Warning: GRIM and Magnus Android Botnets are Underground

fortinet.com/blog/threat-research/grim-magnus-android-botnets

April 29, 2022

The lifecycle of an Android banking botnet typically consists of two stages: **rise** and **fall**. During the rising phase, the malware author promotes their new code and rents it underground—MaaS (Malware as a Service). As the botnet gains popularity, it evolves with new features and pricing. At some point, though, an issue occurs, triggering its fall. For example, the author gets caught (e.g Anubis) or its source code gets released on underground forums (either willingly by the authors themselves, by a competitor, or perhaps an unhappy customer). As a result, the botnet gradually dies. And unfortunately, others pop up on the market to take its place.

As malware analysts, the Android/Marcher, Locker, and Anubis malware we used to see have been replaced by BianLian, Cerberos, and Flubot (and still Anubis). A year ago, threat actor(s) started advertising a newcomer, the Huracan botnet. We haven’t seen it in the wild yet—or if we have, we haven't recognized it (it's not always obvious to match underground names with the samples we analyze).

> Since the **beginning of 2022, there are even more newcomers**. I have **spotted at least two future banking botnets: GRIM** and **Magnus**. You should be keep an eye on those two, as they will probably emerge in the wild in the next few months.

Underground advertisement

The **Magnus** Botnet has been repeatedly advertised underground by a threat actor named *whit3_d3vil* since February 2022. It is unclear whether *whi3_d3vil* is the author or just a reseller. The botnet implements all the typical features that banking trojans currently have: overlay injection over mobile banking applications, sending SMS, SMS interception, 2FA bypass, remote administration via VNC, etc. And unlike BianLian, **communication with C2s is encrypted using AES**.

Figure 1: Magnus bot advertised on an underground forum

The botnet can be rented for *1,000 USD per month*.

Should we be amused or anxious that malware are being sold like boxes of cookies on the web? There are even **sales** (prices marked down from 1,600 USD to 1,000 USD), watermarked screenshots (against competitors?), and **videos** demonstrating the product!

Figure 2: Magnus bot advertisement with lowered price

The **Grim** botnet is less expensive: only 500 USD/month. It is being advertised on a specialized Telegram channel. It implements more or less the same features as the Magnus bot. Prices for underground botnet packages are freely fixed by the authors/resellers. They don't necessarily match features. A lower price for Grimbot can mean the malware has less notoriety, for instance, rather than fewer features.

Figure 3: Screen capture of a demo video of Grimbot exhibiting its injection features on various mobile banking apps (targets)

How does this concern me?

If you are a **malware analyst**, be on the lookout for **a new banking botnet whose communication with its C2 is encrypted with AES (Magnus) or a botnet with tags such as "grim" that poses as a "Security" application**.

Fortunately, if you are protected by Fortiguard Antivirus (e.g. FortiGate, FortiClient, FortiMail, FortiWeb, FortiProxy), you are automatically protected against many Android banking trojans.

However, there are a few other precautions you should take:

1. Android banking trojans typically pose as famous applications: Video Player, Play Store, Flash Player, etc. Be sure to download such applications only from a trusted marketplace. **Never follow a link (email or SMS) to download the app**, even if it comes from a presumed friend. ***Important:*** Note that banking trojans do not usually pose as a mobile banking app. Rather, they pose as another app, detect when you use your (genuine) mobile banking app, and display (overlay) malicious windows on top of the real ones.
2. All those banking trojans also **abuse Android Accessibility Services**. Accessibility Services are meant to help people with disabilities. **Do not grant such rights** to any other application!

Figure 4: This is the standard alert screen on Android that shows when an application tries to use Accessibility Services. You should **not** accept this. Instead, click Cancel immediately, uninstall the corresponding app, and scan your smartphone

Figure 5: This screen is a very good indicator of an infection by Android/BianLian. Do not activate accessibility services! Uninstall the application immediately and scan your smartphone for viruses with AV for higher security

Fortinet Protection

Fortinet products detect malware discussed in this blog:

Anubis

- Android/Anubis.AOG!tr
- Android/Anubis.CST!tr
- Android/Anubis.BIR!tr
- Android/Anubis.AMB!tr

Marcher

Android/Marcher.X!tr

Locker

- Android/Locker.KV!tr
- Android/Agent.BFQ!tr
- Android/Agent.BDH!tr

BianLian

Android/BianLian.10484!tr

Cerberus

- Android/Cerberus.DF!tr
- Android/Agent.DDF!tr

Flubot

- Android/Flubot.G!tr
- Android/Agent.HWW!tr

Learn more about Fortinet’s FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.