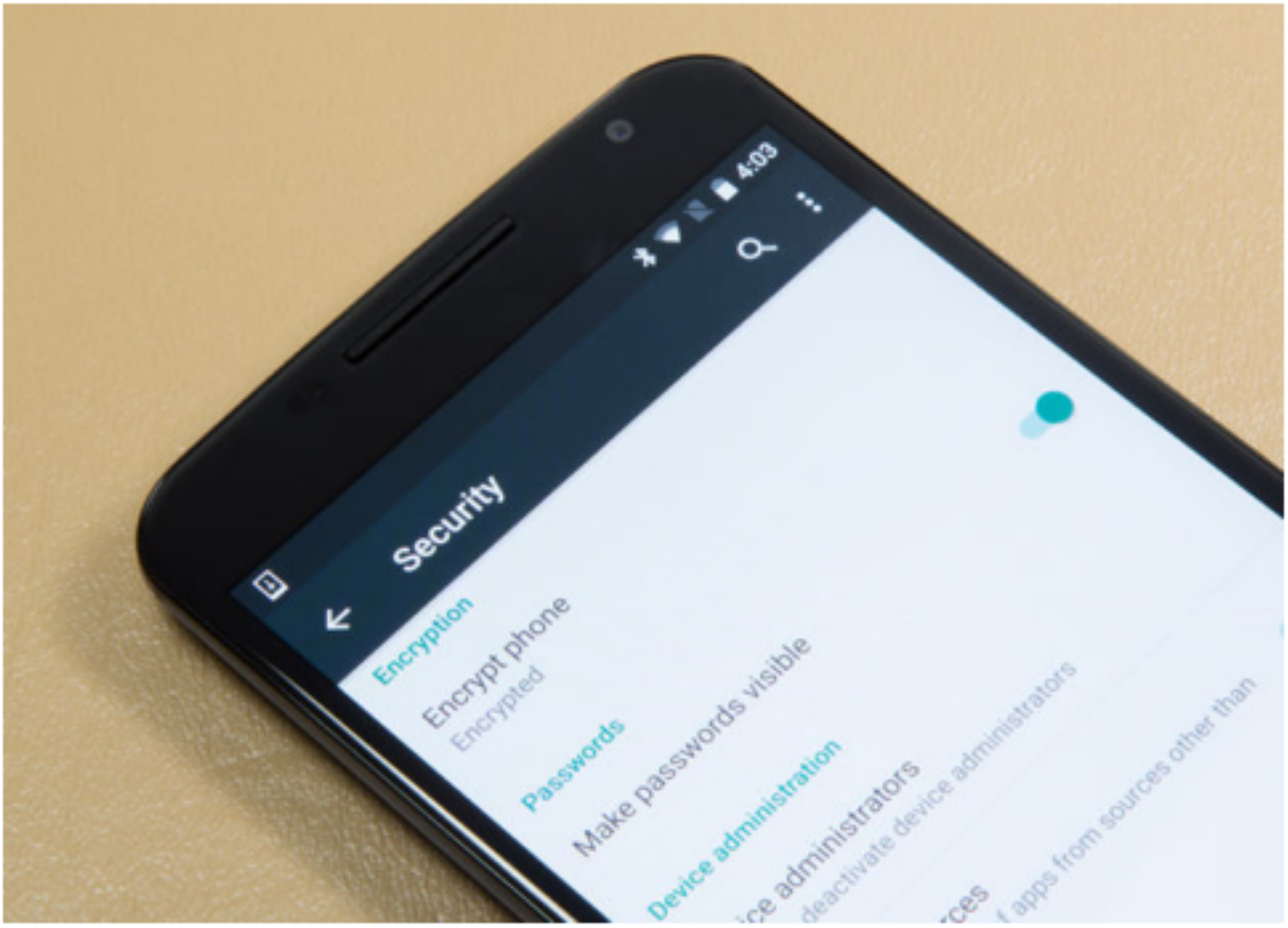
SIGN IN

RISK ASSESSMENT —

1 million Google accounts compromised by Android malware called Gooligan

86 apps available in third-party marketplaces can root 74 percent of Android phones.

DAN GOODIN - 11/30/2016, 6:01 AM



Ron Amadeo

Researchers say they've uncovered a family of Android-based malware that has compromised more than 1 million Google accounts, hundreds of them associated with enterprise users.

Gooligan, as researchers from security firm Check Point Software Technologies have dubbed the malware, has been found in at least 86 apps available in third-party marketplaces. Once installed, it uses a process known as rooting to gain highly privileged system access to devices running version 4 (Ice Cream Sandwich, Jelly Bean, and KitKat) and version 5 (Lollipop) of Google's Android operating system. Together, the vulnerable versions account for about 74 percent of users.

The rooted devices then download and install software that steals the authentication tokens that allow the phones to access the owner's Google-related accounts without having to enter a password. The tokens work for a variety of Google properties, including Gmail, Google Photos, Google Docs, Google Play, Google Drive, and G Suite. In a blog post published Wednesday morning, Check Point researchers wrote:

> The infection begins when a user downloads and installs a Gooligan-infected app on a vulnerable Android device. Our research team has found infected apps on third-party app stores, but they could also be downloaded by Android users directly by tapping malicious links in phishing attack messages. After an infected app is installed, it sends data about the device to the campaign's Command and Control (C&C) server.
>
> Gooligan then downloads a rootkit from the C&C server that takes advantage of multiple Android 4 and 5 exploits including the well-known VROOT (CVE-2013-6282) and Towelroot (CVE-2014-3153). These exploits still plague many devices today because security patches that fix them may not be available for some versions of Android, or the patches were never installed by the user. If rooting is successful, the attacker has full control of the device and can execute privileged commands remotely.
>
> After achieving root access, Gooligan downloads a new, malicious module from the C&C server and installs it on the infected device. This module injects code into running Google Play or GMS (Google Mobile Services) to mimic user behavior so Gooligan can avoid detection, a technique first seen with the mobile malware HummingBad. The module allows Gooligan to:
>
> - Steal a user's Google email account and authentication token information
> - Install apps from Google Play and rate them to raise their reputation
> - Install adware to generate revenue
>
> Ad servers, which don't know whether an app using its service is malicious or not, send Gooligan the names of the apps to download from Google Play. After an app is installed, the ad service pays the attacker. Then the malware leaves a positive review and a high rating on Google Play using content it receives from the C&C server.

Update: In a separate blog post also published Wednesday morning, Director of Android Security Adrian Ludwig said he and other Google officials have worked closely with Check Point over the past few weeks to investigate Gooligan and to protect users against the threat it poses. He said there's no evidence data was accessed from compromised accounts or that individual users were targeted. He also said Google has been using a service called Verify Apps to scan individual handsets for signs of Gooligan and other Ghost Push apps. When detected, device owners receive a warning and installations are halted.

"We've taken many actions to protect our users and improve the security of the Android ecosystem overall," Ludwig wrote. "These include: revoking affected users' Google Account tokens, providing them with clear instructions to sign back in securely, removing apps related to this issue from affected devices, deploying enduring Verify Apps improvements to protect users from these apps in the future and collaborating with ISPs to eliminate this malware altogether."

Gooligan is an aggressive variant of Ghost Push, a piece of Android malware that came to light in September 2015. There's no indication that any of the fraudulent apps containing the new Gooligan code have ever been available in the official Google Play Market. About 57 percent of devices infected by Gooligan are located in Asia, about 19 percent are in the Americas, about 15 percent are in Africa, and about 9 percent are in Europe.

Android users who have downloaded apps from third-party markets can visit the Check Point blog post for a list of the 86 apps known to contain Gooligan. Alternatively, users can visit this link to see if the Google account associated with their device has been compromised. Infected phones can only be disinfected by reflashing them with a clean installation of Android. Passwords for the associated Google account should be changed immediately afterward.

Post updated to reflect a change Check Point made to geographical infection figures.

Promoted Comments

QuidNYC / Ars Centurion / *et Subscriptor* **JUMP TO POST**

So is this the moment when Google finally has its come-to-Jesus moment on Android security, and uses all of its leverage with OEMs to enforce a serious update model -- at the risk of losing a few OEMs from the Google Play platform (and ad revenue)?

380 posts | registered 6/29/2014

citizencoyote / Wise, Aged Ars Veteran **JUMP TO POST**

There's not a whole lot Google can do if Android OEMs refuse to update handsets with new versions of the OS and/or security updates, especially in markets where the Google Play store is not available. Updating older Android handsets is a complex stew of needing the drivers for the hardware (provided by chip makers) and the resources (time and money) by the software team to build the update. All three are probably lacking when you're dealing with cheap phones made with low-end chipsets.

109 posts | registered 12/21/2012

Fibonaccied / Wise, Aged Ars Veteran **JUMP TO POST**

> Adam Starkey wrote:
>
> > qazwart wrote:
> >
> > Walled gardens also keep out weeds.

> Walled gardens *help* keep out weeds.

have you guys ever been inside a real garden, ever? that analogy doesn't work. walls don't keep weeds out, unless the wall is a dome. gardeners do.

135 posts | registered 8/8/2016

DAN GOODIN
Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 99

SHARE THIS STORY

← PREVIOUS STORY

NEXT STORY →

Related Stories

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US

CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS