Security

Dangerous Android banking bot leak signals new malware wave

26

GM Bot can rip creds, steal SMS and phone two factor tokens

23 Feb 2016 at 08:30, Darren Pauli 41 91

Android users could be hit with a new wave of dangerous banking malware following the leak of source code for a capable Android trojan.

Users could be targeted with variants of the malware, known as "GM Bot", that is capable of harvesting usernames and passwords using slick keystroke-capturing website overlays.

Since it infects mobile handsets it can steal two factor authentication including SMS and even redirect phone calls.

IBM threat bod Limor Kessem says the leak appears to have come from a GM Bot buyer and is bad news for users.

"This turnkey capability is the true differentiator; previous mobile malware could steal SMS codes, but those would have been meaningless without phishing schemes or a trojan on the victim's PC to steal access credentials," Kessem says.

"The reverse was also true: phishers and PC trojan operators could not facilitate fraudulent transactions without mobile malware to intercept the SMS codes or calls from the bank.

"In short, mobile banking trojans such as GM Bot are a one-stop fraud shop for criminals."

Attackers can target any website or banking app to harvest credentials and tokens from infected phones.

GM Bot was first discovered late last year when CERT Poland described the malware as a simple but effective bank raiding tool.

The CERT's researchers said of the malware that "... the attacker needs only to infect the Android phone and there is no need for a Windows counterpart."

The malware joins the ranks of other leaked PC trojans including Zeus, SpyEye, and Carberp.

If history is a judge, it is likely the malware will result in various low- and high- quality spin-offs.

Users should update their handsets to the latest Android versions which contain more rigorous security and permission checks. Those who cannot upgrade from old versions on account of vendors no longer shipping updates can consider installing custom but well-supported-and-maintained ROMs such as Cyanogenmod and NamelessROM. ®

Tips and corrections 26 Comments

More from The Register

More like this

Malware Security

Most read

'I bet Russian hackers weren't expecting their target to suck so epically hard as this'

Reminder: How to get a grip on your files, data that Windows 10 phones home to Microsoft

Between you, EE and the lamppost ... this UK cell network is knackered

FBI v Apple spat latest: Bill Gates is really upset that you all thought he was on the Feds' side

Apple hasn't announced the new iPhone 5SE and pundits already hate it

Spotlight

Connecting to the Tor network

Loading relay information

Please wait while we establish a connection to the Tor network.

Akamai buys out Scottish web security firm Bloxx

Unspecified cash deal to embiggen cloud security

4 Comments

FBI has its fingers deep in NSA surveillance pie, declassified report shows

Feds had a hand in PRISM, too

8 Comments

Undetectable NSA-linked hybrid malware hits Intel Security radar

While Flash malware nastiness detections quadruple – we're all clearly doomed

56 Comments

FBI opens Malware Investigator portal to industry

Agency trades malware samples for intel reports

7 Comments

White hats, FBI and cops team up for Dorkbot botnet takedown

Your four-year reign of terror is (temporarily) over

5 Comments

Court to Wikimedia: Your NSA spying evidence is inadmissable, so you can't prove NSA spying

Catch-22: It's the best catch there is

35 Comments

Whitepapers

Data theft prevention

This data theft prevention report focuses on how to stay secure while you innovate from a broader, in-scope, more intelligent in application perspective.

Securing Your Network and Application Infrastructure

A range of industry analysts, consultants, and hands-on security experts provided responses to this question.

The 2016 Cyber Risk Executive Summary

Hacker attacks are evolving to target applications and to focus on financial gain. This report brings you the key findings and conclusions of this year-long research effort.

Strengthening networks and endpoints with behaviour-based protection

How integrated, intelligent solutions from IBM can detect and help prevent threats from the network perimeter to remote endpoints

Tor users are actively discriminated against by website operators

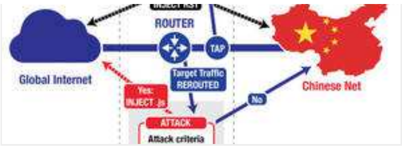
Row over GCHQ-built voice algo MIKEY SAKKE rumbles on

Techie on the ground disputes BlackEnergy Ukraine power outage story

Asda slammed for letting vulns fester on its cyber shelves

Australia and America working on global no-state-hacking pact

PDF redaction is hard, NSW Medical Council finds out - the hard way



What if China went all GitHub on your website? Grab this coding tool

Invite-only bug bounty criticised for turning up the heat on Tor

Sponsored links

Sign up to The Register to receive newsletters and alerts

The Register

Independent news, views, opinions and reviews on the latest in the IT industry. Offices in London, San Francisco and Sydney.

About us

- Privacy
- Company info
- Advertise with us
- Syndication
- Send us news tips
- Know HTML? We're hiring!

More content

- Subscribe to newsletter
- Top 20 stories
- Week's headlines
- Archive
- eBooks
- Webcasts

Follow us