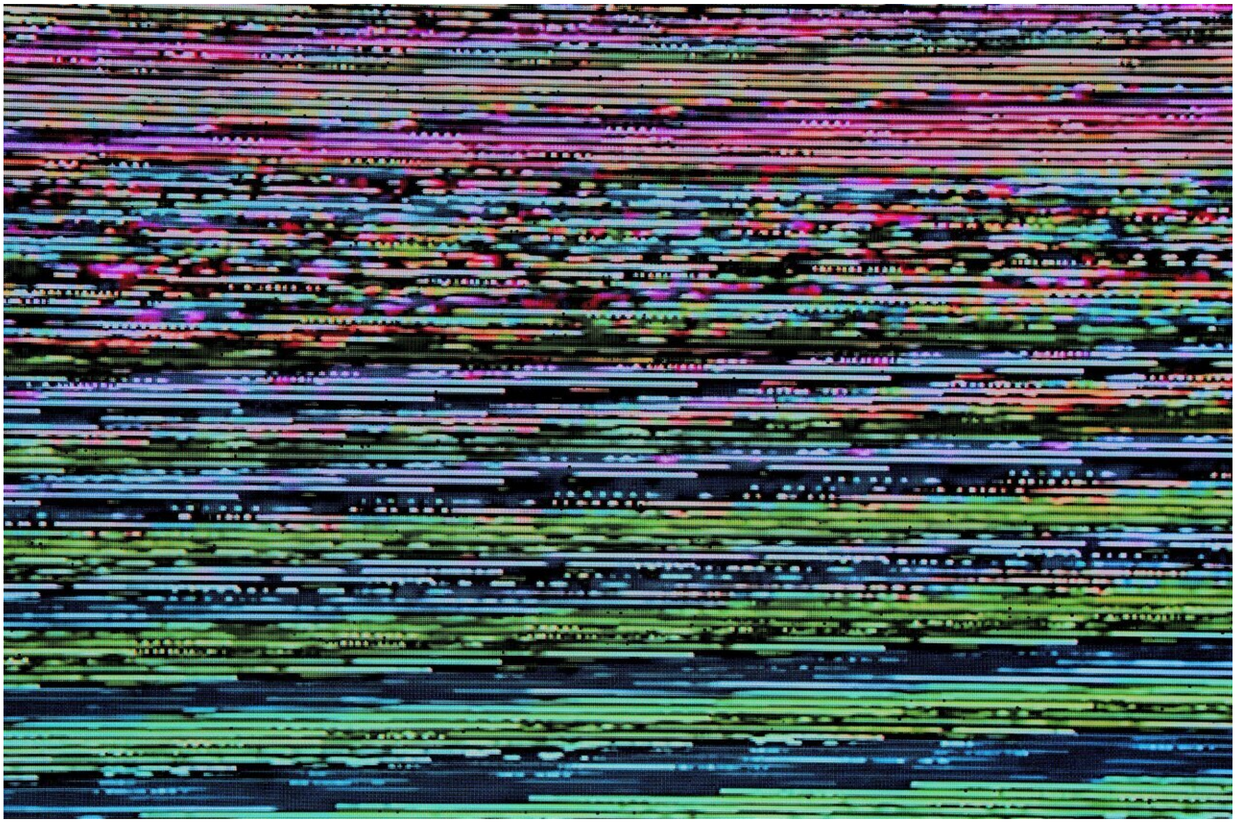
'Vultur' malware uses new technique to steal banking credentials

August 2 2021, by Bob Yirka



Credit: Unsplash/CC0 Public Domain

A team of researchers at the security firm ThreatFabric is reporting on their website blog page that they have found instances of a new kind of malware in Android apps downloaded from Google Play that attempt to steal banking login information. They have named the new malware Vultur, after the birds that prey on wounded or dead targets.

The team at ThreatFabric note that prior efforts to steal banking login and password information from users of Android-based devices have used overlays; where an image is pasted over the top of an application's login page and data from it is then routed to the hackers. In this new threat, the Vultur software instead uses code to recognize when a data entry form is being used, takes a screen grab, and then begins keylogging. All of the data captured by the malware is then routed to a site specified by its creators.

The team at ThreatFabric notes that thus far, Vultur has mostly affected people living in Italy, Australia, the U.K and the Netherlands—and while its prime mission appears to be capturing banking login information, instances of keylogging have also been found for social media apps, such as TikTok, Facebook and WhatsApp—they have also seen a few instances of cryptocurrency apps being targeted as well.

The malware can make its way onto user devices via a "dropper" called Brunhilda, which has been found in several phone-security, fitness and authentication apps—all on Google Play. The team at ThreatFabric is estimating that approximately 30,000 Android-based devices have been infected with Brunhilda to date, which suggests that thousands of users have likely been infected with Vultur. They also note that Vultur makes use of Accessibility Services on infected devices to prevent users from removing it from their device—it instigates a Back button press if such an attempt is made.

Users can prevent the malware from stealing their data by denying access when notified by Accessibility Services. Also, the malware can be detected by a casting icon appearing when users are not casting something. ThreatFabric also suggests installing Android antivirus apps.

More information: threatfabric.com/blogs/vultur-v-for-vnc.html

Citation: 'Vultur' malware uses new technique to steal banking credentials (2021, August 2) retrieved 3 May 2024 from https://techxplore.com/news/2021-08-vultur-malware-technique-banking-credentials.html