in that one app had a visible icon while the other had a transparent icon. Once installed, both apps gave remote attackers control over a compromised device," according to Trend Micro's report. The attackers appear to be working on ways to hide the app on the victim's Android as well, the report says.

Have a comment on this story? Please click "Add Your Comment" below. If you'd like to contact Dark Reading's editors directly, send us a message.

About the Author

Editor-in-Chief, Dark Reading

Kelly Jackson Higgins is the Editor-in-Chief of Dark Reading and VP, cybersecurity editorial at Informa TechTarget, where she leads editorial strategy for the company's three cybersecurity media brands: Dark Reading, SearchSecurity and Cybersecurity Dive. She is an award-winning veteran technology and business journalist with three decades of experience in reporting and editing for various technology and business publications and major media properties. Jackson Higgins was selected three consecutive times as one of the Top 10 Cybersecurity Journalists in the U.S., and was named as one of Folio's 2019 Top Women in Media. She has been with Dark Reading since its launch in 2006.
