flare

The Ouroboros of Cybercrime

Witnessing threat actors go from Pwn to Pwn’d.

flare.io

About us

Cyber Threat Intelligence Researcher

Offensive Security Background

British gentleman pursuing Professor Moriarty's career path (legally)

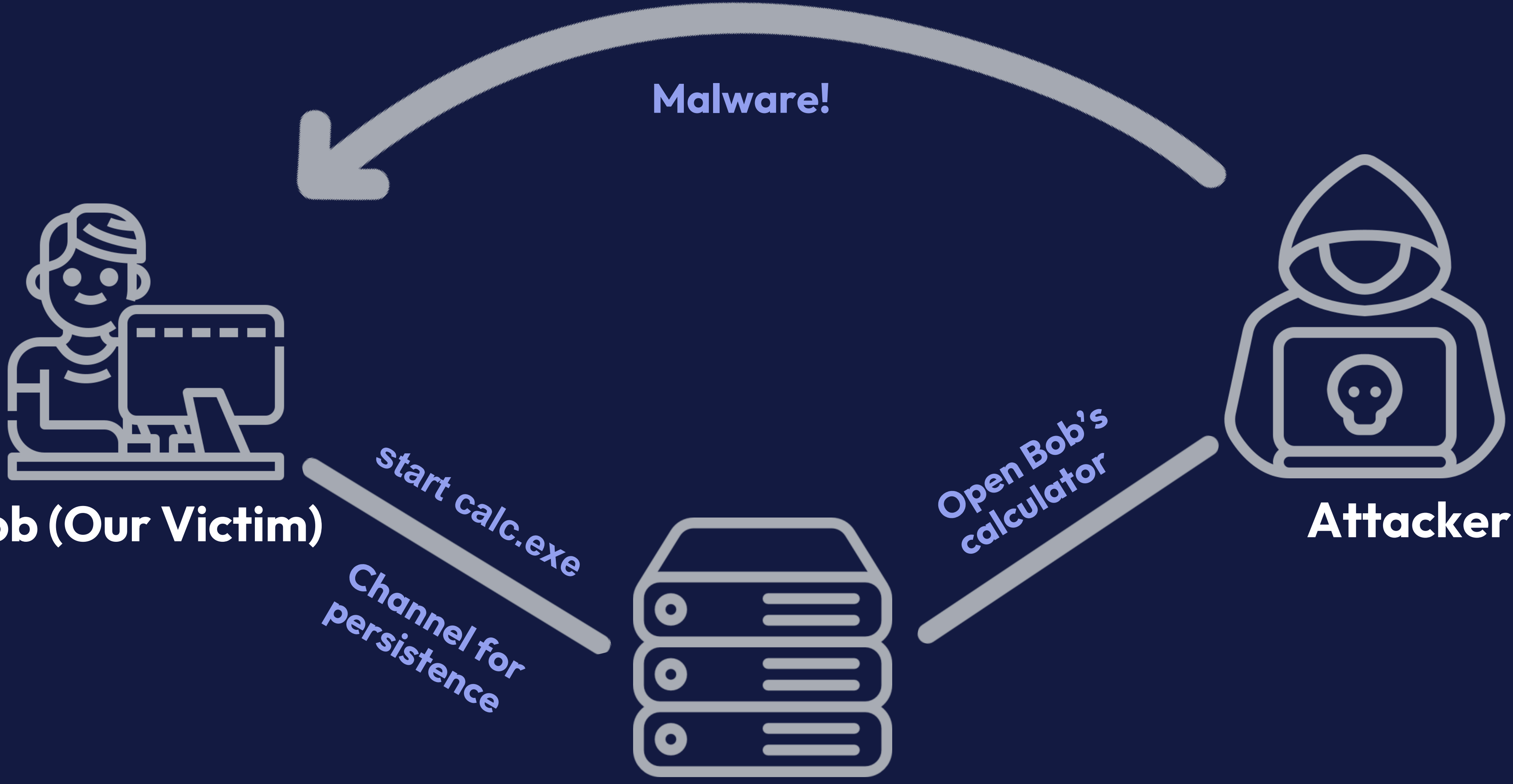
Cyber Threat Intelligence Researcher

Mathematics and Criminology Background

French Lady on a mission to uphold Sherlock Holmes's legacy (minus the hat)

What if C2 operators also fell victim to their own skim : the biter bit.

Command & Control (C2) Servers



Malware!

Bob (Our Victim)

start calc.exe

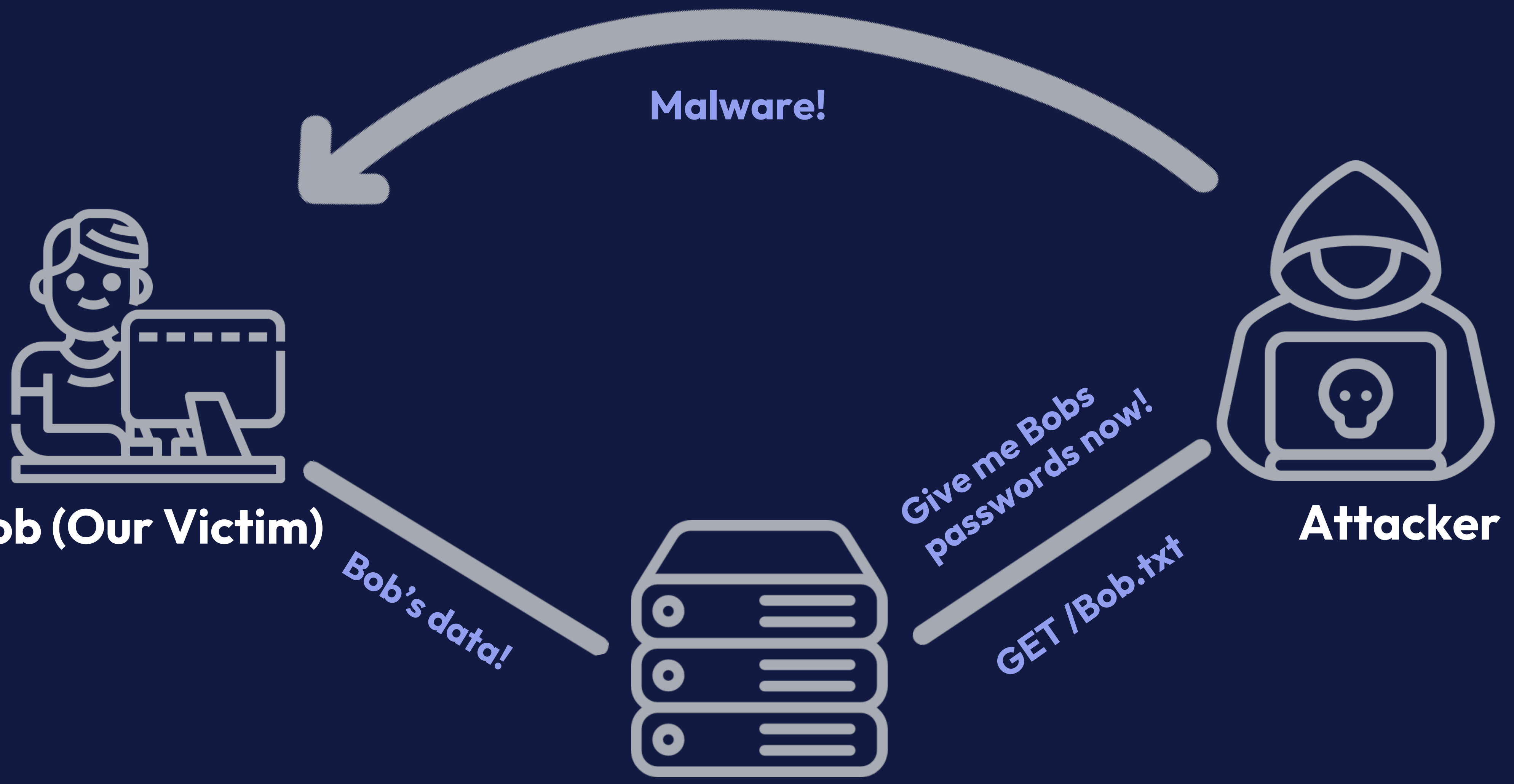
Channel for persistence

Open Bob's calculator

Attacker

frailedfederaldemeanour.com

Infostealers & C2s: The Exfiltration Link



fraileddfederaldemeanour.com

DATA

Data

4,258 Stealer Logs

25% cross-forum logs

CRACKED.IO
BEYOND THE LIMITS
BHF
eXploit.in
XSS.is
BF BreachForums
RAID FORUMS
Nulled
CRAX

DEVELOPING SCOPE

C2 Detection with Viriback and URLScan

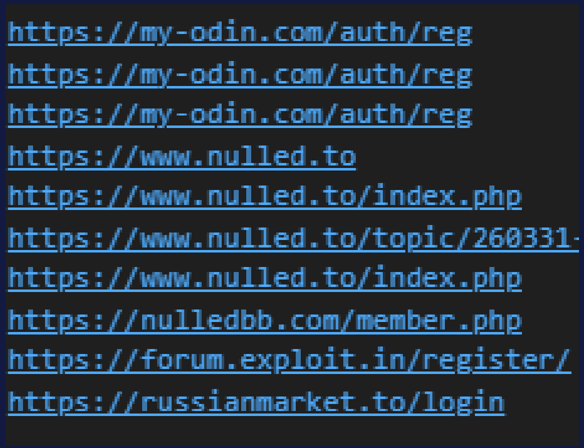
11,000 C2 Hostnames

8,049 C2 Hostnames

The BITERS BIT

From thousands to few.

The bitters bit



```
https://my-odin.com/auth/reg
https://my-odin.com/auth/reg
https://my-odin.com/auth/reg
https://www.nulled.to
https://www.nulled.to/index.php
https://www.nulled.to/topic/260331-
https://www.nulled.to/index.php
https://nulledbb.com/member.php
https://forum.exploit.in/register/
https://russianmarket.to/login
```

RHADAMANTHYS

1 C2 IP

1 C2 IP

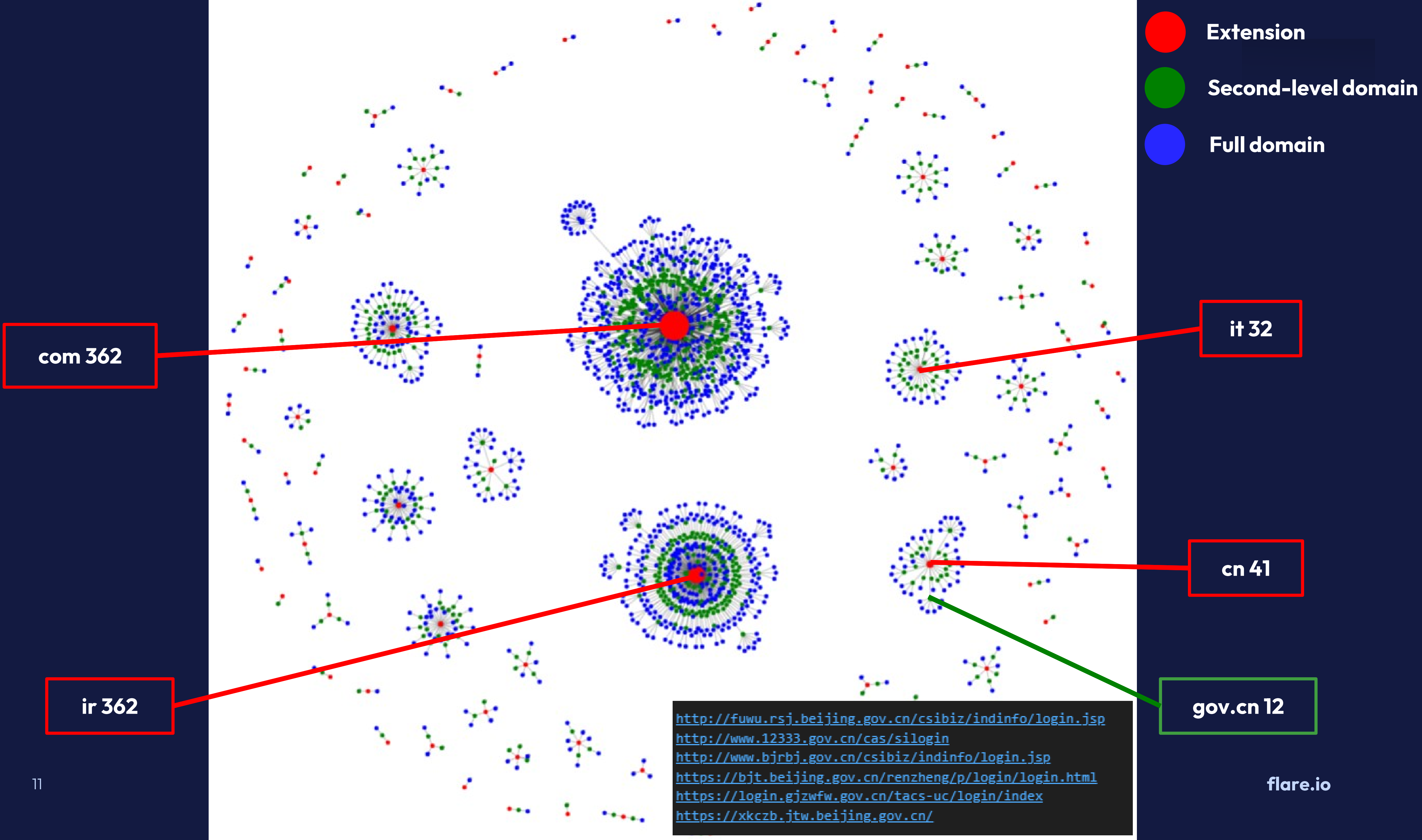
RHADAMANTHYS

1 C2 IP

REDLINE
INFOSTEALER

3 C2 IPs

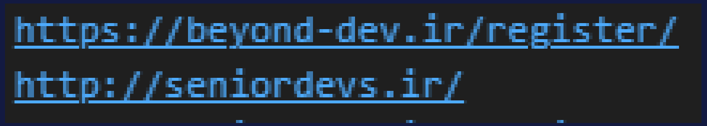
1 C2 IP



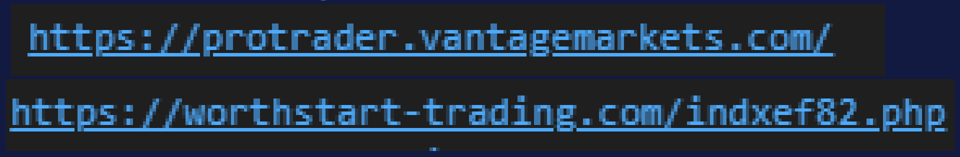
http://fuwu.rsj.beijing.gov.cn/csibiz/indinfo/login.jsp
http://www.12333.gov.cn/cas/silogin
http://www.bjrbj.gov.cn/csibiz/indinfo/login.jsp
https://bjt.beijing.gov.cn/renzheng/p/login/login.html
https://login.gjzwfw.gov.cn/tacs-uc/login/index
https://xkczb.jtw.beijing.gov.cn/

FROM THOUSANDS TO FEW.

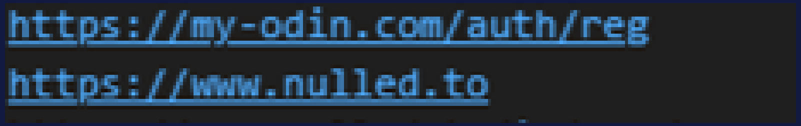
The bitters bit



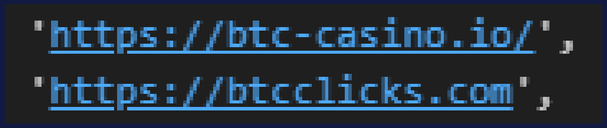
```
https://beyond-dev.ir/register/
http://seniordevs.ir/
```



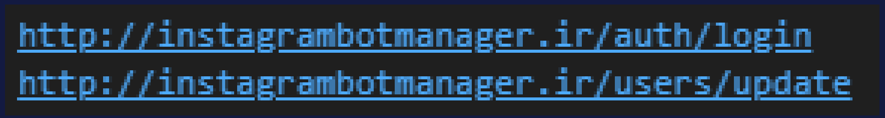
```
https://protrader.vantagemarkets.com/
https://worthstart-trading.com/indxef82.php
```



```
https://my-odin.com/auth/reg
https://www.nulled.to
```



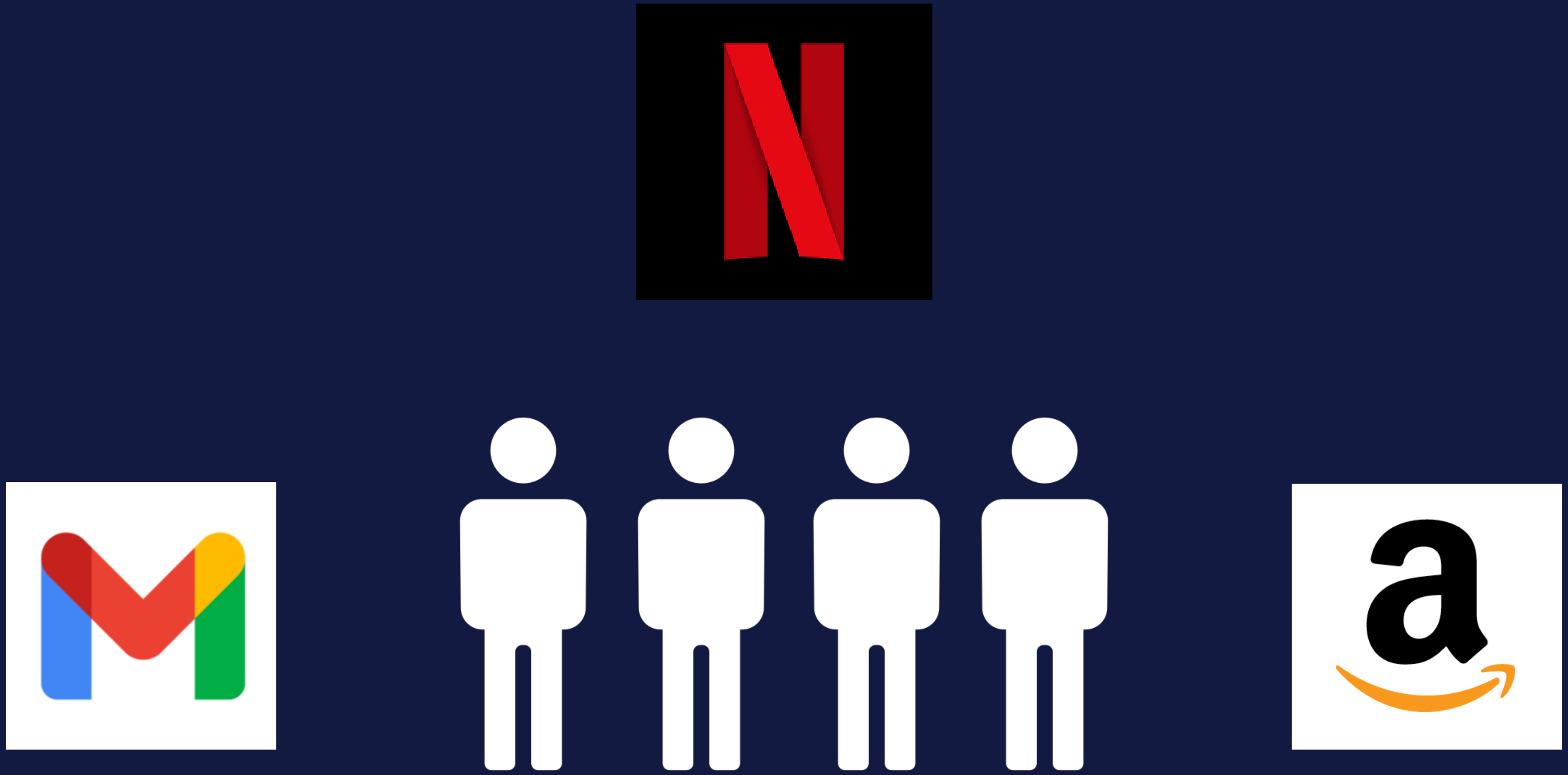
```
'https://btc-casino.io/',
'https://btcclicks.com',
```



```
http://instagrambotmanager.ir/auth/login
http://instagrambotmanager.ir/users/update
```

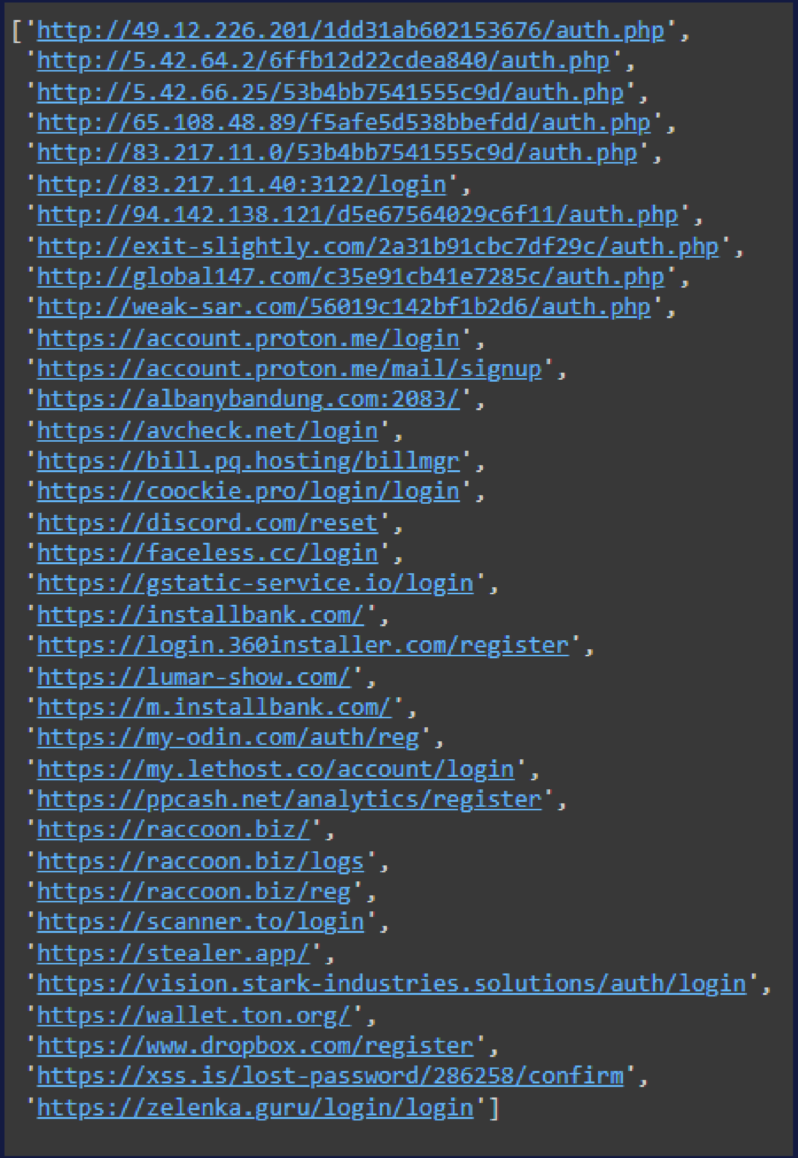
BEGINNING OF SUSPISCIONS

Beginning of Suspiscions

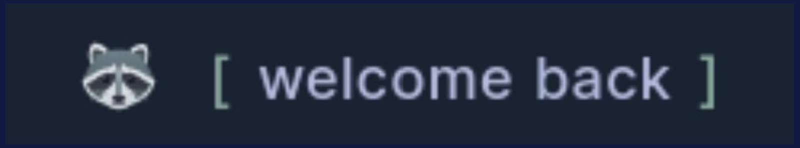


>100 credentials

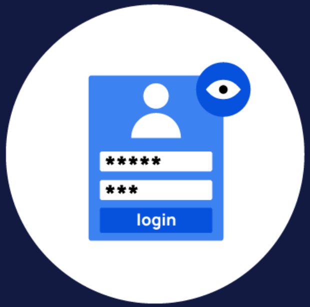
Beginning of Suspiscions



```
['http://49.12.226.201/1dd31ab602153676/auth.php',
 'http://5.42.64.2/6ffb12d22cdea840/auth.php',
 'http://5.42.66.25/53b4bb7541555c9d/auth.php',
 'http://65.108.48.89/f5afe5d538bbefdd/auth.php',
 'http://83.217.11.0/53b4bb7541555c9d/auth.php',
 'http://83.217.11.40:3122/login',
 'http://94.142.138.121/d5e67564029c6f11/auth.php',
 'http://exit-slightly.com/2a31b91cbc7df29c/auth.php',
 'http://global147.com/c35e91cb41e7285c/auth.php',
 'http://weak-sar.com/56019c142bf1b2d6/auth.php',
 'https://account.proton.me/login',
 'https://account.proton.me/mail/signup',
 'https://albanybandung.com:2083/',
 'https://avcheck.net/login',
 'https://bill.pq.hosting/billmgr',
 'https://coockie.pro/login/login',
 'https://discord.com/reset',
 'https://faceless.cc/login',
 'https://gstatic-service.io/login',
 'https://installbank.com/',
 'https://login.360installer.com/register',
 'https://lumar-show.com/',
 'https://m.installbank.com/',
 'https://my-odin.com/auth/reg',
 'https://my.lethost.co/account/login',
 'https://ppcash.net/analytics/register',
 'https://raccoon.biz/',
 'https://raccoon.biz/logs',
 'https://raccoon.biz/reg',
 'https://scanner.to/login',
 'https://stealer.app/',
 'https://vision.stark-industries.solutions/auth/login',
 'https://wallet.ton.org/',
 'https://www.dropbox.com/register',
 'https://xss.is/lost-password/286258/confirm',
 'https://zelenka.guru/login/login']
```



🦝 [welcome back]



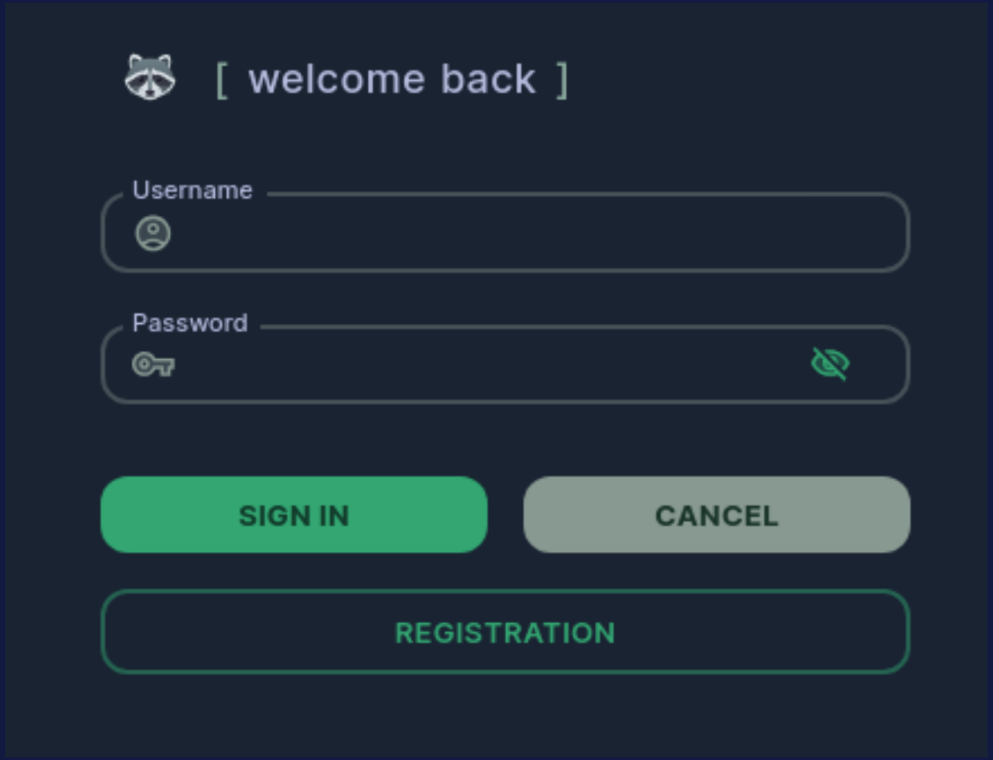
~30 credentials

THE MALWARE MAESTRO

The Malware Maestro

- ❑ Raccoon[.]biz
- ❑ Faceless[.]cc
- ❑ Scanner[.]to
- ❑ Stealer[.]app

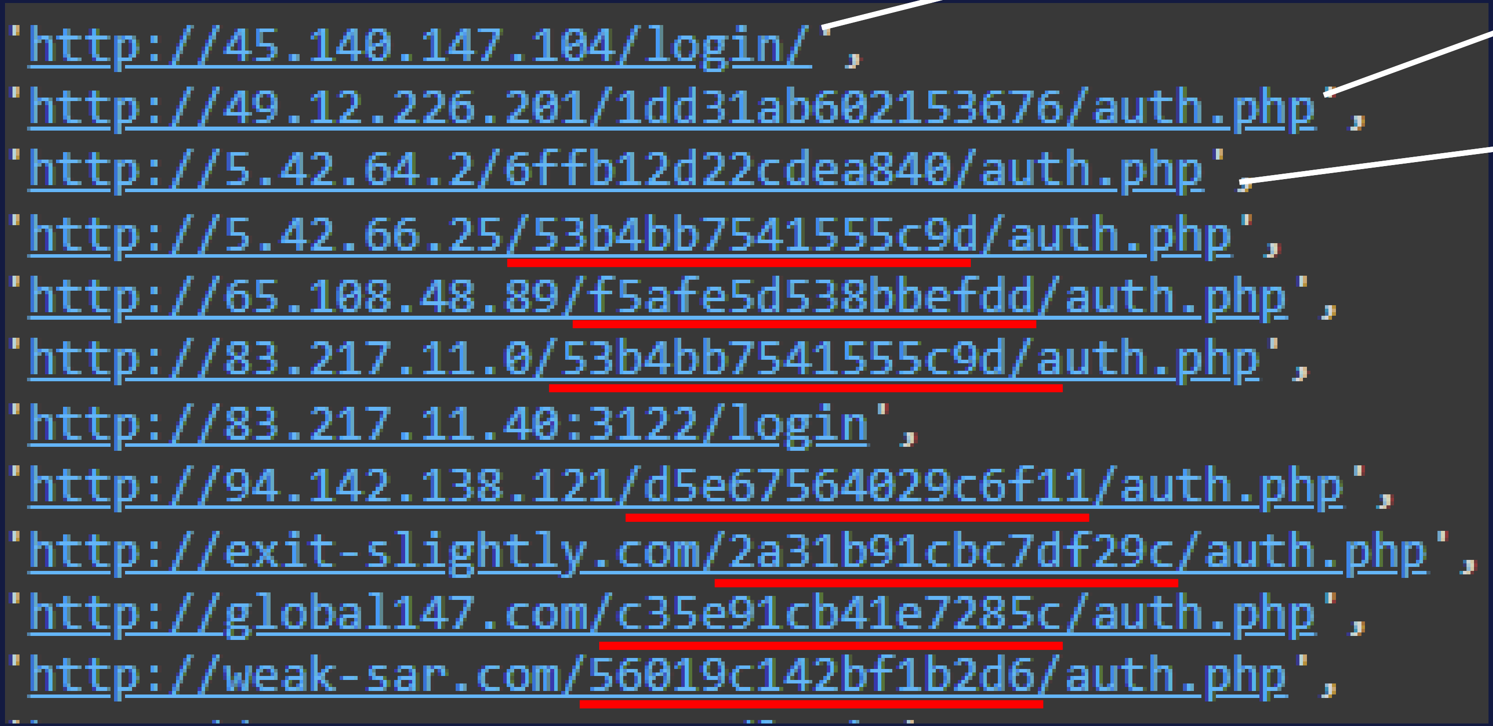
```
Raccoon[.]biz/logs
Raccoon[.]biz/reg
```



ACCESS.

The Malware Maestro

Username	Password
admin	HW4*********
[UNKNOWN]	adm*******



```
'http://45.140.147.104/login/',
'http://49.12.226.201/1dd31ab602153676/auth.php',
'http://5.42.64.2/6ffb12d22cdea840/auth.php',
'http://5.42.66.25/53b4bb7541555c9d/auth.php',
'http://65.108.48.89/f5afe5d538bbefdd/auth.php',
'http://83.217.11.0/53b4bb7541555c9d/auth.php',
'http://83.217.11.40:3122/login',
'http://94.142.138.121/d5e67564029c6f11/auth.php',
'http://exit-slightly.com/2a31b91cbc7df29c/auth.php',
'http://global147.com/c35e91cb41e7285c/auth.php',
'http://weak-sar.com/56019c142bf1b2d6/auth.php',
```

Mystic – Multi-Functional Malware

PrivateLoader – Malware Loader

Asuka - Trojan

Hashed Victim

THE MAESTRO'S SYMPHONY

QUADRUPLE THREAT.

The Malware's Symphony

PrivateLoader

Mystic

Raccoon

Asuka

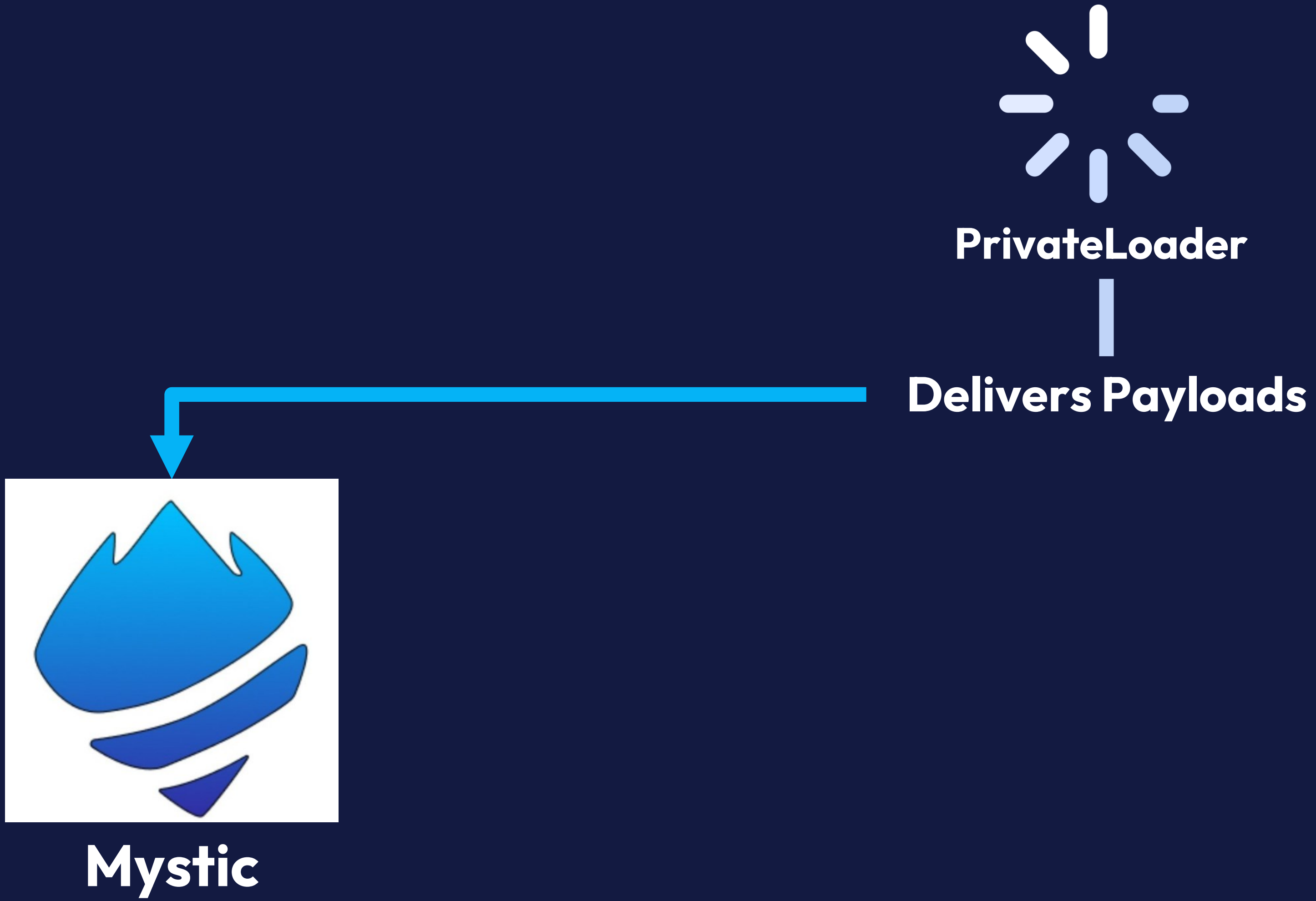
Movement I – Initial Infection

PrivateLoader

Malware Loader

↓

Deliver Malicious Payloads



PrivateLoader

Delivers Payloads

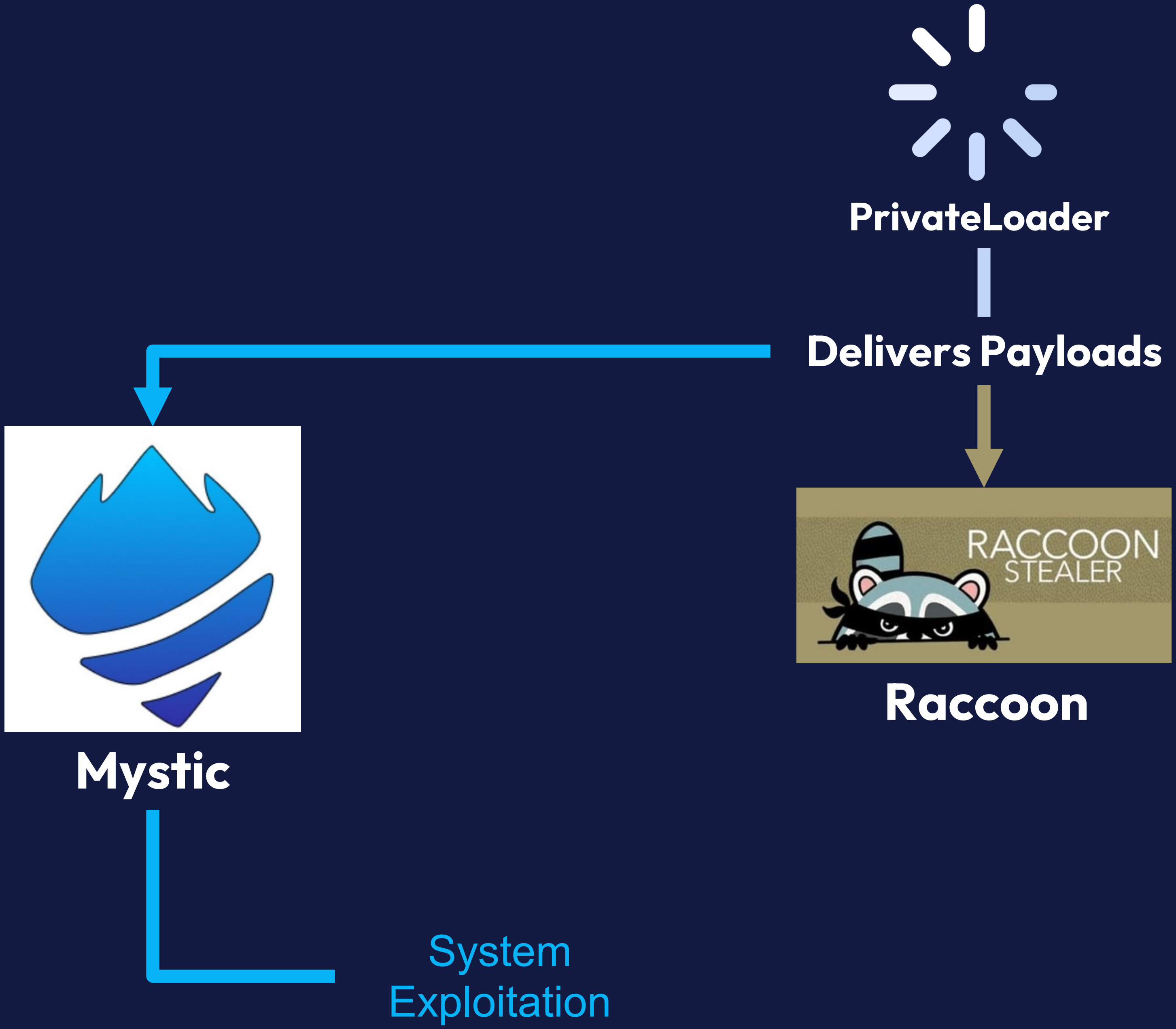
Mystic

Movement II – System Exploitation

Mystic

Multifunctional Malware

- □ Stealing data
- □ Keylogging
- □ Persistence



PrivateLoader

Delivers Payloads

Mystic

Raccoon

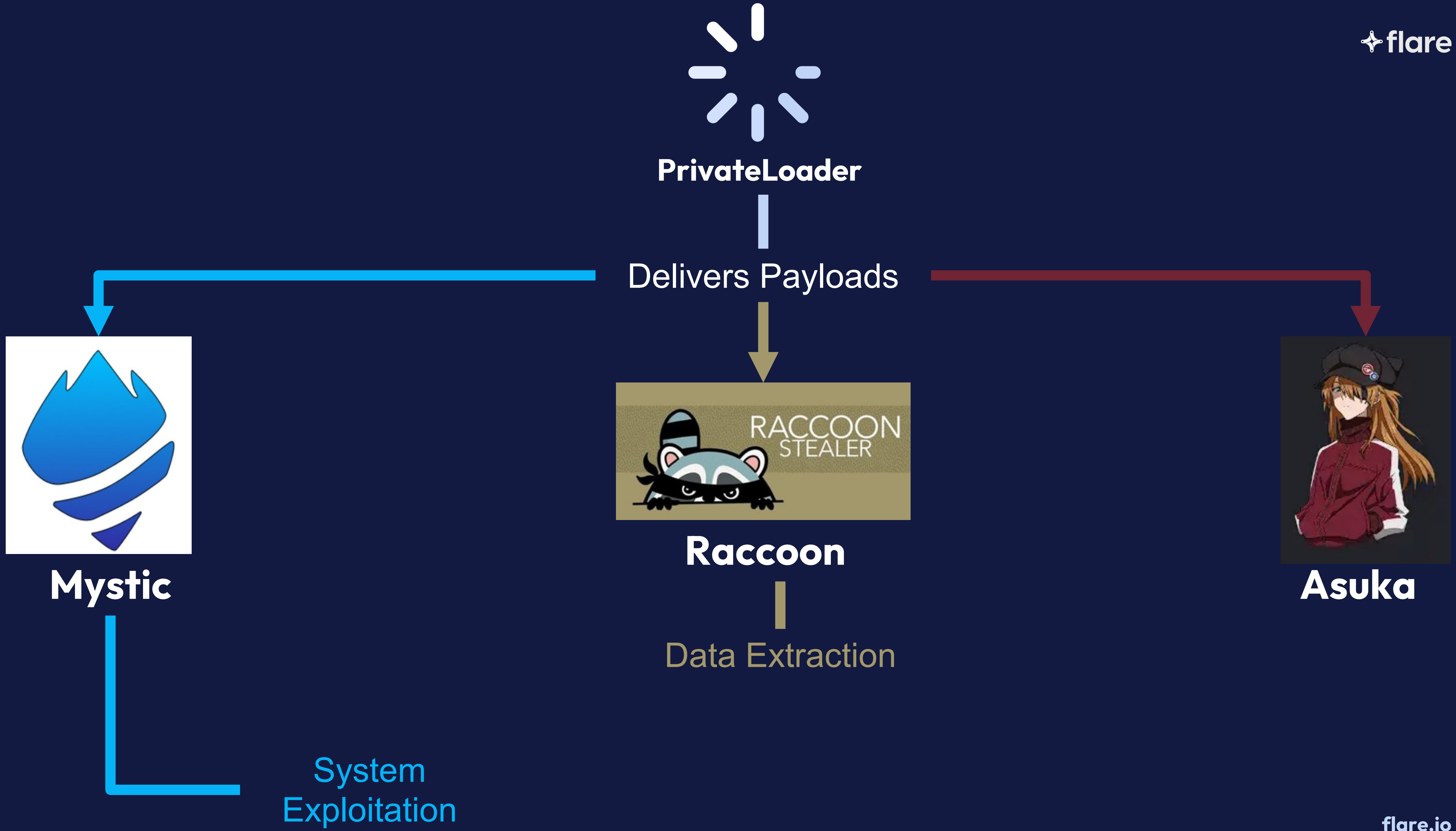
System Exploitation

Movement III – Data Extraction

Raccoon

Infostealer

- ❑ Loggin Credentials
- ❑ Cookies
- ❑ Wallets



PrivateLoader

Delivers Payloads

Mystic

System Exploitation

Raccoon

Data Extraction

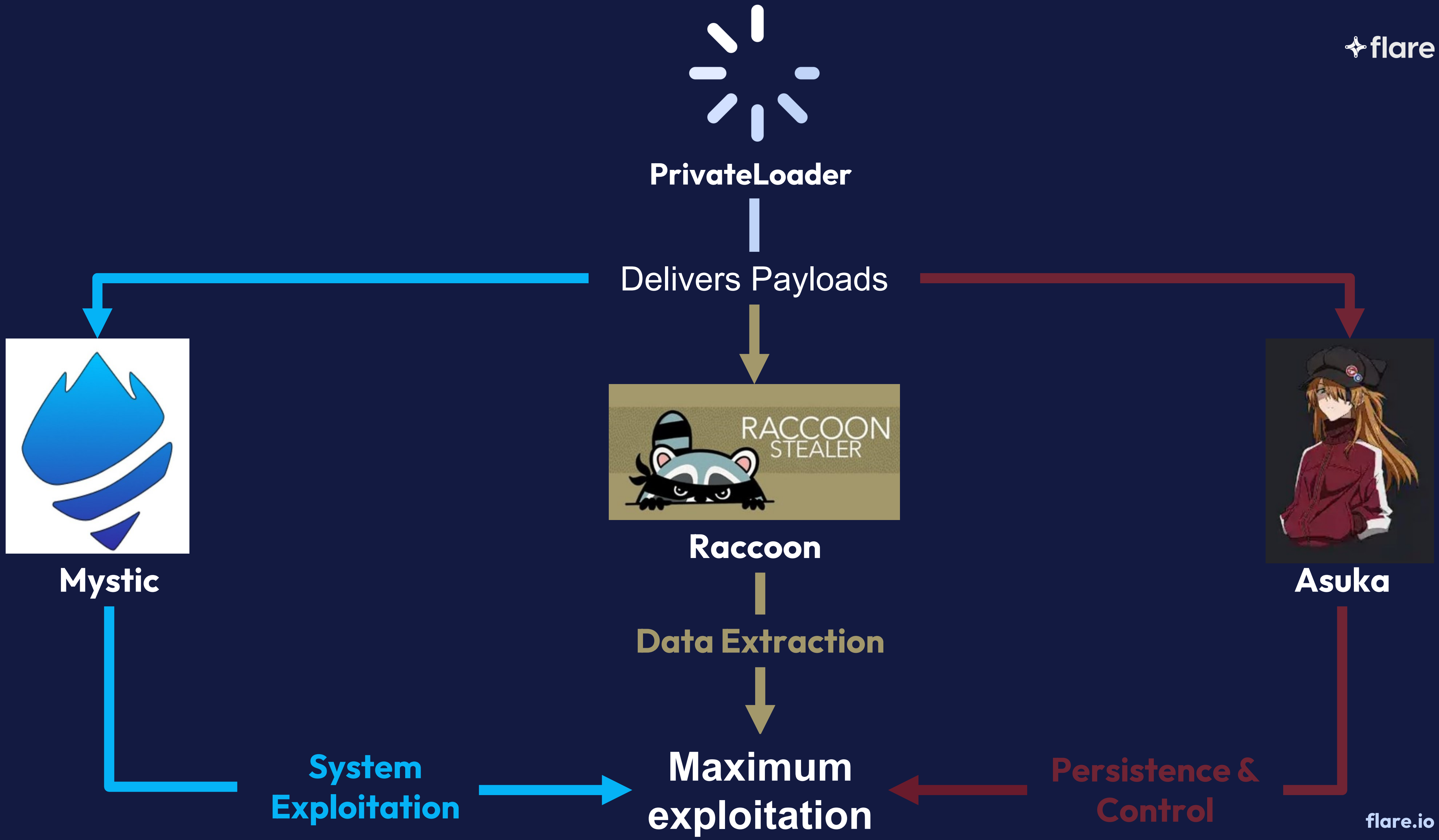
Asuka

Movement IV – Persistence

Asuka

Trojan

- ❑ Maintain Control
- ❑ Persistent Backdoors



PrivateLoader

Delivers Payloads

Mystic

Raccoon

Asuka

Data Extraction

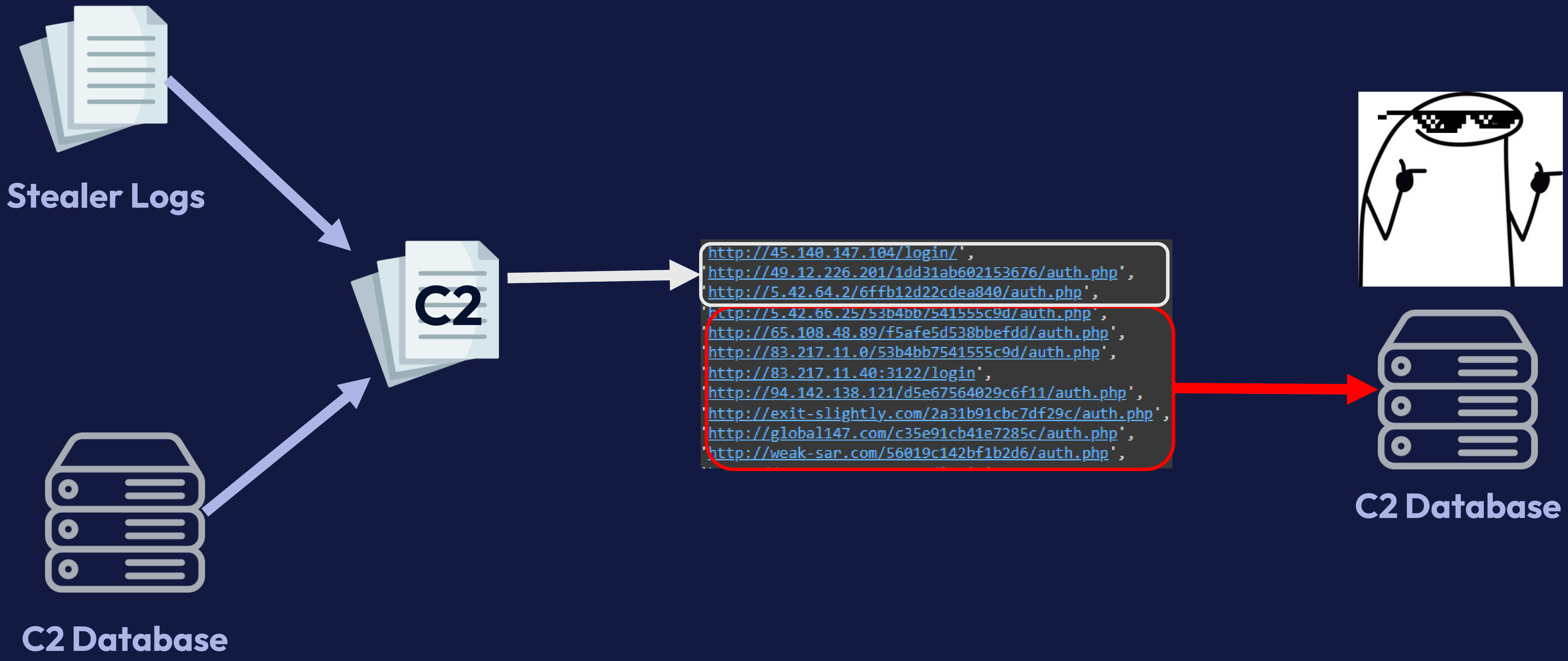
System Exploitation

Persistence & Control

Maximum exploitation

flare

FROM LOGS TO ACTION:
Practical Applications in Security



```
'http://45.140.147.104/login/',
'http://49.12.226.201/1dd31ab602153676/auth.php',
'http://5.42.64.2/6ffb12d22cdea840/auth.php',
'http://5.42.66.25/53b4bb7541555c9d/auth.php',
'http://65.108.48.89/f5afe5d538bbefdd/auth.php',
'http://83.217.11.0/53b4bb7541555c9d/auth.php',
'http://83.217.11.40:3122/login',
'http://94.142.138.121/d5e67564029c6f11/auth.php',
'http://exit-slightly.com/2a31b91cbc7df29c/auth.php',
'http://global147.com/c35e91cb41e7285c/auth.php',
'http://weak-sar.com/56019c142bf1b2d6/auth.php',
```

flare

Stuart Beck
Cyber Threat Intelligence Researcher

Estelle Ruellan
Cyber Threat Intelligence Researcher