Uncovering a broad criminal ecosystem powered by one of the largest botnets, Glupteba Luca Nagy Goog

Published: 2022-10-24 · Archived: 2026-04-02 11:07:30 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 ✪ • Luca Nagy (Google) ✪ ABSTRACT ✪ Botnets continue to be a serious threat against companies and individuals worldwide. However, little is known about exactly how botnets are monetized and how revenues flow to criminal actors. Our research uncovers a whole criminal network of organizations behind a one million sized botnet, named Glupteba. The Glupteba botnet rose to our attention after being downloaded tens of thousands of times per day through traffic distributors and pay-per-install networks. The botnet is known to steal user credentials and cookies from infected hosts, mine cryptocurrencies and deploy and operate proxy components. Given the botnet's size, its technical sophistication and the wide range of functionality provided by the botnet, we decided to map out the ecosystem and understand the incentives and functioning of this underground economy to better disrupt it and build better defences in the future. Our investigation led us to uncover a complex ecosystem formed by the botnet, its operators and victims and the customers of the various illicit services provided by the botnet. For instance, a cookie theft service aimed at abusing advertising networks including Google, Facebook and Twitter (dontfarm), a proxy provider giving botnet customers the ability to proxy traffic through victim machines (awmproxy), or a service which sells credit card numbers to be used for malicious activities such as purchasing malicious ads or conducting payment fraud (extracard). The Glupteba ecosystem is one of the most complex we have witnessed that also supports multiple platforms. We have identified and analysed multiple components used by the Glupteba actors. We will share details of many of them, including proxy and ad fraud components running on Windows and IOT devices. Our year-long study of this broad ecosystem led to novel findings and attributions that led to disruption and legal actions undertaken against the Glupteba operators. In this presentation we will walk through our in-depth investigations starting with the botnet’s distribution techniques, its capabilities and how each capability was monetized in this broad criminal ecosystem.
