Hunting the AndroidBianLian botnet Axelle Apvrille Fortinet

Published: 2022-10-24 · Archived: 2026-04-05 16:03:04 UTC

Presented at the VB2022 conference in Prague, 28 - 30 September, 2022. ↓ Slides: https://www.virusbulletin.com/uploads... ↓ Paper: https://www.virusbulletin.com/uploads... → Details: https://www.virusbulletin.com/confere... ✪ PRESENTED BY ✪ • Axelle Apvrille (Fortinet) ✪ ABSTRACT ✪ The Android BianLian is a banking trojan botnet which was discovered in 2018. Also known as Hydra, it shares roots with Anubis and BankBot. So, why talk about it in 2022? Because the botnet is surprisingly resilient and has been very active again since the beginning of 2022! Its code is carefully designed: a core with extendable features implemented as plug-ins (called 'components' in the implementation). In the talk, we remind the audience of the available features implemented by the malware, its three-stage payloads, and show the evolution of Accessibility Services abuses. We explain how we built a fake, local, C2 to test features and communication with bots. Among the very recent novelties, we witnessed an ongoing effort to bypass 2FA used by some German banks (e.g. photoTAN). Next, we focus on a few implementation errors (e.g. authorization code is not checked on the C2) and new concepts the malware author(s) tested. For instance, they implemented access to the Tor network to talk to onion websites. They also tested different packers through time to harden reverse engineering. Yet sometimes, later on, we were surprised to see them fall back to less advanced features. In the second part of the talk, we focus on threat actors' organization: who and where botnet builders & panels are sold, which host and domain providers they prefer, and how we manage to hunt them. As expected, some discussions occur on the Darknet, but since many forums and marketplaces were taken down a few years ago, lots of underground discussions now take place through Telegram or Discord channels, hidden forums, etc. We have identified a few 'credible' actors who have been selling BianLian and other Android botnets since 2020. The prices range from 150 USD to over 1500 USD (or cryptocurrencies), depending on the botnet, whether the botnet supports recent versions or not, and if the threat actor offers support (and even hosting) or not. The sellers promote their work with demo videos. The BianLian botnet does not have any easily identifiable name, signature, banner or string to search for it. Despite this, we managed to locate 20+ C2 admin panels (we'll explain the trick we used), 10 of which are currently active. Those C2s are maintained: malicious domain names change every two to three days; IP addresses usually live longer (around a month). Each botmaster connects regularly – every few days, at most every two weeks – via the web admin panel or through SSH. They cover their tracks and connect from different geographical locations, using compromised networks particularly from universities or educational institutions. Those 10 botnets run the same BianLian source code (or very similar versions), but we believe they are run by independent threat actors because they target different banks, in different regions, and use a different pattern of host providers or domain names.
