Booby-trapped messaging apps used for spying

SAN FRANCISCO, US: An espionage campaign using malware-infected messaging apps has been stealing smartphone data from activists, soldiers, lawyers, journalists and others in more than 20 countries, researchers said in a report on Thursday.

© Sergey Nivens via 123RF

A report authored by digital rights group Electronic Frontier Foundation (EFF) and mobile security firm Lookout detailed discovery of "a prolific actor" with nation-state capabilities "exploiting targets globally across multiple platforms."

Desktop computers were also targeted, but getting into data-rich mobile devices was a primary objective, according to the report.

With fake versions of secure messaging services like WhatsApp and Signal, the scheme has enabled attackers to take pictures, capture audio, pinpoint locations, and mine handsets for private data.

"Dark Caracal"

EFF and Lookout researchers dubbed the threat "Dark Caracal".

People in the US, Canada, Germany, Lebanon, and France have been hit by Dark Caracal, according to EFF director of

cybersecurity Eva Galperin.

"This is a very large, global campaign, focused on mobile devices," Galperin said.

"Mobile is the future of spying, because phones are full of so much data about a person's day-to-day life."

Hundreds of gigabytes of data have been taken from thousands of victims in more than 21 countries, according to Lookout and the EFF.

There were indications that Dark Caracal might be an infrastructure hosting a number of widespread, global cyberespionage campaigns, some of which date back years, the report said.

Because the apps fool people into thinking they are legitimate, users give them access to cameras, microphones and data.

"All Dark Caracal needed was application permissions that users themselves granted when they downloaded the apps, not realising that they contained malware," said EFF staff technologist Cooper Quintin.

"This research shows it's not difficult to create a strategy allowing people and governments to spy on targets around the world."

Dark Caracal to a building in Beirut

Researchers reported that they tracked Dark Caracal to a building in Beirut belonging to the Lebanese General Security Directorate.

Analysis showed that devices of military personnel, businesses, journalists, lawyers, educators, and medical professionals have been compromised, according to the report.

"Not only was Dark Caracal able to cast its net wide, it was also able to gain deep insight into each of the victim's lives," the report concluded.

Cybersecurity professionals consistently warn people to be wary when downloading software, avoiding programs shared through links or email and instead relying on trusted sources.

Source: AFP