

Quick Update: Kraken Completes Its Rebrand to Anubis

zerofox.com/blog/quick-update-kraken-completes-its-rebrand-to-anubis/

February 22, 2022



BLOG

February 22, 2022 | by [Stephan Simon](#)



4 minute read

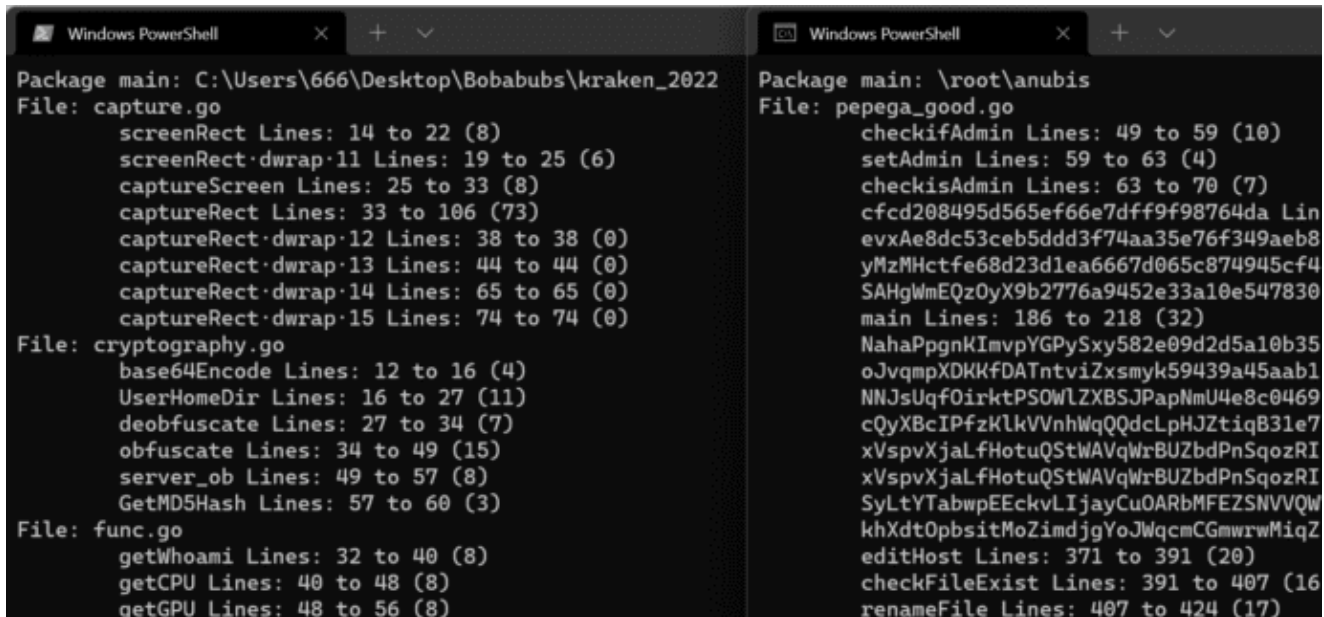
In a blog post dated February 16, 2022, ZeroFox Intelligence [detailed Kraken](#), a new botnet targeting Windows that we discovered in October 2021. The botnet is still undergoing active development, experimenting with new features, and attempting to find a brand for itself. After our publication, ZeroFox learned that the botnet has undergone a rebranding to more closely align with its administration dashboard. Sometime between January 4, 2022, and January 7, 2022, the operator(s) began using the names “Anubis” and “Pepega” for the project internally.

Recommendations

- Ensure antivirus and intrusion detection software is up to date with all patches and rule sets.
- Enable two-factor authentication for all organizational accounts to help mitigate phishing and credential stuffing attacks.
- Maintain regularly scheduled backup routines, including off-site storage and integrity checks.
- Avoid opening unsolicited attachments and never click suspicious links.
- Log and monitor all administrative actions as much as possible. Alert on any suspicious activity.
- Review network logs for potential signs of compromise and data egress.

Details

ZeroFox Intelligence has been following the development of this previously unknown botnet since October 2021. Originally named “Kraken,” builds discovered between January 4, 2022, and January 7, 2022, reveal that the internal name has changed.



```
Windows PowerShell
Package main: C:\Users\666\Desktop\Bobabubs\kraken_2022
File: capture.go
  screenRect Lines: 14 to 22 (8)
  screenRect·dwrap·11 Lines: 19 to 25 (6)
  captureScreen Lines: 25 to 33 (8)
  captureRect Lines: 33 to 106 (73)
  captureRect·dwrap·12 Lines: 38 to 38 (0)
  captureRect·dwrap·13 Lines: 44 to 44 (0)
  captureRect·dwrap·14 Lines: 65 to 65 (0)
  captureRect·dwrap·15 Lines: 74 to 74 (0)
File: cryptography.go
  base64Encode Lines: 12 to 16 (4)
  UserHomeDir Lines: 16 to 27 (11)
  deobfuscate Lines: 27 to 34 (7)
  obfuscate Lines: 34 to 49 (15)
  server_ob Lines: 49 to 57 (8)
  GetMD5Hash Lines: 57 to 60 (3)
File: func.go
  getWhoami Lines: 32 to 40 (8)
  getCPU Lines: 40 to 48 (8)
  getGPU Lines: 48 to 56 (8)

Windows PowerShell
Package main: \root\anubis
File: pepega_good.go
  checkifAdmin Lines: 49 to 59 (10)
  setAdmin Lines: 59 to 63 (4)
  checkisAdmin Lines: 63 to 70 (7)
  cfcd208495d565ef66e7dff9f98764da Lin
  evxAe8dc53ceb5ddd3f74aa35e76f349aeb8
  yMzMHctfe68d23d1ea6667d065c874945cf4
  SAHgWmEQz0yX9b2776a9452e33a10e547830
  main Lines: 186 to 218 (32)
  NahaPpgnKImvpYGPYsxy582e09d2d5a10b35
  oJvqmpXDKKfDATntviZxsmyk59439a45aab1
  NNJsUqfOirktpSOWLZXBSJPapNmU4e8c0469
  cQyXBcIPfzKlkVvnhWqQQdclpHJZtiqB31e7
  xVspvXjalFHotuQStWAVqWrBUZbdPnSqozRI
  xVspvXjalFHotuQStWAVqWrBUZbdPnSqozRI
  SyLTYTabwpEEckvLIjayCuOARbMFEZSNVVQW
  khXdtOpbsitMoZimdJgYoJwqcmCGmwrwMiqZ
  editHost Lines: 371 to 391 (20)
  checkFileExist Lines: 391 to 407 (16)
  renameFile Lines: 407 to 424 (17)
```

Figure 1. On the left, a build from January 4, 2022; on the right, a January 7, 2022, build.

Source: ZeroFox Intelligence

As seen in **Figure 1**, the Golang project path has changed from “C:\Users\666\Desktop\Bobabubs\kraken_2022” to “\root\anubis”, which more closely aligns with the dashboard after it received its own rebrand. The source code also appears to have been merged into one main file with most of the function names being obfuscated, as opposed to the previously separated but clear functionality. Another notable change made is to the main source file. The name “pepega” may be in reference to a Twitch emote of the same name, which is itself a variation of the meme “Pepe the Frog.”

Anubis Dashboard No Longer Available

Shortly after our publication, ZeroFox Intelligence also observed that the Anubis dashboard is no longer available. Attempting to view the dashboard now results in a “404 page not found” message being displayed.

New Exfiltration Targets

In addition to the previously-added cryptocurrency wallets, Anubis now appears to be targeting specific Chromium-based browsers. Builds obtained by ZeroFox Intelligence from February 17, 2022, onwards have added the following paths targeting the Brave, Google Chrome, and Microsoft Edge browsers:

- \AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cookies
- \AppData\Local\Google\Chrome\User Data\Default\Network\Cookies

- \AppData\Local\Microsoft\Edge\User Data\Default\Cookies

```

0065103b 488b4c2430 mov rcx, qword [rsp+0x30 {var_78}] {0x0}
00651040 488d3d2dc31a00 lea rdi, [rel data_7fd374] {"\AppData\Local\BraveSoftware\Bra..."}
00651047 be44000000 mov esi, 0x44
0065104c 31c0 xor eax, eax {0x0}
0065104e 488b5c2478 mov rbx, qword [rsp+0x78 {var_50}]
00651053 e8a8dadfff call runtime.concatstring2
00651058 4889842490000000 mov qword [rsp+0x90 {var_38}], rax
00651060 48899c2498000000 mov qword [rsp+0x98 {var_38+0x8}], rbx
00651068 31c0 xor eax, eax {0x0}
0065106a 488b5c2470 mov rbx, qword [rsp+0x70 {var_58}]
0065106f 488b4c2448 mov rcx, qword [rsp+0x48 {var_80}] {0xb}
00651074 488d3d73ba1a00 lea rdi, [rel data_7fcaee] {"\AppData\Local\Google\Chrome\Use..."}
0065107b be3e000000 mov esi, 0x3e
00651080 e87bdadfff call runtime.concatstring2
00651085 48898424a0000000 mov qword [rsp+0xa0 {var_28}], rax
0065108d 48899c24a8000000 mov qword [rsp+0xa8 {var_28+0x8}], rbx
00651095 31c0 xor eax, eax {0x0}
00651097 488b5c2468 mov rbx, qword [rsp+0x68 {var_60}]
0065109c 488b4c2440 mov rcx, qword [rsp+0x40 {var_88}] {0xb}
006510a1 488d3de9a81a00 lea rdi, [rel data_7fb991] {"\AppData\Local\Microsoft\Edge\Us..."}
006510a8 be37000000 mov esi, 0x37
006510ad e84edadfff call runtime.concatstring2
006510b2 48898424b0000000 mov qword [rsp+0xb0 {var_18}], rax
006510ba 48899c24b8000000 mov qword [rsp+0xb8 {var_18+0x8}], rbx
006510c2 31c0 xor eax, eax {0x0}
006510c4 488d1d35601b00 lea rbx, [rel data_807100]
006510cb e8d012dfff call runtime.newproc

```

Figure 2. Multiple Chromium-based web browser paths appearing in the latest Anubis build
Source: ZeroFox Intelligence

Until recently, Anubis relied entirely on secondary payloads such as Redline to steal data from victims. If this trend of feature additions continues, Anubis may become capable of doing the job itself, ending its reliance on third-party infostealers.

Conclusion

The additional capability to target a victim’s browser data seems limited to just cookie data currently. Whether Anubis decides to collect more data (such as saved credentials and browser history) or even target more browsers based on the Chromium source currently remains to be seen. Though the pace of Anubis’ development has slowed down since its initial discovery, the various changes its operator(s) are making indicate they are still deciding what the future of this botnet holds. ZeroFox will continue to monitor this emerging botnet as it evolves.

MITRE ATT&CK

ID	Description
T1027.002	Obfuscated Files or Information: Software Packing
T1033	System Owner/User Discovery
T1047	Windows Management Instrumentation

<u>T1059.001</u>	Command and Scripting Interpreter: PowerShell
<u>T1059.003</u>	Command and Scripting Interpreter: Windows Command Shell
<u>T1082</u>	System Information Discovery
<u>T1113</u>	Screen Capture
<u>T1132.001</u>	Data Encoding: Standard Encoding
<u>T1547.001</u>	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
<u>T1571</u>	Non-Standard Port

IOCs

SHA256 Hashes

5d99125b0d97ba0abfcf9916c1a05081c1cc117eb2afaaab39a6f95a60e42ab3

Tags: Botnet, Cybersecurity, Threat Intelligence