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

Sept, 2022

LUCA NAGY

Threat Analysis Group

twitter: @luca_nagy_

Luca Nagy

Security Engineer @ Google

Threat Analysis Group (TAG)

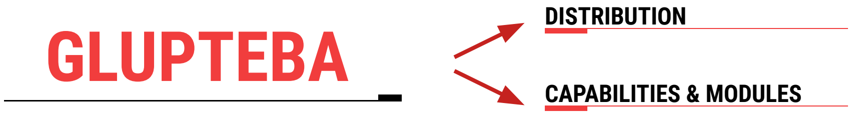
CRIME

Threat Analysis Group

twitter: @luca_nagy_

DISCLAIMER

AGENDA

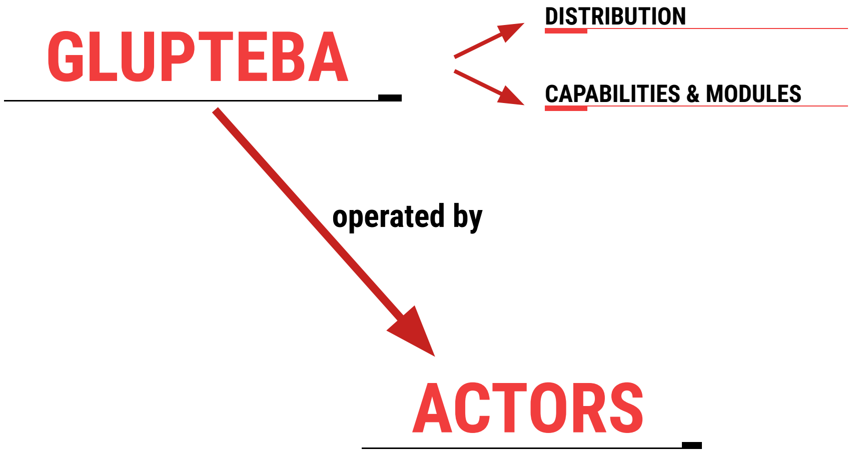


GLUPTEBA

DISTRIBUTION

CAPABILITIES & MODULES

AGENDA



GLUPTEBA

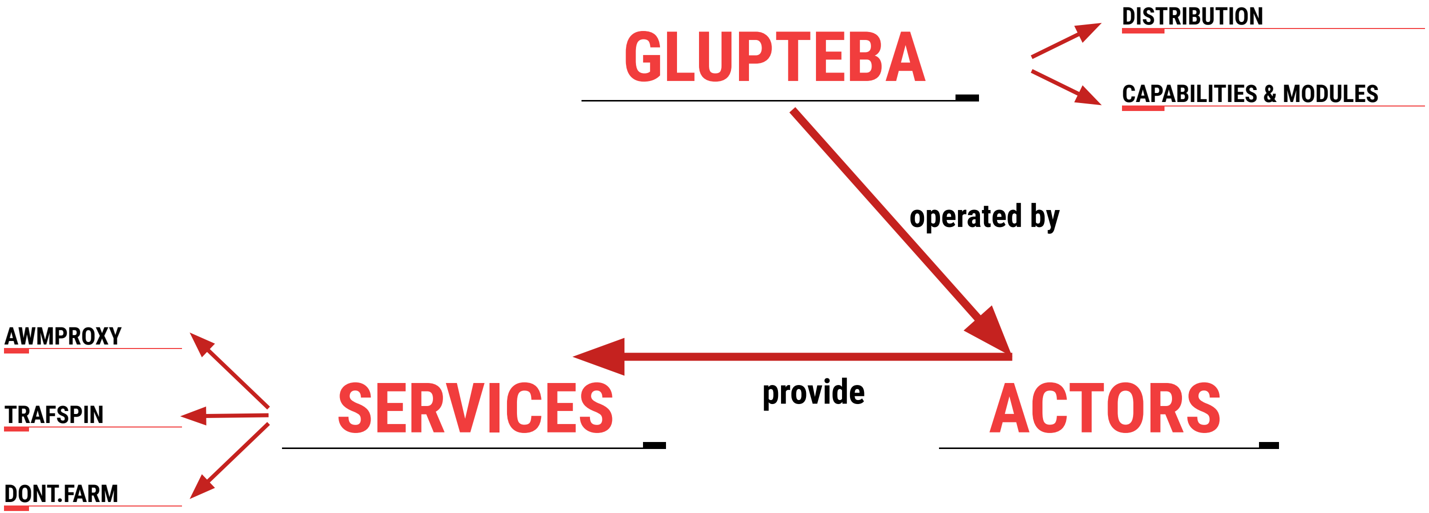
DISTRIBUTION

CAPABILITIES & MODULES

operated by

ACTORS

AGENDA



GLUPTEBA

DISTRIBUTION

CAPABILITIES & MODULES

operated by

ACTORS

provide

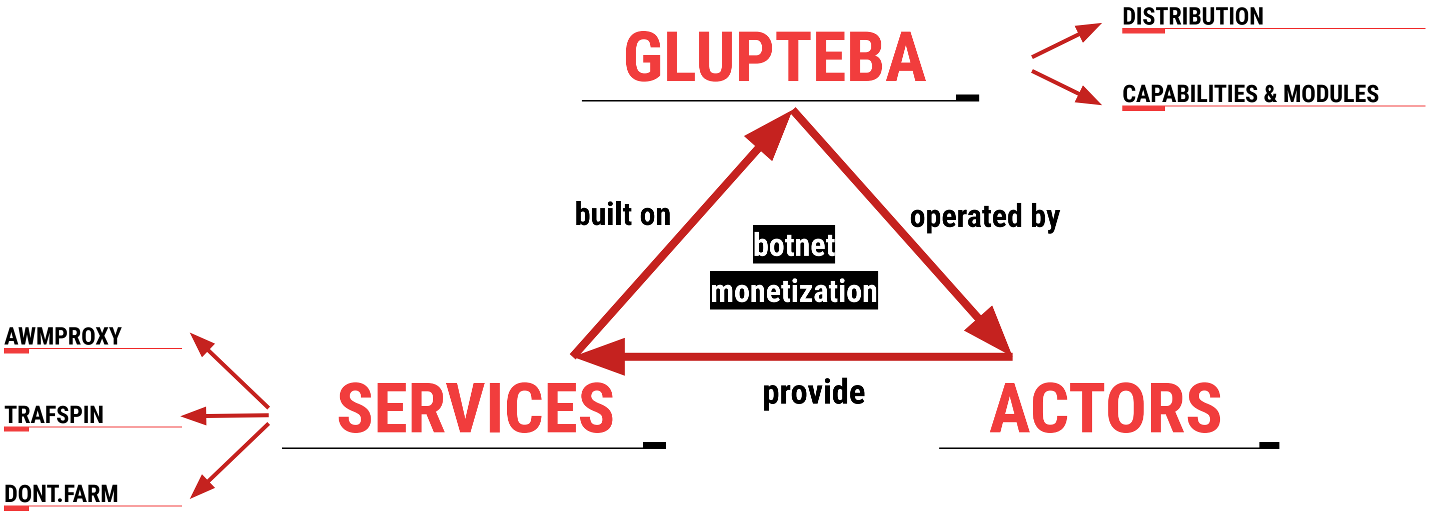
SERVICES

AWMPROXY

TRAFSPIN

DONT.FARM

AGENDA



GLUPTEBA

DISTRIBUTION

CAPABILITIES & MODULES

built on

botnet monetization

operated by

SERVICES

provide

ACTORS

AWMPROXY

TRAFSPIN

DONT.FARM

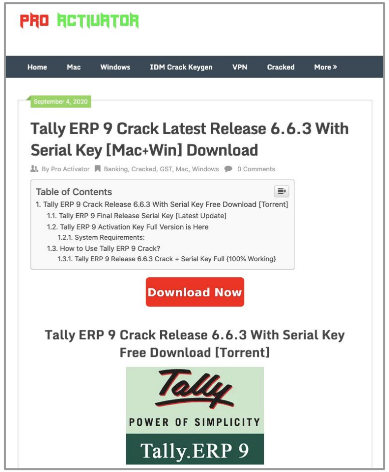
GLUPTEBA

Threat Analysis Group

twitter: @luca_nagy_

DISTRIBUTION

- Since 2011
- PPI network/TDS
- 1M bot



September 4, 2020

Tally ERP 9 Crack Latest Release 6.6.3 With Serial Key [Mac+Win] Download

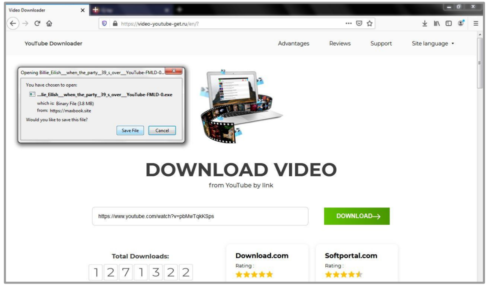
By Pro Activator Banking, Cracked, GST, Mac, Windows 0 Comments

Table of Contents

1. Tally ERP 9 Crack Release 6.6.3 With Serial Key Free Download [Torrent]
   1.1. Tally ERP 9 Final Release Serial Key [Latest Update]
   1.2. Tally ERP 9 Activation Key Full Version is Here
      1.2.1. System Requirements:
   1.3. How to Use Tally ERP 9 Crack?
      1.3.1. Tally ERP 9 Release 6.6.3 Crack + Serial Key Full {100% Working}

Tally ERP 9 Crack Release 6.6.3 With Serial Key Free Download [Torrent]

Click_here



Opening Billie_Eilish__when_the_party__39_s_over__YouTube-FMLD-0...

You have chosen to open:

...lie_Eilish__when_the_party__39_s_over__YouTube-FMLD-0.exe

which is: Binary File (3.8 MB)

from: https://maxbook.site

Would you like to save this file?

DOWNLOAD VIDEO

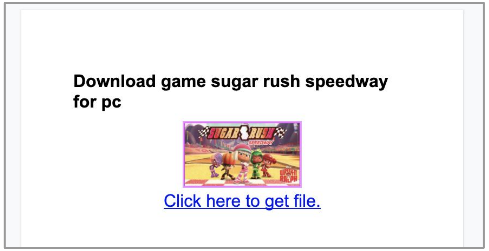
from YouTube by link

https://www.youtube.com/watch?v=pbMwTqkKSps

Total Downloads: 1 2 7 1 3 2 2

Download.com Rating : ★★★★★

Softportal.com Rating : ★★★★★


Download game sugar rush speedway for pc

Click here to get file.

DROPPER CAPABILITIES

ROOTKIT

Kernel drivers to hide itself.

- **Winmon**
  - Process concealment (EPROCESS list)
- **WinmonFS**
  - Hiding objects (FsFilter callback)
- **WinmonProcessMonitor**
  - Monitoring and terminating service processes (1224 process)

DROPPER CAPABILITIES

BACKDOOR

Controlling the machine by using backdoor functions.

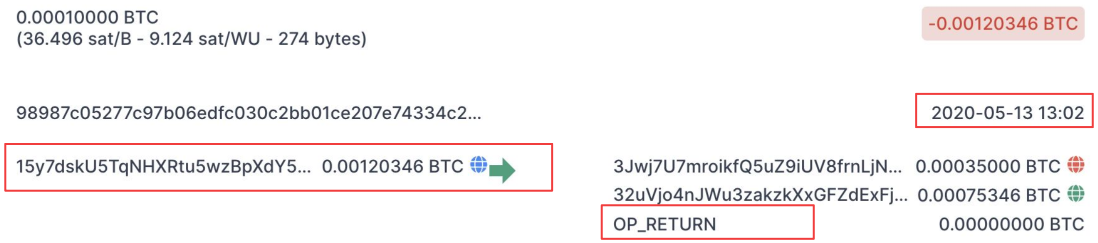
- update
- get_app_name
- is_admin
- process_is_running
- exec
- download
- run
- run-v2
- exit
- update-data
- update-cloudnet
- stop-wup
- stop-wupv
- stop-mrt
- notify
- notify-host
- event-exists
- mutex-exists
- registry-get-startup
- verify-signature
- registry-get-startup-signatures
- verify-processes-signatures
- get-unverified-files
- get-stats-wup
- upload-file
- update-service
- get-logfile-proxy
- install
- get-logfile-i2pd
- sc
- update-cdn
- discover-electrum
- discover-blockchaincome

DROPPER CAPABILITIES

BLOCKCHAIN

For updating C2 domains.

- Hardcoded btc address
- Hardcoded AES key



0.00010000 BTC
(36.496 sat/B - 9.124 sat/WU - 274 bytes)

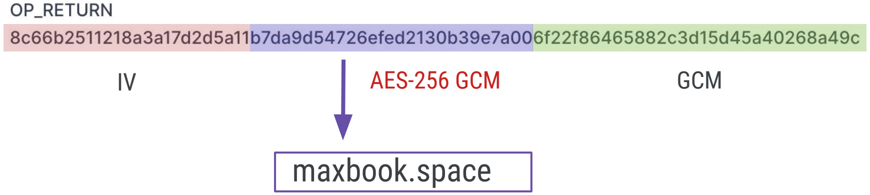
-0.00120346 BTC

98987c05277c97b06edfc030c2bb01ce207e74334c2...

2020-05-13 13:02

15y7dskU5TqNHXRtu5wzBpXdY5... 0.00120346 BTC

3Jwj7U7mroikfQ5uZ9iUV8frnLjN... 0.00035000 BTC
32uVjo4nJWu3zakzkXxGFZdExFj... 0.00075346 BTC
OP_RETURN 0.00000000 BTC



OP_RETURN
8c66b2511218a3a17d2d5a11b7da9d54726efed2130b39e7a006f22f86465882c3d15d45a40268a49c

Threat Analysis Group

twitter: @luca_nagy_

DROPPER CAPABILITIES

BLOCKCHAIN

For updating C2 domains.

- **Github**
  - Public json list of default electrum servers
- **Hardcoded list**
  - Electrum servers
- **Blockchain.com**
  - HTTP request for blockchain.com

DROPPER CAPABILITIES

GAIN PERSISTENCE

Autorun registry key, scheduled tasks.

SPREADING ON LAN

EternalBlue.

DROPPER CAPABILITIES

ANTI-VM TECHNIQUES

Checking VM environment.

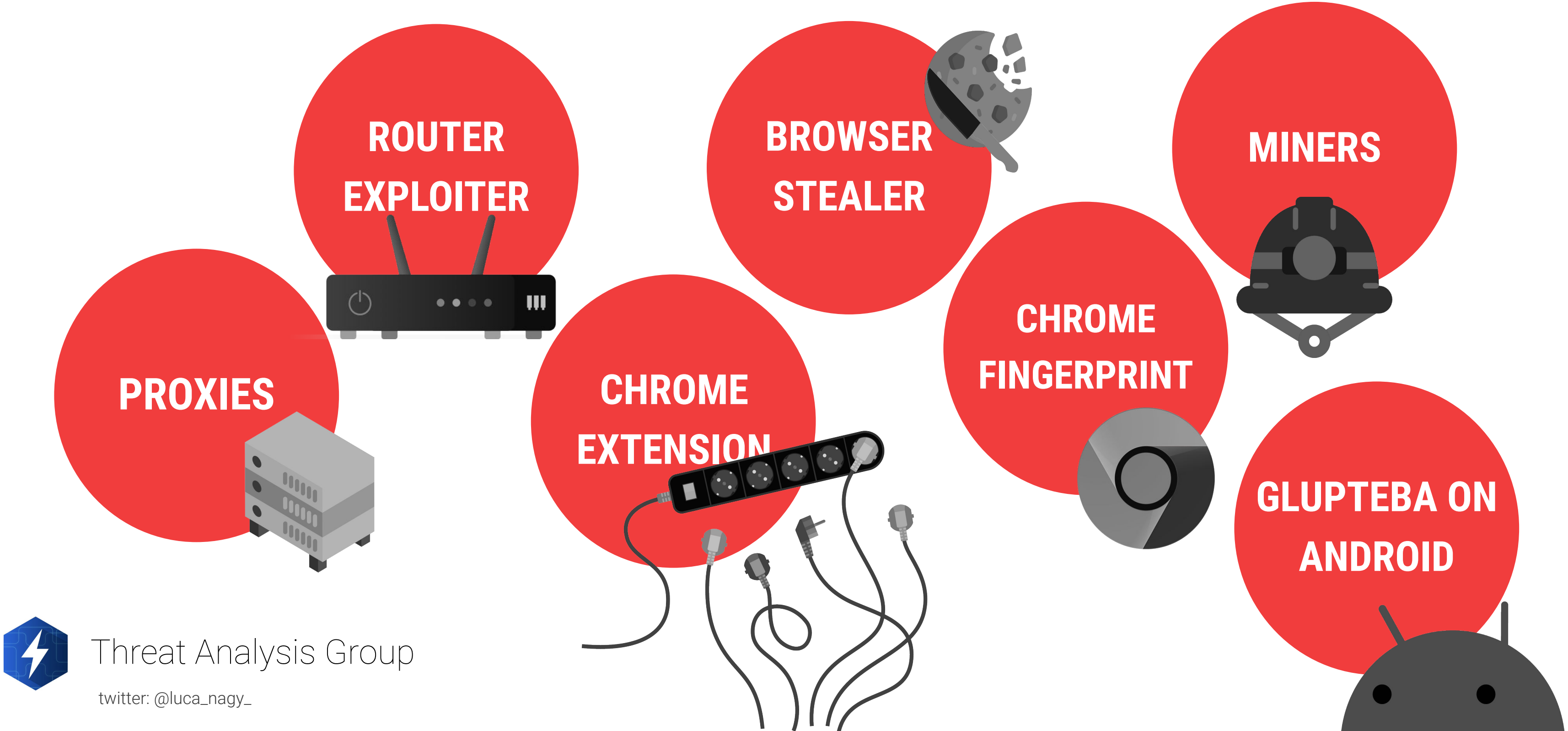
SUPPRESS SECURITY

Adding Windows Defender exclusions,

Firewall rules,

Disabling PatchGuard, DSE.

GLUPTEBA MODULES



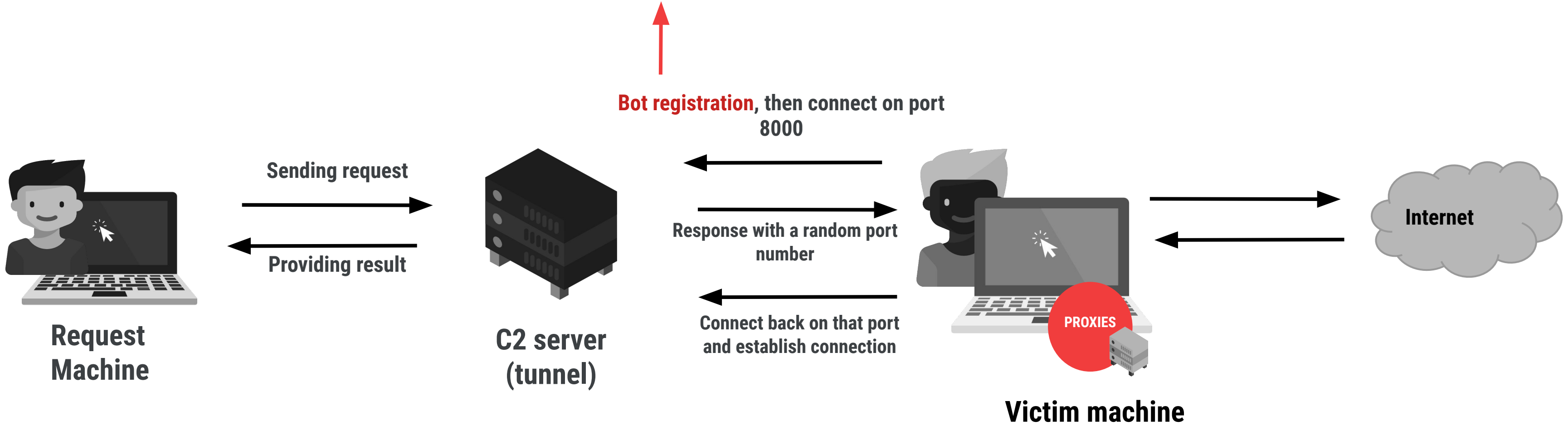
- PROXIES
- ROUTER EXPLOITER
- CHROME EXTENSION
- BROWSER STEALER
- CHROME FINGERPRINT
- MINERS
- GLUPTEBA ON ANDROID

PROXY MODULE

PROXIES

- TUNNELED PROXY

<GUID>.server-<d>.domain, where the <d> is randomly selected then incremented.
E.G.: **808f38e3-d84b-45c8-b461-2a4c006a0f4a.server-3.easywbdesign.com**



Bot registration, then connect on port 8000

Sending request

Providing result

Response with a random port number

Connect back on that port and establish connection

Request Machine

C2 server (tunnel)

Victim machine

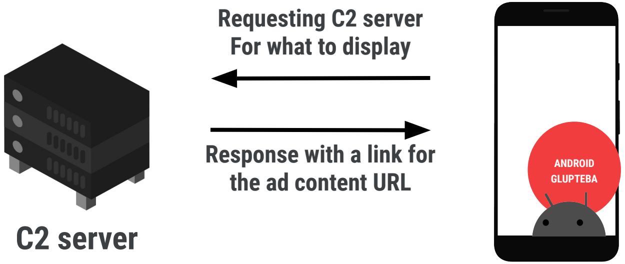
PROXIES

Internet

ANDROID - ADS MODULE

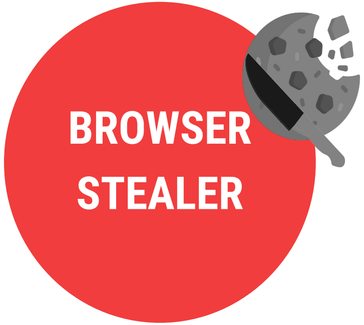
1. Glupteba APK requests: http://domainforwork.com/api/pollc with sent information
2. Received response

[{"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=...

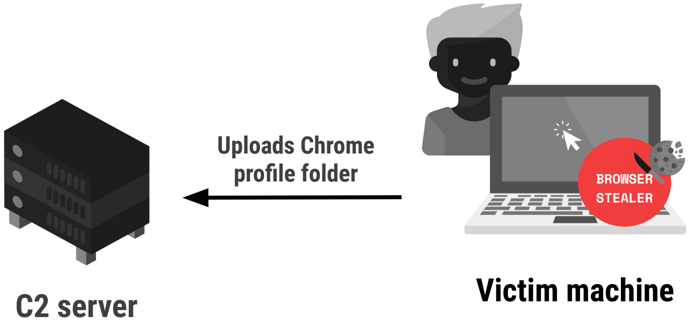


GLUPTEBA ON ANDROID

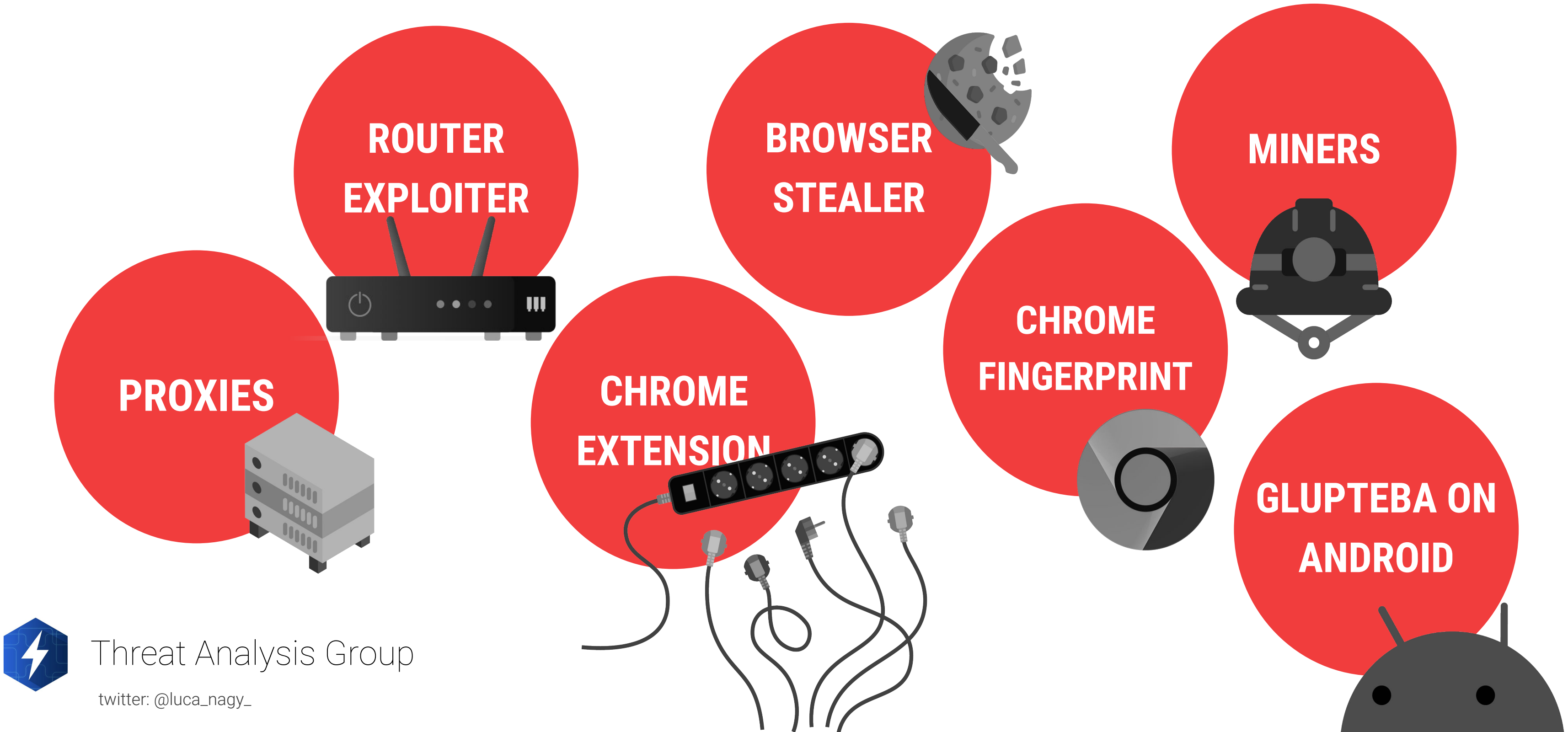
BROWSER STEALER



- Locate Chrome profile folder: Cookies + History, etc.
- Decrypt passwords, cookies
- Upload to http://oknazasto.info/pupload/%s/%s?%s



WHERE ARE THESE MONETISED?



ROUTER EXPLOITER

BROWSER STEALER

MINERS

PROXIES

CHROME EXTENSION

CHROME FINGERPRINT

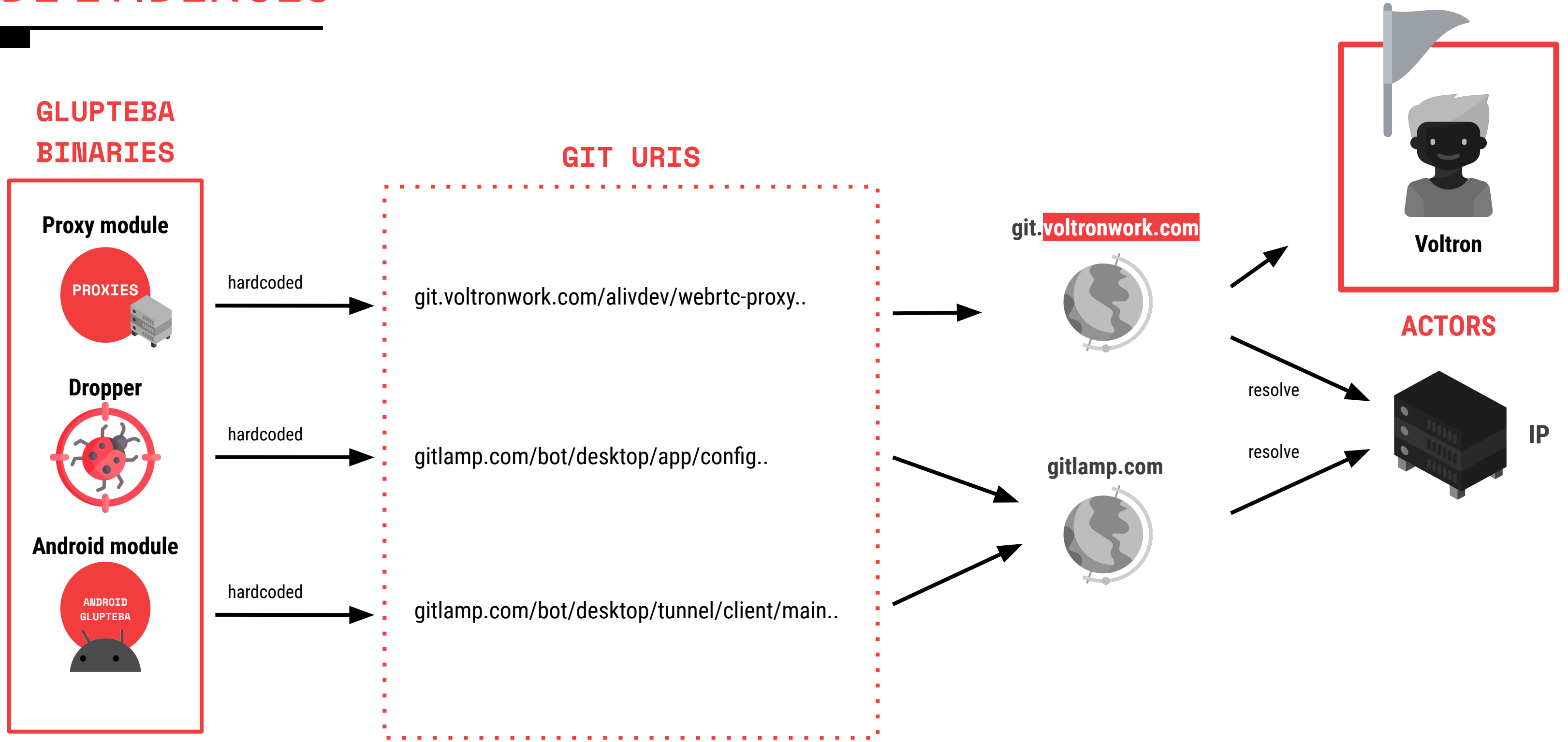
GLUPTEBA ON ANDROID

ACTORS

Threat Analysis Group

twitter: @luca_nagy_

CODE EVIDENCES



GLUPTEBA BINARIES

Proxy module

Dropper

Android module

hardcoded

hardcoded

hardcoded

GIT URIS

git.voltronwork.com/alivdev/webrtc-proxy..

gitlamp.com/bot/desktop/app/config..

gitlamp.com/bot/desktop/tunnel/client/main..

git.voltronwork.com

gitlamp.com

resolve

resolve

Voltron

ACTORS

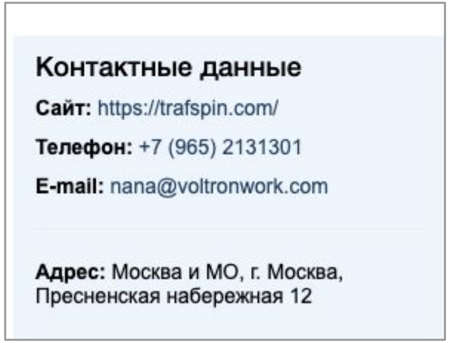
IP

Threat Analysis Group

twitter: @luca_nagy_

SERVICES

LEGAL ENTITY BASED EVIDENCES



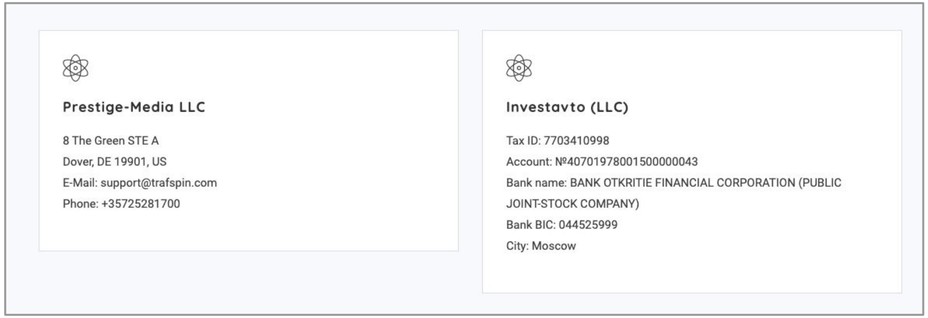
Контактные данные

Сайт: https://trafspin.com/

Телефон: +7 (965) 2131301

E-mail: nana@voltronwork.com

Адрес: Москва и МО, г. Москва,
Пресненская набережная 12

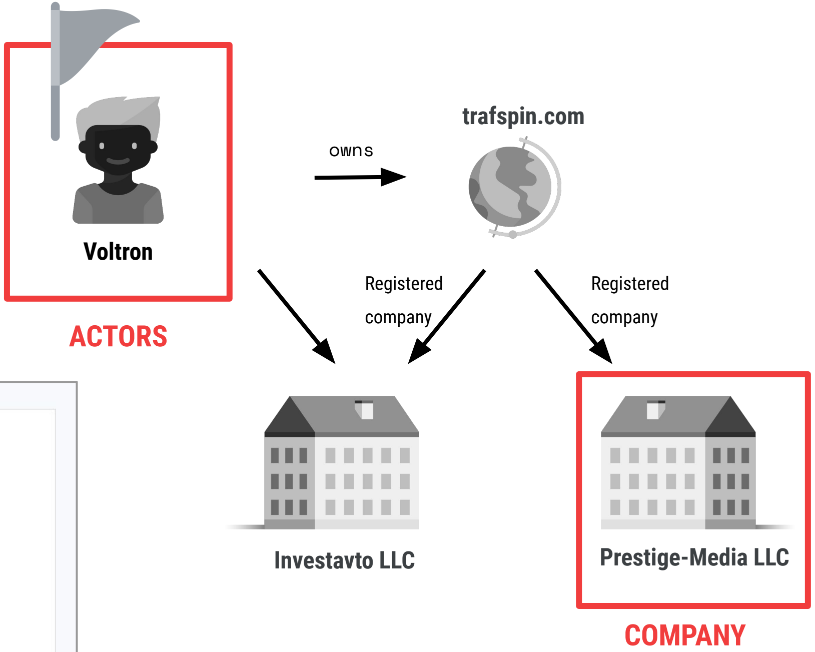


Prestige-Media LLC

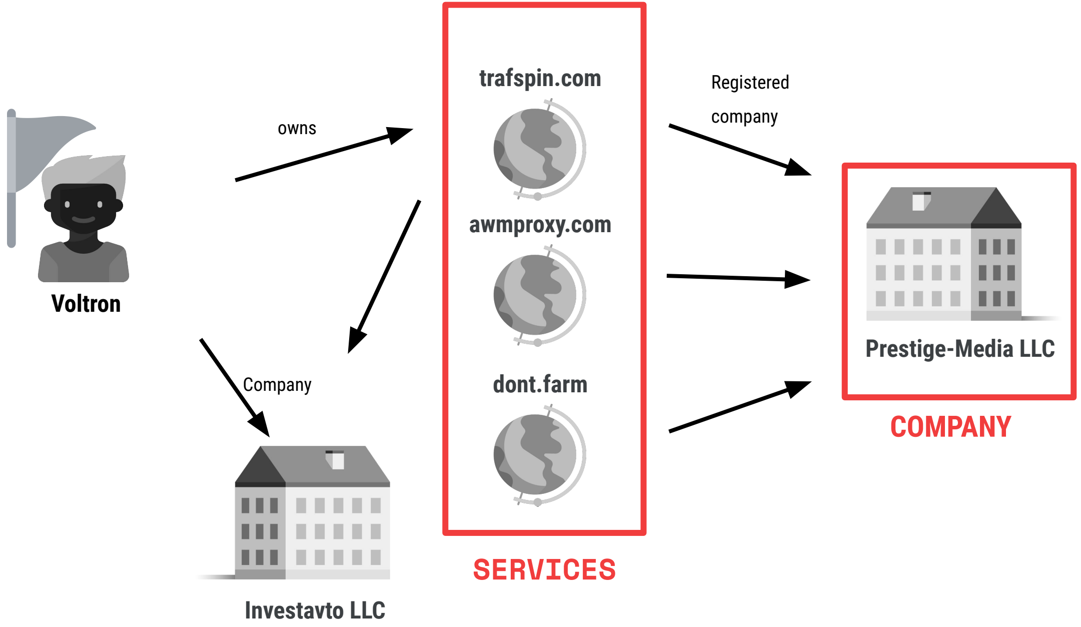
8 The Green STE A
Dover, DE 19901, US
E-Mail: support@trafspin.com
Phone: +35725281700

Investavto (LLC)

Tax ID: 7703410998
Account: №40701978001500000043
Bank name: BANK OTKRITIE FINANCIAL CORPORATION (PUBLIC JOINT-STOCK COMPANY)
Bank BIC: 044525999
City: Moscow



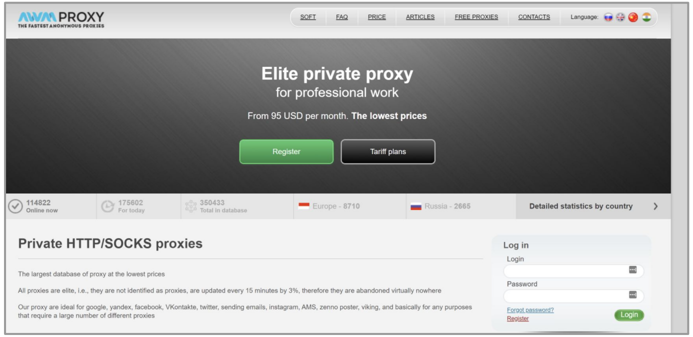
LEGAL ENTITY BASED EVIDENCES



WHAT ARE THESE SERVICES?

AWMPROXY

Residential proxy provider



Elite private proxy
for professional work

From 95 USD per month. **The lowest prices**

114822 Online now

175602 For today

350433 Total in database

Europe - 8710

Russia - 2665

Detailed statistics by country

Private HTTP/SOCKS proxies

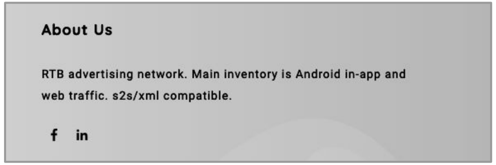
The largest database of proxy at the lowest prices

All proxies are elite, i.e., they are not identified as proxies, are updated every 15 minutes by 3%, therefore they are abandoned virtually nowhere

Our proxy are ideal for google, yandex, facebook, VKontakte, twitter, sending emails, instagram, AMS, zenno poster, viking, and basically for any purposes that require a large number of different proxies

TRAFSPIN

Advertising network

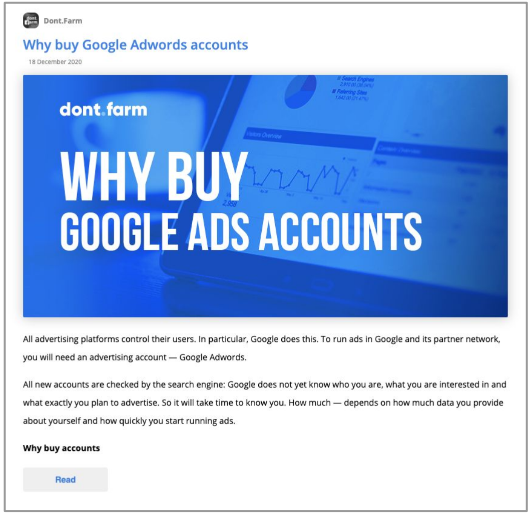


About Us

RTB advertising network. Main inventory is Android in-app and web traffic. s2s/xml compatible.

DONT.FARM

Ads account service



Why buy Google Adwords accounts

18 December 2020

All advertising platforms control their users. In particular, Google does this. To run ads in Google and its partner network, you will need an advertising account — Google Adwords.

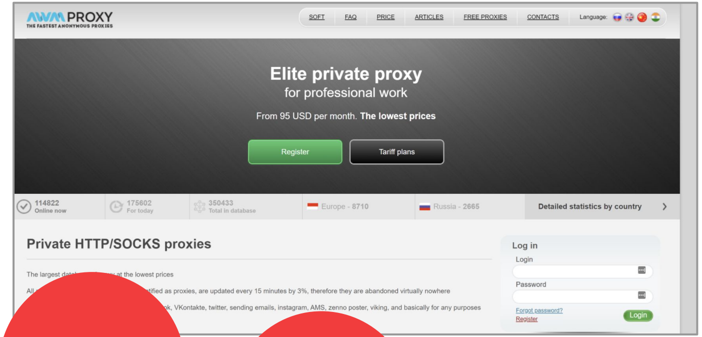
All new accounts are checked by the search engine: Google does not yet know who you are, what you are interested in and what exactly you plan to advertise. So it will take time to know you. How much — depends on how much data you provide about yourself and how quickly you start running ads.

Why buy accounts

ARE THESE ASSOCIATED WITH THE MODULES?

AWMPROXY

Residential proxy provider



Elite private proxy
for professional work

From 95 USD per month. **The lowest prices**

Private HTTP/SOCKS proxies

The largest data … at the lowest prices

All … tified as proxies, are updated every 15 minutes by 3%, therefore they are abandoned virtually nowhere

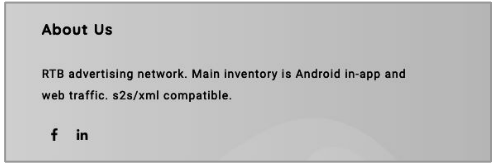
… ok, VKontakte, twitter, sending emails, instagram, AMS, zenno poster, viking, and basically for any purposes

PROXIES

ROUTER EXPLOITER

TRAFSPIN

Advertising network



About Us

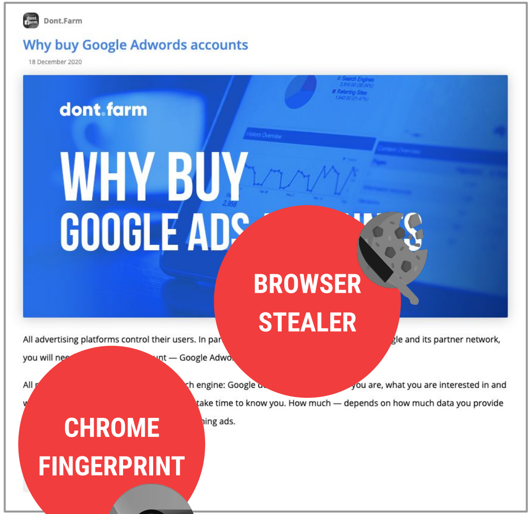
RTB advertising network. Main inventory is Android in-app and web traffic. s2s/xml compatible.

CHROME EXTENSION

GLUPTEBA ON ANDROID

DONT.FARM

Ads account service



Why buy Google Adwords accounts

18 December 2020

All advertising platforms control their users. In par… gle and its partner network, you will nee… unt — Google Adwo…

All … ch engine: Google d… you are, what you are interested in and w… take time to know you. How much — depends on how much data you provide … ing ads.

BROWSER STEALER

CHROME FINGERPRINT

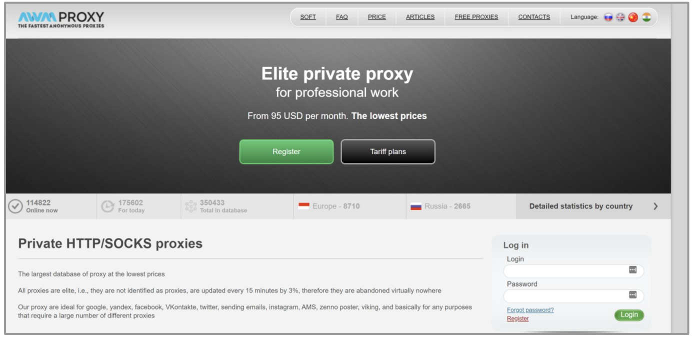
Threat Analysis Group

twitter: @luca_nagy_

AWMPROXY

AWMPROXY

Residential proxy provider



Elite private proxy
for professional work

From 95 USD per month. **The lowest prices**

114822 Online now

175602 For today

350433 Total in database

Europe - 8710

Russia - 2665

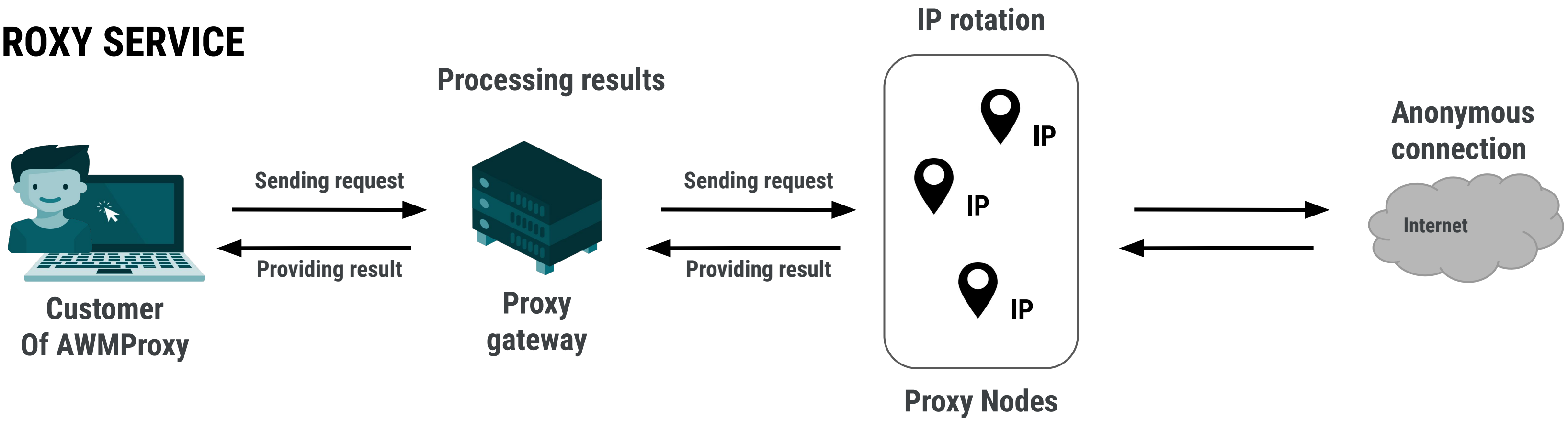
Private HTTP/SOCKS proxies

The largest database of proxy at the lowest prices

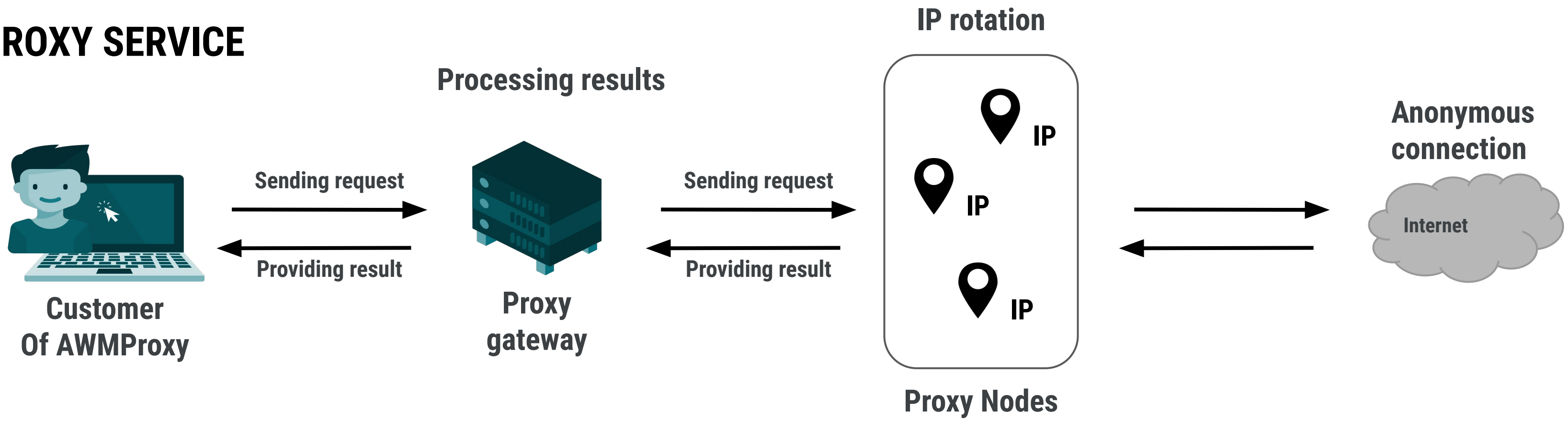
All proxies are elite, i.e., they are not identified as proxies, are updated every 15 minutes by 3%, therefore they are abandoned virtually nowhere

Our proxy are ideal for google, yandex, facebook, VKontakte, twitter, sending emails, instagram, AMS, zenno poster, viking, and basically for any purposes that require a large number of different proxies

PROXY SERVICE



PROXY SERVICE



IP rotation

Processing results

Sending request

Providing result

Sending request

Providing result

IP

IP

IP

Anonymous connection

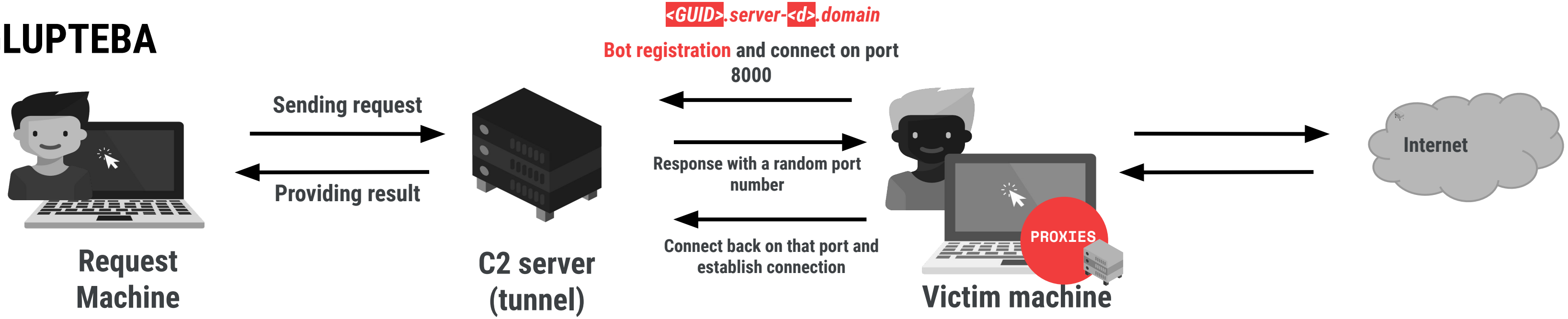
Internet

Customer Of AWMProxy

Proxy gateway

Proxy Nodes

GLUPTEBA



<GUID>.server-<d>.domain

Bot registration and connect on port 8000

Sending request

Providing result

Response with a random port number

Connect back on that port and establish connection

PROXIES

Internet

Request Machine

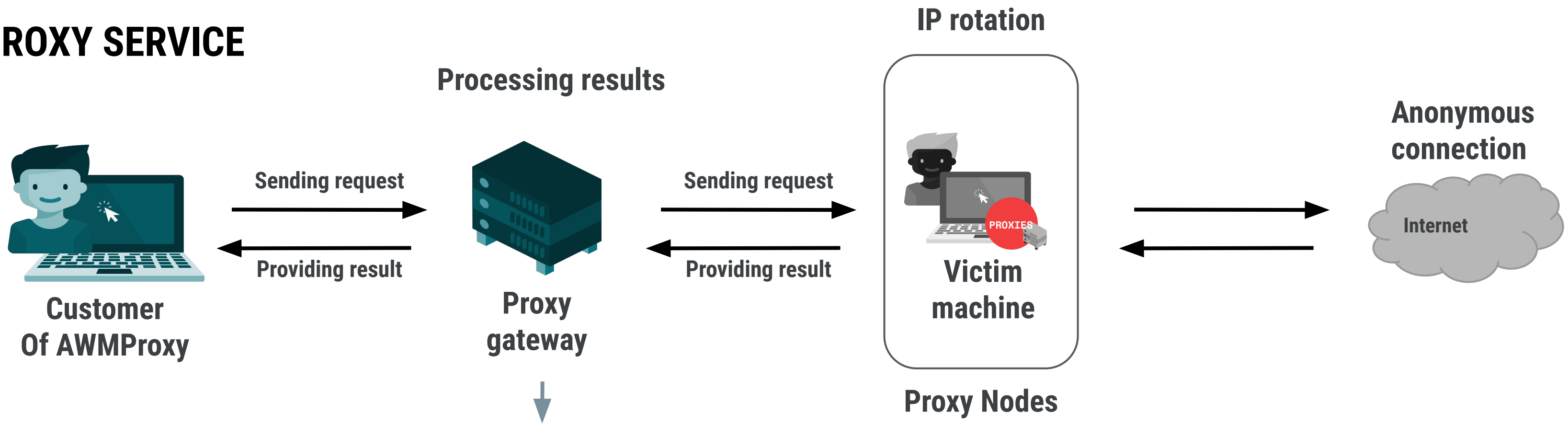
C2 server (tunnel)

Victim machine

Threat Analysis Group

twitter: @luca_nagy_

PROXY SERVICE



Processing results

IP rotation

Anonymous connection

Customer Of AWMProxy

Sending request

Providing result

Proxy gateway

Sending request

Providing result

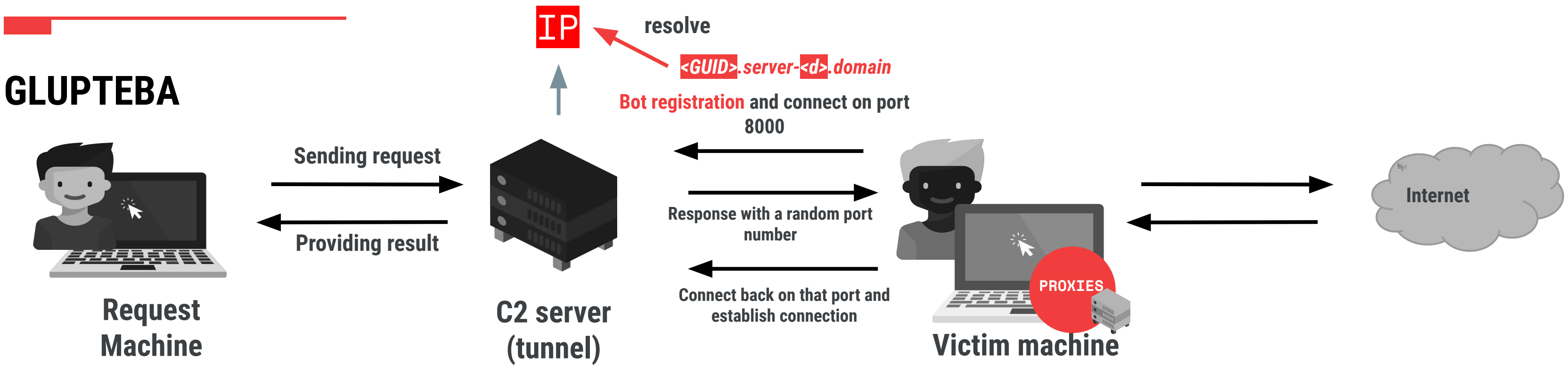
Victim machine

PROXIES

Internet

Proxy Nodes

GLUPTEBA



IP

resolve

<GUID>.server-<d>.domain

Bot registration and connect on port 8000

Request Machine

Sending request

Providing result

C2 server (tunnel)

Response with a random port number

Connect back on that port and establish connection

Victim machine

PROXIES

Internet

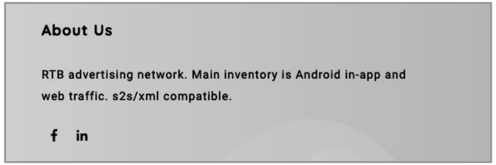
Threat Analysis Group

twitter: @luca_nagy_

TRAFSPIN

TRAFSPIN

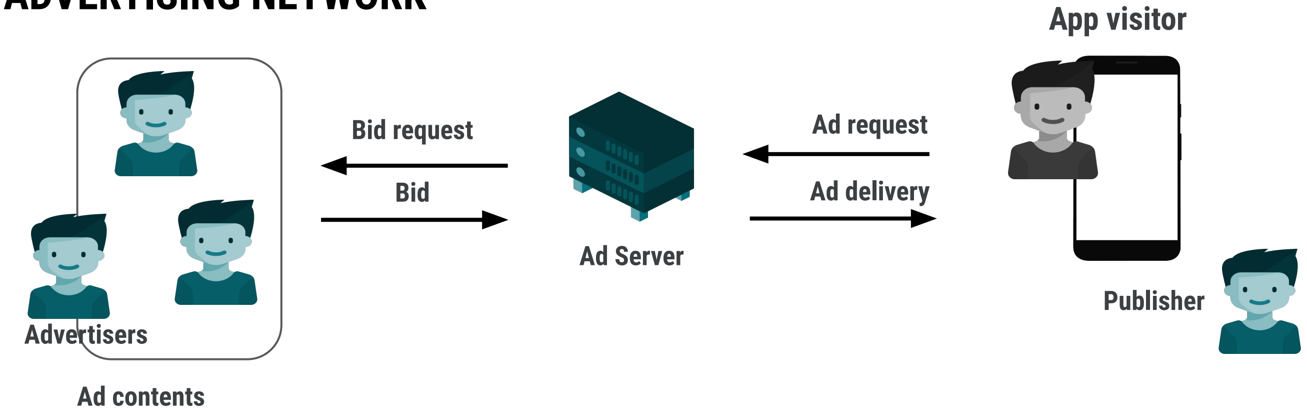
Advertising network



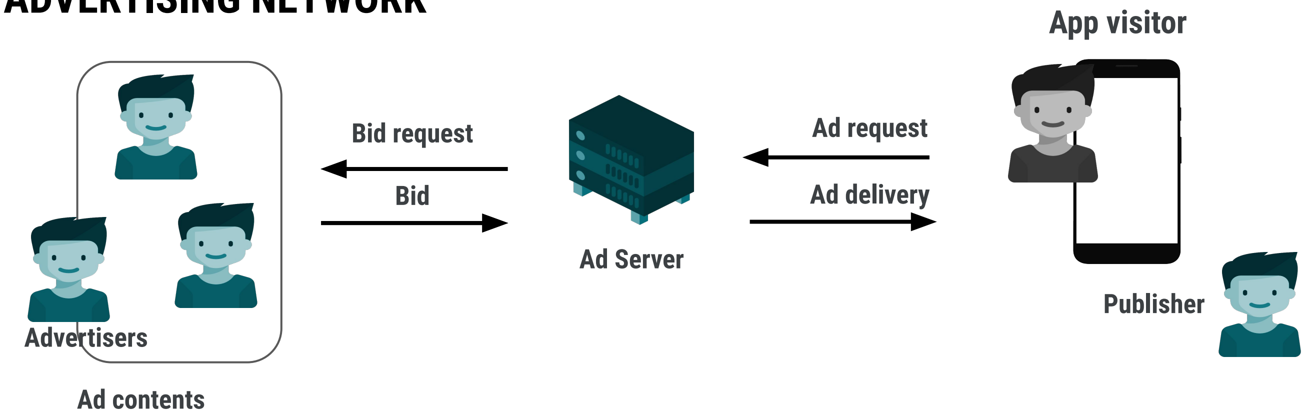
About Us

RTB advertising network. Main inventory is Android in-app and web traffic. s2s/xml compatible.

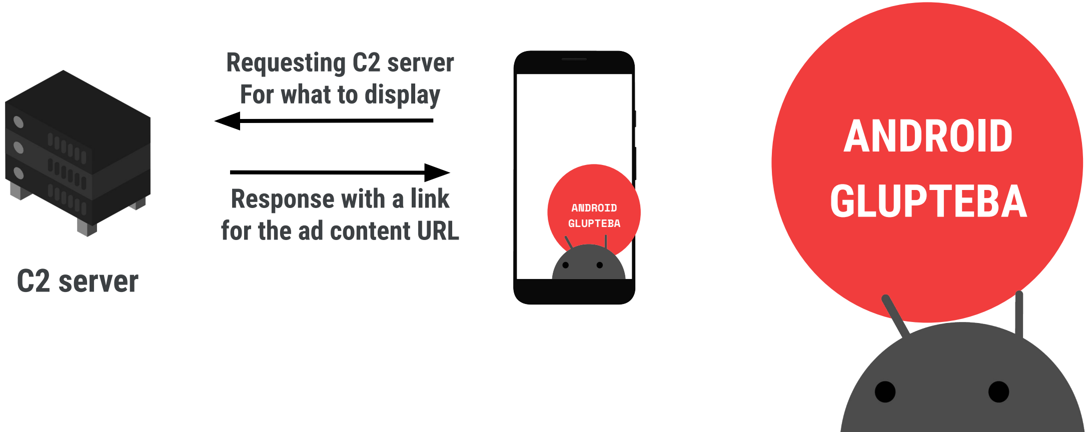
RTB ADVERTISING NETWORK



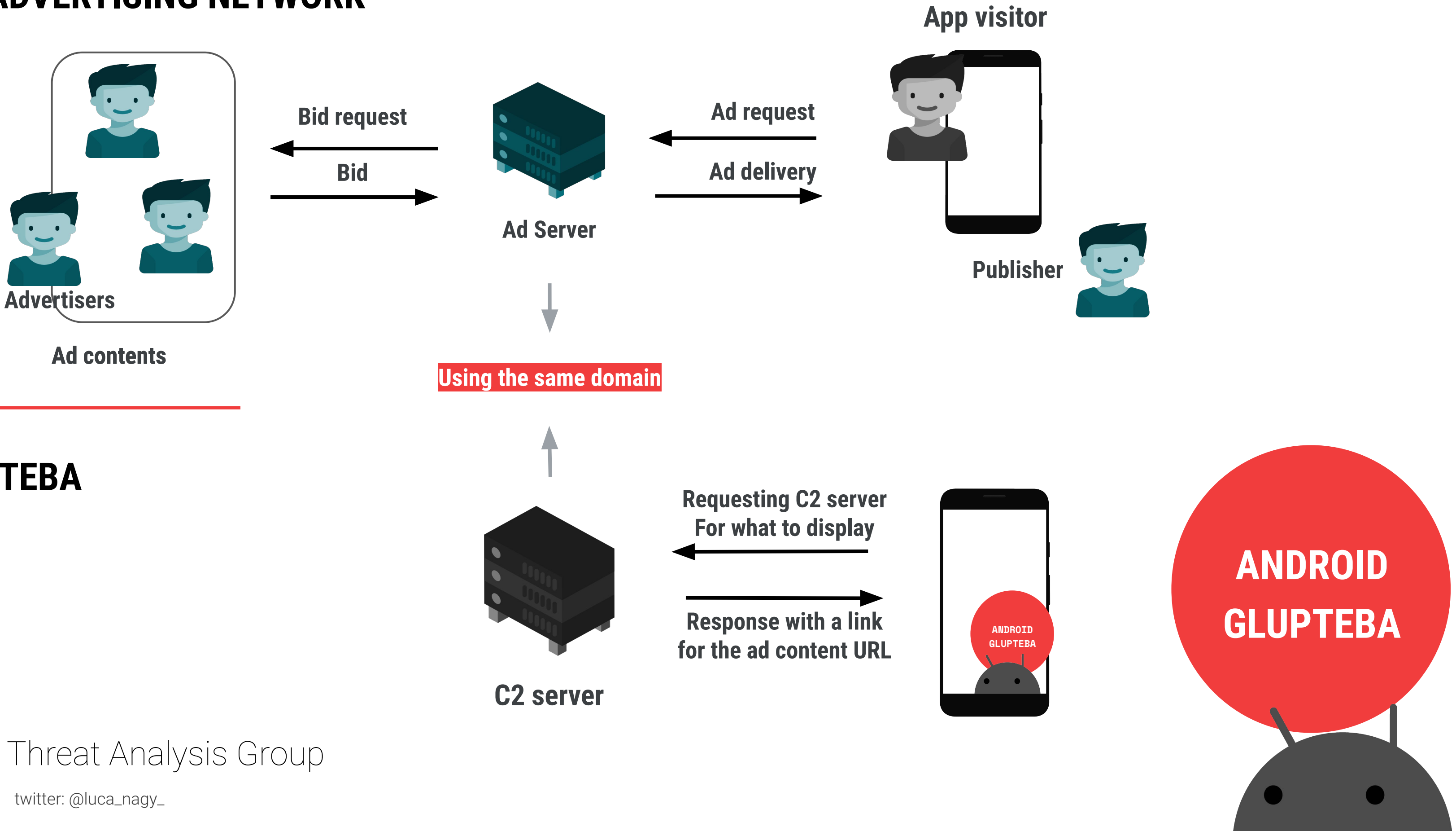
RTB ADVERTISING NETWORK



GLUPTEBA



RTB ADVERTISING NETWORK



App visitor

Bid request

Bid

Ad Server

Ad request

Ad delivery

Publisher

Advertisers

Ad contents

Using the same domain

GLUPTEBA

Requesting C2 server
For what to display

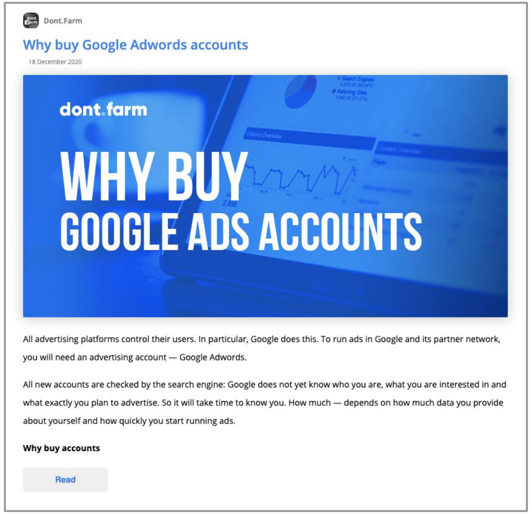
Response with a link
for the ad content URL

C2 server

DONT.FARM

DONT.FARM

Ads account service



Dont.Farm

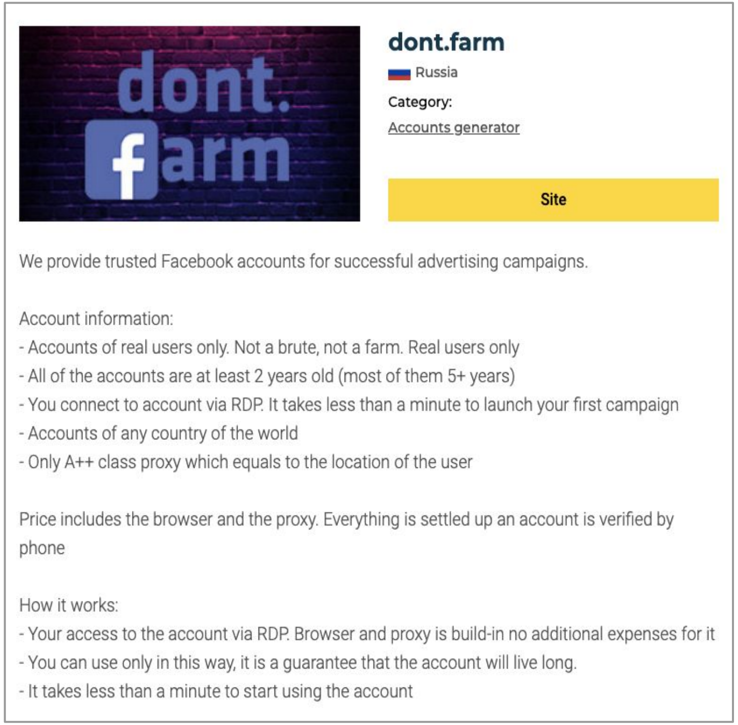
Why buy Google Adwords accounts

18 December 2020

All advertising platforms control their users. In particular, Google does this. To run ads in Google and its partner network, you will need an advertising account — Google Adwords.

All new accounts are checked by the search engine: Google does not yet know who you are, what you are interested in and what exactly you plan to advertise. So it will take time to know you. How much — depends on how much data you provide about yourself and how quickly you start running ads.

Why buy accounts



dont.farm

Russia

Category:

Accounts generator

We provide trusted Facebook accounts for successful advertising campaigns.

Account information:
- Accounts of real users only. Not a brute, not a farm. Real users only
- All of the accounts are at least 2 years old (most of them 5+ years)
- You connect to account via RDP. It takes less than a minute to launch your first campaign
- Accounts of any country of the world
- Only A++ class proxy which equals to the location of the user

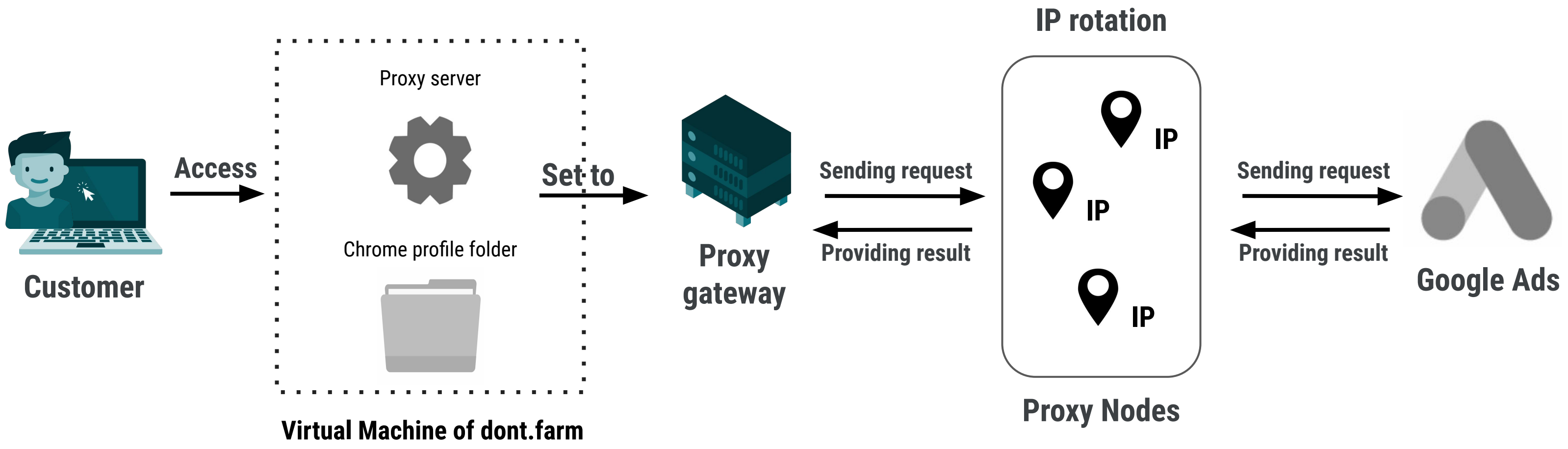
Price includes the browser and the proxy. Everything is settled up an account is verified by phone

How it works:
- Your access to the account via RDP. Browser and proxy is build-in no additional expenses for it
- You can use only in this way, it is a guarantee that the account will live long.
- It takes less than a minute to start using the account

Threat Analysis Group

twitter: @luca_nagy_

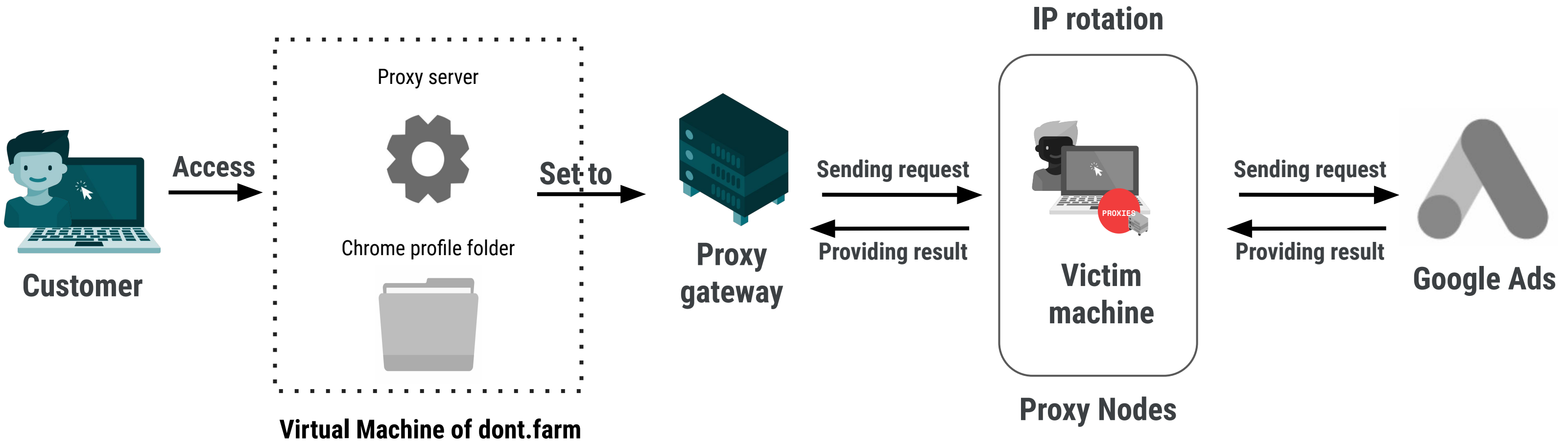
ADS ACCOUNT SERVICE



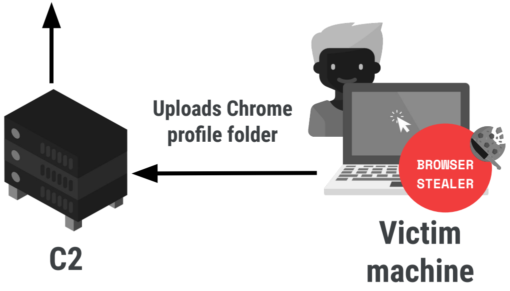
Threat Analysis Group

twitter: @luca_nagy_

ADS ACCOUNT SERVICE



GLUPTEBA



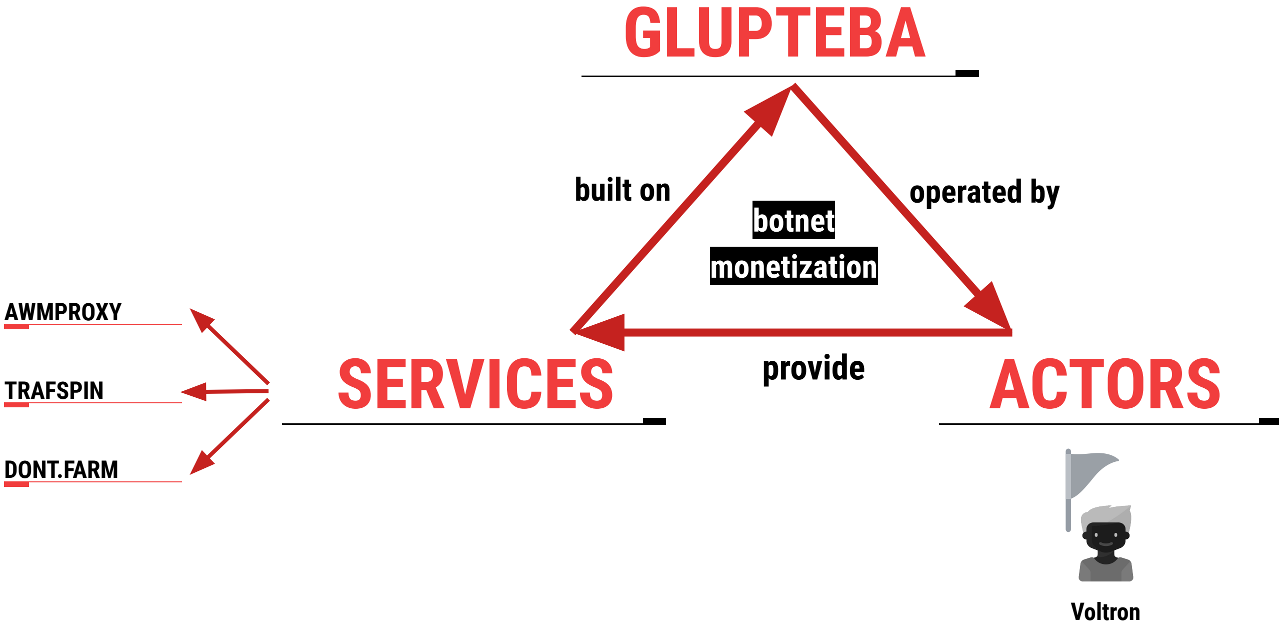
CRIMINAL ECOSYSTEM

Threat Analysis Group

twitter: @luca_nagy_

ECOSYSTEM

- BROWSER STEALERS
- PROXY MODULES
- ANDROID VARIANT, ETC.



GLUPTEBA

built on

botnet monetization

operated by

SERVICES

provide

ACTORS

AWMPROXY

TRAFSPIN

DONT.FARM

Voltron

CLOSING REMARKS

AFTER DISRUPTION

- Overall botnet size decreased to less than its quarter (from 1M to 220K)
- Went away from Google products
- Partially disrupted services
- No new distribution until end of May
- Distribution of new samples by Integral PPI network since May -> Botnet size slightly increasing.
  - New BTC addresses
  - Simple XOR encoded C2 domains in blockchain
  - .onion C2 domains
  - Using Discord for downloading TOR
  - Using Opera VPN - opera-proxy client (recently started)

LESSONS LEARNED

- Glupteba actors make mistakes
- Diverse botnet, diverse usage (services)
- Complex, organized ecosystem, end-to-end solution
- TAG continues to monitor

THANK YOU!

Threat Analysis Group

twitter: @luca_nagy_