ESET Research: Bahamut group targets Android users with fake VPN apps; spyware steals users' conversations

DUBAI, UNITED ARAB EMIRATES, November 29, 2022 / EINPresswire.com/ -- ESET researchers have identified an active campaign targeting Android users, conducted by the Bahamut APT group. This campaign has been ongoing since the start of this year. Malicious spyware apps are distributed through a fake SecureVPN website that provides only trojanized Android apps to download. This website has no association whatsoever with the legitimate, multiplatform SecureVPN software and service. Malicious apps used in this campaign are able to exfiltrate contacts, SMS messages, recorded phone calls, and even chat messages from apps such as WhatsApp, Facebook Messenger, Signal, Viber, and Telegram. ESET researchers discovered at least eight versions of the Bahamut spyware, which could mean the campaign is well-maintained. The malicious apps were never available for download from Google Play.

"The data exfiltration is done via the keylogging functionality of the malware, which misuses accessibility services. The campaign appears to be highly targeted, as we see no instances in our telemetry data," explains ESET researcher Lukáš Štefanko, who discovered and analyzed the dangerous Android malware. "Additionally, the app requests an activation key before the VPN and spyware functionality can be enabled. Both the activation key and website link are likely sent to targeted users," adds Štefanko. This layer aims to protect the malicious payload from being triggered right after launch on a non-targeted user device or when being analyzed. ESET Research has already seen similar protection being used in another campaign by the Bahamut group.

All exfiltrated data is stored in a local database and then sent to the Command and Control (C&C) server. The Bahamut spyware functionality includes the ability to update the app by

receiving a link to a new version from the C&C server.

If the Bahamut spyware is enabled, then it can be remotely controlled by Bahamut operators and can exfiltrate various sensitive device data, such as contacts, SMS messages, call logs, a list of installed apps, device location, device accounts, device info (type of internet connection, IMEI, IP, SIM serial number), recorded phone calls, and a list of files on external storage. By misusing accessibility services, the malware can steal notes from the SafeNotes application and actively spy on chat messages and information about calls from popular messaging apps, such as imo-International Calls & Chat, Facebook Messenger, Viber, Signal Private Messenger, WhatsApp, Telegram, WeChat, and Conion apps.

The Bahamut APT group typically uses spearphishing messages and fake applications as the initial attack vector, against entities and individuals in the Middle East and South Asia. Bahamut specializes in cyberespionage, and ESET Research believes that its goal is to steal sensitive information from its victims. Bahamut is also referred to as a mercenary group offering hack-for-hire services to a wide range of clients. The name was given to this threat actor, which appears to be a master in phishing, by the Bellingcat investigative journalism group. Bellingcat named the group after the enormous fish floating in the vast Arabian Sea mentioned in the Book of Imaginary Beings written by Jorge Luis Borges. Bahamut is frequently described in Arabic mythology as an unimaginably enormous fish.

For more technical information about the latest Bahamut APT group campaign, check out the blog post “Bahamut cybermercenary group targets Android users with fake VPN apps” on WeLiveSecurity. Make sure to follow ESET Research on Twitter for the latest news from ESET Research.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET’s high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET’s R&D centers worldwide, working in support of our shared future. For more information,
visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here