OopSec: The Short Lived Campaign of Cthulhu Stealer



Topics Covered

01 Speaker

02 macOS malware landscape

03 Cthulhu Stealer

04 Opsec Mistakes

Speaker

- Tara Gould
- Belfast
- Threat Research Lead at Cado (acquired by Darktrace)



02

macOS malware landscape

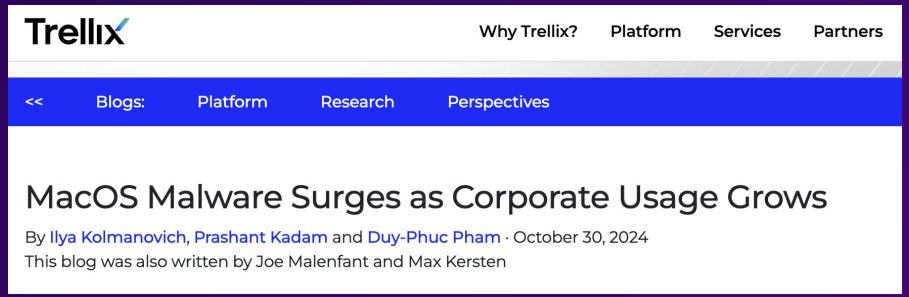
macOS malware landscape

⬆️

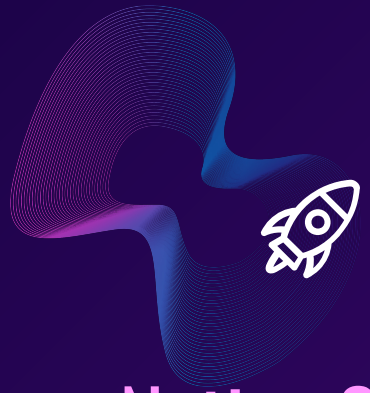
400% increase

Larger amount of enterprise users

Shift from adware to stealers

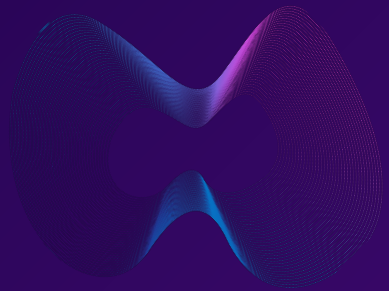


Who?



Nation State

Various APT





Cybercrime

MaaS affiliates
Traffer groups

Malwares

NimDoor
DPRK

RustBucket
DPRK

SysJoker
Hamas Affiliated



Atomic Stealer
MaaS



Poseidon
MaaS



Banshee Stealer
MaaS

03

Cthulhu Stealer

GTAIV_EarlyAccess_MACOS

STEP 1

Right click



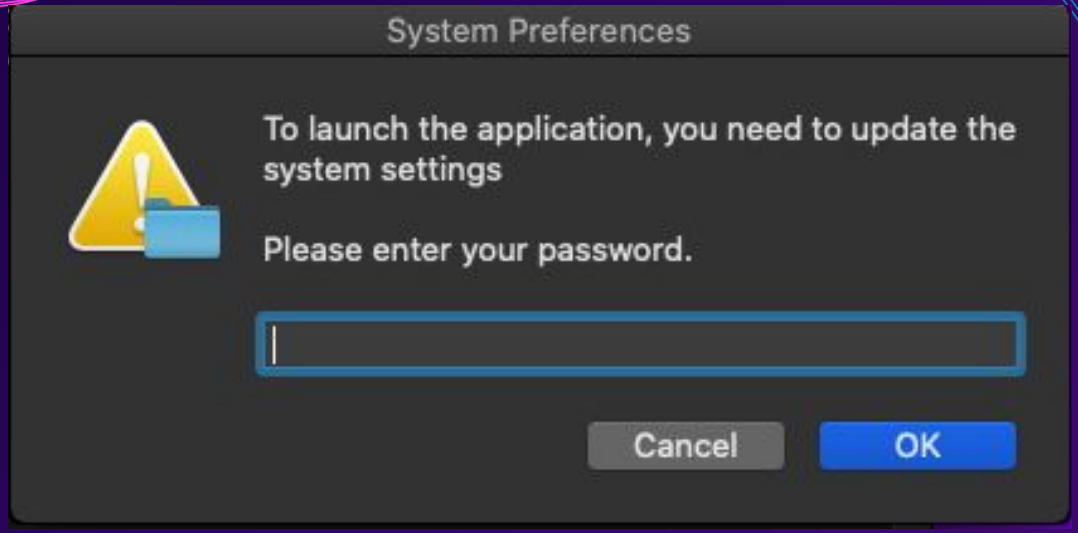


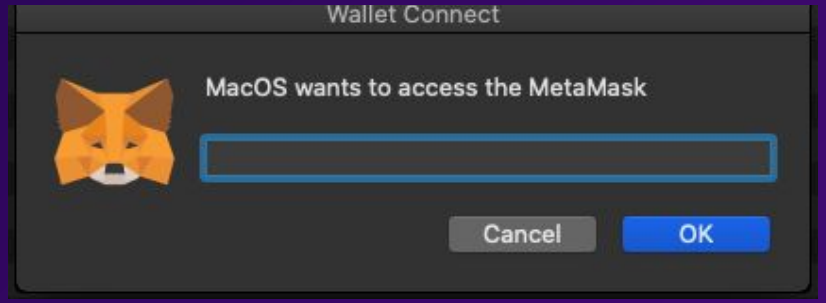
GTAIV_EarlyAccess_MACOS

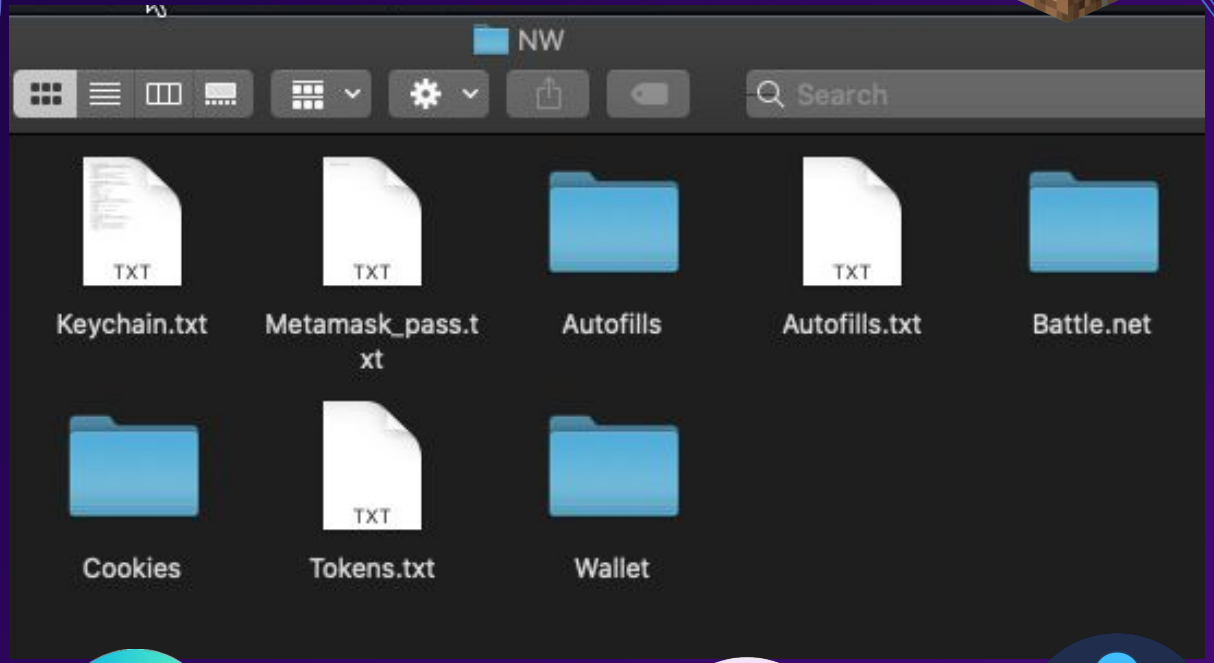
STEP 2

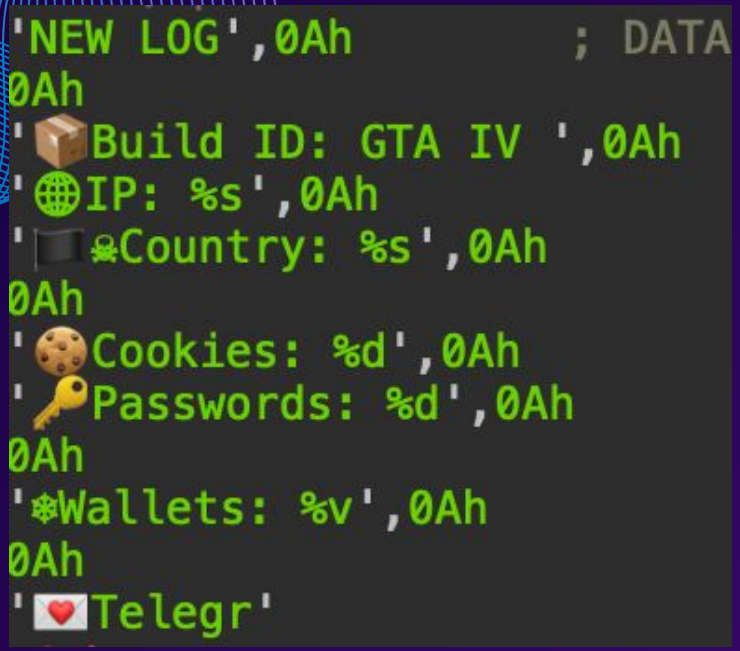
Click "Open"




System Preferences
To launch the application, you need to update the system settings
Please enter your password.
Cancel
OK


Wallet Connect
MacOS wants to access the MetaMask
Cancel
OK


NW
Search
TXT
Keychain.txt
TXT
Metamask_pass.txt
Autofills
TXT
Autofills.txt
Battle.net
Cookies
TXT
Tokens.txt
Wallet



@====)>>>>>>>>>> CTHULHU STEALER - BOT <<<<<<<<<(====@
MAC PASSWORD: [redacted]

System and IP Information

System Information for macOS:

* **System:** [redacted]
* **Node Name:** [redacted]
* **Release:** [redacted]
* **Version:** [redacted]
* **Machine:** [redacted]
Hardware:

    Hardware Overview:

      Model Name: [redacted]
      Model Identifier: [redacted]
      Processor Speed: [redacted]
      Number of Processors: [redacted]
      Total Number of Cores: [redacted]
      L2 Cache (per Core): [redacted]
      L3 Cache: 16 MB
      Memory: 6,28 GB
      Boot ROM Version: [redacted]
      Apple ROM Info: [redacted]
      SMC Version (system): [redacted]
      Serial Number (system): [redacted]
      Hardware UUID: [redacted]

Software:

    System Software Overview:

      System Version: [redacted]
      Kernel Version: [redacted]
      Boot Volume: [redacted]
      Boot Mode: [redacted]
      Computer Name: [redacted]
      User Name: [redacted]
      Secure Virtual Memory: [redacted]
      System Integrity Protection: [redacted]
      Time since boot: [redacted]

Overview

DMG

Multi arch ARM and x86





Social Engineering

Osascript password prompt

Exfiltrated Data

Crypto Wallets, browser data, Telegram & gaming, system & network information



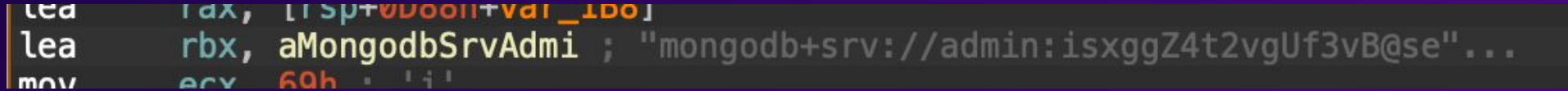
Credential Theft

Chainbreaker used to dump Keychain passwords



04

OpSec Mistakes


lea rax, [rsp+0D80h+var_1B8]
lea rbx, aMongodbSrvAdmi ; "mongodb+srv://admin:isxggZ4t2vgUf3vB@se"...
mov ecx, 69h ; 'i'

{} My Queries

CONNECTIONS (1)

Search connections

- serverlessinstance1.oxvg3re.mongodb...
  - admin
  - config
  - local
  - main
    - users

serverlessinstance1.oxvg3re.mongodb.net > main > users

Documents 151 | Aggregations | Schema | Indexes 1 | Validation

Type a query: { field: 'value' } or Generate query

ADD DATA | EXPORT DATA | UPDATE | DELETE

```
date_of_build : "2024-02-18 17:49:41.459629"
winmeta : 0
```

```
_id: ObjectId('658ec713bf75ded38aea7ef4')
userid : "5028511554"
username : "AtlantCC"
ban : 0
sub : "No"
logs : 0
cookie : 0
cards : 0
wallets : 0
passwords : 0
textfile : 0
photos : 0
telegram : 0
team_archive : 5028511554
channel : 5028511554
lang : "ru"
date_of_build : "2023-12-29 16:23:37.493755"
winmeta : 0
```

```
_id: ObjectId('65a1f37ec55d586a57499fe3')
userid : "322535461"
username : "Andrulio"
ban : 0
```

```
_id: ObjectId('658d8dcdaddc437ad41ba6bc')
userid : "5193141796"
username : "balaclavv"
ban : 0
sub : "2024-12-01 05:11"
logs : 85
cookie : 186720
cards : 28
wallets : 100
passwords : 10327
textfile : 0
photos : 0
telegram : 0
team_archive : "5193141796"
channel : "-1001939687263"
lang : "ru"
date_of_build : "2024-02-18 17:49:41.459629"
winmeta : 0
```





Переслано из LOGS | CTHULHU NFT
Лендинг: MTRX
IP: 1.163.73.5
Страна: TW
Пароли: 359
Куки: 6902
Кошельки: Binance,MetaMask,Binance Chain Wallet,Rabby,Sui,BinanceWallet,Phantom
684 18:41

Cthulhu Team

Russian Speaking

Underground marketplaces

Operate on Telegram and forums

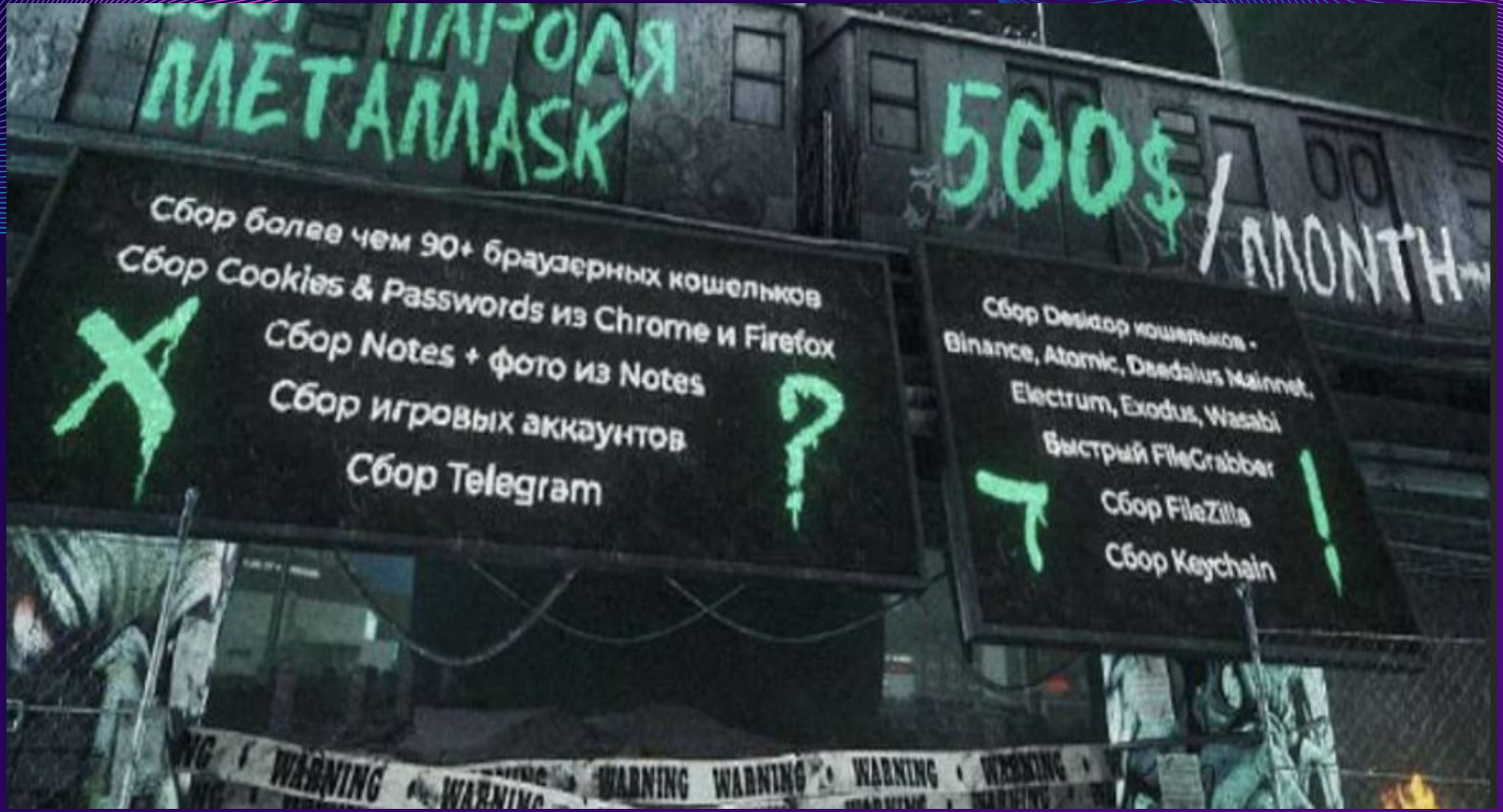


Formed of affiliates

Affiliates rent the malware each month for $500 and earn a percentage of earnings

Active since 2022

Previous activity involves NFT and Twitter scams. Previous Mac and Windows malware campaigns.


ПАРОЛЯ
METAMASK
500$ / MONTH
Сбор более чем 90+ браузерных кошельков
Сбор Cookies & Passwords из Chrome и Firefox
Сбор Notes + фото из Notes
Сбор игровых аккаунтов
Сбор Telegram
X
?
Сбор Desktop кошельков -
Binance, Atomic, Daedalus Mainnet,
Electrum, Exodus, Wasabi
Быстрый FileGrabber
Сбор FileZilla
Сбор Keychain
!
WARNING
WARNING
WARNING
WARNING

Search more



Not a market **Claim to Cthulhu ($4500)** Message

...Claim amount: $4,500 Wallets, defendant's contacts: Telegram: BALACLAVV Topic in which the defendant provided a service or sold/bought...

Buloklover , 17 Mar 2024 in section: Resolved claims

VA

Not a market **Claim to Cthulhu ($299.99)** Message

...@Cthulhu Claim amount: $300 Wallets, defendant's contacts: @ balaclavv Funds transfer receipt: No Screenshot showing the defendant's login...

valeryvodila , 17 Mar 2024 in section: Resolved claims

CR

Not a market **Claim to Cthulhu ($51,891)** Message

...Claim amount: $51,891 Wallets, defendant's contacts: Telegram: BALACLAVV Topic in which the defendant provided a service or sold/bought...

CryptoUrus , 13 Jan 2024 in section: Resolved claims



Not a market **Claim to Cthulhu ($2500)** Message

...@Cthulhu Claim amount: $2,500 Wallets, defendant's contacts: @ balaclavv Receipt of funds transfer: no Screenshot showing the defendant's login...

id787776908 , 15 Nov 2023 in section: Resolved claims



Not a market **Claim to Cthulhu ($100)** Message

...Claim amount: $100 Wallets, defendant's contacts: Telegram: BALACLAVV Topic in which the defendant provided a service or sold/bought...

worldhacker , Oct 31, 2023 in section: Resolved claims

OX

Not a market **Claim to Cthulhu ($156,189)** Message

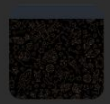
...claims: $156,189 Wallets, defendant's contacts: Telegram: BALACLAVV Topic in which the defendant provided a

Subscribe to the topic Search Sort



Buloklover **Plaintiff**

Defendant: ~~Cthulhu~~
Claim amount: $4,500
Defendant's wallets and contacts: Telegram: BALACLAVV
Thread in which the defendant provided a service or sold/purchased a product: https://zelenka.guru/threads/3619368/
Funds transfer receipt: no
Screenshot showing the defendant's Telegram login:



Imgur: The magic of the Internet

Discover the magic of the internet at Imgur, a community powered entertainment destination. Lift your spirits with funny jokes, trending memes, entertaining gifs, inspiring st...

imgur.com

Description of the situation:
On February 2nd I startedlog, 6k$ were successfully withdrawn and paid out from it, and another 3k$ remained in the stake until March 12. During this period of time, the Cthulhu team managed to disintegrate, and on the walletmammoth(https://debank.com/profile/0xf0dede477e1f4283c8bd47d8d7e21ee7c7922e12) there was already $4.5k
on March 11, the day before the possibility of withdrawal, I write to Balaclava so that he can see exactly how much time is left and he can withdraw the money beforemammoth, I'm throwinglog. then I notice that 2k$ came and went in less than a minute, it is clear that this is an automatic withdrawal. I write about it and of course the bookmaker says that he did not put it (having his own automatic withdrawal, pon). I ask for a seat, but the bookmaker starts repeating that he is busy and that's it. It's a long process, since he hasn't been able to withdraw one stake for almost a week , now it is unclear why 2.5k$ are still being held there,
the next few days of attempts to contact were successfully ignored (everything is visible in imgur), although there were his tags in the pro chat and he saw it. it would seem, why ignore if you have nothing to do with it?logor doesn't give a seat, doesn't even read messages.



17 Mar 2024

9

Cthulhu Timeline

2023 Balaclavv is scammed by 0xfff

Cthulhu Stealer operates from late 2023 to early 2024

Balaclavv dips

To Conclude...

Criminals targeting other criminals

Malware developers are prone to the same mistakes as anyone else

Be careful on a Mac!

Thank You!