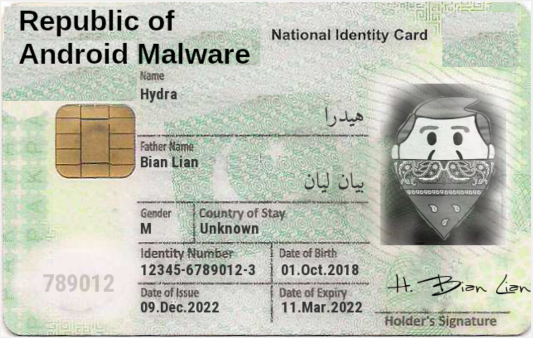
Hunting the Android/BianLian botnet

Axelle Apvrille

Virus Bulletin, Prague, September 2022

Android/BianLian



Republic of
Android Malware

National Identity Card

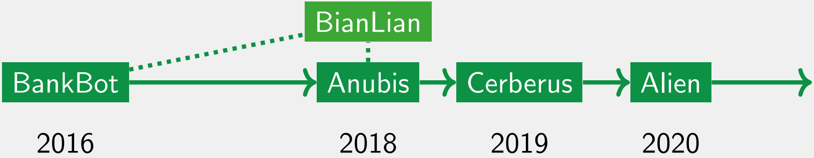
Name	Hydra هيدرا
Father Name	Bian Lian بيان ليان
Gender	M
Country of Stay	Unknown
Identity Number	12345-6789012-3
Date of Birth	01.Oct.2018
Date of Issue	09.Dec.2022
Date of Expiry	11.Mar.2022

789012

H. Bian Lian

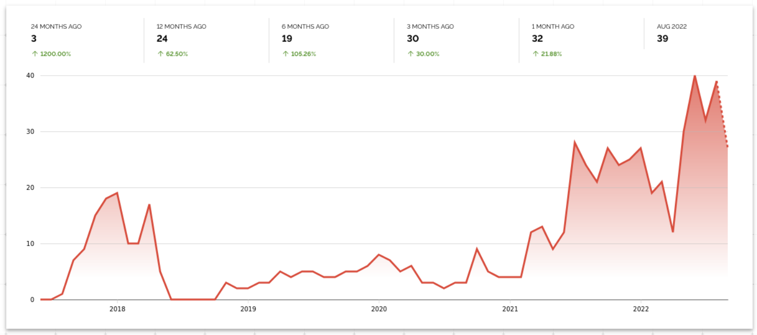
Holder's Signature

- Author: ?
- Parents: orphan
- Ancestor: **BankBot**
- Cousin: **Anubis**
- Job: Android **banking botnet**
- Characteristics: clean-cut, intelligent, resilient



2018? Isn’t that old?

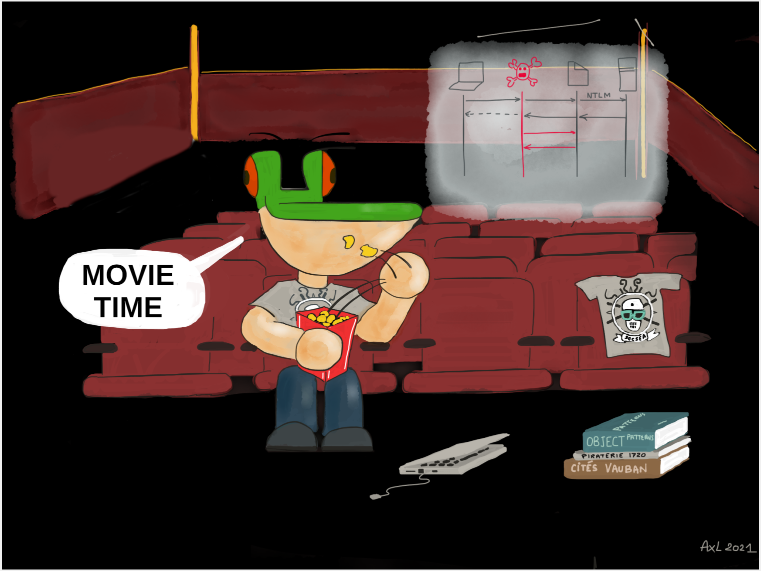
Particularly **active** in 2022



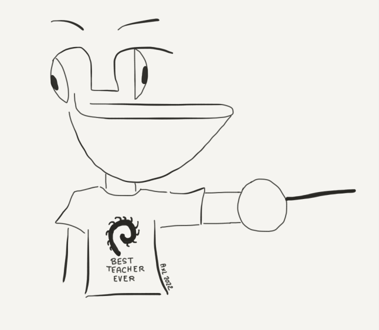
24 MONTHS AGO	12 MONTHS AGO	6 MONTHS AGO	3 MONTHS AGO	1 MONTH AGO	AUG 2022
3	24	19	30	32	39
↑ 1200.00%	↑ 62.50%	↑ 105.26%	↑ 30.00%	↑ 21.88%	

Clever, Precursor

Android/BianLian in action



Key Points



- High **longevity**
- The **banking app** is usually the **official** one. The **malware** is inside **another** app

Underground ecosystem

Malware author

Sales team

Affiliates

Active C2

Underground ecosystem

BianLian: 1-2 authors

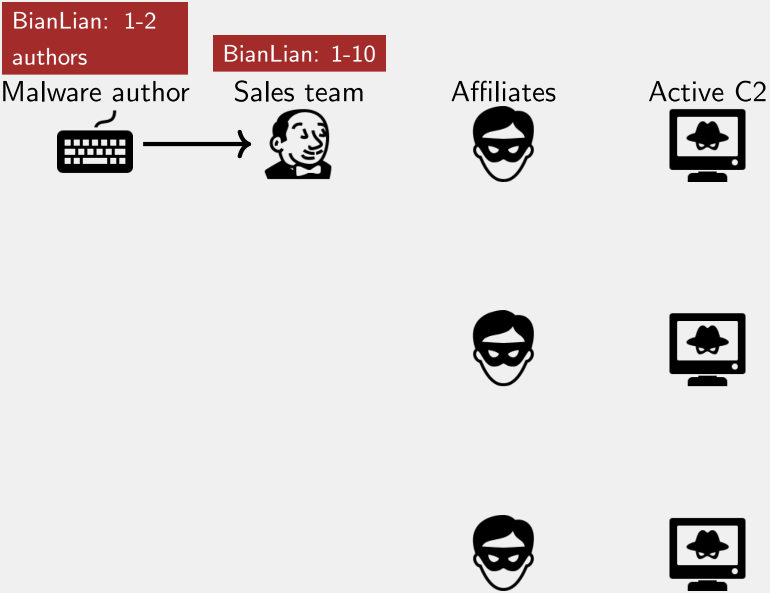
Malware author

Sales team

Affiliates

Active C2

Underground ecosystem



BianLian: 1-2 authors

BianLian: 1-10

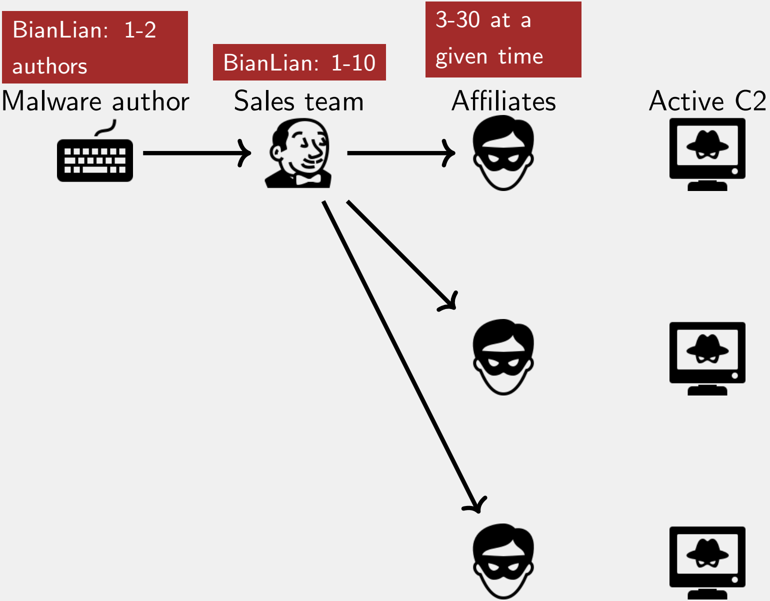
Malware author

Sales team

Affiliates

Active C2

Underground ecosystem



BianLian: 1-2 authors

BianLian: 1-10

3-30 at a given time

Malware author

Sales team

Affiliates

Active C2

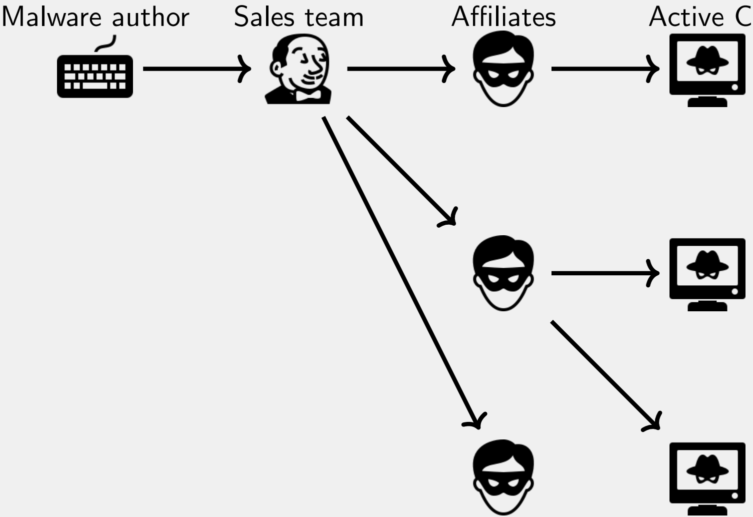
Underground ecosystem

BianLian: 1-2 authors

BianLian: 1-10

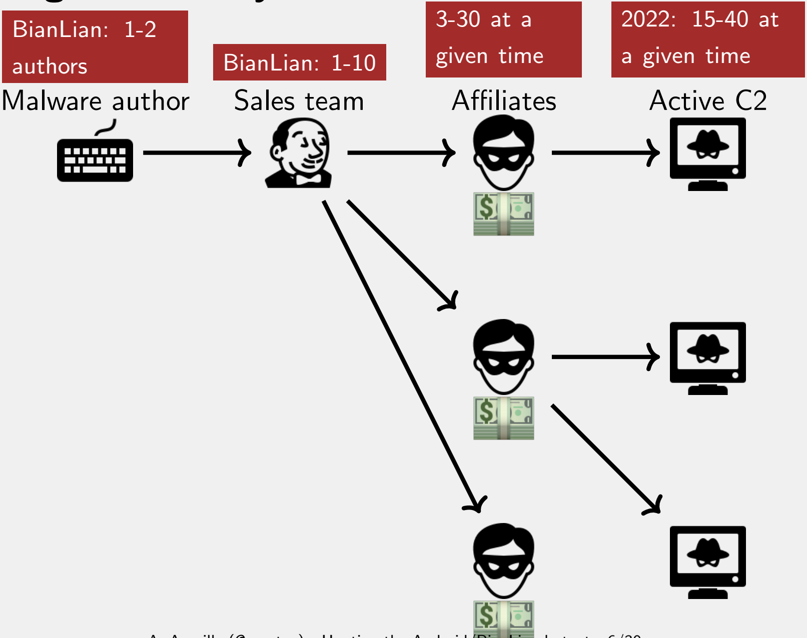
3-30 at a given time

2022: 15-40 at a given time



Icons from https://icons8.com/icons/

Underground ecosystem



BianLian: 1-2 authors

Malware author

BianLian: 1-10

Sales team

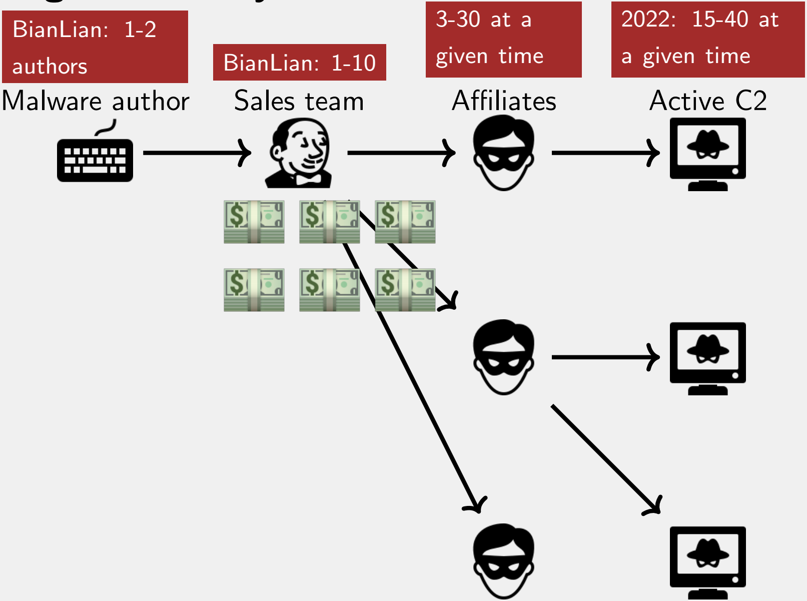
3-30 at a given time

Affiliates

2022: 15-40 at a given time

Active C2

Underground ecosystem



BianLian: 1-2 authors

Malware author

BianLian: 1-10

Sales team

3-30 at a given time

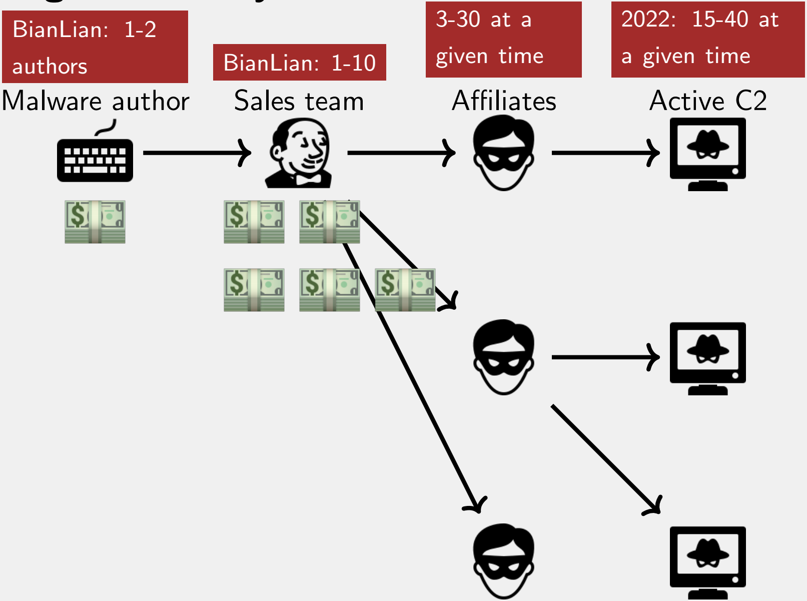
Affiliates

2022: 15-40 at a given time

Active C2

Icons from https://icons8.com/icons/

Underground ecosystem



BianLian: 1-2 authors

BianLian: 1-10

3-30 at a given time

2022: 15-40 at a given time

Malware author

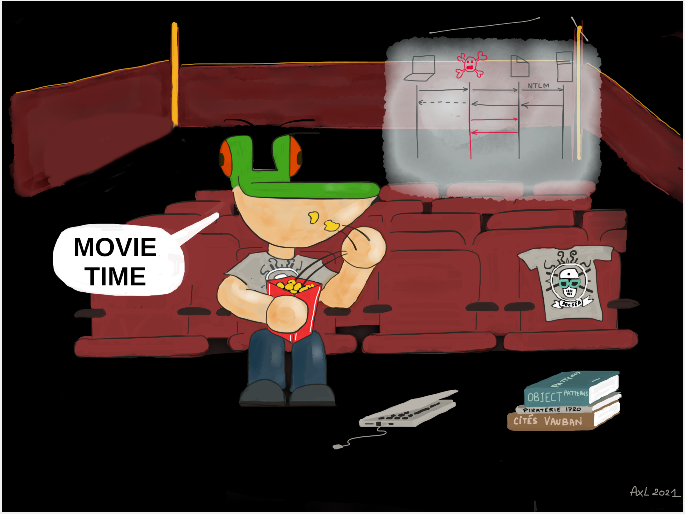
Sales team

Affiliates

Active C2

Icons from https://icons8.com/icons/

Advertising techniques



https://www.youtube.com/watch?v=NTDu_pT94IQ

Finding BianLian underground

It is named **Hydra** (not Bian Lian).

Finding BianLian underground

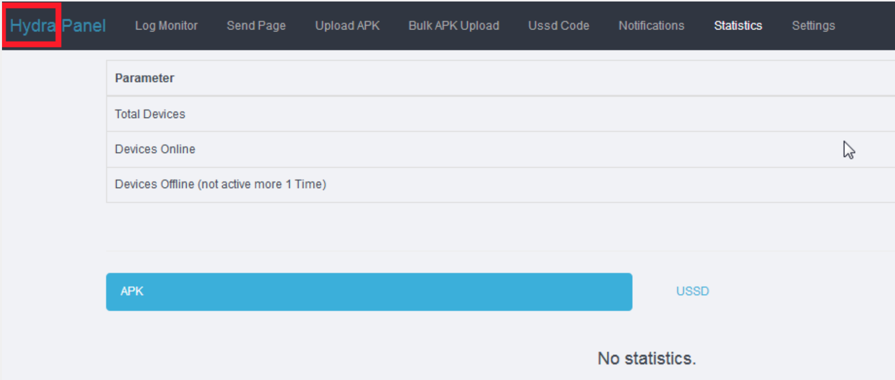
It is named **Hydra** (not Bian Lian).

Unfortunately, https://github.com/vanhauser-thc/thc-hydra is the name of a famous **Password Cracker**

Hi, David!

Finding BianLian underground

It is named **Hydra** (not Bian Lian).



Parameter
Total Devices
Devices Online
Devices Offline (not active more 1 Time)

No statistics.

The panel has **no remarkable word** or feature

Screenshot: https://twitter.com/prodaft/status/1096458491852664840

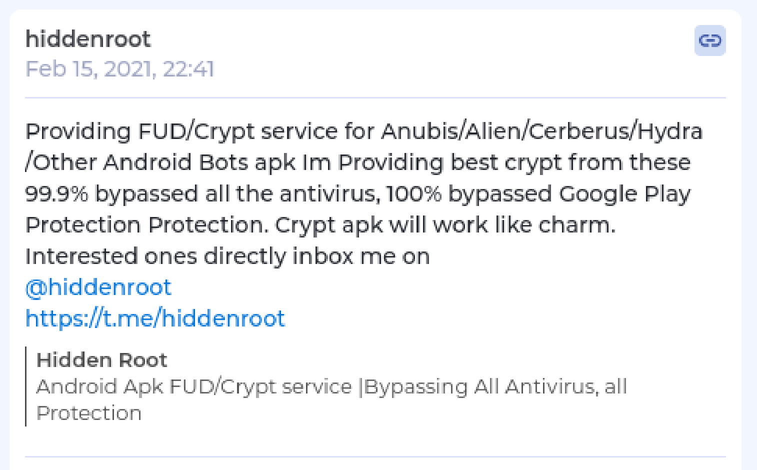
Finding BianLian underground

Difficult to find BianLian/Hydra underground.
Could it just be that the *name is wrong*?
Mistaken for:

- **Cerberus**? No
- **Bankbot**? No
- **Alien**? No
- **Huracan**? No
- **UB3L**? No

Features and panel do *not* match with BianLian's

Advertisement on Telegram

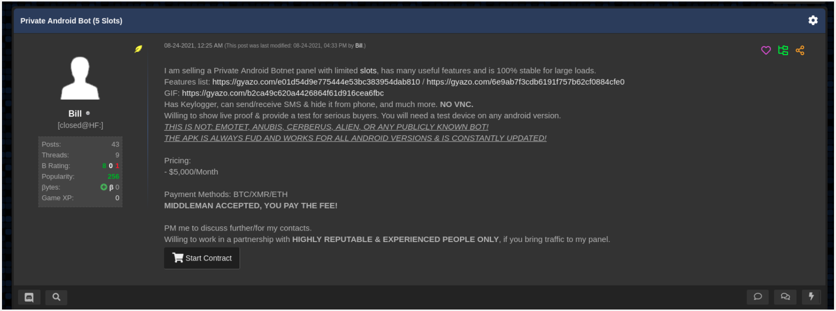


hiddenroot
Feb 15, 2021, 22:41

Providing FUD/Crypt service for Anubis/Alien/Cerberus/Hydra /Other Android Bots apk Im Providing best crypt from these 99.9% bypassed all the antivirus, 100% bypassed Google Play Protection Protection. Crypt apk will work like charm. Interested ones directly inbox me on
@hiddenroot
https://t.me/hiddenroot

> **Hidden Root**
> Android Apk FUD/Crypt service |Bypassing All Antivirus, all Protection

Advertisement on hacking forums



Private Android Bot (5 Slots)

Bill ●
[closed@HF:]

Posts:	43
Threads:	9
B Rating:	8 0 1
Popularity:	256
βytes:	β 0
Game XP:	0

08-24-2021, 12:25 AM (This post was last modified: 08-24-2021, 04:33 PM by Bill.)

I am selling a Private Android Botnet panel with limited **slots**, has many useful features and is 100% stable for large loads.
Features list: https://gyazo.com/e01d54d9e775444e53bc383954dab810 / https://gyazo.com/6e9ab7f3cdb6191f757b62cf0884cfe0
GIF: https://gyazo.com/b2ca49c620a4426864f61d916cea6fbc
Has Keylogger, can send/receive SMS & hide it from phone, and much more. **NO VNC.**
Willing to show live proof & provide a test for serious buyers. You will need a test device on any android version.
THIS IS NOT: EMOTET, ANUBIS, CERBERUS, ALIEN, OR ANY PUBLICLY KNOWN BOT!
THE APK IS ALWAYS FUD AND WORKS FOR ALL ANDROID VERSIONS & IS CONSTANTLY UPDATED!

Pricing:
- $5,000/Month

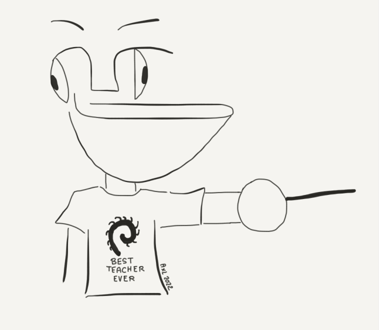
Payment Methods: BTC/XMR/ETH
MIDDLEMAN ACCEPTED, YOU PAY THE FEE!

PM me to discuss further/for my contacts.
Willing to work in a partnership with **HIGHLY REPUTABLE & EXPERIENCED PEOPLE ONLY**, if you bring traffic to my panel.

"Selling Private Android Botnet panel with limited slots [..] 100% stable for large loads [..] NO VNC. THIS IS NOT: EMOTET, ANUBIS, [..] $5,000/Month"

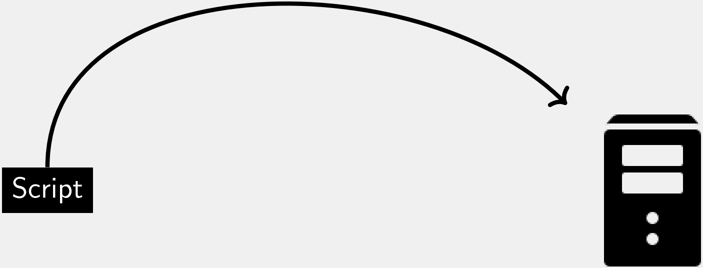
Resiliency: limited slots, remain under the radar...

Key Points



- Keeps a **low profile** underground
- Selling with **limited slots**

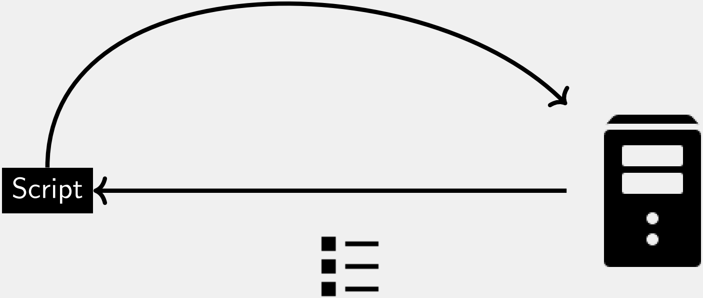
Locating Operational C2s



Script

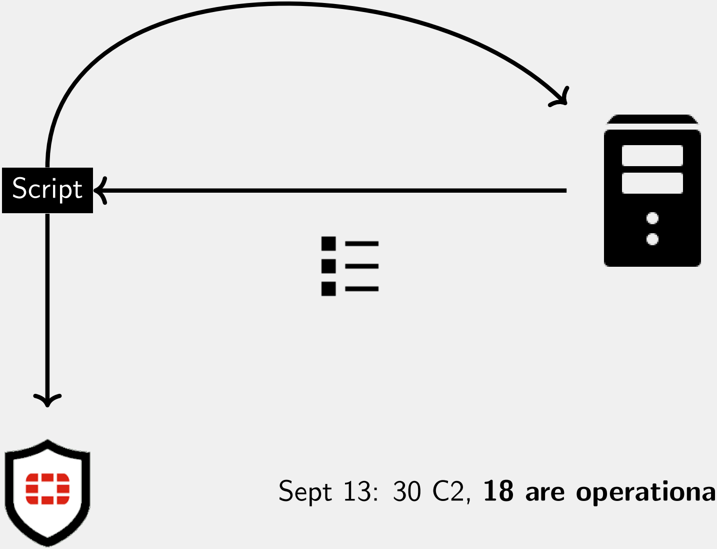
Sept 13: 30 C2, **18 are operational**

Locating Operational C2s



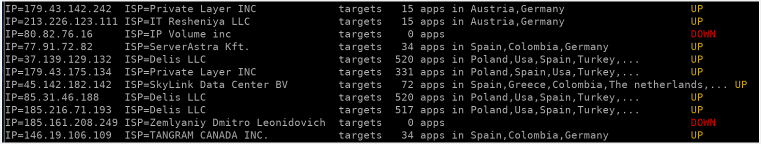
Sept 13: 30 C2, **18 are operational**

Locating Operational C2s



Sept 13: 30 C2, **18 are operational**

Demo time



```
IP=179.43.142.242  ISP=Private Layer INC               targets   15 apps in Austria,Germany                  UP
IP=213.226.123.111 ISP=IT Resheniya LLC                targets   15 apps in Austria,Germany                  UP
IP=80.82.76.16     ISP=IP Volume inc                   targets    0 apps                                     DOWN
IP=77.91.72.82     ISP=ServerAstra Kft.                targets   34 apps in Spain,Colombia,Germany           UP
IP=37.139.129.132  ISP=Delis LLC                       targets  520 apps in Poland,Usa,Spain,Turkey,...      UP
IP=179.43.175.134  ISP=Private Layer INC               targets  331 apps in Poland,Spain,Usa,Turkey,...      UP
IP=45.142.182.142  ISP=SkyLink Data Center BV          targets   72 apps in Spain,Greece,Colombia,The netherlands,... UP
IP=85.31.46.188    ISP=Delis LLC                       targets  520 apps in Poland,Usa,Spain,Turkey,...      UP
IP=185.216.71.193  ISP=Delis LLC                       targets  517 apps in Poland,Usa,Spain,Turkey,...      UP
IP=185.161.208.249 ISP=Zemlyaniy Dmitro Leonidovich  targets    0 apps                                     DOWN
IP=146.19.106.109  ISP=TANGRAM CANADA INC.             targets   34 apps in Spain,Colombia,Germany           UP
```

Sept 23, 2022

C2 Examples - Operational yesterday (Sept 27 2022)

146.19.106.109

Targets mostly 🇪🇸

179.43.162.102

Targets 🇹🇷 🇮🇱 🇩🇪

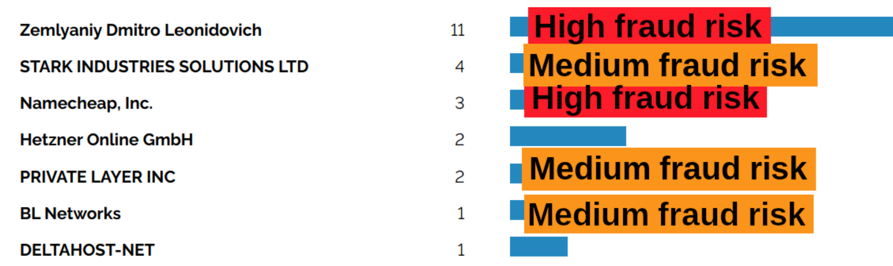
179.43.142.189

Targets 🇦🇹 🇩🇪

37.139.129.132

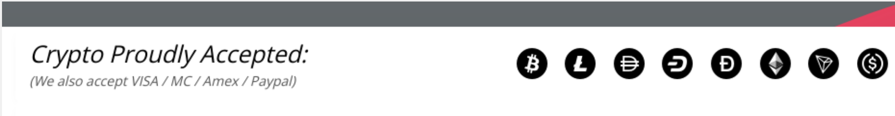
Targets 369 banks, 58 crypto currency apss, 49 finance institutions etc in many countries

Preference for low reputation ISPs



Zemlyaniy Dmitro Leonidovich	11	High fraud risk
STARK INDUSTRIES SOLUTIONS LTD	4	Medium fraud risk
Namecheap, Inc.	3	High fraud risk
Hetzner Online GmbH	2	
PRIVATE LAYER INC	2	Medium fraud risk
BL Networks	1	Medium fraud risk
DELTAHOST-NET	1	

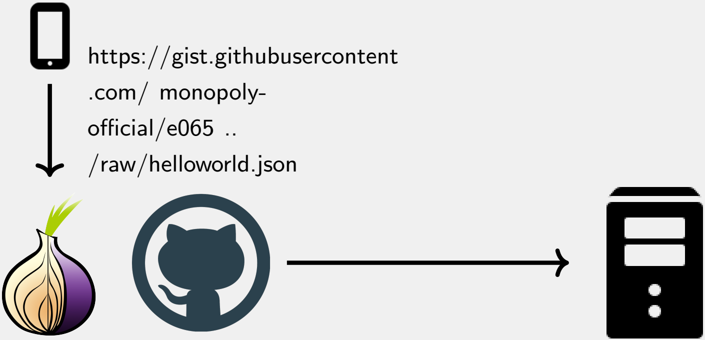
Fraud risk evaluated by Scamalytics



Crypto Proudly Accepted:

(We also accept VISA / MC / Amex / Paypal)

Domain names, IP addresses



https://gist.githubusercontent.com/ monopoly-official/e065 .. /raw/helloworld.json

base64: {"domains":["http://tomoschester84.top"]}

Change every 2-6 months

Change name every 2-3 days

Change IP address every 1-2 months

Targeted applications

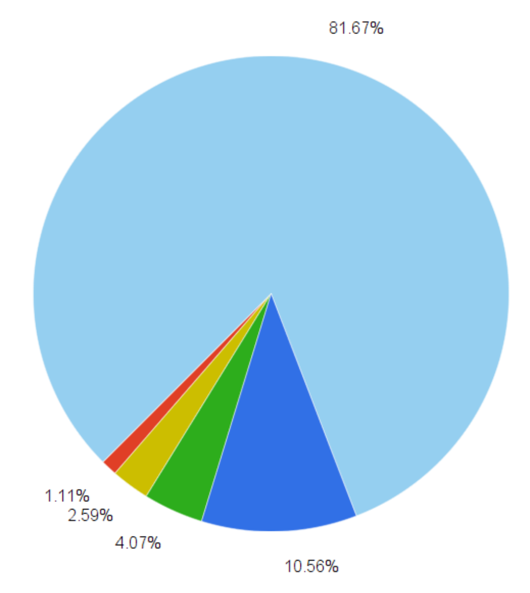
Czech Republic:

```
cz.airbank.android
cz.csas.business24
cz.csas.georgego
cz.csob.ceb
...
```

Recently added:

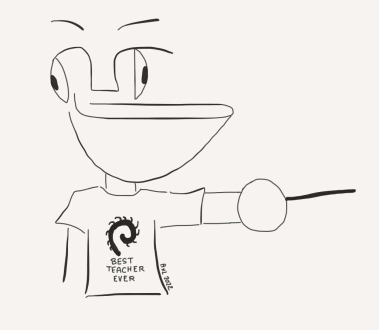
```
[+] New package supported: com.abanca.bancaempresas
[+] New package supported: com.bancsabadell.wallet
[+] New package supported: com.bankinter.bkwallet
[+] New package supported: es.correos.widget
[+] New package supported: es.unicajabanco.app
[+] New package supported: com.grupocajamar.wefferent.huawei
[+] New package supported: es.bancosantander.apps.huawei
[+] New package supported: net.inverline.bancosabadell.officelocator.an
[+] New package supported: com.sa.baj.aljazirasmart
[+] New package supported: sa.com.se.alkahraba
```

Type of apps



- 80% banks
- 10% cryptocurrency apps
- Rest: mail, security, 2FA...

Key Points



- Approx **20 operational C2** at all time
- **Maintained**
- Several different **affiliates**
- Targets **banks** and finance worldwide

Android/BianLian: what's special?

1. Very good code structure and **plug-ins** ("components")
2. State of the Art implementation in many domains
3. Uses **TeamViewer** - not "VNC"

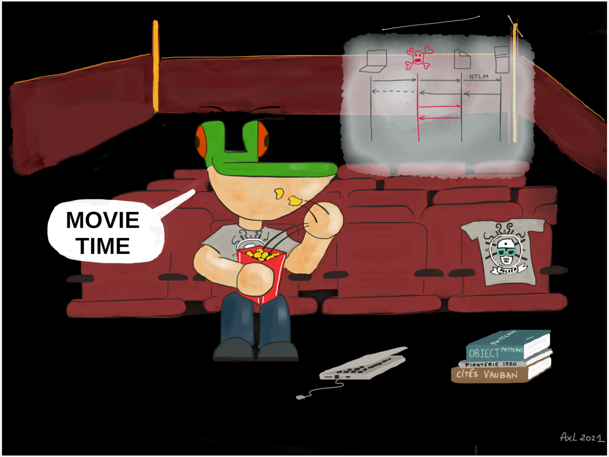
State of the Art implementation

Detect top application	Parse `/proc` and `/proc/PID/` Best solution in 2018 Now rather `UsageStats`
Disable Play Protect	Starts `VerifyAppsSettingsActivity` activity + automatic disable through Accessibility Services State of the Art
Doze mode	Starts `REQUEST_IGNORE_BATTERY_OPTIMIZATIONS` activity End-user still needs to accept doze mode. Flubot uses Accessibility Services to automatically accept
Notifications	Disable notifications via Accessibility Services Best implementation

State of the Art implementation

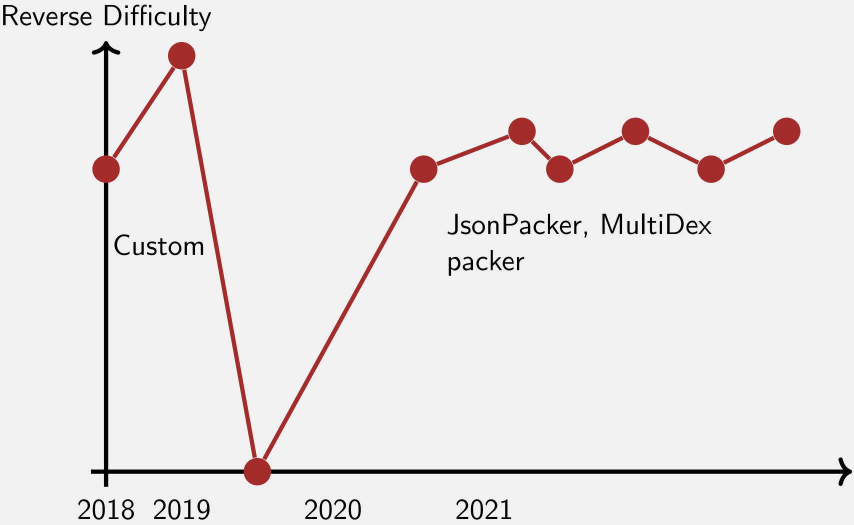
Sound switch	Mute + handles Do Not Disturb with `NOTIFICATION_POLICY_ACCESS_SETTINGS‘` + Accessibility Services Best implementation
Screenshots	`createScreenCaptureIntent` + Accessibility Services Best implementation
TeamViewer	Configure app via Accessibility Setting Only Alien and BianLian support TeamViewer

Manipulating BianLian locally

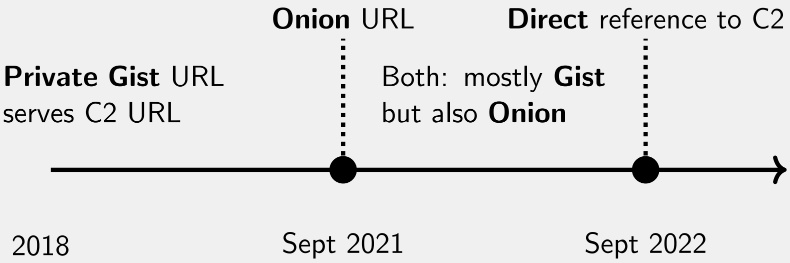


- Flask mini server: https://github.com/cryptax/misc-code
- Configurable: screencast, lock ...
- Redirect IP address see blog post

Packing evolution



Redirecting to C2: evolution



Private Gist URL serves C2 URL

Onion URL

Both: mostly **Gist** but also **Onion**

Direct reference to C2

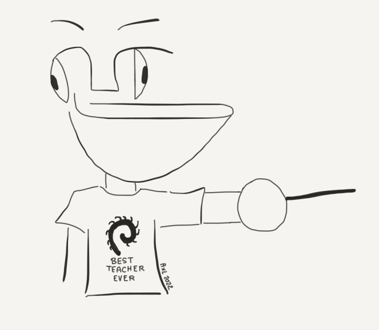
2018

Sept 2021

Sept 2022

Resilience 101

Key Points



- Excellent code **architecture**
- Choice for **simple but proved techniques**
- Stay **under the radar**: never too greedy

How can we stop this?

A nightmare to stop

- Sinkhole?
- Too many registrars, hosting services do not care at all
- Banks: file complaints
- Europol?
- Ideas? Let's chat!

References

- Unpackers, Fake Server: https://github.com/cryptax/misc-code
- Video of malware, photoTAN: https://www.fortinet.com/blog/threat-research/android-bianlian-botnet-mobile-banking
- Android/BianLian analysis: https://cryptax.medium.com (several posts)
- **Thanks to colleagues Bhumit Mali + team and Aamir Lakhani**
- Sept 19, 2022 sample:
  152c236f84d44d34c3d0c6a6450ed933893fb6ea274e5561157f8a92966c0448

Thanks for attending!

FORTINET®