Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:55:06 UTC

Tool: callCam

Names	callCam
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Trend Micro) The apps Camero and FileCrypt Manger act as droppers. After downloading the extra DEX file from the C&C server, the second-layer droppers invoke extra code to download, install, and launch the callCam app on the device. The app callCam hides its icon on the device after being launched. It collects the following information and sends it back to the C&C server in the background: • Location • Battery status • Files on device • Installed app list • Device information • Sensor information • Camera information • Screenshot • Account • Wifi information • Data of WeChat, Outlook, Twitter, Yahoo Mail, Facebook, Gmail, and Chrome The app encrypts all stolen data using RSA and AES encryption algorithms. It uses SHA256 to verify data integrity and customize the encoding routine. When encrypting, it creates a block of data we named headData. This block contains the first 9 bytes of origin data, origin data length, random AES IV, the RSA-encrypted AES encrypt key, and the SHA256 value of AES-encrypted origin data. Then the headData is encoded through the customized routine. After the encoding, it is stored in the head of the final encrypted file followed by the data of the AES-encrypted original data.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group/>

Last change to this tool card: 29 April 2020

Download this tool card in JSON format

All groups using tool callCam

Changed	Name	Country	Observed	
APT groups				
	SideWinder, Rattlesnake		2012-2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=c5e4e318-c0f6-4b6e-b74b-935daae939ee