WireX DDoS Botnet: tens of thousands of Android phones are hacked

If you believe that just because you download the app from the official Google store will not be malware, think again.

A group of security researchers from several security companies have discovered a new botnet with a wide network of tens of thousands of Android phones.

Called WireX and discovered under the name **Android Clicker,** this botnet network consists of infected Android devices running 1 of hundreds of malicious applications installed from the Google Play Store. It is designed to perform attack type DDoS into the application layer.

Researchers from various security and technology companies, including *Akamai, CloudFlare, Flashpoint, Google, Oracle Dyn, RishIQ, Team Cymru* , discovered a string of cyber attacks earlier this month. and work together to fight them.

Although malware cases on Android are also quite popular today, this new discovery is much more complicated. Although they are rivals, these companies have shared information and put together this botnet. WireX was used for DDoS attacks earlier this month, but since about mid-August, attacks have become increasingly common.

WireX botnet currently infected more than 120,000 Android devices and reached the peak at the beginning of this month. On August 17, the researchers noticed a wide-area DDoS attack (primarily requiring HTTP GET) derived from more than 70,000 poisoned mobile devices from more than 100 countries.

If your website has been attacked by DDoS, check the User-Agent chain to see if you have joined the WireX botnet.

```
User-Agent: jigpuzbcomkerhvladtwysqfxr
User-Agent: yudjmikcvzoqwsbflghtxpanrc
User-Agent: mckvhaflwzbdcriysoguxnqtpj
User Agent: deogjvtynmcxzwfsbahirukqpl
User Agent: fdmjczoeyarnuqkbgtlivsxhwp
User Agent: yczfxlrenuqtwmavhojpigkdsb
User-Agent: cnlseufokcgvmajqzpbtrwyxih
```

Check User Agent on the website

After the investigation, the researchers discovered more than 300 tainted applications on the official Google Play Store store, forged as multimedia files, video players, ringtones, memory management tools, application . contains WireX malicious code.

Like many other poisoning applications, applications infected with WireX do not execute immediately after installation to avoid detection. They wait for a command from the C&C server located at multiple subdomains of axclick.store.

Google has detected and blocked almost 300 applications, mostly downloaded by users in Russia, China and Asian countries. Even so. The botnet WireX still works on a small scale.

If your device is running Android with a new version of Google Play Protect, WireX apps will automatically be deleted from the device. This is a new security feature that uses the machine learning method and rate analysis to use the application to remove (uninstall) the poisoned application.