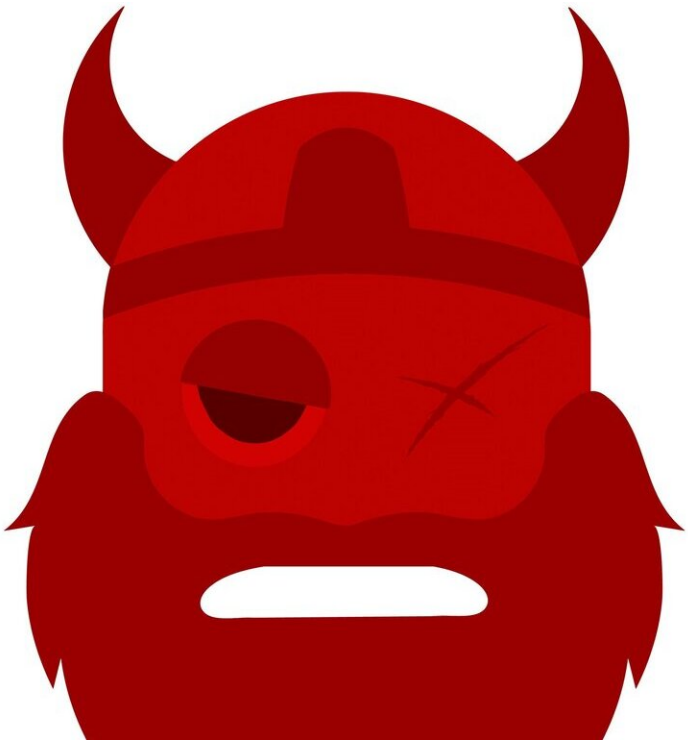
Old Norse plunder tactic inspires Oslo team to call Android flaw StrandHogg

December 3 2019, by Nancy Cohen



An Android bug can steal bank credentials, namely bank logins. The flaw is called StrandHogg and security investigators at an Oslo, Norway-based security company say it has been targeting 60 financial institutions—at least.

StrandHogg takes its name from the old Norse for a Viking tactic of coastal raids in order to plunder and hold people for ransom.

In Silicon UK, Matthew Broersma on Monday said that the flaw affects Android's multitasking system, and it "allows malicious apps to overlay fake login screens on legitimate apps," and that was according to the security firm that studied the vulnerability, Promon.

What does that really mean—multitasking system? *Dark Reading* referred to "its ability to run several apps at the same time and switch from app to app on the screen."

"This exploit," said the Promon site, is based on an Android control setting called 'taskAffinity' which allows any app—including malicious ones—to freely assume any identity in the multitasking system they desire.

Silicon UK showed a photo of a fake permissions pop-up appearing while an app was in use. "Allow to access photos, media and files on your device." Below that is a box for clicking "Don't ask again" and two boxes for "Deny" and "Allow."

You would be unaware that something is out there to harvest your data. The Promon researchers consider the bug as "dangerous." They said the vulnerability was such that all versions of Android were affected, and that would include Android 10.

The security company Lookout similarly wrote in a blog that StrandHogg attackers could mount an attack even against current versions of Android.

How did Promon discover this? The BBC said Promon, working along with US security firm Lookout, set out to scan apps in Android's Play

store just to see if any were being abused via the StrandHogg bug. That is how Lookout came up with the number 60—the sum of financial institutions that were being targeted via apps that sought to exploit the loophole, said the BBC.

Dark Reading went further in the discovery story: Promon researchers found StrandHogg when its customer, an Eastern European security firm, noticed a trend of money being siphoned from accounts at some banks. They traced the root of the problem to StrandHogg.

Results of the Promon search of malware under study found all of the top 500 most popular apps (as ranked by app intelligence company 42 Matters) were at risk.

Welcome to a nefarious world of "permission harvesting."

Dark Reading said that "malicious apps can request any permission while pretending to be legitimate. An attack could be designed to ask for permissions that seem natural for the targeted apps. By doing this, adversaries could lower the chance of victims realizing something is wrong. Users have no indication they're granting permission to a malicious app and not the authentic one."

A discomforting side note is that in spite of Google's Play Protect security suite, dropper apps continue to be published and frequently slip under the radar, with some being downloaded millions of times before being spotted and deleted, found Promon's researchers.

"The potential impact of this could be unprecedented in terms of scale and the amount of damage caused," said Promon CTO Tom Hansen.

What has been the damage thus far? Hansen, in the BBC News report, said It targeted several banks in several countries. The malware

"successfully exploited end users to steal money." The Lookout blog said that "Screen overlay attacks on financial institutions have increased significantly in the past 18 months."

Promon said they submitted their report to Google earlier this year.

BBC News reported on Monday that "Google said it had taken action to close the loophole and was keen to find out more about its origin." They referred to a Google statement that voiced appreciation of the research. Google said they suspended the potentially harmful apps that were identified.

Google is now to look at how they can improve Google Play Protect's ability to protect users against similar issues.

This is what Promon had to say about Google's response, which it did welcome, as other apps were potentially exploitable via the bug. At the same time, however, Promon's chief technology officer noted that it still remained possible to create fake overlay screens in Android 10 and earlier versions of the operating system.

Meanwhile, the Promon partner called Lookout, which is in the business of cybersecurity, went to recognized some variants of the BankBot banking trojan observed as early as 2017. BankBot was called one of the most widespread banking trojans around by Promon, "with dozens of variants and close relatives springing up all the time."

You can catch an especially helpful video presentation by the Promon researchers John Høegh-Omdal and Lars Lunde Birkeland about the victim experience. At least you can know the type of behavior that ensues if you are hacked.

"I will now demonstrate how hackers can read your SMS, steal your

private photos, and hijack your social media accounts." The video showed one of the two researchers sitting on a park bench with a Samsung Galaxy S10 running the latest Android version. On this weather app you see the fake permission pop-up asking if it is ok to send SMS messages.

The StrandHogg vulnerability makes it possible for a malicious app to replace a legitimate permission pop-up with its own fake version that asks for access to any permission, including SMS, photos, microphone, and GPS, allowing them to read messages, view photos, eavesdrop, and track the victim's movements.

Two noteworthy messages appeared in the reader comments section of the Dec. 2 video. One asked if this was only an Android headache—would iOS devices be vulnerable to this as well? The Promon reply was that the research only applied to Android, not iOS. The second interesting message from the researchers said that although Google removed the affected apps, "to the best of our knowledge, the vulnerability has not yet been fixed for any version of Android (incl. Android 10)."

More information: promon.co/security-news/strandhogg/

Citation: Old Norse plunder tactic inspires Oslo team to call Android flaw StrandHogg (2019, December 3) retrieved 4 April 2024 from https://techxplore.com/news/2019-12-norse-plunder-tactic-oslo-team.html