Hacking group used Facebook lures to trick victims into downloading Android spyware

By Danny Palmer

Published: 2018-02-22 · Archived: 2026-04-05 20:40:41 UTC

A hacking campaign used fake Facebook profiles to trick targets into downloading malware capable of stealing vast swathes of information, including messages, photos, audio recordings and even the exact location of victims.

The group has been operating since as early as 2015 and is thought to have infected the Android phones of hundreds selected targets across the Middle East. The the highest concentration of infections is in Israel, but victims have also been seen in the US, China, Germany and France.

Uncovered by researchers at Avast, the operation has been dubbed 'Tempting Cedar Spyware'. The name combines the main means of attack - by tricking victims using fake social media profiles purporting to be those of a young woman - with the Cedar tree, which features prominently on the flag of Lebanon.

The campaign for distributing the malware begins with fake Facebook profiles which are designed to lure in victims - predominantly men - with 'flirty' conversations.

At least three Facebook accounts - Alona, Rita and Christina - use a series of images stolen from online profiles of real people and even interact with one another in an effort to make the catfishing accounts appear more authentic.

One of the Facebook profiles used to distribute malware.

Image: Avast

Those behind the fake accounts send suggestive Facebook messages to their selected targets, before asking that the chat is taken to a more "secure and private" platform for further messages in what's really a ploy to infect the target with malware.

Victims are sent a link to install what they're told is the Kik messaging platform in order to continue the conversation.

If the target goes through with the installation - which requires them to allow apps to be installed from unknown sources - they're provided with a very convincing copy of Kik, but one which is laced with commands for conducting espionage.

The malware contains a variety of modules for collecting information about the victim, including their contacts, photos, call logs and text messages, as well as information about the device including its geolocation - meaning the user can be physically tracked - number, network operator and model.

Tempting Cedar spyware is even capable of recording audio, meaning it is able to secretly record the conversations of users, as well as anyone else within earshot of the device. It isn't, however, capable of spreading itself across networks from an infected device.

See also: What is phishing? Everything you need to know to protect yourself from scam emails and more

What researchers have determined is that the operation runs out of Lebanon. The 'working hours' of the campaign match up with a Middle Eastern time-zone, but more significantly, a trail points to the domains of the links used to distribute the malware being registered by a user in Lebanon, with logins from Lebanese IP addresses.

However, researchers note that it's rarely one hundred percent possible to attribute attacks to particular threat actors.

It's unclear if this particular operation is still currently active, but Tempting Cedar is known to have still been trying to attempt to infect victims just a few months ago - it's how the hacking operation came to the attention of researchers, who are now working with law enforcement to combat the the effects of the campaign.

"We are working in parallel with a law enforcement agency that is following standard procedure to collaborate with other local agencies in the respective countries," said Michal Salat, Threat Intelligence Director at Avast

While the method of attack appears crude, it has been effective, infiltrating devices of hundreds of targets over a sustained period of time.

"The cybercriminals behind the Tempting Cedar Spyware were able to install a persistent piece of spyware by exploiting social media, like Facebook, and people's lack of security awareness, and were thus able to gather sensitive and private data from their victims' phones including real-time location data which makes the malware exceptionally dangerous," said an Avast blog post.

A simple techniques which victims could've employed to avoid falling victim to Tempting Cedar is to not reply to unsolicited messages received from a stranger on the internet and especially not to click on any links which they send.

It's also good practice to only download applications from trusted marketplaces, instead of from strange links.

"Had the victims done this, they would have avoided the fake and malicious Kik app," said researchers. "The "girls" probably would have stopped talking to them, but that would have been for their own good!"

READ MORE ON CYBER CRIME

- How these fake Facebook and LinkedIn profiles tricked people into friending state-backed hackers
- How to become a master cyber-sleuth [TechRepublic]
- Hackers are using this Android malware to spy on Israeli soldiers
- Yes, that free iPhone X offer is too good to be true [CNET]
- Facebook Messenger user? Watch out for fake messages rigged with malware

---