Catelites Bot - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:33:20 UTC

Tool: Catelites Bot

Names	Catelites Bot Catelites
Category	Malware
Type	Banking trojan
Description	(Avast) Now, the Avast Threat Labs team have uncovered and analyzed with SfyLabs a new version of the malware, dubbed Catelites Bot, which shares similarities with the malware used for CronBot. While we are still investigating the details of this malware, here is what we know: this malware gets “dropped” onto your device after you download an app from a third-party app store (not official shops like Google Play) or from malicious adware (malvertisements) or phishing sites. Once dropped onto your Android device, the malicious app looks like the icon seen in the screen below and is titled “System Application.” Worse still, this piece of malware can also go after your bank account login details. This malware has the ability to pose as over 2,200 banks and financial institutions. It does so by adopting the logo and mobile application name of a bank used in the Google Play Store, allowing the author to use simple templates to harvest username and password or credit card information. The overlay is HTML-based and not as sophisticated as other Android banking malware such as LokiBot, Red Alert, or ExoBot, but the power here is clearly in the shotgun approach: using simple phishing overlay screens, the criminals are able to target many more users, increasing their likelihood of financial gain.
Information	<https://blog.avast.com/new-version-of-mobile-malware-catelites-possibly-linked-to-cron-cyber-gang>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.catelites>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Catelites>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool Catelites Bot

Changed	Name	Country	Observed	
Other groups				
	Cron		2015-Dec 2017	

1 group listed (0 APT, 1 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7792fc81-4715-436d-8eab-ccc560958972