2022 PRAGUE

28 - 30 September, 2022 / Prague, Czech Republic

UNCOVERING A BROAD CRIMINAL ECOSYSTEM POWERED BY ONE OF THE LARGEST BOTNETS, GLUPTEBA

Luca Nagy

Google, Switzerland

lucanagy@google.com

ABSTRACT

Botnets continue to represent a serious threat for 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 it provides, we decided to map out the ecosystem and try to understand the incentives and functioning of this underground economy in order to be better able to disrupt it and to 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* (dont[.]farm), a proxy provider giving botnet customers the ability to proxy traffic through victim machines (AWMProxy), and a service that 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 being taken against the Glupteba operators.

INTRODUCTION

Glupteba was first spotted in the wild in 2011. We have observed the botnet targeting victims worldwide, including in the US, India, Brazil, Vietnam and Southeast Asia.

The Glupteba malware family is distributed primarily through pay-per-install (PPI) networks and via traffic purchased from traffic distribution systems (TDS). For a period of time, we observed thousands of instances of malicious Glupteba downloads per day and estimated around one million infected machines. Figure 1 shows a web page mimicking a software crack download which delivers a variant of Glupteba to users instead of the promised software.

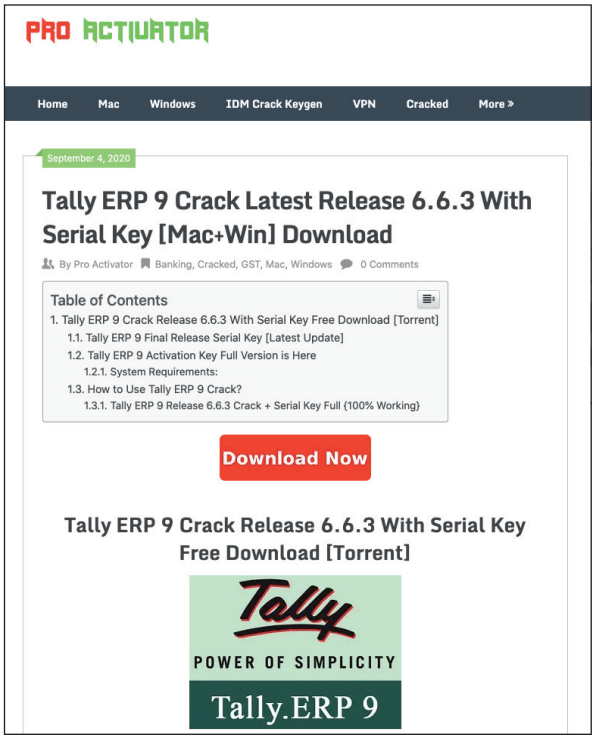

Figure 1: Example of a cracked software download site distributing Glupteba.

CAPABILITIES OF GLUPTEBA

The Glupteba dropper is known for using the blockchain for updating its C2 domains. When the main C2 servers do not respond, infected systems can retrieve backup domains encrypted in the latest transaction from Bitcoin wallet addresses that are hard coded in the binaries. Glupteba also acts as a rootkit by dropping vulnerable kernel drivers in order to hide itself from different kernel structures. Glupteba can spread on the local network by using EternalBlue, and the dropper is capable

of backdooring the infected machine. Based on dynamic analysis we observed many components dropped by the dropper. The most frequent are the proxy components, router exploiters, browser stealers and miners. Additionally, even in low volume, we observed some side-loaded *Android* samples of Glupteba downloaded from third-party APK downloader sites.

ACTORS

While analysing Glupteba binaries, we identified a few containing a git repository URL: git.voltronwork.com. This finding sparked an investigation that led us to identify, with high confidence, the individuals operating the Glupteba botnet. Voltronwork, or Voltron, is a Russia-based developer company using git.voltronwork.com and gitlamp.com for developing different components of Glupteba. We found these git domains in some droppers as well. These git repositories led us to find the *Android* variants.

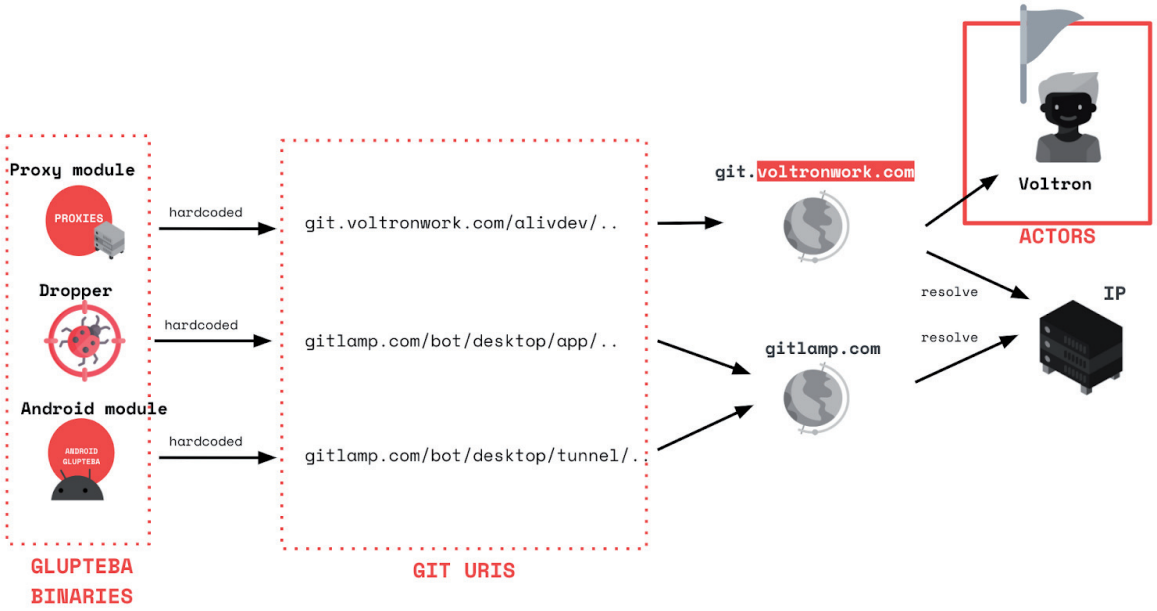

Figure 2: Hard-coded git URIs in Glupteba binaries.

SERVICES

In investigating the registered companies associated with Voltronwork we observed a service, named trapspin.com, which is supported by Prestige-Media, Valtron LLC and Investavto LLC. These companies led us to find more services belonging to these entities, such as AWMProxy and dont[.]farm.

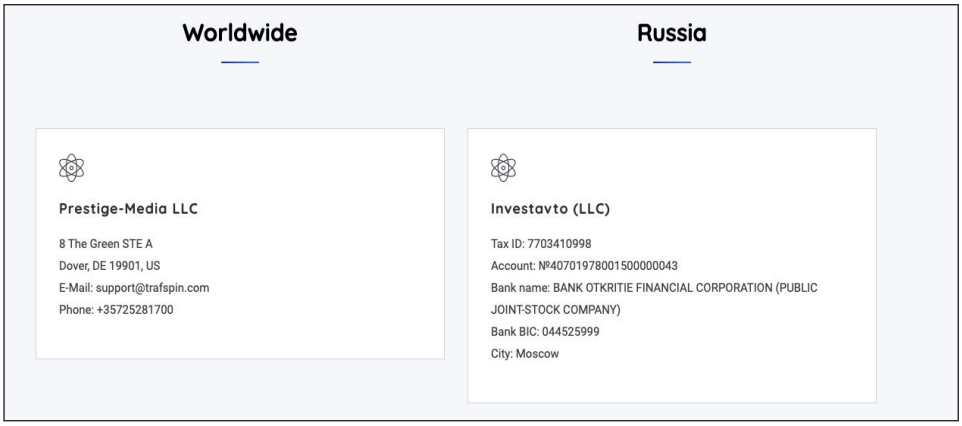

Figure 3: Contact page of trafspin.com.

AWMProxy

AWMProxy is a residential proxy provider. To access the proxy pool, the customer has to configure their device with a given IP and port number which points to the gateway server. The Glupteba tunnelled proxy is installed on the victim machine and it registers the bot to the server via a DNS request, such as:

```
808f38e3-d84b-45c8-b461-2a4c006a0f4a.server-3.easywbdesign.com
```

We observed that these gateway IP addresses overlapped with the Glupteba tunnelled proxy's C2 IPs.

This overlap suggests to us that the actors behind Glupteba are developing AWMProxy, leveraging the proxy capabilities of the Glupteba botnet.

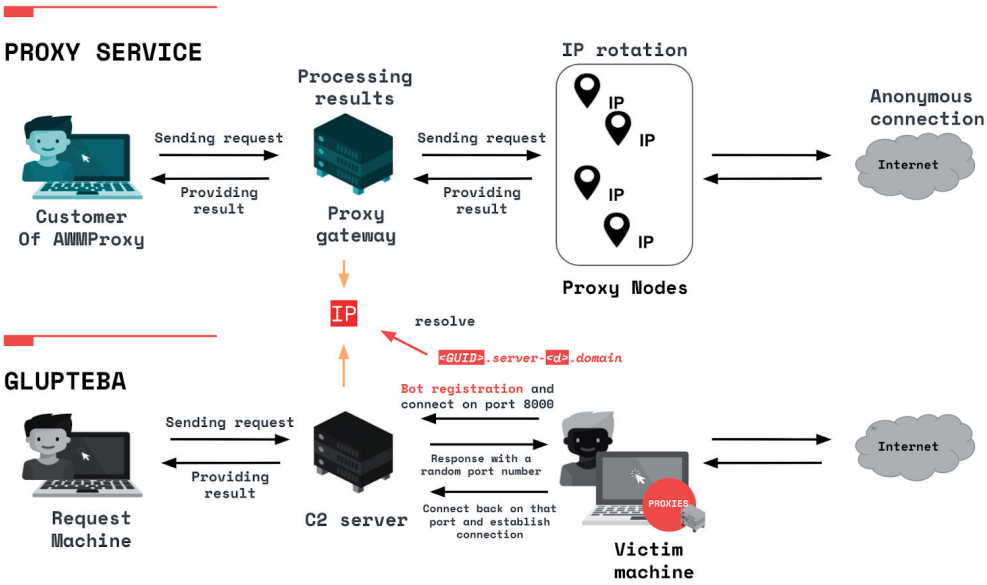

Figure 4: AWMProxy and Glupteba.

Trafspin

Trafspin.com is a real-time bidding advertising network that sells disruptive in-app advertising on *Android* and web traffic through the botnet's proxy connections to mobile devices infected by the Glupteba malware. The *Android* variants of Glupteba that we discovered through the hard-coded gitlamp.com git URIs in old ELF proxy modules led us to find Glupteba APKs which were acting in a very similar way to the Glupteba desktop variant. They had an interesting method of showing advertisements in a disruptive way: the 'close' button of the shown advertisement was hidden. We caught a configuration response from 2018 using the trafspin.com domain which suggested to us that the *Android* Ads module uses the trafspin advertisement network. The APK's network response from the C2 was as follows:

```
[{"command":"showDialog","payload":{"arg":"{\"link\":true,\"advanced_webview\":true,\"can_
close\":true,\"block_back\":false,\"click_url\":\"http://domainforwork.com/ads/
click?id=7132411\",\"content\":\"https://click.trafspin.com/ads/view-url?id=xxx&url=...
```

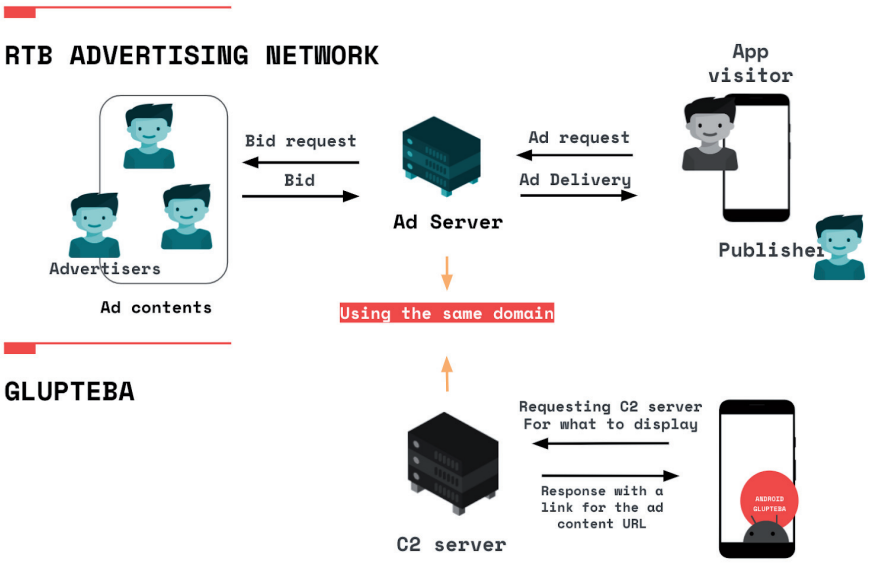

Figure 5: RTB advertising network and Glupteba.

Dont[.]farm

Dont[.]farm is an ads account service. It sells access to users' accounts with *Google* and other online platforms. The operator loads stolen credentials and cookies of the stolen accounts to virtual machines, to which they sell access. On their website, the operators claimed that they support blackhat advertisements for *Google Ads*. They also claimed that they provide a proxy pointing to the same geolocation as the hijacked user's location. It is likely that the service uses the Glupteba infected machines for proxying in the same way as AWMProxy, and the accounts are hijacked by the Glupteba browser stealer module.

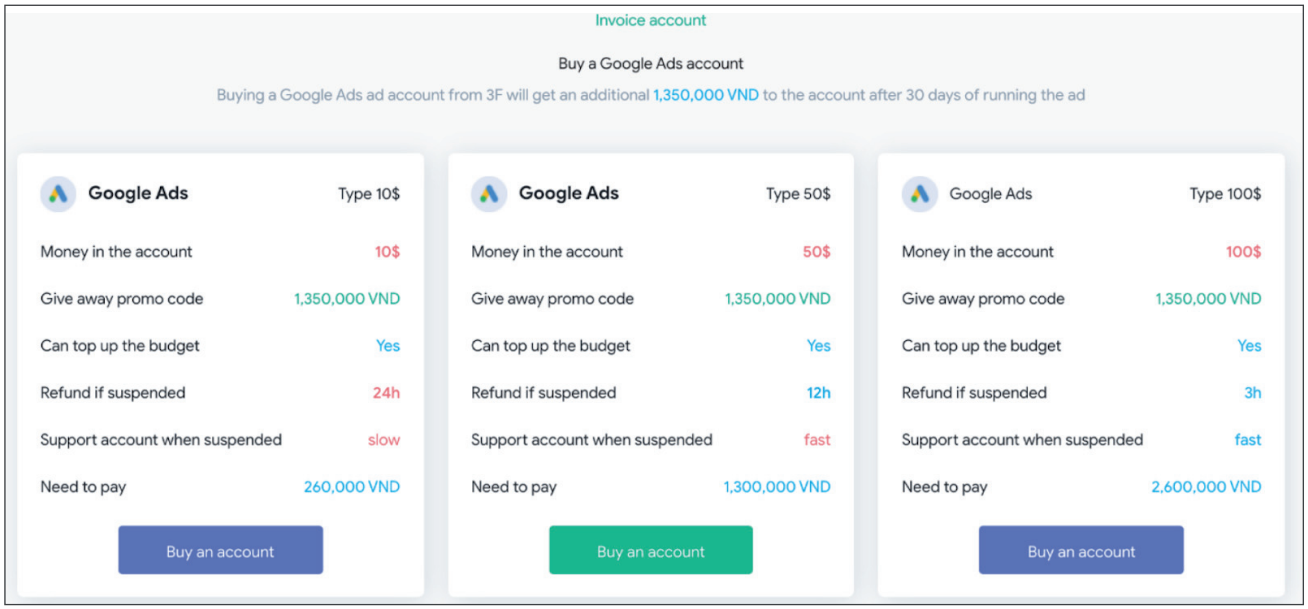

Figure 6: Dont[.]farm offers Google Ads accounts.

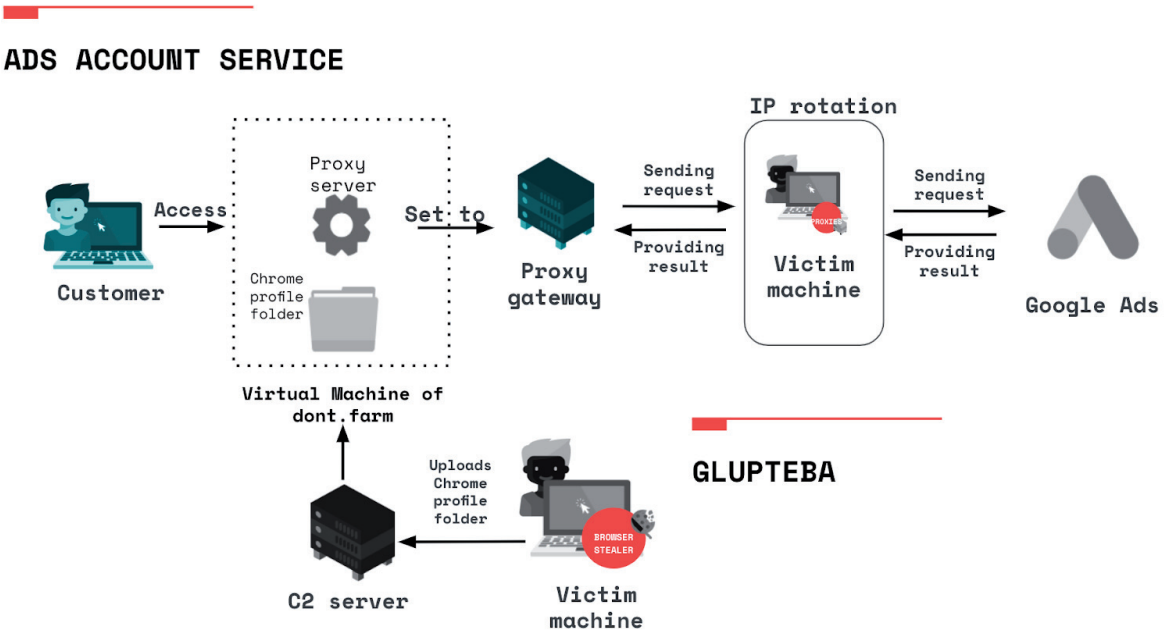

Figure 7: Dont[.]farm infrastructure.

ECOSYSTEM

Based on our research we discovered the actors behind Glupteba developing the different components. We learned that the Glupteba actors provide other services which are leveraged on Glupteba's capabilities. We found evidence for connections between different components of Glupteba and the services, such as AWMProxy, Trafspin and dont[.]farm. These led us to the conclusion that Glupteba is monetized by these services, and helped in disrupting the botnet.

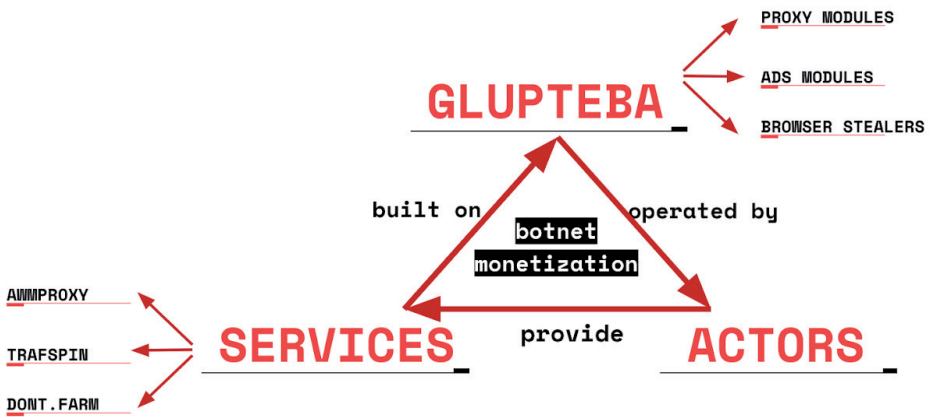

Figure 8: Ecosystem.

DISRUPTION

Since 2021, multiple teams at *Google* have coordinated their efforts to disrupt Glupteba activity. The company terminated around 63 million *Google Docs* observed to have distributed Glupteba, 1,183 *Google Accounts*, 908 *Cloud Projects* and 870 *Google Ads* accounts associated with their distribution. Furthermore, 3.5 million users were warned before downloading a malicious file through *Google Safe Browsing* warnings.

In December 2021, TAG partnered with Internet infrastructure providers and hosting providers, including *CloudFlare*, to disrupt Glupteba's operation by taking down servers and placing interstitial warning pages in front of the malicious domain names. During this time, an additional 130 *Google* accounts associated with this operation were terminated. In parallel with the analysis, tracking and technical disruption of this botnet, *Google* has filed a lawsuit against two individuals believed to be located in Russia for operating the Glupteba botnet and its various criminal schemes.

Since then we have seen a significant decrease in the size of the botnet. However, technically, the operators of Glupteba are still able to attempt to regain control of the botnet using a backup command-and-control mechanism that uses data encoded on the Bitcoin blockchain.

ACKNOWLEDGEMENT

Would like to thank all individuals and teams involved, both within *Google* and externally.

REFERENCES

[1] Huntley, S.; Nagy, L. Disrupting the Glupteba operation. Google Updates from Threat Analysis Group (TAG). December 2021. https://blog.google/threat-analysis-group/disrupting-glupteba-operation/.

[2] Hansen, R.; DeLaine Prado, H. New action to combat cyber crime. Google. The Keyword. December 2021. https://blog.google/technology/safety-security/new-action-combat-cyber-crime/.

[3] Google LLC v. Dmitry Starovikov, et al. https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/1_Complaint.pdf.

[4] Nagy, L. Glupteba: Hidden Malware Delivery in Plain Sight. Sophos. June 2020. https://news.sophos.com/wp-content/uploads/2020/06/glupteba_final-1.pdf.