CROWDSTRIKE

# macOS Stealers: Stealing Your Coins, Cookies and Keychains

® CrowdStrike, Inc. All Rights Reserved



**Maddie Stewart**
Sr. Intelligence Analyst
Global Threat Analysis Cell
(GTAC) eCrime



**Suweera De Souza**
Sr. Security Researcher
Technical Analysis Cell
(TAC) eCrime

® CrowdStrike, Inc. All Rights Reserved

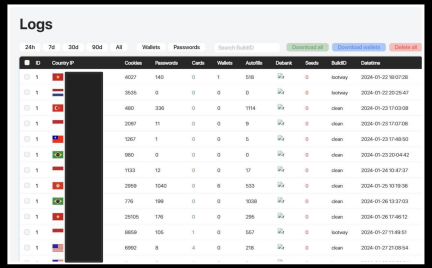
# Topics Covered

- Operations
- Campaigns/Delivery
- Comparing Popular and Private Stealers
  - Diving into *Cuckoo Stealer*'s Command-and-Control (C2)

® CrowdStrike, Inc. All Rights Reserved

# macOS eCrime Infostealer Expansion



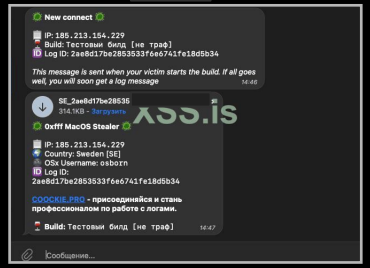


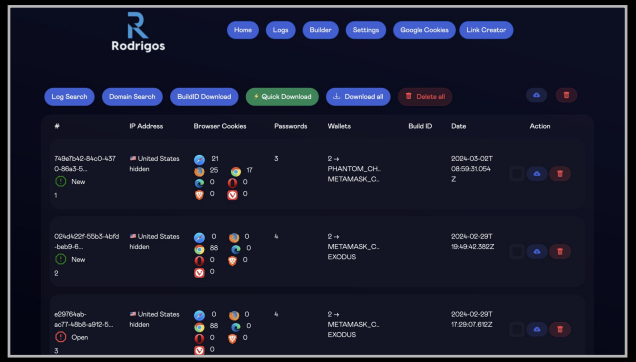










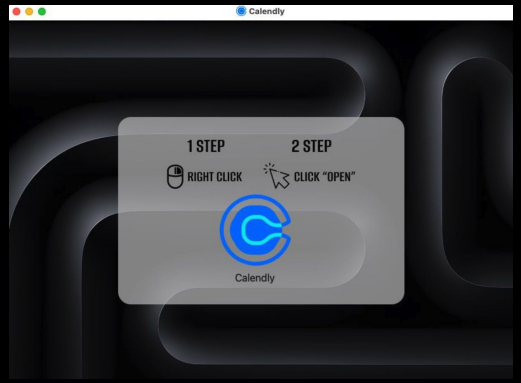



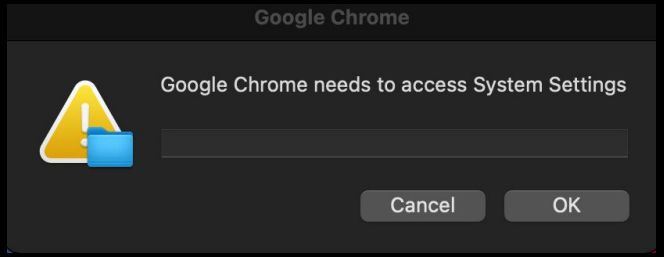

® CrowdStrike, Inc. All Rights Reserved

| macOS Stealer | Price | Windows Stealer | Price |
|---|---|---|---|
| *AMOS* | $3000 USD per month per license | *Lumma Stealer* | Pricing tiers range from $100 USD to $500 USD per month |
| *Doshell Stealer* | $2500 USD per month per license | *Rhadamanthys* | Pricing tiers range from $199 USD per month to $499 USD for 3 months |
| *Banshee Stealer* | Initially $3000 USD per month, later became $1999 USD per month | *Stealc* | Pricing tiers range from $200 USD per month, $500 USD for 3 months, and $800 for 6 months |

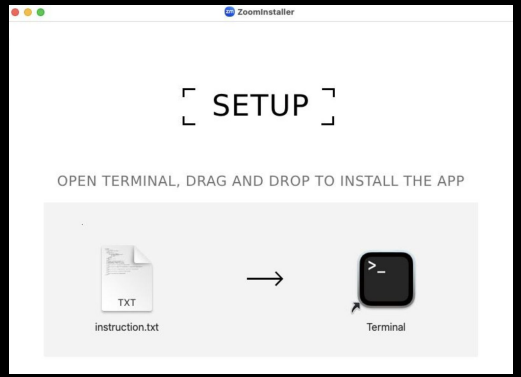


® CrowdStrike, Inc. All Rights Reserved













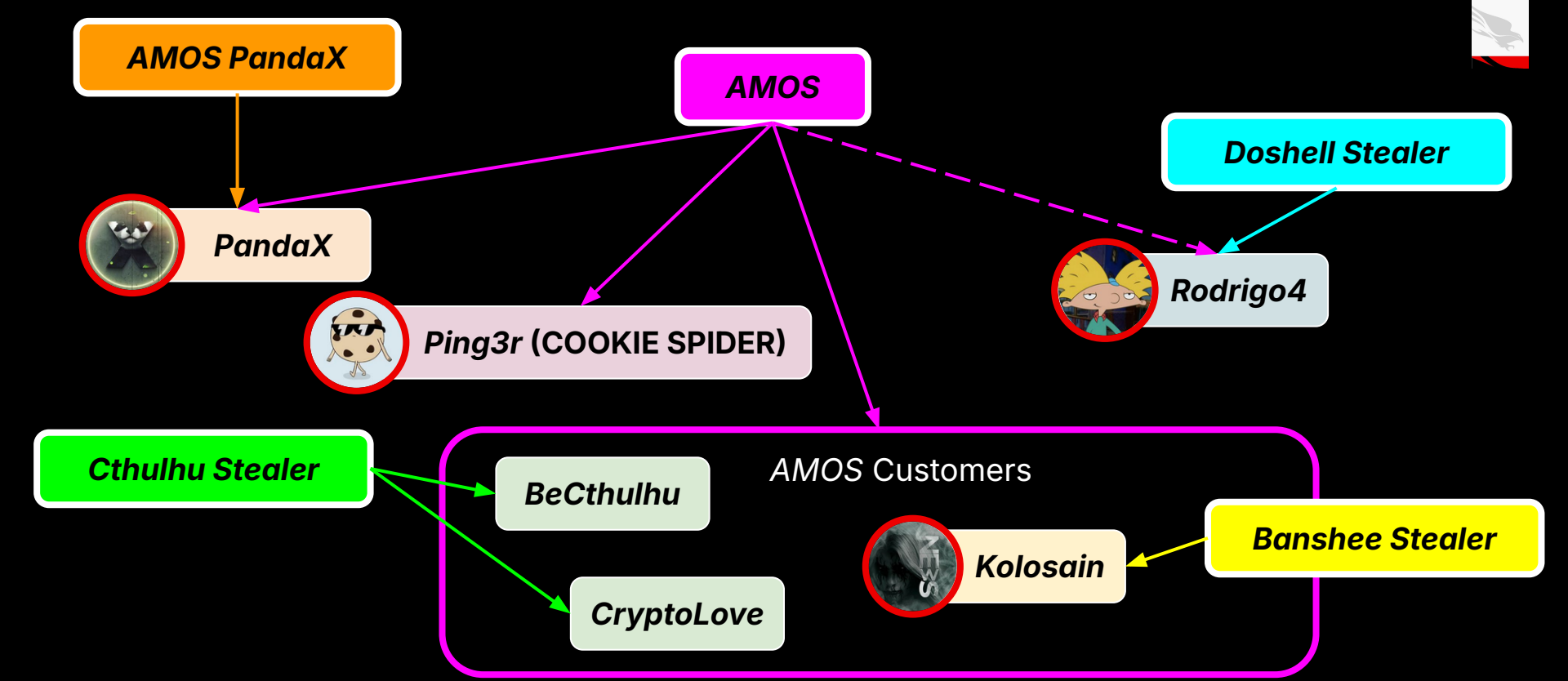
More reading:
https[:]//moonlock[.]com/oftw-macos-stealers-paper

® CrowdStrike, Inc. All Rights Reserved

# Operations

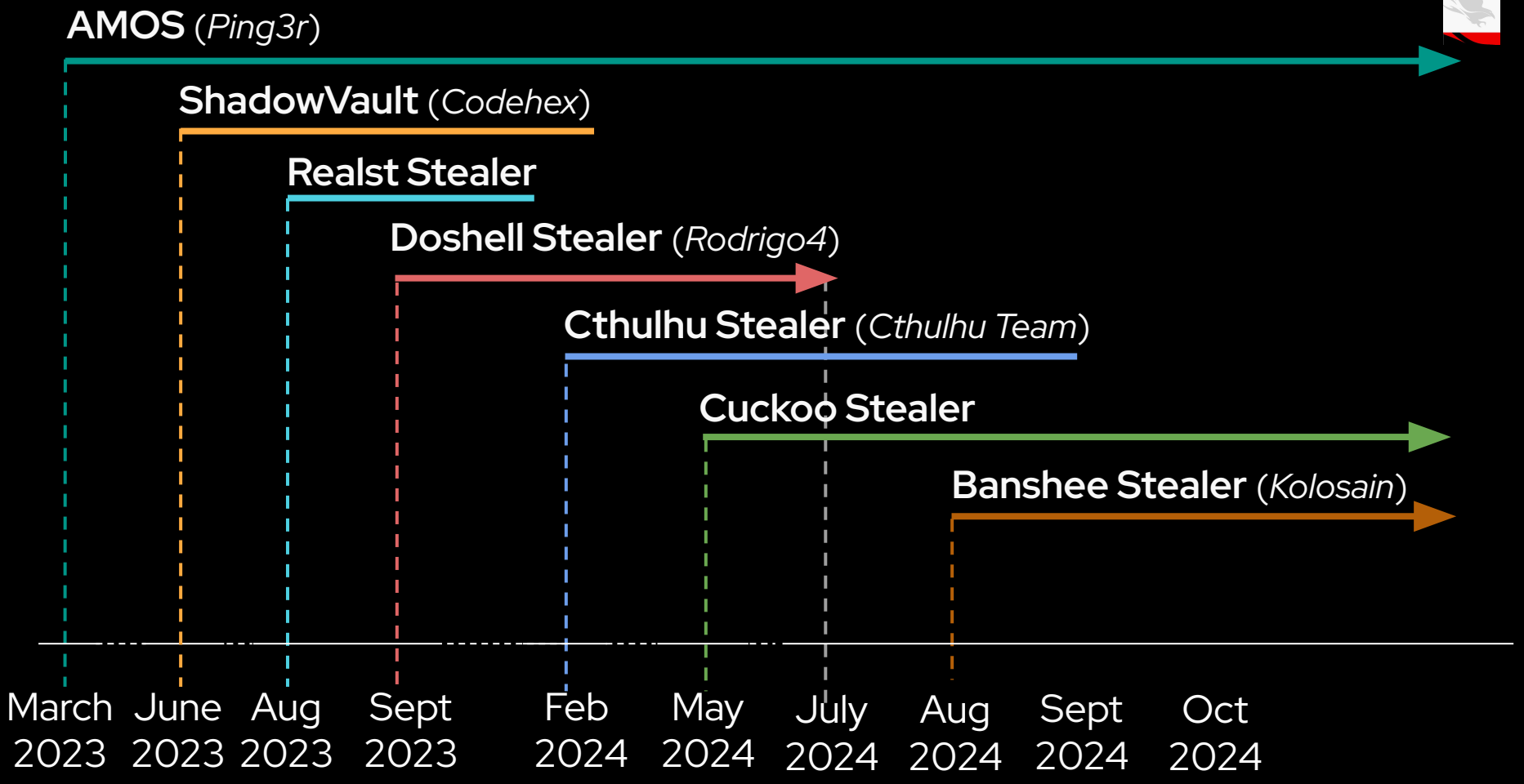



© CrowdStrike, Inc. All Rights Reserved




More insights:
https[:]//g0njxa.medium[.]com/the-journey-into-mac-os-infostealers-81873ef6d0b2

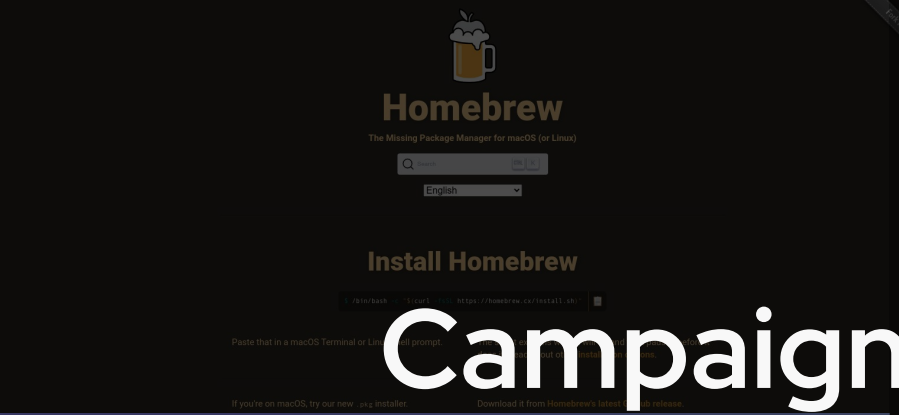
® CrowdStrike, Inc. All Rights Reserved

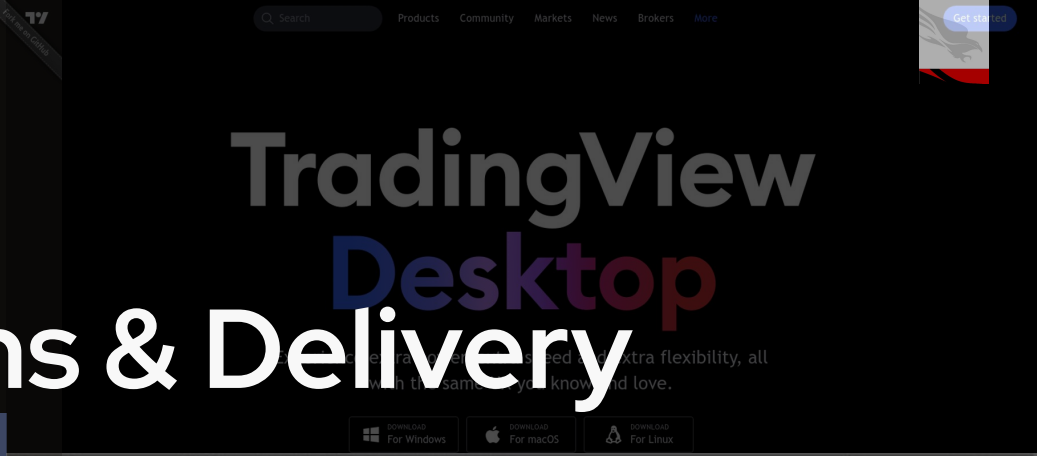


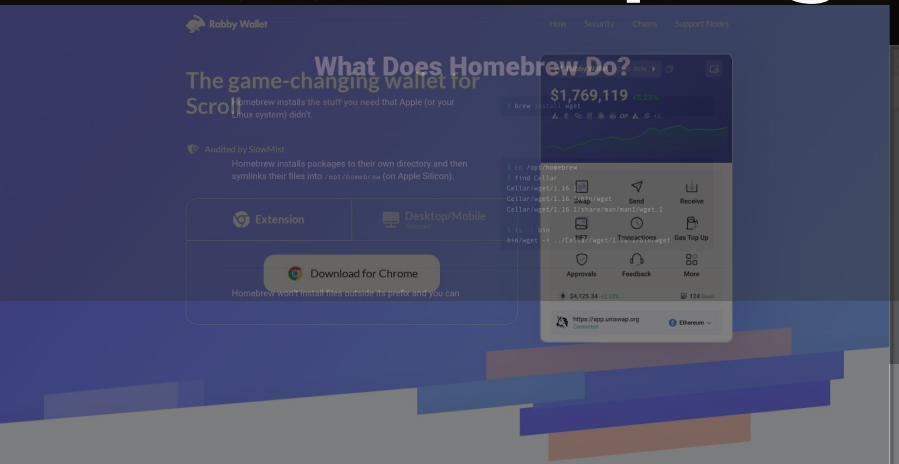

CROWDSTRIKE

® CrowdStrike, Inc. All Rights Reserved

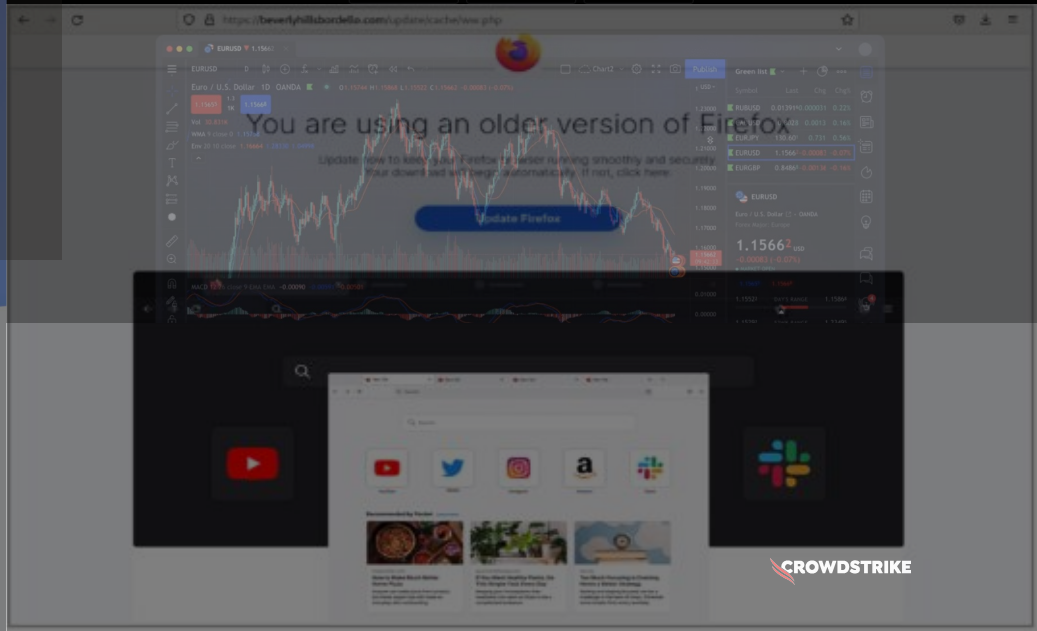
# Campaigns & Delivery

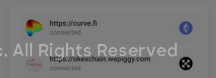



How is Rabby different from MetaMask

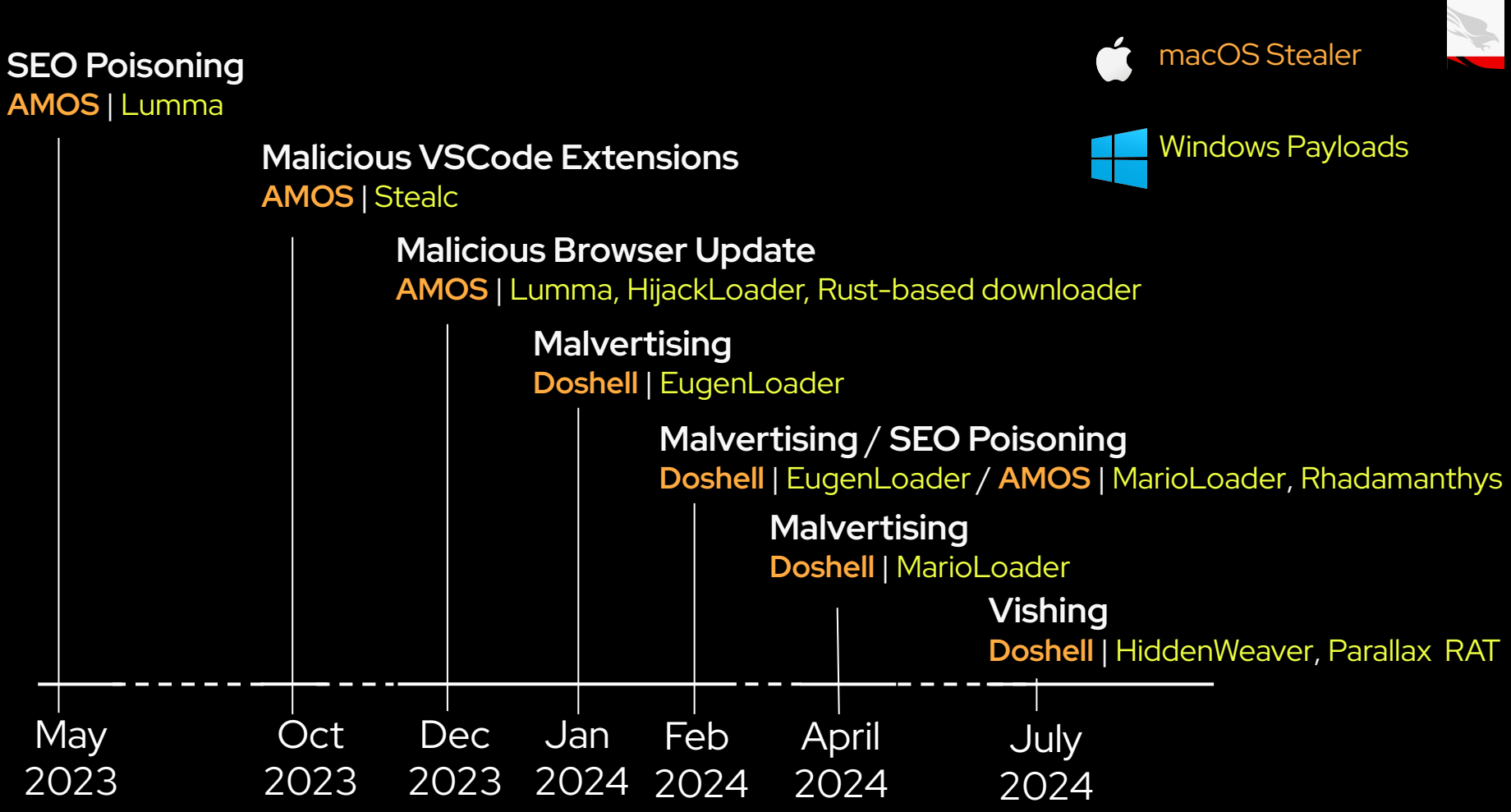


MULTI-CHAIN

Smooth multi-chain experience

® CrowdStrike, Inc. All Rights Reserved




© CrowdStrike, Inc. All Rights Reserved

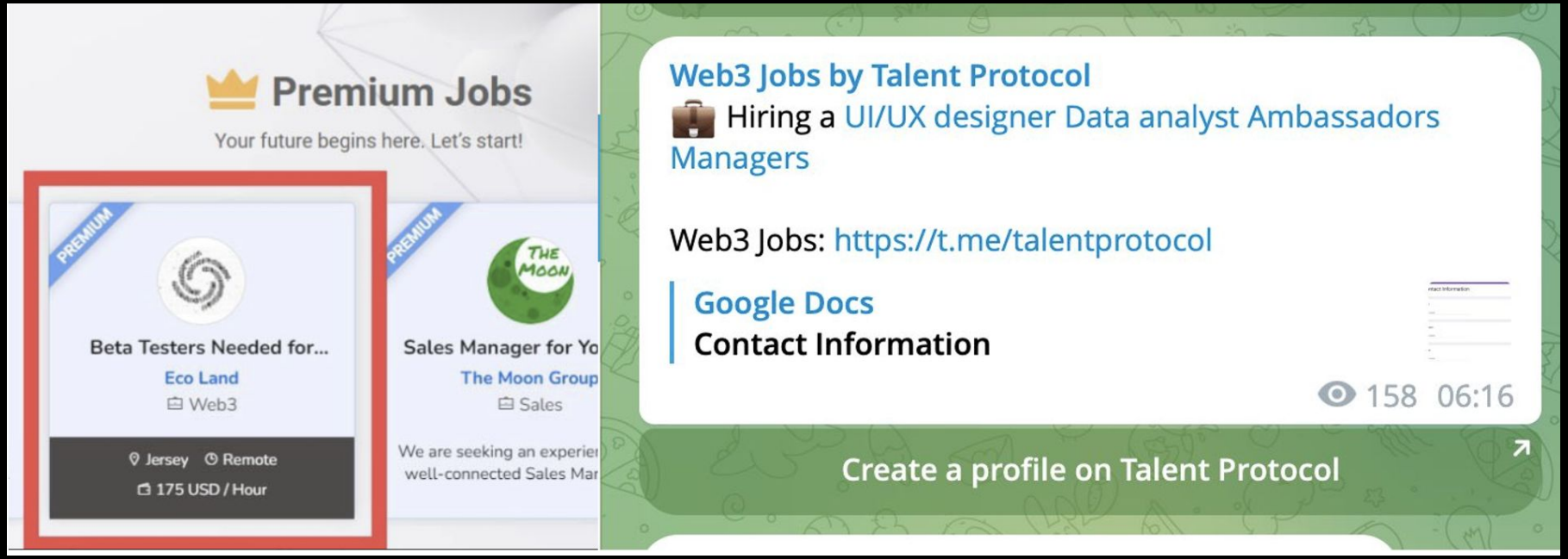
# Fake Play-to-Earn Games




Ref: https://x.com/eviliongamenews

© CrowdStrike, Inc. All Rights Reserved

# Fake Job Advertisements




Ref: https[:]//x[.]com/zachxbt/status/1689300596627587072

® CrowdStrike, Inc. All Rights Reserved







Ref: https[:]//x[.]com/bochenn/status/1687104829292941312

© CrowdStrike, Inc. All Rights Reserved

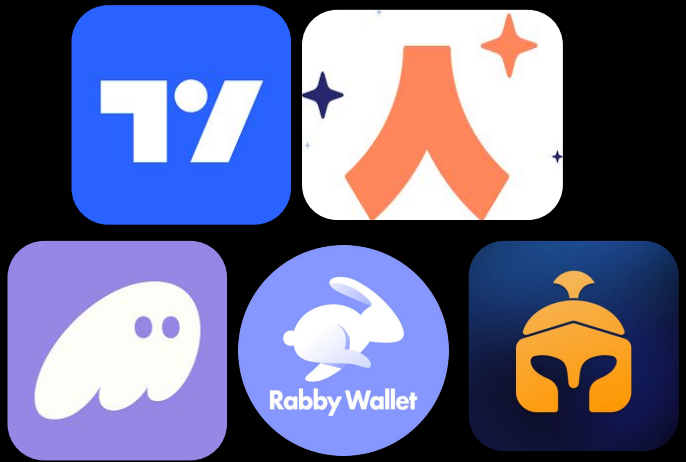
CROWDSTRIKE

# Malvertising and SEO Poisoning Campaign Lure Groupings

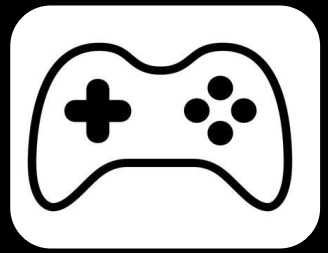
## Applications used by IT Professionals and Corporate Employees



## Cryptocurrency and Financial Applications




## Video Game Lures



® CrowdStrike, Inc. All Rights Reserved

# Malicious VSCode Extensions




® CrowdStrike, Inc. All Rights Reserved

# Vishing

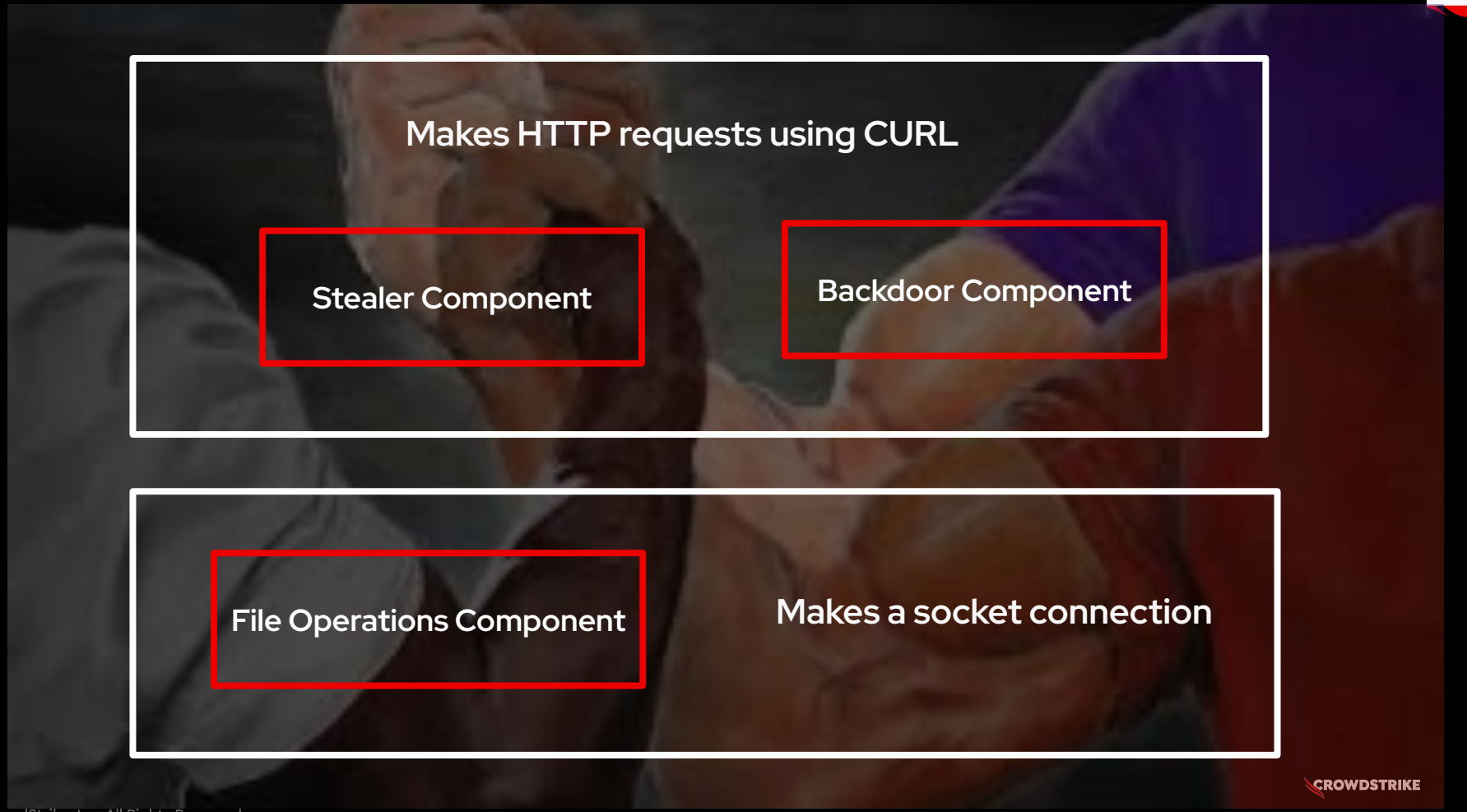
- TA impersonated legitimate staff
- Obtained a few sets of credentials for initial access
- Pentesting tool → configured victim's customer settings to malicious DNS resolvers → malicious website prompted users to download a tool to assist with internet connectivity issues → *Doshell Stealer* and *HiddenWeaver* and *Parallax RAT* downloaded

© CrowdStrike, Inc. All Rights Reserved

# Let’s compare popular and private stealers with a *Cuckoo Stealer* deep dive



® CrowdStrike, Inc. All Rights Reserved

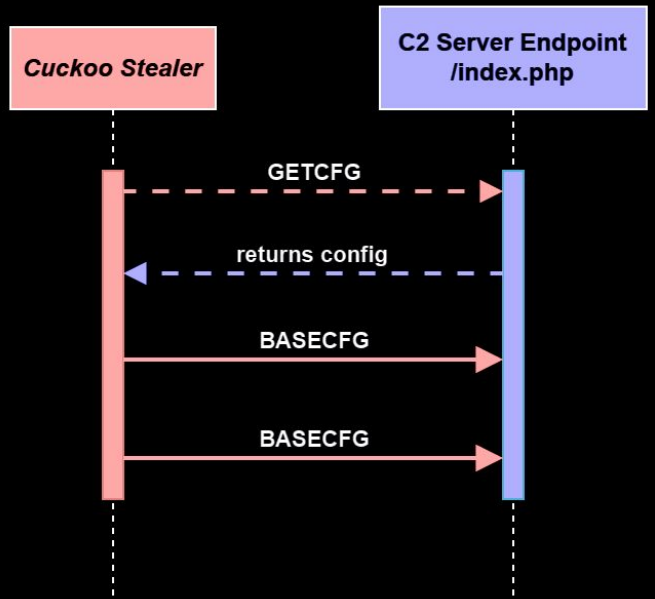



® CrowdStrike, Inc. All Rights Reserved

`GETCFG|<uuid>[1]|<campaign>`

Harvests browser extensions

Likely targets `Wallet` and time-based one-time password (`TOTP`) files




[1] Hardware UUID

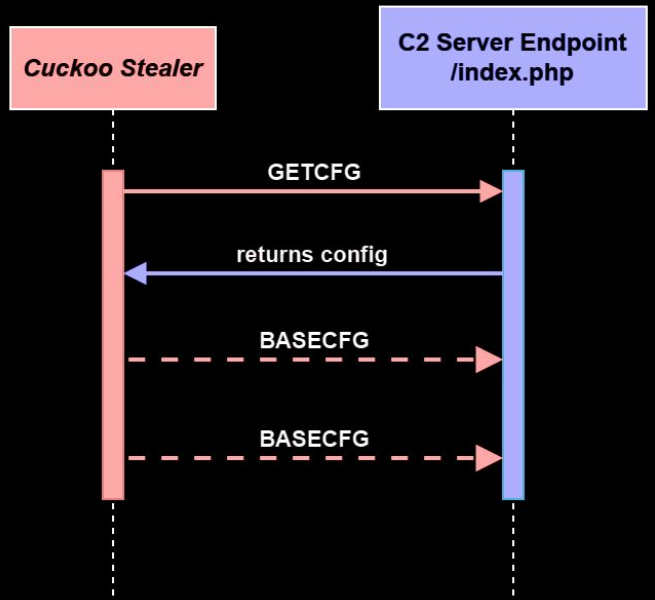
© CrowdStrike, Inc. All Rights Reserved

```
BASECFG|<uuid>|<campaign>|<data
>

tccutil reset
AppleEvents

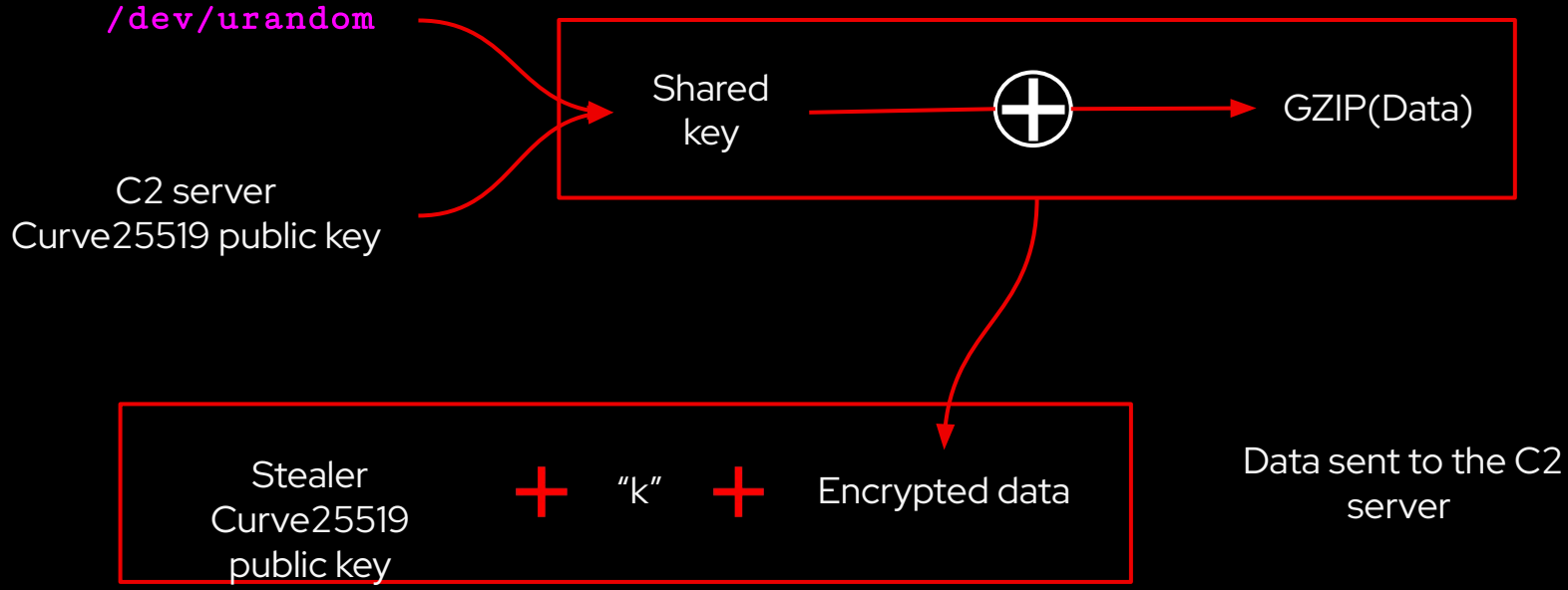
osascript -e 'set volume
output muted true'


osascript -e 'set volume
output muted false'
```




© CrowdStrike, Inc. All Rights Reserved

# Stealer Component: Encryption Scheme

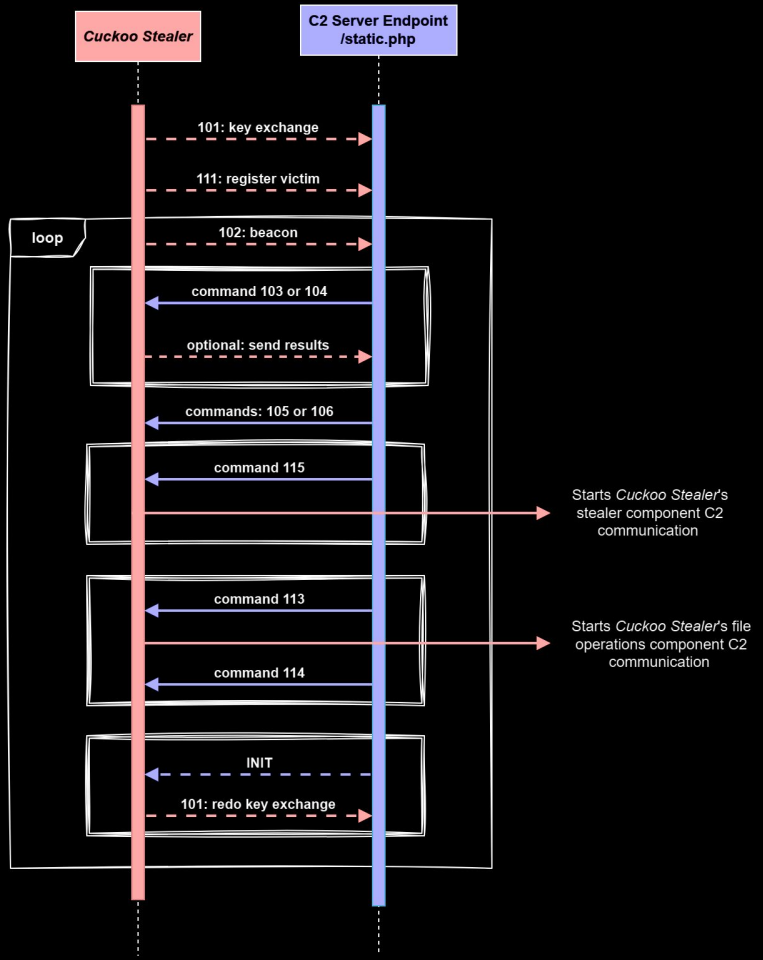



® CrowdStrike, Inc. All Rights Reserved

| Cuckoo Stealer | AMOS  | Doshell Stealer  | Banshee Stealer  |
|---|---|---|---|
| Stealer configuration | ✗ | ✗ | ✗ |
| TCC Bypass | ✗ | ✗ | ✓ |
| Asymmetric Encryption | ✗ | ✗ | ✗ |

CROWDSTRIKE

® CrowdStrike, Inc. All Rights Reserved

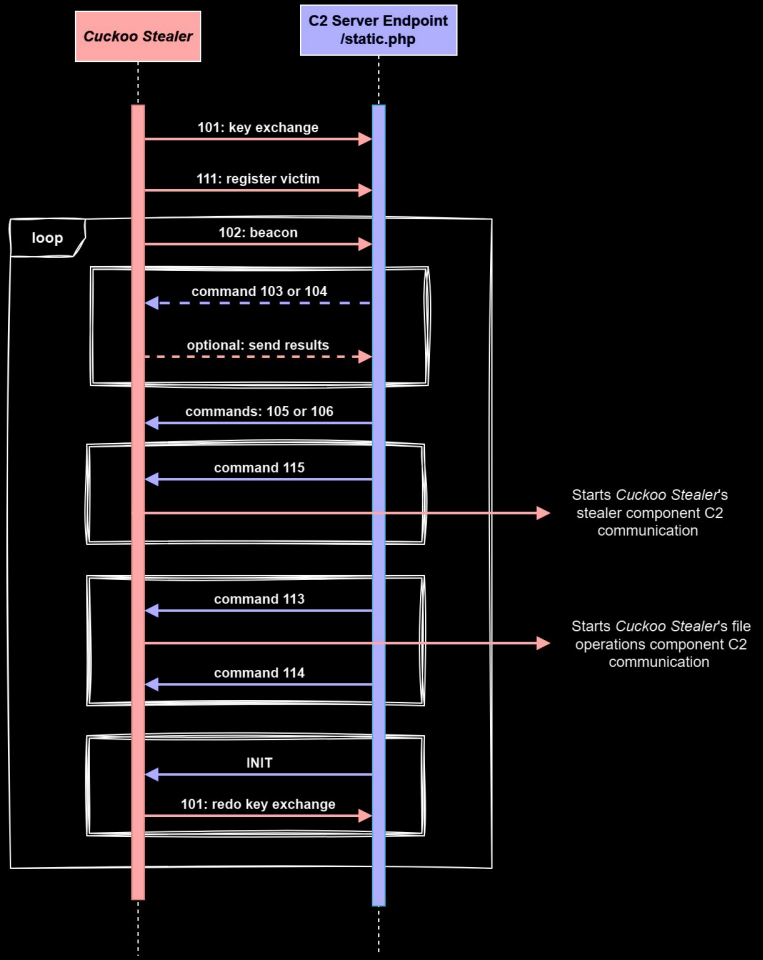



```
101|<uuid>|<campaign>|<key
>

111|<uuid>|<random-string>|<dat
a>

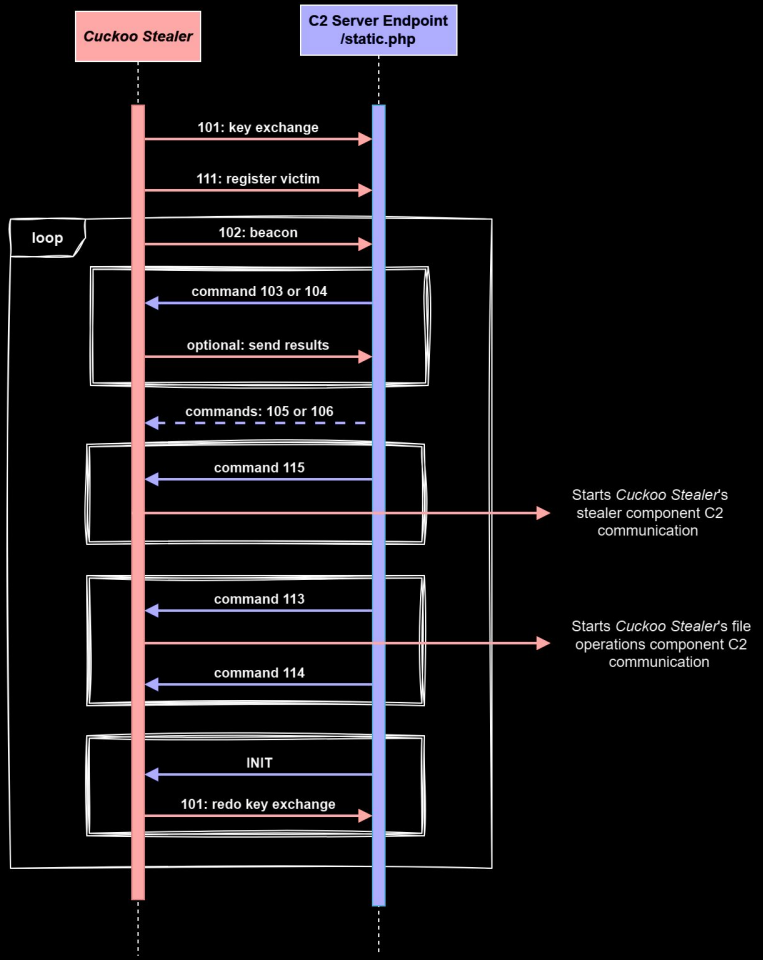
102|<uuid>
```

® CrowdStrike, Inc. All Rights Reserved




`103` or `104`: Execute shell commands

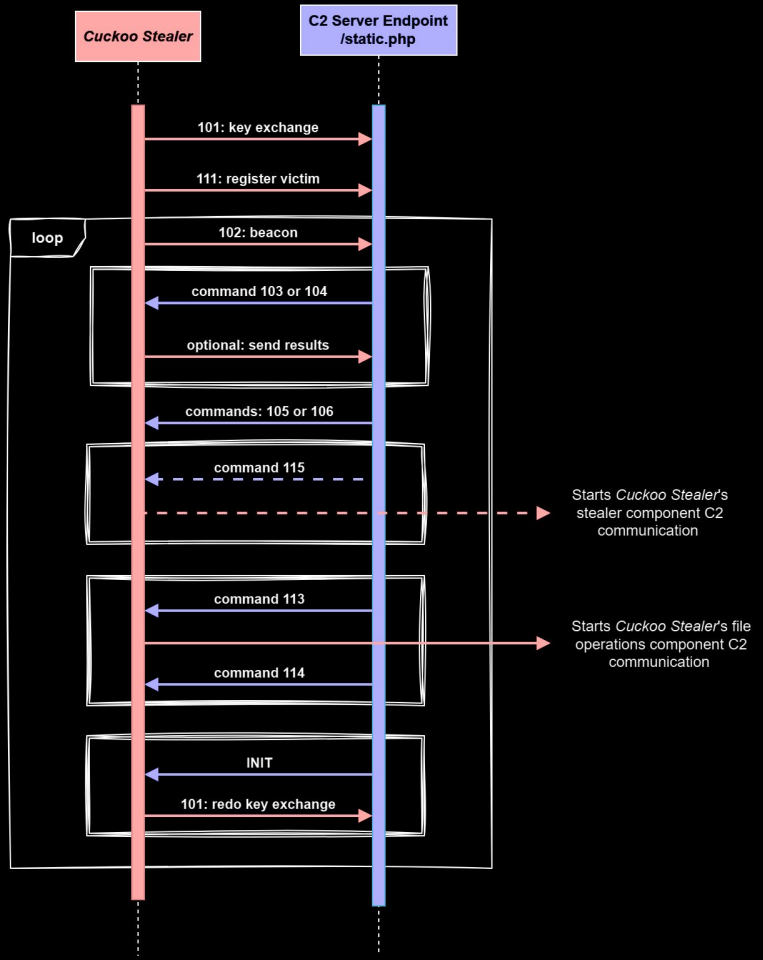
© CrowdStrike, Inc. All Rights Reserved




105: Reboot the machine

106: Uninstall itself

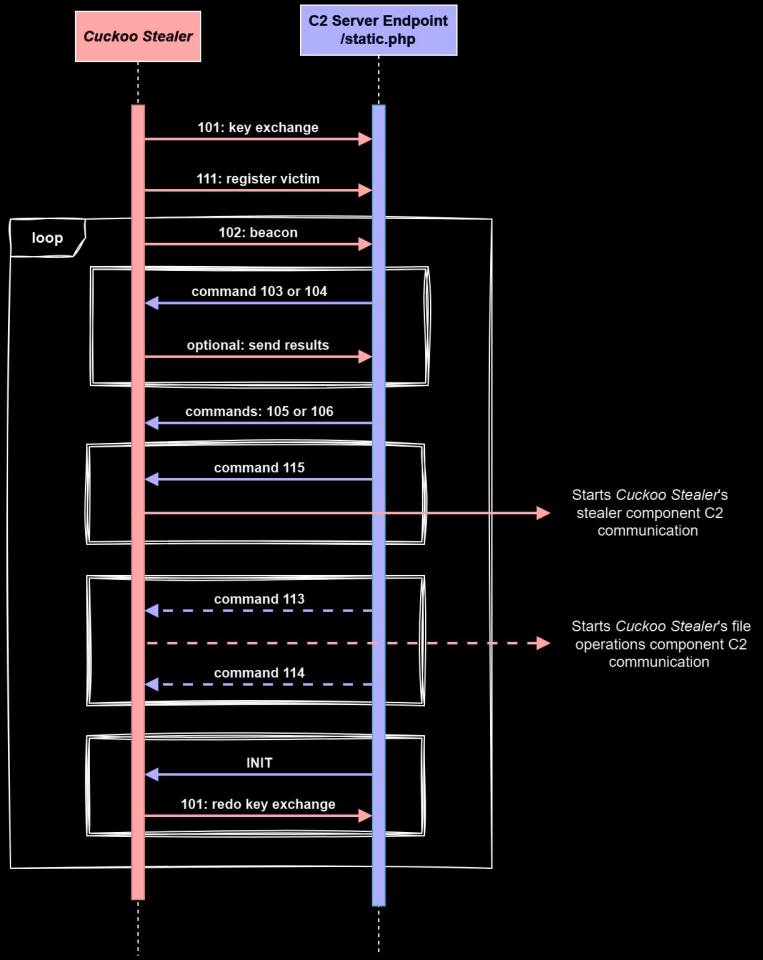
© CrowdStrike, Inc. All Rights Reserved




`115`:

- Restart stealer component
- Optionally exfiltrate to a new C2 server

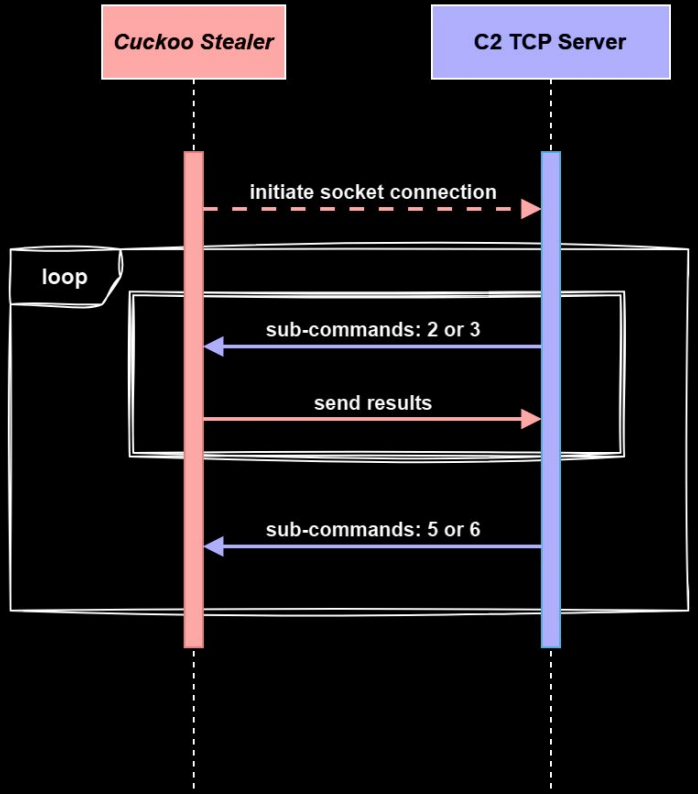
© CrowdStrike, Inc. All Rights Reserved




`113` : Create a TCP socket connection to a specified IP and port

`114` : Terminate the TCP socket connection

® CrowdStrike, Inc. All Rights Reserved

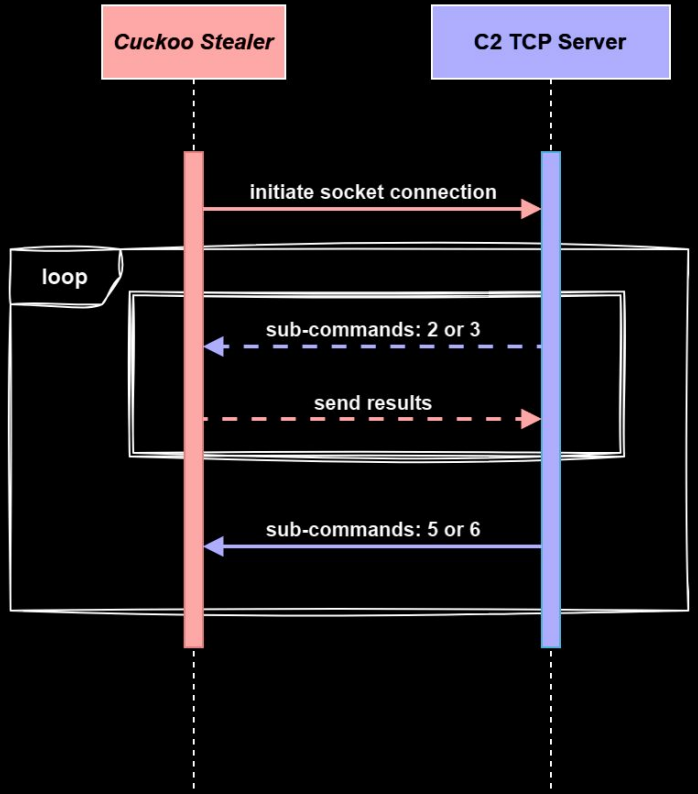



```
00000000  5d da 76 41 24 00 00 00 58 58 58 58 58 58 58 58  |]ZvA$...XXXXXXXX|
00000010  2d 58 58 58 58 2d 58 58 58 58 2d 58 58 58 58 2d  |-XXXX-XXXX-XXXX-|
00000020  58 58 58 58 58 58 58 58 58 58 58 58 0d 00 00 00  |XXXXXXXXXXXX....|
00000030  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  |AAAAAAAAAAAAAAAA|
00000040  31 7c 2f 55 73 65 72 73 2f 74 65 73 74           |1|/Users/test|
```

`0x4176da5d` : Magic DWORD

`AAAAAAAAAAAAAAAA` : Embedded string

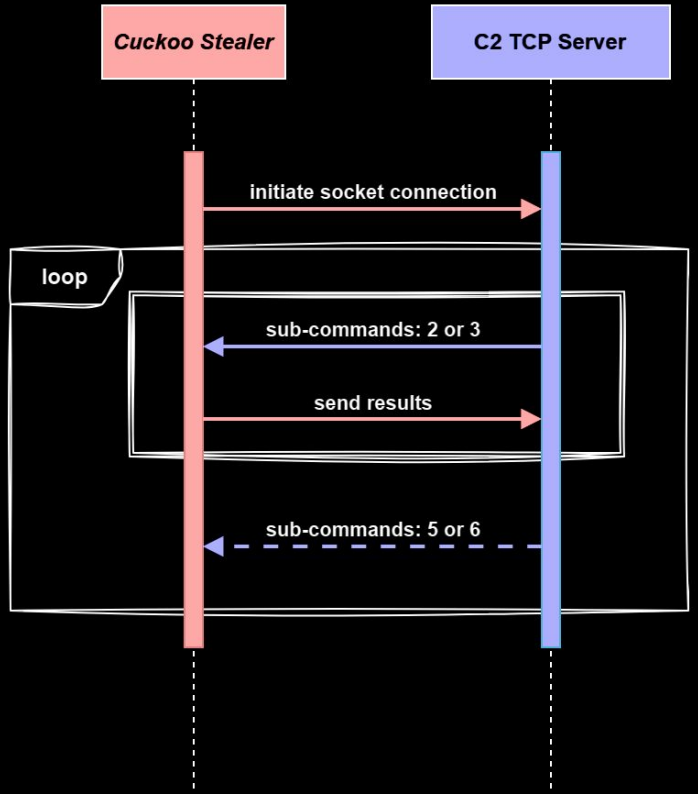
© CrowdStrike, Inc. All Rights Reserved




2: List files in directory

3: Upload files

© CrowdStrike, Inc. All Rights Reserved




5: Move file

6: Delete file

© CrowdStrike, Inc. All Rights Reserved

# Plot Twist...





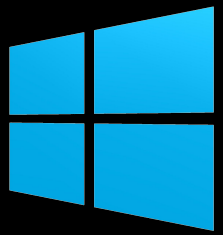
*Cuckoo Stealer*





*TMStealer*
*(a.k.a KoiStealer)*





® CrowdStrike, Inc. All Rights Reserved

CROWDSTRIKE

# Conclusion

- Revolving door **competitive** landscape
- **Malvertising** plays a big role
- MacOS stealer trend will likely **grow**

® CrowdStrike, Inc. All Rights Reserved



# Thank you.

## Questions?

® CrowdStrike, Inc. All Rights Reserved

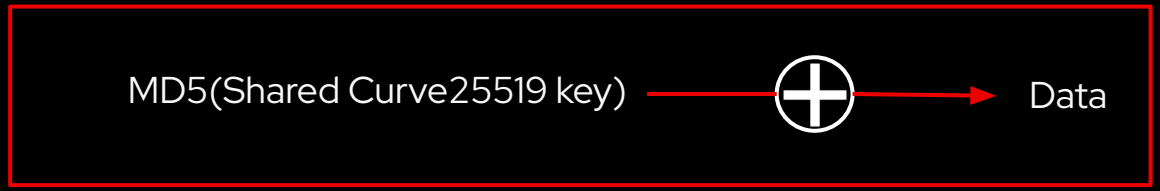
CROWDSTRIKE



# Bonus Slides

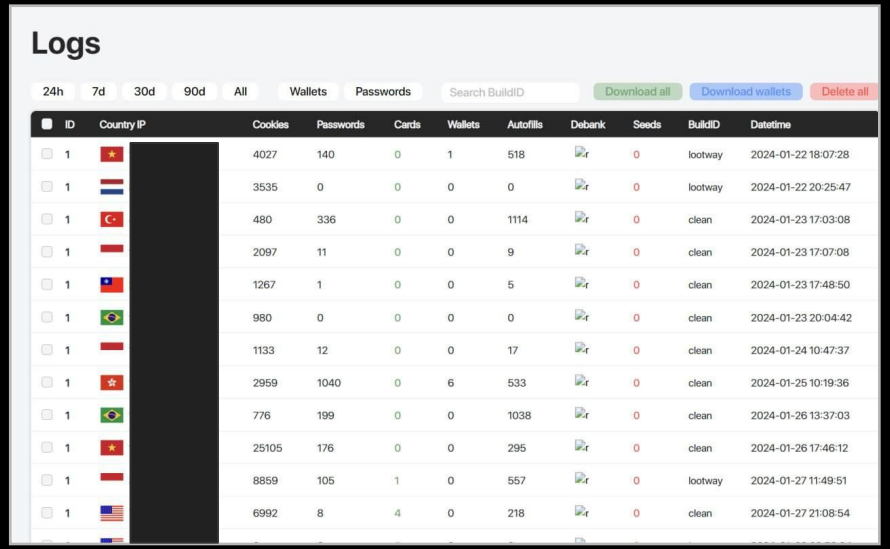
® CrowdStrike, Inc. All Rights Reserved

# Backdoor Component: Encryption Scheme

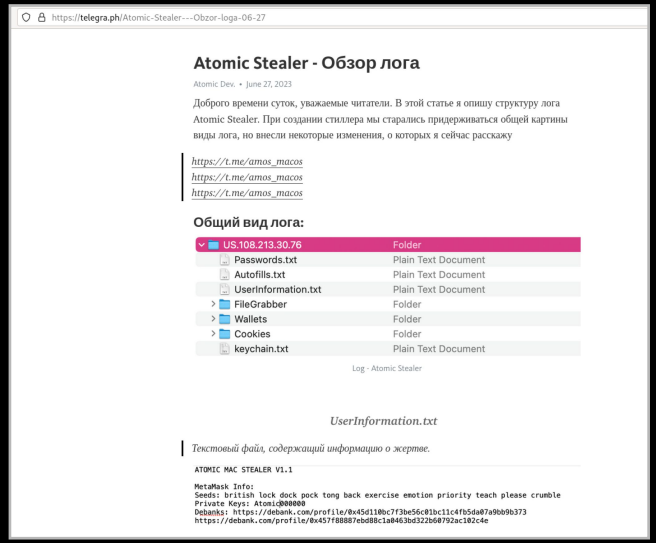



® CrowdStrike, Inc. All Rights Reserved

# AMOS




AMOS Panel




AMOS’s Blogpost

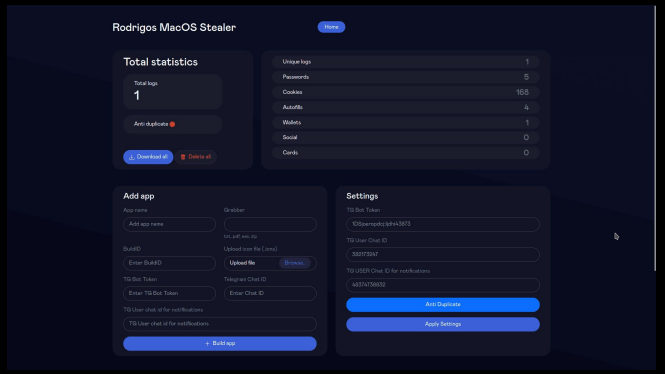
® CrowdStrike, Inc. All Rights Reserved

# Rodrigo4

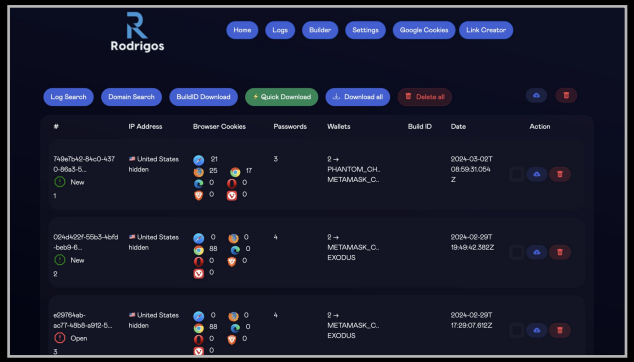
## 4 September 2023




## 7 November 2023




## 4 March 2024




## 21 June 2024




® CrowdStrike, Inc. All Rights Reserved