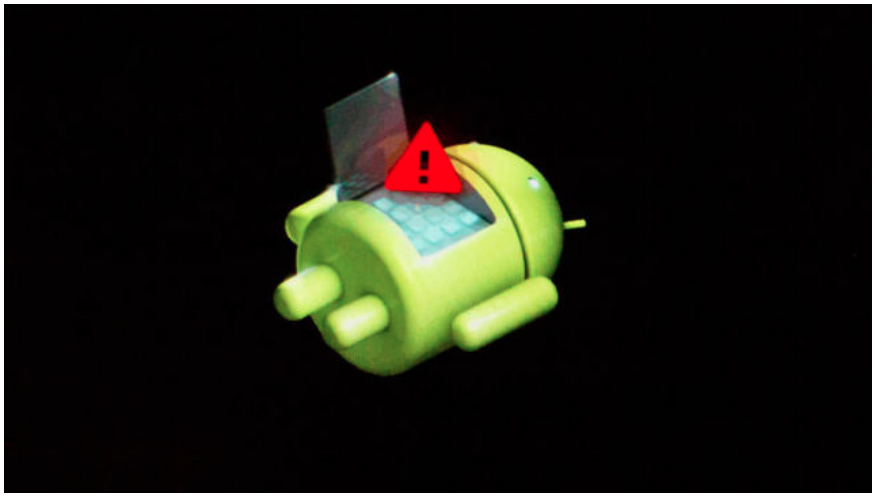
RISK ASSESSMENT / SECURITY & HACKTIVISM

10 million Android phones infected by all-powerful auto-rooting apps

First detected in November, Shedun/HummingBad infections are surging.

by **Dan Goodin** - Jul 7, 2016 10:50am PDT

144



Security experts have documented a disturbing spike in a particularly virulent family of Android malware, with more than 10 million handsets infected and more than 286,000 of them in the US.

Researchers from security firm Check Point Software said the malware installs more than 50,000 fraudulent apps each day, displays 20 million malicious advertisements, and generates more than $300,000 per month in revenue. The success is largely the result of the malware's ability to silently root a large percentage of the phones it infects by exploiting vulnerabilities that remain unfixed in older versions of Android. The Check Point researchers have dubbed the malware family "HummingBad," but researchers from mobile security company Lookout say HummingBad is in fact Shedun, a family of auto-rooting malware that came to light last November and had already infected a large number of devices.

FURTHER READING

NEW TYPE OF AUTO-ROOTING ANDROID ADWARE IS NEARLY IMPOSSIBLE TO REMOVE

20,000 samples found impersonating apps from Twitter, Facebook, and others.

For the past five months, Check Point researchers have quietly observed the China-based advertising company behind HummingBad in several ways, including by infiltrating the command and control servers it uses. The researchers say the malware uses the unusually tight control it gains over infected devices to create windfall profits and steadily increase its numbers. HummingBad does this by silently installing promoted apps on infected phones, defrauding legitimate mobile advertisers, and creating fraudulent statistics inside the official Google Play Store.

"Accessing these devices and their sensitive data creates a new and steady stream of revenue for cybercriminals," Check Point researchers wrote in a recently published report. "Emboldened by financial and technological independence, their skillsets will advance–putting end users, enterprises, and government agencies at risk."

The report said HummingBad apps are developed by Yingmob, a Chinese mobile ad server company

LATEST FEATURE STORY

FEATURE STORY (5 PAGES)

iOS 10 preview: Apple goes back to ignoring the iPad in a wide-ranging update

iOS 10 gives developers plenty to do and lets its users have a little fun, too.

WATCH ARS VIDEO

Ars delivers with Amazon Flex for a day

Sam becomes an Amazon Flex delivery man for a day.

STAY IN THE KNOW WITH

LATEST NEWS

Feds asked to investigate live-streamed death of motorist killed by cop

PASS CS:GO, COLLECT $200?

Mom takes on Valve, third-party “trading” sites, alleges “illegal scheme”

How an Illinois man’s flag-burning 4th of July celebration ended in jail

CAVEAT EMPTOR

Umeng, a tracking and analytics service attackers use to manage their campaign. Check Point analyzed Yingmob's Umeng account to gain further insights into the HummingBad campaign and found that beyond the 10 million devices under the control of malicious apps, Yingmob has non-malicious apps installed on another 75 million or so devices. The researchers wrote:

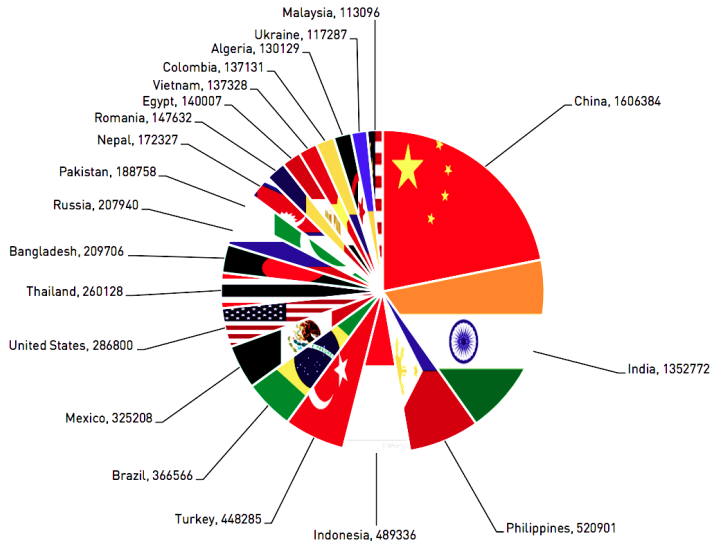
> While profit is powerful motivation for any attacker, Yingmob's apparent self-sufficiency and organizational structure make it well-positioned to expand into new business ventures, including productizing the access to the 85 million Android devices it controls. This alone would attract a whole new audience–and a new stream of revenue–for Yingmob. Quick, easy access to sensitive data on mobile devices connected to enterprises and government agencies around the globe is extremely attractive to cybercriminals and hacktivists.

Drive-by downloads and multiple rooting exploits

The malware uses a variety of methods to infect devices. One involves drive-by downloads, possibly on booby-trapped porn sites. The attacks use multiple exploits in an attempt to gain root access on a device. When rooting fails, a second component delivers a fake system update notification in hopes of tricking users into granting HummingBad system-level permissions. Whether or not rooting succeeds, HummingBad downloads a large number of apps. In some cases, malicious components are dynamically downloaded onto a device after an infected app is installed.

From there, infected phones display illegitimate ads and install fraudulent apps after certain events, such as rebooting, the screen turning on or off, a detection that the user is present, or a change in Internet connectivity. HummingBad also has the ability to inject code into Google Play to tamper with its ratings and statistics. It does this by using infected devices to imitate clicks on the install, buy, and accept buttons.

Many of the 10 million infected phones are running old versions of Android and reside in China (1.6 million) and India (1.35 million). Still, US-based infected phones total almost 287,000. The most widely infected major Android versions are KitKat with 50 percent, followed by Jelly Bean with 40 percent. Lollipop has 7 percent, Ice Cream Sandwich has 2 percent, and Marshmallow has 1 percent. It's often hard for average users to know if their phones have been rooted, and Shedun apps often wait some period of time before displaying obtrusive ads or installing apps. The best bet for Readers who want to make sure their phone isn't infected is to scan their phones using the free version of the Lookout Security and Antivirus app. Android malware has drastically lower rates of success when app installations outside of Google Play are barred. Readers should carefully think through the risks before changing this default setting.



Enlarge / Top 20 countries targeted by Hummingbad/Shedun.
Check Point Software

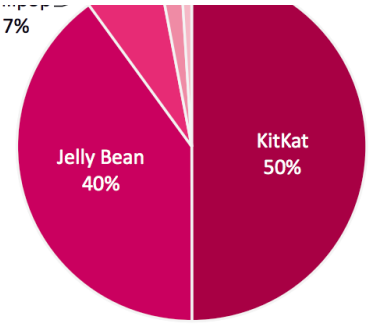
Recode says

ON THE HOME STRAIGHT

Windows 10 Anniversary Update nears RTM with bugfixes galore

SAVE THE HABITAT

LucasArts' long lost, 30-year-old MMO is now preserved on Github



Enlarge / Hummingbad/Shedun infections by Android version.
Check Point Software

So far, HummingBad has been observed using its highly privileged status only to engage in click fraud, display pop-up ads, tamper with Google Play, and install additional apps that do more of the same. But there's little stopping it from doing much worse. That's because the malware roots most of the phones it infects, a process that subverts key security mechanisms built into Android. Under a model known as sandboxing, most Android apps aren't permitted to access passwords or other data available to most other apps. System applications with root, by contrast, have super-user permissions that allow them to break out of such sandboxes. From there, root-level apps can read or modify data and resources that would be off-limits to normal apps.

As Lookout first reported more than eight months ago, the problem with Shedun/HummingBad and similar malicious app families that silently exploit Android rooting vulnerabilities is that the infections can survive normal factory resets. Lookout said in its own blog post published Wednesday that its threat detection network has recently observed a surge of Shedun attacks, indicating the scourge won't be going away any time soon.

Post updated to correct revenue amount in the second paragraph, add details about third-party app stores in the ninth paragraph.

READER COMMENTS 144

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.
@dangoodin001 on Twitter

← OLDER STORY NEWER STORY →

YOU MAY ALSO LIKE