



How Some Chinese Hackers Started Making Big Money

Tuesday, October 13, 2015 Khyati Jain
 G+ 48 f Like 639 f Share 906 Tweet 135 in Share 5 ShareThis 1089



We know that Hackers hack for a variety of reasons:

...some hack to test their skills,
 ...some hack to gain recognition,
 ...some hack to make money,
 ...some hack to support their Nation-State strategy,
 ...and, some hack alone, and some hack in Groups.

And Chinese Hackers are the ones who are infamous for their dedication towards Hacking.

Chinese hacking groups are better known for attacking and stealing information, organized cyber crimes, theft of intellectual property and state-sponsored cyber espionage attacks.



Ads by Google

- [▶ Hack Download](#)
- [▶ Mobile Hacking](#)
- [▶ Computer Hacking](#)

But it seems that several Chinese hacker groups have now shifted their motive of hacking towards 'making money'.

How much Money Hackers Actually Make?

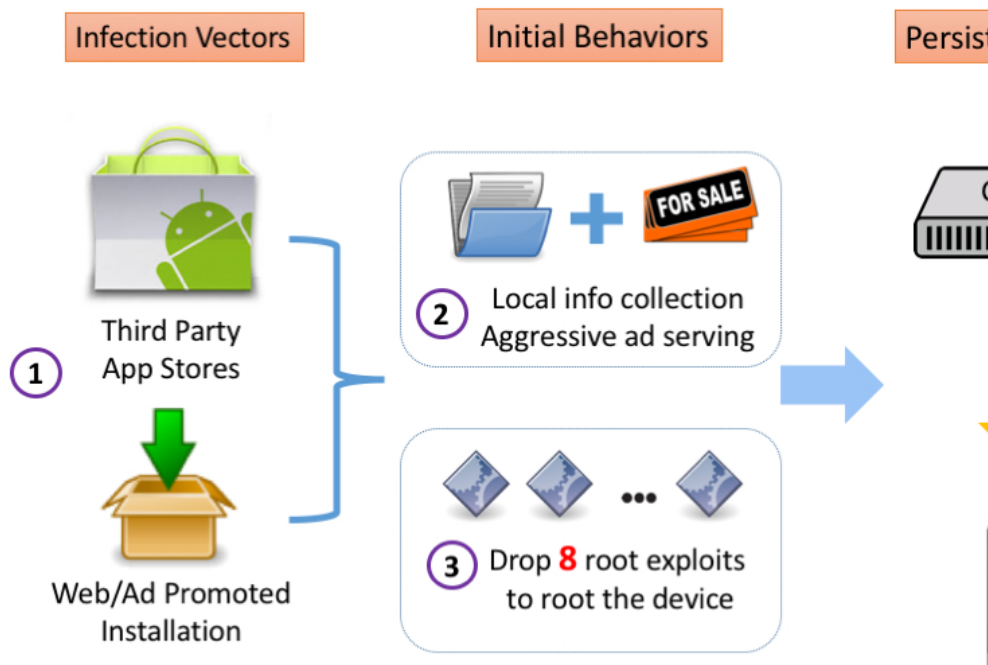
It is a known fact that hacking makes money, but how much?

Answer: At least \$4,500,000/year from one malware campaign.

How? We often observe mobile and desktop applications bundled with Ad-displaying programs, called Adware, to generate revenue.

Just last week we reported about "Kemoge Android Adware," disguising itself as popular apps, is making the rounds in as many as 20 countries. Kemoge malware, whose origin is suspected from China, can root vulnerable Android devices, which practically allows hackers to take over victim's Android device.

Once installed, the malware automatically download other Apps it gets paid to promote.



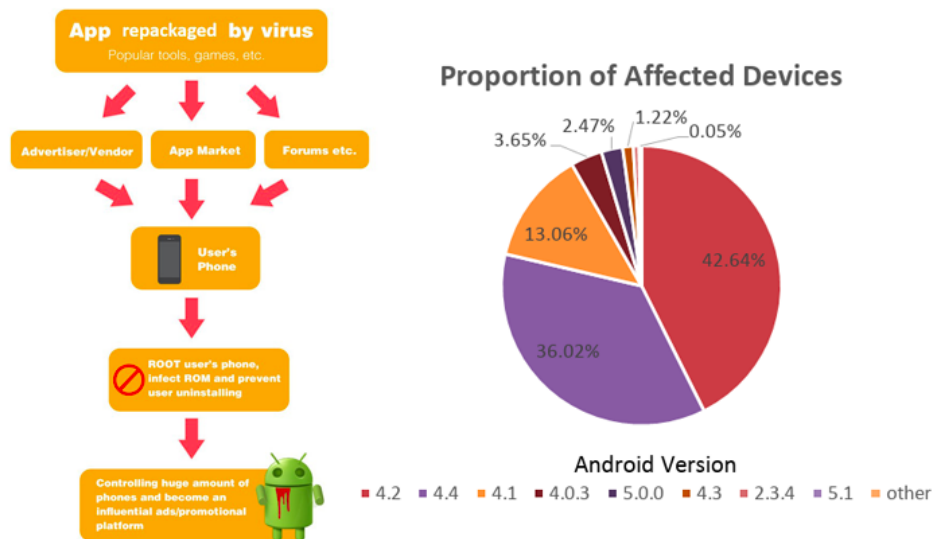
But Kemoge adware is not alone, the researchers have discovered some of its variants that belong to the same malware family.

Chinese Adware Family Threatening your Android

In a recent [blog post](#), Security experts at *Cheetah Mobile* company, developers of CM Security and Antivirus apps, detailed about how Chinese hackers are making millions of profits from underground App distribution chains.

Other members of the same family are:

- Ghost Push
- Braintest
- Guaranteed Clicks
- RetroTetri



All these malware under same illegal Mobile Marketing Industry Chain follow a similar modus operandi; which is:

- Repackage popular apps to injected malicious code and Ad components
- Bypass Google Play Store's Bouncer Security
- Exploiting existing Android vulnerabilities to gain Admin-level permissions
- Root users' devices that make them unable to uninstall the virus
- And then promote malicious apps through legitimate channels

"As users are completely unable to uninstall these malicious apps, the virus developers soon get a massive number of active users." Cheetah Mobile researcher said.

"With this user base, the virus developer is able to set up a marketing promotion company and become a mobile dealer. Then they have the qualifications to cooperate with ad"

sponsors, making money by distributing products for advertisers.”

These malicious apps were found on some famous App Stores, including Google Play, Aptoide and Mobogonie.

Some Critical Findings from their Research are:

- This Virus family includes 4000 Samples
- The Adware is affecting Android versions from 2.3 to 5.1.
- More than 10,000 phone types and 2,742 brands have been affected.
- The virus has affected more than 900,000 Android users in over 116 countries, especially Southeast Asia.
- More than four suspicious domain names have been identified.

Tips for keeping your Android Device Safe

Users are advised to:

- never click on suspicious links from emails or websites,
- be careful what you download,
- don't install apps without reviewing them,
- inspect each and every permission an Android app asks for,
- keep your Android device updated.

Read More:

- [China Admits It Has Army of Hackers](#)
- [China arrested Hackers](#) at U.S. Government Request
- [China Using A Powerful 'Great Cannon' Weapon to Censor The Internet](#)
- [China Demands Tech Companies to give them Backdoor and Encryption Keys](#)


To grab more of what China-based hacks and attacks are capable of, [Follow us](#) and Stay Tuned.

Ads by Google

- ▶ [Chinese Hackers](#)
- ▶ [Hack Hacking](#)
- ▶ [Ethical Hacking](#)

Android, Android Adware, Android Malware, Android Rooting, Chinese Hackers, Hacking News, Malware

ABOUT THE AUTHOR



Khyati Jain

Researcher and Technical Writer at The Hacker News. An Information Security Consultant and System Auditor, a keen Security Evangelist for all forms of Cyber Security and Denotational Counter Hack Requirements of the Industry, Academia and Society.

The Hacker News

WANT MORE STUFF LIKE THIS?

Want more Interesting News like this? [Sign up](#) here to receive the best of 'The Hacker News' delivered daily straight to your inbox.

 Email address

Subscribe

LATEST STORIES



Every Call You Make or Text You Send, They'll Be Tracking From Today



How Some Chinese Hackers Started Making Big Money



USB Killer v2.0 — Latest USB Device that Can Easily Burn Your Computer



w00t! Google OnHub Router actually Runs on Chrome OS; Here's How to Root it



Record-Breaking Deal: Dell to Buy EMC for \$67 Billion



THN Weekly RoundUp – 12 Hacking Stories You Don't Want To Miss This Week



Apple Kicks Out some iOS Store

Malicious Ad-Blocker Apps from its Online Store



Critical Netgear Router Exploit allows anyone to Hack You Remotely

COMMENTS

0 Comments

The Hackers News

Исследовательс...

Recommend

Share

Sort by Newest



Start the discussion...

Be the first to comment.

ALSO ON THE HACKERS NEWS

WHAT'S THIS?

USB Killer v2.0 — Latest USB Device that Can Easily Burn Your Computer
8 comments • 18 hours ago
Nooble — ultimate phaser when the feds drop in. lol

Apple Kicks Out some Malicious Ad-Blocker Apps from its Online Store
1 comment • 3 days ago
Edith Reese! — Crap?

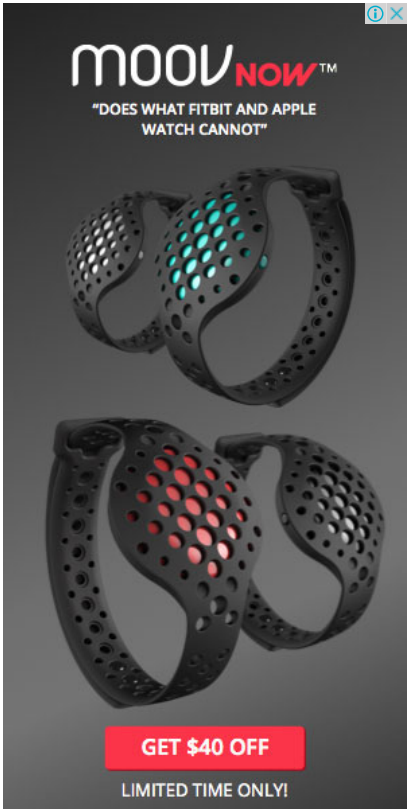
WordPress Security: Brute Force Amplification Attack Targeting Thousand ...
3 comments • 5 days ago
savenaturefree google-me — Is a VPN secure enough for business paypal transactions?

This Secure Operating System Can Protect You Even if You Get Hacked
1 comment • 6 days ago
bakwud — Will check this out...sounds very interesting.


Subscribe Add Disqus to your site Privacy


DISQUS








Popular Stories


 How to Weaponize your Cat to Hack Neighbours' Wi-Fi Passwords


 Google rewarded the Guy who Accidentally bought Google.com, But he Donated it to Charity


 USB Killer v2.0 — Latest USB Device that Can Easily Burn Your Computer


 British Intelligence Agency Can Hack Any Smartphone With Just a Text Message

 This Secure Operating System Can Protect You Even if You Get Hacked

 Critical Netgear Router Exploit allows anyone to Hack You Remotely

 Collision Attack: Widely Used SHA-1 Hash Algorithm Needs to Die Immediately

 How to Activate GodMode in Windows 10

 WordPress Security: Brute Force Amplification Attack Targeting Thousand of Blogs

Microsoft Pays \$24,000 Bounty to Hacker for Finding 'Account Hacking'

4,000 B

Technique

for Hacking Hotma
outlook.com) Accou

Hey Hackers!

Call For Papers

ASIA'S FOREMOST INFORMATION SECURITY CONFERENCE

GROUND ZERO

SUMMIT 2015

Submit Now

Register

EYESCREEN

Classic Check Dress

復古英倫

珍珠扣傘擺洋裝

\$ 399 UP

SHOP NOW

Powered by Google

Change privacy options

Let apps use my advertising ID for experient apps (turning this off will reset your ID)

OFF

Turn on SmartScreen Filter to check web co that Windows Store apps use

ON

Send Microsoft info about how I write to be improve typing and writing in the future

OFF

Deleting WhatsApp Messages Could Land you in Jail

lenovo

CAUGHT RED-HANDED (3RD TIME)

Pre-Installed Spyware Found in Lenovo Laptops

How Amazon Employee bought 'Google.com' Domain for Only \$12 from Google

How to Run Multiple Whatsapp Account on Your Android Phone

Hacker Finds a Simple Way to Bypass Android 5.x Lock Screen [Screenshot Video]

NEXT >

About | THN Magazine | The Hackers Conference | Sitemap | Advertise on THN | Submit News | Privacy Policy | Contact