Babuk is distributed packed

By Sebdraven

Published: 2021-02-08 · Archived: 2026-04-29 07:25:38 UTC

4 min read

Feb 8, 2021

a new babuk ransomware was uploaded on Virustotal.
bc4066c3b8d2bb4af593ced9905d1c9c78fff5b10ab8dbed7f45da913fb2d748

This version is packed with the same technics of GandGrab described here.

[Threat Profile: GandCrab Ransomware (morphisec.com)]

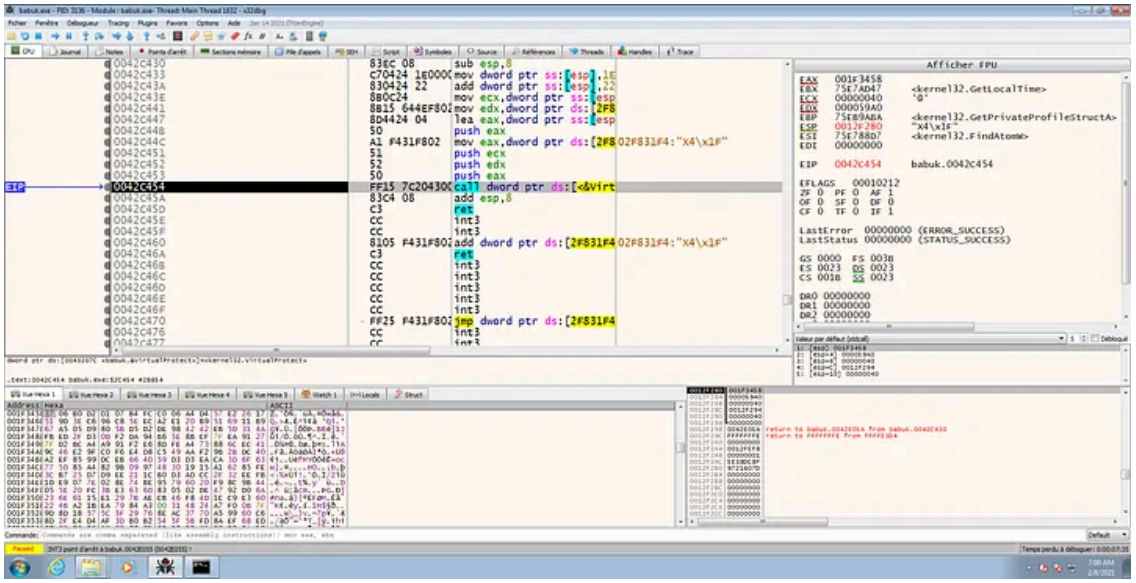
Packer

The first stage is a first shellcode loaded with GloballAlloc and VirtualProtect in function 0042df00

Press enter or click to view image in full size

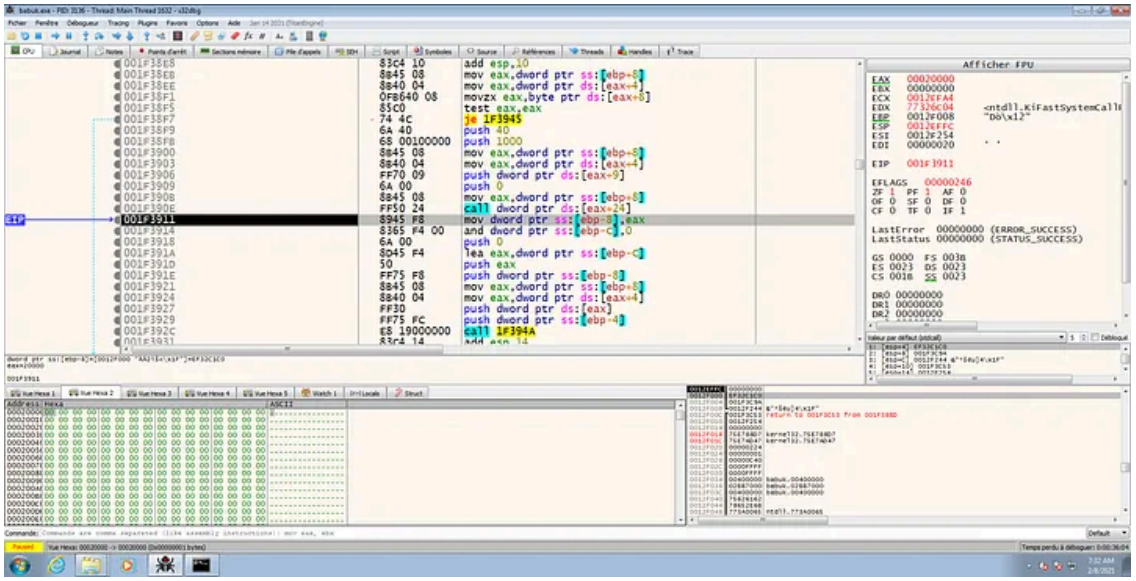
```
} while (((int)uVar2 >> 0x1f < 0x14) || (((int)uVar2 >> 0x1f < 0x15 && (uVar2 < 0xc7cfc130))));
DAT_02f831f4 = GlobalAlloc(0,DAT_02f84e64);
```

Press enter or click to view image in full size

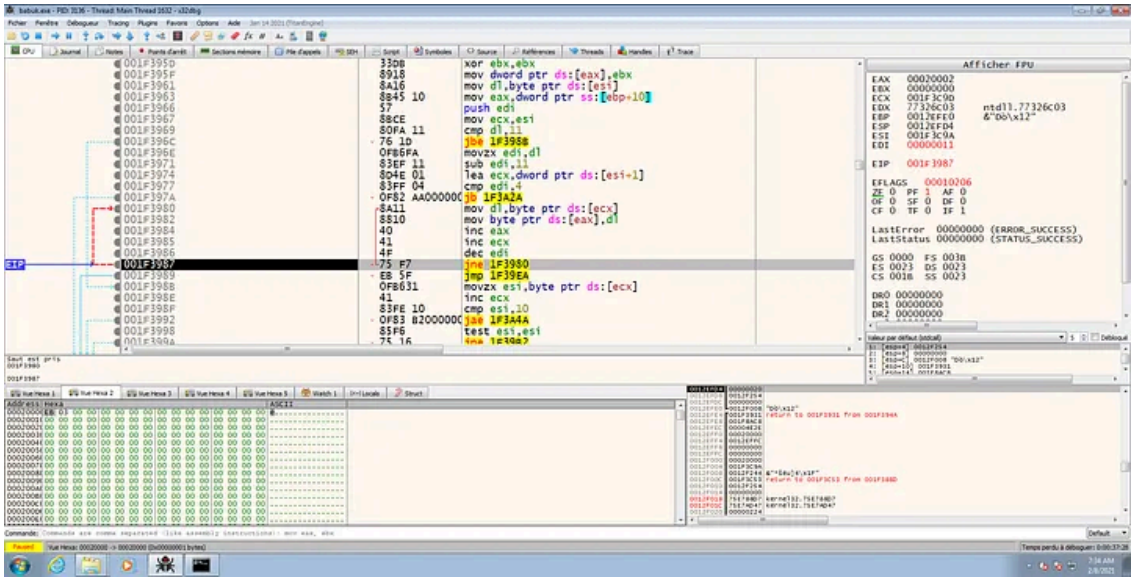


This shellcode create a second shellcode after a VirtualAlloc and VirtualProtect to change rights of the memory page

Press enter or click to view image in full size

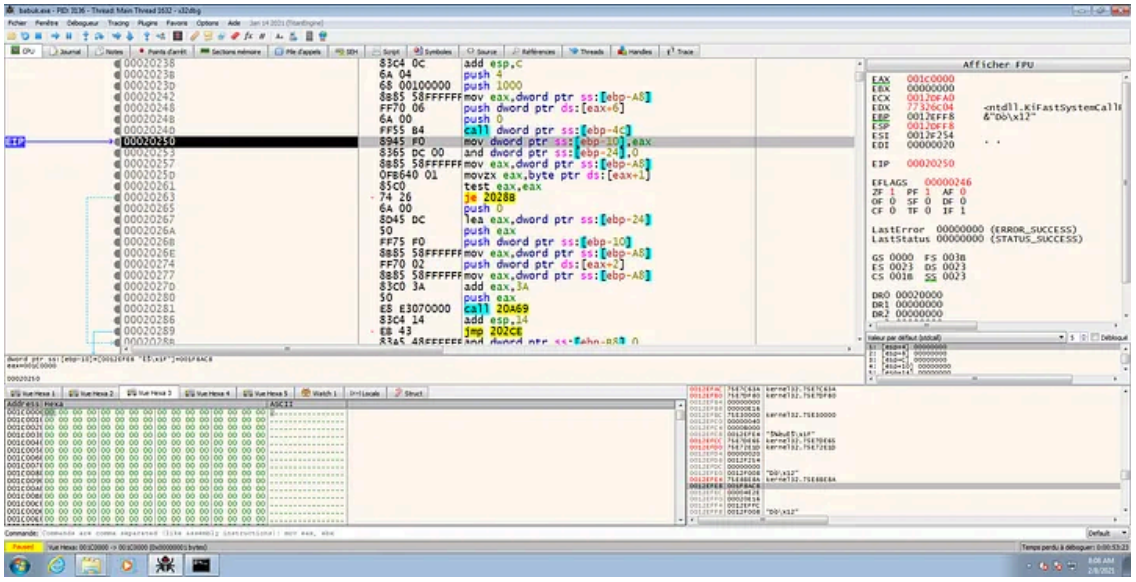


Press enter or click to view image in full size



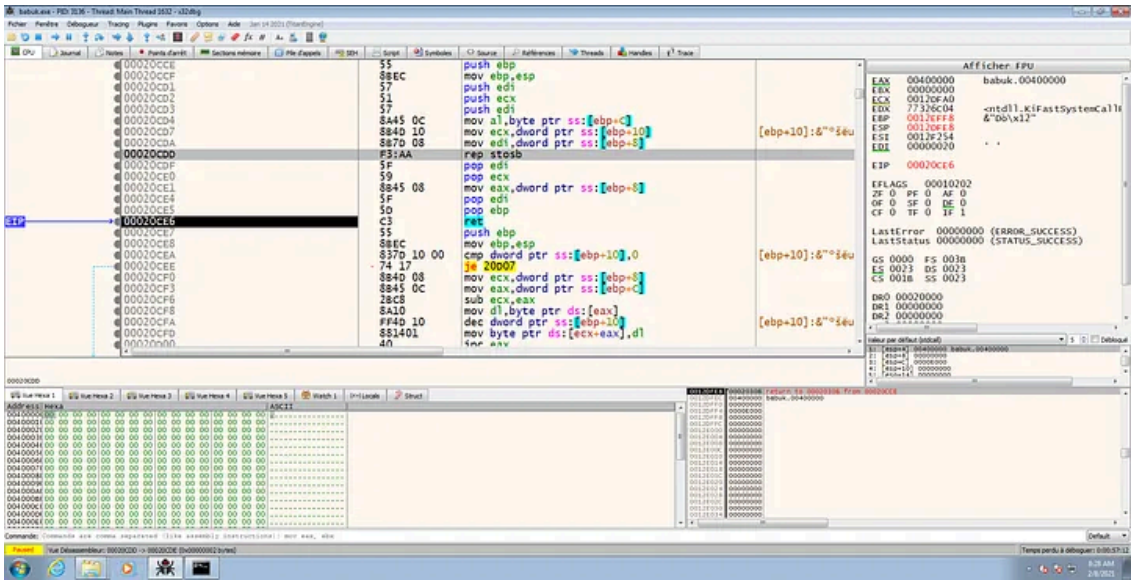
The second shellcode decodes babuk malware in memory to execute it with a VirtualAlloc in a first page memory.

Press enter or click to view image in full size

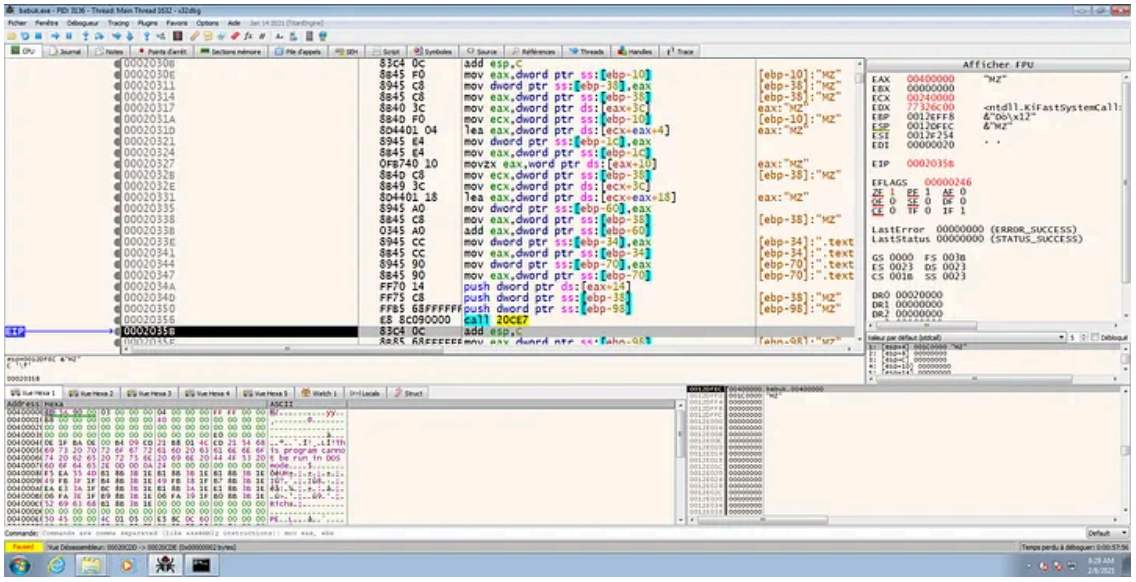


And the shellcode deletes the malware packed and copy the babuk at the same place

Press enter or click to view image in full size

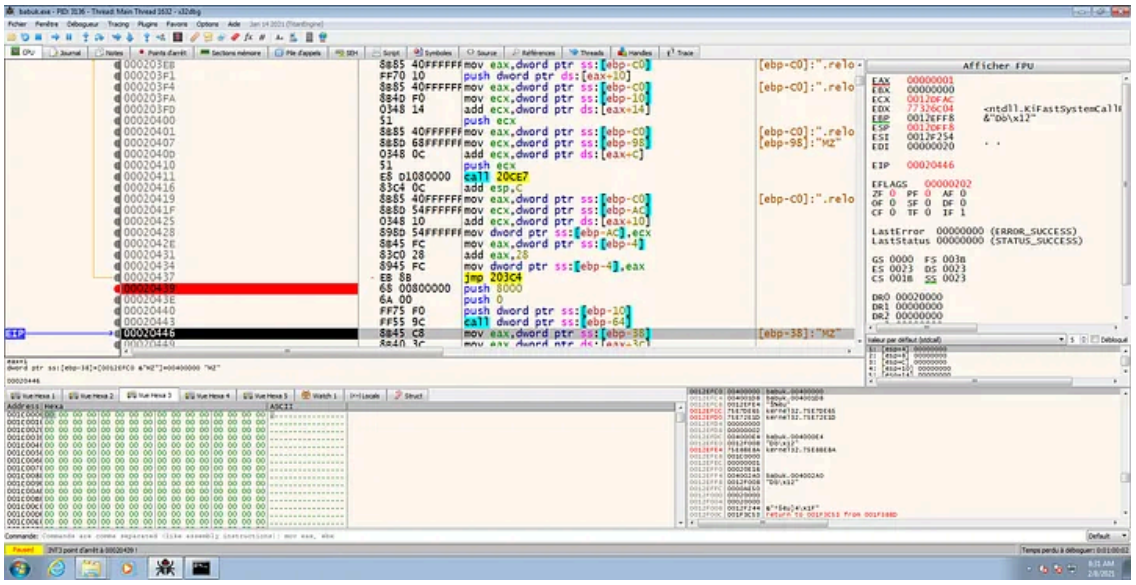


Press enter or click to view image in full size



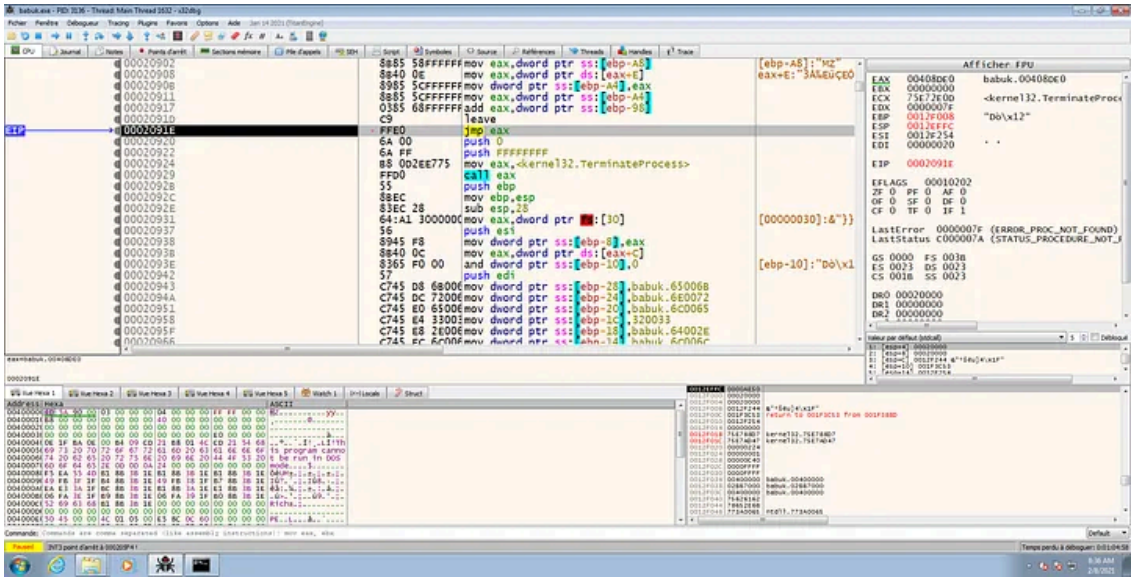
And the shellcode deletes the first malware unpacked.

Press enter or click to view image in full size



The shellcode fixes the import before to jump in babuk malware.

Press enter or click to view image in full size



Babuk analysis

Get Sebdraven's stories in your inbox

the version of babuk is the version v4 to use the mutex "DoYouWantToHaveSexWithCoungDong" with the chacha20 for the symetric encryption and curve2559 for the exchange key with the good base Point for the elyptic curve. The crypto of babuk is explained here. [Babuk Ransomware v3 | Chuong Dong]

```
                        DAT_00401784
00401784 09             ??          09h
00401785 00             ??          00h
00401786 00             ??          00h
00401787 00             ??          00h
00401788 00             ??          00h
00401789 00             ??          00h
0040178a 00             ??          00h
0040178b 00             ??          00h
0040178c 00             ??          00h
0040178d 00             ??          00h
0040178e 00             ??          00h
0040178f 00             ??          00h
00401790 00             ??          00h
00401791 00             ??          00h
```

The curve2559 is the function FUN_004035b0(local_1b04,(int)local_28,&DAT_00401784);

and the chacha encryption.

FUN_00402fa0((int)local_48,0x14,(int)&DAT_00401778,(int)lpBuffer,(int)lpBuffer,local_1aa8)

The files are encrypted in the function: FUN_00408060

> The ransomnote is ############## [babyk ransomware] ##############
> * What happend?
> —
> Your computers and servers are encrypted, backups are deleted from your network and copied.
> We use strong encryption algorithms, so you cannot decrypt your data without us.
> But you can restore everything by purchasing a special program from us — a universal decoder.
> This program will restore your entire network. Follow our instructions below and you will recover all your data.
> If you continue to ignore this for a long time, we will start reporting the hack to mainstream media and posting
> your data to the dark web.
> * What guarantees?
> —
> We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
>
> All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
> We guarantee to decrypt one file for free. Go to the site and contact us.
> * What information compromised?
> —
> We copied many data from your internal network,
> here are some proofs (private link): http://gtmx56k4hutn3ikv.onion/?JJ2Sdd8mtObS8tBQv5mM
> For additional confirmations, please chat with us/
> In cases of ignoring us, the information will be released to the public in blog
> http://gtmx56k4hutn3ikv.onion/
> * How to contact us?
> —
> 1) Download for browser: https://www.torproject.org/download/
> 2) Open it
> 3) Follow this link in tor browser: http://babukq4e2p4wu4iq.onion/login.php?id=UDFfRZirMNY2ENxMGJ9xczl3CTcie3

Conclusion

It seems to Babuk is distributed packed. The packer has many similarities with the packer of GandGrab. This packer should be downable on forum of malware developpers.

Thanks to Valery Marchive (@ValeryMarchive) / Twitter for the sample !
