Facebook Catches Palestinian Hackers Targeting Users with Malware

vice.com/en/article/dyvzjx/facebook-catches-palestinian-hackers-targeting-users-with-malware

A worker wearing a protective face mask talks on a mobile phone as he waits for customers in the gold market in Gaza City, Gaza, on Tuesday, Jan. 19, 2020. Image: Ahmad Salem/Bloomberg via Getty Image

Hacking. Disinformation. Surveillance. CYBER is Motherboard's podcast and reporting on the dark underbelly of the internet.

Two separate groups of hackers from Palestine have been targeting Facebook users with Android, iOS, and Windows malware, according to a report published by Facebook on Wednesday.

Facebook security researchers identified two separate hacking campaigns, one by a group linked to the Preventive Security Service (PSS), an intelligence and law enforcement agency established by Palestine's ruling party in the West Bank Fatah; and another one called Arid Viper, which other security researchers have linked to Hamas, the governing authority in Gaza. Facebook wrote in its report that the company "cannot conclusively confirm this connection based on our evidence."

“To us this looks like a targeted campaign that’s aimed at compromising people’s devices primarily for surveillance,” David Agranovich, the director of threat disruption at Facebook, told Motherboard in a phone call.

The hacker group Facebook suggested is linked to the PSS "originated in the West Bank and focused on the Palestinian territories and Syria, and to a lesser extent Turkey, Iraq, Lebanon and Libya." Their goal was to trick people into clicking on malicious links and to get them to install malware on their devices. This group targeted "journalists, people opposing the Fatah-led government, human rights activists and military groups including the Syrian opposition and Iraqi military," according to Facebook.

Facebook said Arid Viper activity "originated in Palestine" and created dozens of fake Facebook and Instagram profiles to target people who work in the Palestinian National Authority, Fatah, the PSS, several ministries, student groups, and other government employees. The hackers used phishing messages to lure targets into visiting fake websites—a total of 41—that advertised malicious versions of legitimate popular chat, banking, and dating apps. The hackers also created a fake chat app called MagicSmile. If the victims fell for it and downloaded the apps, they would install Android, iOS, or Windows malware, depending on what device they were using, according to Facebook.

On iOS, the hackers did not use any zero-days, but rather relied on an increasingly popular technique to hack targets: use mobile configuration profiles, or MDM certificates. These require targets to go through several steps to install a profile that then lets the hackers install malware on the victim's iPhones. At that point, the hackers used a known exploit and a publicly available jailbreak to collect personal data from the compromised phones, according to Facebook.

The company said that it did not see evidence of widespread compromises, "which suggests Arid Viper sparingly used this malware," as Facebook wrote in its technical report.

Agranovich said that Facebook will notify "just under 50 people that they were impacted by the Arid Viper threat actor," and "just under 800 people that they were impacted by the PSS-linked activity."

Both the iOS and Android malware were designed to collect a large swath of personal data, such as photos, contacts, text messages, as well as record audio at any time, record calls, and track location data, according to Facebook.

Facebook researchers also observed new versions of Arid Viper's Windows malware.

A Google spokesperson said that the company works "closely with others in the industry, including Facebook, on tracking threat actors. In this case, we have taken down associated domains, added domains to Safe Browsing blocklists and related accounts have been disabled."

Apple, and Microsoft did not respond to a request for comment.