From the Depths: Analyzing the Cthulhu Stealer Malware for macOS

cadosecurity.com/blog/from-the-depths-analyzing-the-cthulhu-stealer-malware-for-macos

Tara Gould

Written by: Tara Gould

For years there has been a general belief in the Zeitgeist that macOS systems are immune to malware. While MacOS has a reputation for being secure, macOS malware has been trending up in recent years with the emergence of Silver Sparrow, KeRanger, and Atomic Stealer, among others. Recently, Cado Security has identified a malware-as-a-service (MaaS) targeting macOS users named “Cthulhu Stealer”. This blog will explore the functionality of this malware and provide insight into how its operators carry out their activities.

Technical Analysis

File details:

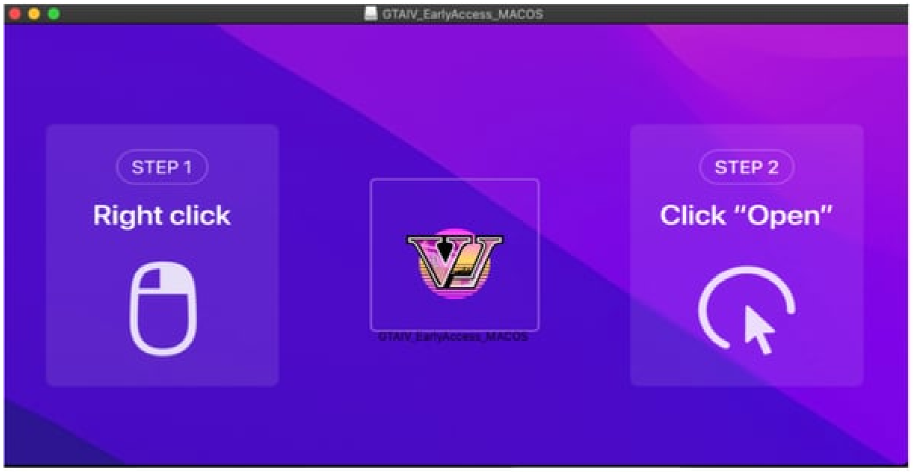
Language: Go

Not Signed

Stripped

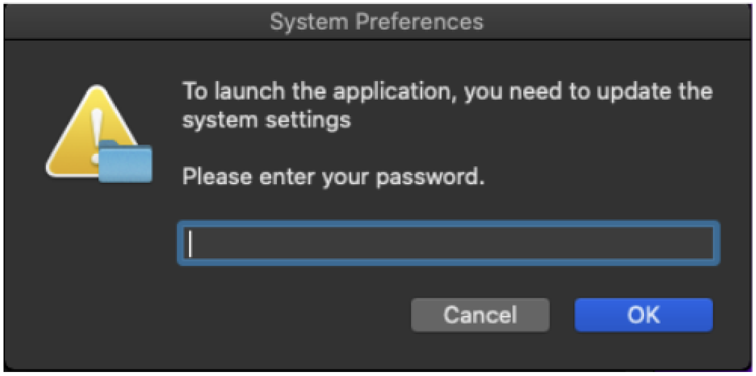
Multiarch: x86_64 and arm

Figure 1: Screenshot of disk image when mounted



Cthulhu Stealer is an Apple disk image (DMG) that is bundled with two binaries, depending on the architecture. The malware is written in GoLang and disguises itself as legitimate software. Once the user mounts the dmg, the user is prompted to open the software. After opening the file, osascript, the macOS command-line tool for running AppleScript and JavaScript is used to prompt the user for their password.

Figure 2: Password Prompt

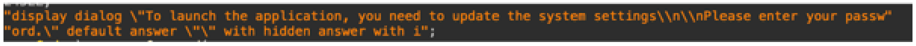


System Preferences

To launch the application, you need to update the system settings

Please enter your password.

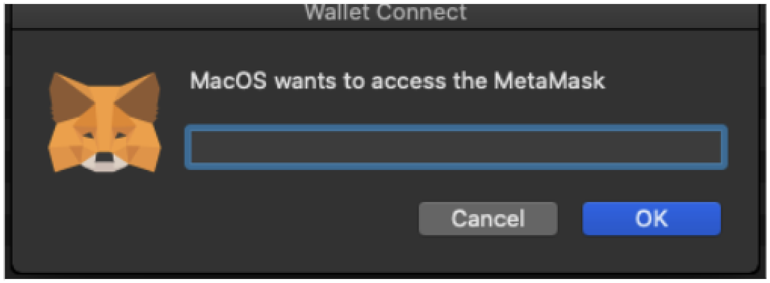
Figure 3: Osascript prompting user for password



```
"display dialog \"To launch the application, you need to update the system settings\\n\\nPlease enter your passw"
"ord.\" default answer \"\" with hidden answer with i";
```

Once the user enters their password, a second prompt requests the user’s MetaMask password. A directory is created in ‘/Users/Shared/NW’ with the credentials stored in textfiles. Chainbreak is used to dump Keychain passwords and stores the details in Keychain.txt.

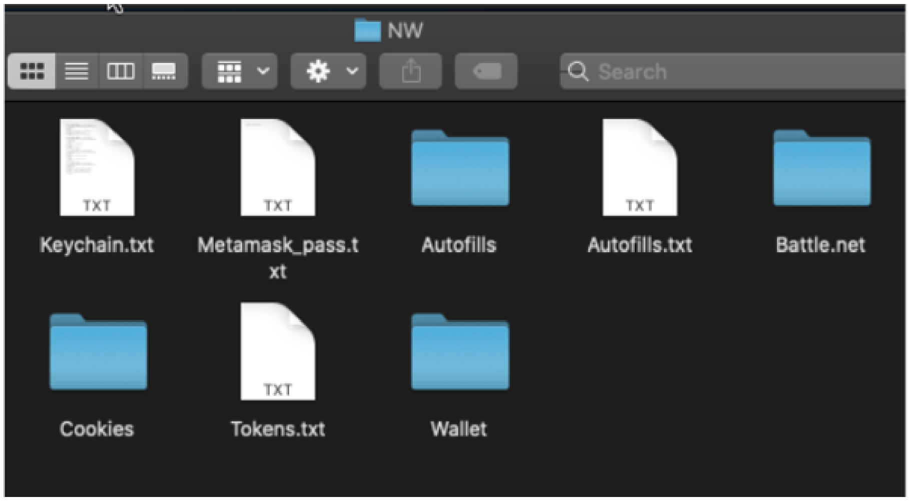
Figure 4: Password prompt for MetaMask



Wallet Connect

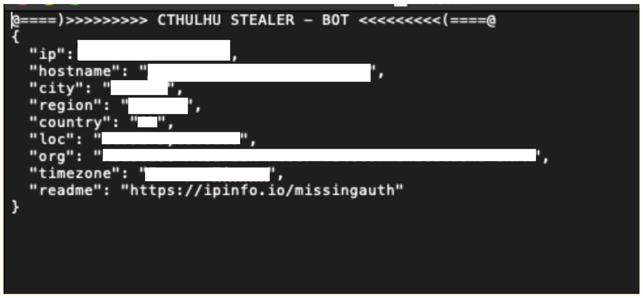
MacOS wants to access the MetaMask

Figure 5: Directory /Users/Shared/NW with created files



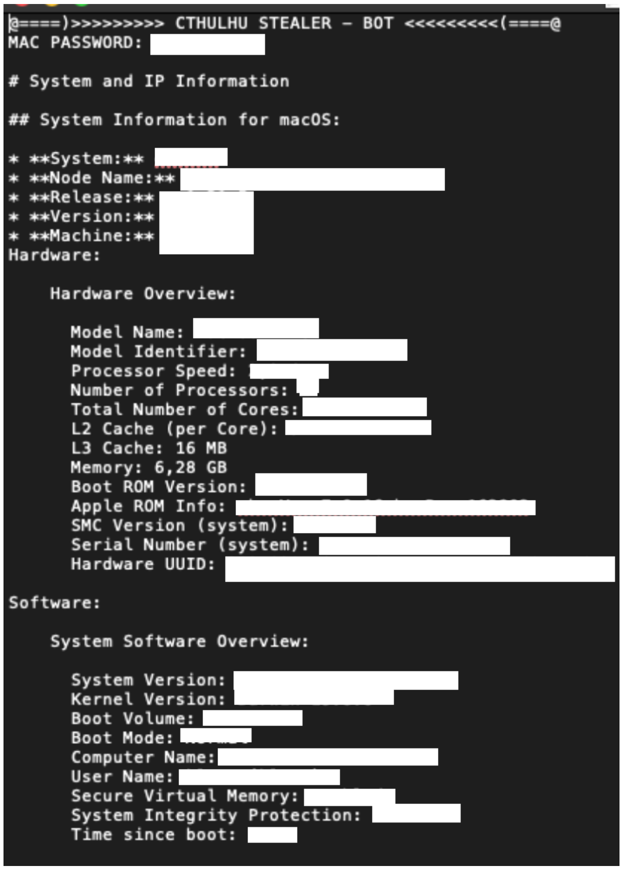
A zip archive containing the stolen data is created in: /Users/Shared/NW/[CountryCode]Cthulhu_Mac_OS_[date]_[time].zip. Additionally, a notification is sent to the C2, to alert to new logs. The malware fingerprints the victim's system, gathering information including IP, with IP details that are retrieved from ipinfo.io. System information including system name, OS version, hardware and software information are also gathered and stored in a text file, shown in Figure 7 and 8.

Figure 6: Parsed IP Details



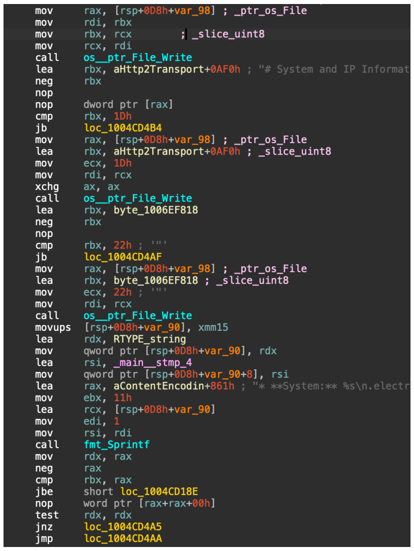
```
@====)>>>>>>>>> CTHULHU STEALER - BOT <<<<<<<<<(====@
{
  "ip": [redacted],
  "hostname": "[redacted]",
  "city": "[redacted]",
  "region": "[redacted]",
  "country": "[redacted]",
  "loc": "[redacted]",
  "org": "[redacted]",
  "timezone": "[redacted]",
  "readme": "https://ipinfo.io/missingauth"
}
```

Figure 7: Contents of 'Userinfo.txt'



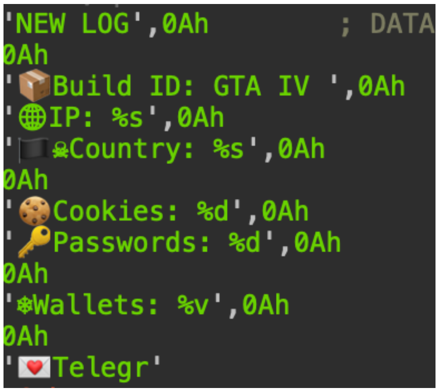
```
@====)>>>>>>>>> CTHULHU STEALER - BOT <<<<<<<<<(====@
MAC PASSWORD: [redacted]

# System and IP Information

## System Information for macOS:

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

Figure 8: Part of the function saving system information to text file



```
mov     rax, [rsp+0D8h+var_98] ; _ptr_os_File
mov     rdi, rbx
mov     rbx, rcx        ; _slice_uint8
mov     rcx, rdi
call    os__ptr_File_Write
lea     rbx, aHttp2Transport+0AF0h ; "# System and IP Informat
neg     rbx
nop
nop     dword ptr [rax]
cmp     rbx, 1Dh
jb      loc_1004CD4B4
mov     rax, [rsp+0D8h+var_98] ; _ptr_os_File
lea     rbx, aHttp2Transport+0AF0h ; _slice_uint8
mov     ecx, 1Dh
mov     rdi, rcx
xchg    ax, ax
call    os__ptr_File_Write
lea     rbx, byte_1006EF818
neg     rbx
nop
cmp     rbx, 22h ; '"'
jb      loc_1004CD4AF
mov     rax, [rsp+0D8h+var_98] ; _ptr_os_File
lea     rbx, byte_1006EF818 ; _slice_uint8
mov     ecx, 22h ; '"'
mov     rdi, rcx
call    os__ptr_File_Write
movups  [rsp+0D8h+var_90], xmm15
lea     rdx, RTYPE_string
mov     qword ptr [rsp+0D8h+var_90], rdx
lea     rsi, _main__stmp_4
mov     qword ptr [rsp+0D8h+var_90+8], rsi
lea     rax, aContentEncodin+861h ; "* **System:** %s\n.electr
mov     ebx, 11h
lea     rcx, [rsp+0D8h+var_90]
mov     edi, 1
mov     rsi, rdi
call    fmt_Sprintf
mov     rdx, rax
neg     rax
cmp     rbx, rax
jbe     short loc_1004CD18E
nop     word ptr [rax+rax+00h]
test    rdx, rdx
jnz     loc_1004CD4A5
jmp     loc_1004CD4AA
```

Figure 9: Alert of Log that is sent to operators



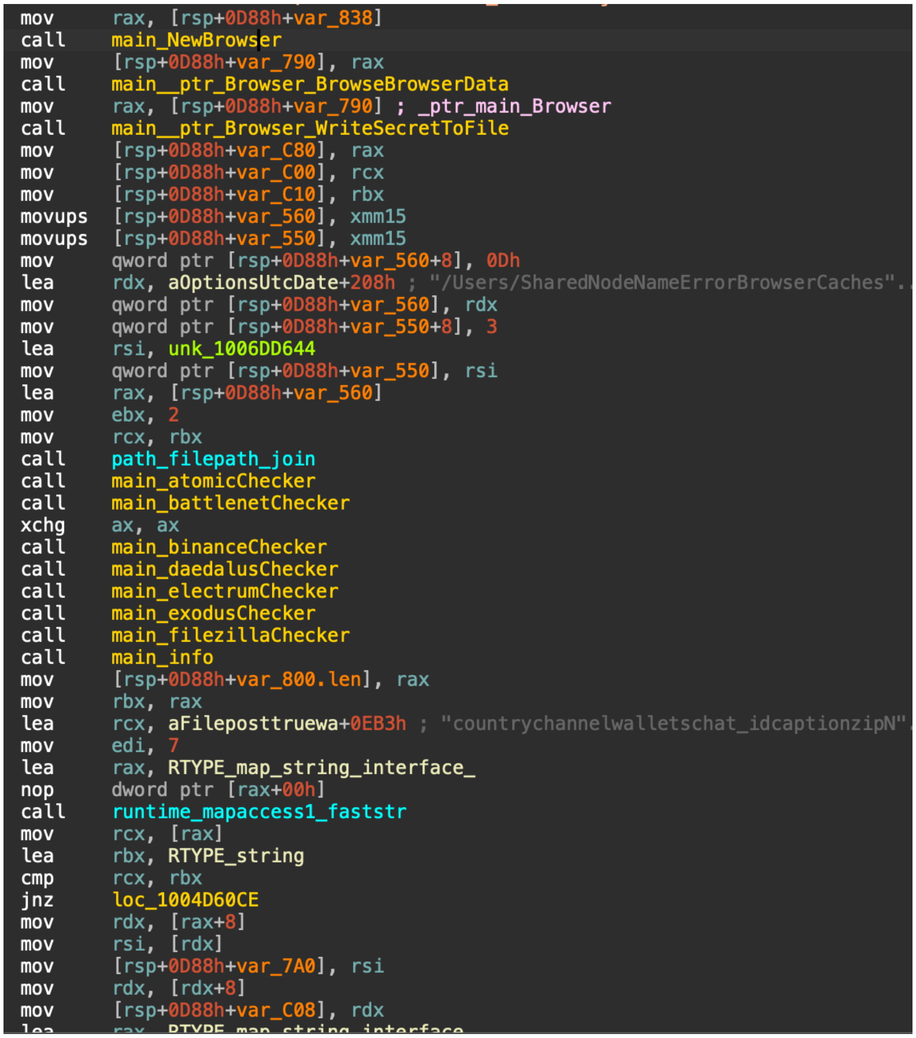
```
'NEW LOG',0Ah          ; DATA
0Ah
'📦Build ID: GTA IV ',0Ah
'🌐IP: %s',0Ah
'🏴☠Country: %s',0Ah
0Ah
'🍪Cookies: %d',0Ah
'🔑Passwords: %d',0Ah
0Ah
'❄Wallets: %v',0Ah
0Ah
'💌Telegr'
```

Cthulhu Stealer impersonates disk images of legitimate software that include:

- CleanMyMac
- Grand Theft Auto IV (appears to be a typo for VI)
- Adobe GenP

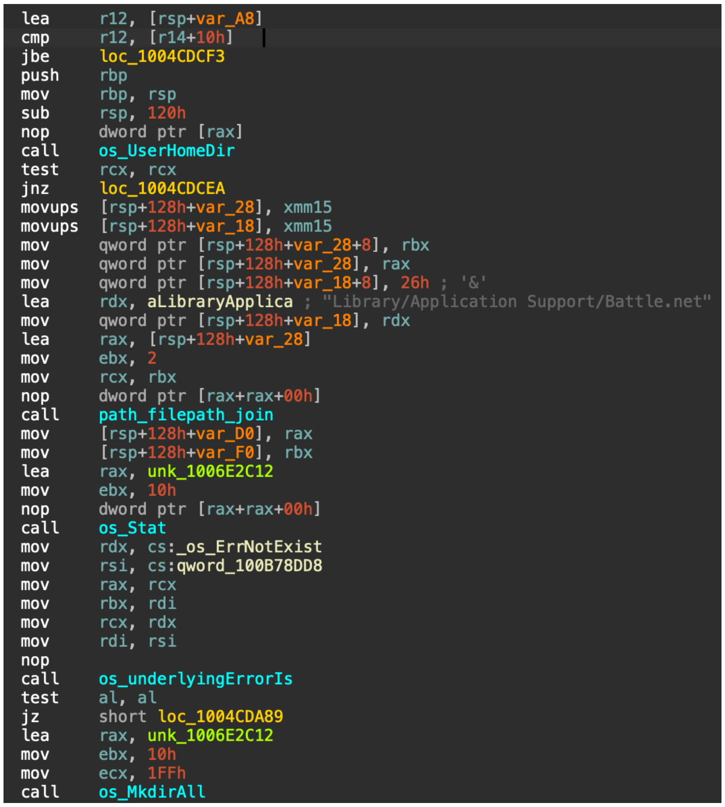
The main functionality of Cthulhu Stealer is to steal credentials and cryptocurrency wallets from various stores, including game accounts. Shown in Figure 10, there are multiple checker functions that check in the installation folders of targeted file stores, typically in “Library/Application Support/[file store]”. A directory is created in /Users/Shared/NW and the contents of the installation folder are dumped into text files for each store.

Figure 10: “Checker” functions being called in main function



```
mov     rax, [rsp+0D88h+var_838]
call    main_NewBrowser
mov     [rsp+0D88h+var_790], rax
call    main__ptr_Browser_BrowseBrowserData
mov     rax, [rsp+0D88h+var_790] ; _ptr_main_Browser
call    main__ptr_Browser_WriteSecretToFile
mov     [rsp+0D88h+var_C80], rax
mov     [rsp+0D88h+var_C00], rcx
mov     [rsp+0D88h+var_C10], rbx
movups  [rsp+0D88h+var_560], xmm15
movups  [rsp+0D88h+var_550], xmm15
mov     qword ptr [rsp+0D88h+var_560+8], 0Dh
lea     rdx, aOptionsUtcDate+208h ; "/Users/SharedNodeNameErrorBrowserCaches"..
mov     qword ptr [rsp+0D88h+var_560], rdx
mov     qword ptr [rsp+0D88h+var_550+8], 3
lea     rsi, unk_1006DD644
mov     qword ptr [rsp+0D88h+var_550], rsi
lea     rax, [rsp+0D88h+var_560]
mov     ebx, 2
mov     rcx, rbx
call    path_filepath_join
call    main_atomicChecker
call    main_battlenetChecker
xchg    ax, ax
call    main_binanceChecker
call    main_daedalusChecker
call    main_electrumChecker
call    main_exodusChecker
call    main_filezillaChecker
call    main_info
mov     [rsp+0D88h+var_800.len], rax
mov     rbx, rax
lea     rcx, aFileposttruewa+0EB3h ; "countrychannelwalletschat_idcaptionzipN".
mov     edi, 7
lea     rax, RTYPE_map_string_interface_
nop     dword ptr [rax+00h]
call    runtime_mapaccess1_faststr
mov     rcx, [rax]
lea     rbx, RTYPE_string
cmp     rcx, rbx
jnz     loc_1004D60CE
mov     rdx, [rax+8]
mov     rsi, [rdx]
mov     [rsp+0D88h+var_7A0], rsi
mov     rdx, [rdx+8]
mov     [rsp+0D88h+var_C08], rdx
lea     rax, RTYPE_map_string_interface
```

Figure 11: Function BattleNetChecker



```
lea     r12, [rsp+var_A8]
cmp     r12, [r14+10h]
jbe     loc_1004CDCF3
push    rbp
mov     rbp, rsp
sub     rsp, 120h
nop     dword ptr [rax]
call    os_UserHomeDir
test    rcx, rcx
jnz     loc_1004CDCEA
movups  [rsp+128h+var_28], xmm15
movups  [rsp+128h+var_18], xmm15
mov     qword ptr [rsp+128h+var_28+8], rbx
mov     qword ptr [rsp+128h+var_28], rax
mov     qword ptr [rsp+128h+var_18+8], 26h ; '&'
lea     rdx, aLibraryApplica ; "Library/Application Support/Battle.net"
mov     qword ptr [rsp+128h+var_18], rdx
lea     rax, [rsp+128h+var_28]
mov     ebx, 2
mov     rcx, rbx
nop     dword ptr [rax+rax+00h]
call    path_filepath_join
mov     [rsp+128h+var_D0], rax
mov     [rsp+128h+var_F0], rbx
lea     rax, unk_1006E2C12
mov     ebx, 10h
nop     dword ptr [rax+rax+00h]
call    os_Stat
mov     rdx, cs:_os_ErrNotExist
mov     rsi, cs:qword_100B78DD8
mov     rax, rcx
mov     rbx, rdi
mov     rcx, rdx
mov     rdi, rsi
nop
call    os_underlyingErrorIs
test    al, al
jz      short loc_1004CDA89
lea     rax, unk_1006E2C12
mov     ebx, 10h
mov     ecx, 1FFh
call    os_MkdirAll
```

A list of stores Cthulhu Stealer steals from is shown in Table 1.

Table 1: List of stolen data

Browser Cookies
Coinbase Wallet
Chrome Extension Wallets
Telegram Tdata account information
Minecraft user information
Wasabi Wallet
MetaMask Wallet
Keychain Passwords
SafeStorage Passwords
Battlenet game, cache and log data
Firefox Cookies
Daedalus Wallet

Electrum Wallet
Atomic Wallet
Binanace Wallet
Harmony Wallet
Electrum Wallet
Enjin Wallet
Hoo Wallet
Dapper Wallet
Coinomi Wallet
Trust Wallet
Blockchain Wallet
XDeFI Wallet

Comparison to Atomic Stealer

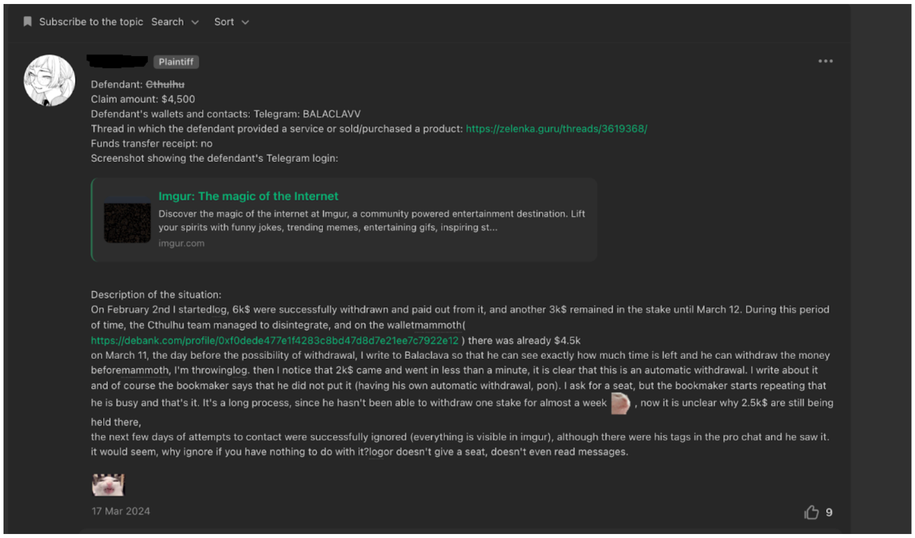
Atomic Stealer is an infostealer that targets macOS written in Go that was first identified in 2023. Atomic Stealer steals crypto wallets, browser credentials, and keychain. The stealer is sold on Telegram to affiliates for $1000 per month. The functionality and features of Cthulhu Stealer are very similar to Atomic Stealer, indicating the developer of Cthulhu Stealer probably took Atomic Stealer and modified the code. The use of osascript to prompt the user for their password is similar in Atomic Stealer and Cthulhu, even including the same spelling mistakes.

Forum and Operators

The developers and affiliates of Cthulhu Stealer operate as “Cthulhu Team” using Telegram for communications. The stealer appears to be being rented out to individuals for $500/month, with the main developer paying out a percentage of earnings to affiliates based on their deployment. Each affiliate of the stealer is responsible for the deployment of the malware. Cado has found Cthulhu stealer sold on two well-known malware marketplaces which are used for communication, arbitration and advertising of the stealer, along with Telegram. The user “Cthulhu” (also known as Balaclavv), first started advertising Cthulhu in at the end of 2023 and appeared to be operating for the first few months of 2024.

Various affiliates of the stealer started lodging complaints against Cthulhu in 2024 with regards to payments not being received. Users complained that Cthulhu had stolen money that was owed to them and accused him of being a scammer or participating in an exit scam. As a result, he received a permanent ban from the marketplace.

Figure 12: Screenshot of an arbitration an affiliate lodged against Cthulhu



[redacted] 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

Key Takeaways

In conclusion, while macOS has long been considered a secure system, the existence of malware targeting Mac users remains an increasing security concern. Although Cthulhu Team is seemingly no longer active, this serves as a reminder that Apple users are not immune to cyber threats. It’s crucial to remain vigilant and exercise caution, particularly when installing software from unofficial sources.

To protect yourself from potential threats, always download software from trusted sources, such as the Apple App Store or the official websites of reputable developers. Enable macOS’s built-in security features such as Gatekeeper, which helps prevent the installation of unverified apps. Keep your system and applications up to date with the latest security patches. Additionally, consider using reputable antivirus software to provide an extra layer of protection.

By staying informed and taking proactive steps, you can significantly reduce the risk of falling victim to Mac malware and ensure your system remains secure.

Indicators of Compromise

Filename	**sha256**
Launch.dmg	6483094f7784c424891644a85d5535688c8969666e16a194d397dc66779b0b12
GTAIV_EarlyAccess_MACOS_Release.dmg	e3f1e91de8af95cd56ec95737669c3512f90cecbc6696579ae2be349e30327a7
AdobeGenP.dmg	f79b7cbc653696af0dbd867c0a5d47698bcfc05f63b665ad48018d2610b7e97b
Setup2024.dmg	de33b7fb6f3d77101f81822c58540c87bd7323896913130268b9ce24f8c61e24
CleanMyMac.dmg	96f80fef3323e5bc0ce067cd7a93b9739174e29f786b09357125550a033b0288

Network Indicators
89[.]208.103.185
89[.]208.103.185:4000/autocheckbytes

89[.]208.103.185:4000/notification_archive

MITRE ATTACK

Technique Name	ID
User Execution	T1204
Command and Scripting Interpreter: Apple Script	T1059.002
Credentials From Password Stores	T1555
Credentials From Password Stores: Keychain	T1555.001
Credentials From Password Stores: Credentials From Web Browser	T1555.003
Account Discovery	T1087
System Information Discovery	T1082
Data Staged	T1074
Data From Local System	T1005
Exfiltration Over C2 Channel	T1041
Financial Theft	T1649

Detection

Yara

```
 rule MacoOS_CthulhuStealer {
  meta:
    Description = "Detects Cthulhu MacOS Stealer Binary"
    author = "Cado Security"
    date = "14/08/2024"
    md5 = "897384f9a792674b969388891653bb58"

  strings:
        $mach_o_x86_64 = {CF FA ED FE 07 00 00 01 00 00 00 00 00 00 00 00}
        $mach_o_arm64 = {CF FA ED FE 0C 00 00 01 00 00 00 00 00 00 00 00}
        $c2 = "http://89.208.103.185:4000"
        $path1 = "/Users/Shared/NW" fullword
        $path2 = "/Users/admin/Desktop/adwans/Builder/6987368329/generated_script.go" fullword
        $path3 = "ic.png" fullword
        $zip = "@====)>>>>>>>>> CTHULHU STEALER - BOT <<<<<<<<<(====@\n" fullword
        $func1 = "copyKeychainFile"
        $func2 = "grabberA1"
        $func3 = "grabberA2"
        $func4 = "decodeIPInfo"
        $func5 = "battlenetChecker"
        $func6 = "binanceChecker"
        $func7 = "daedalusChecker"
        $func8 = "CCopyFFolderContents"
        $func9 = "electrumChecker"

  condition:
      $mach_o_x86_64 or $mach_o_arm64
        and any of ($func*) or any of ($path*) or ($c2) or ($zip)
 }
```

Paths

/Users/Shared/NW

Tag(s): Research & Threat Intel