בס"ד

Finding information with Volatility

By: Tamir Maidani

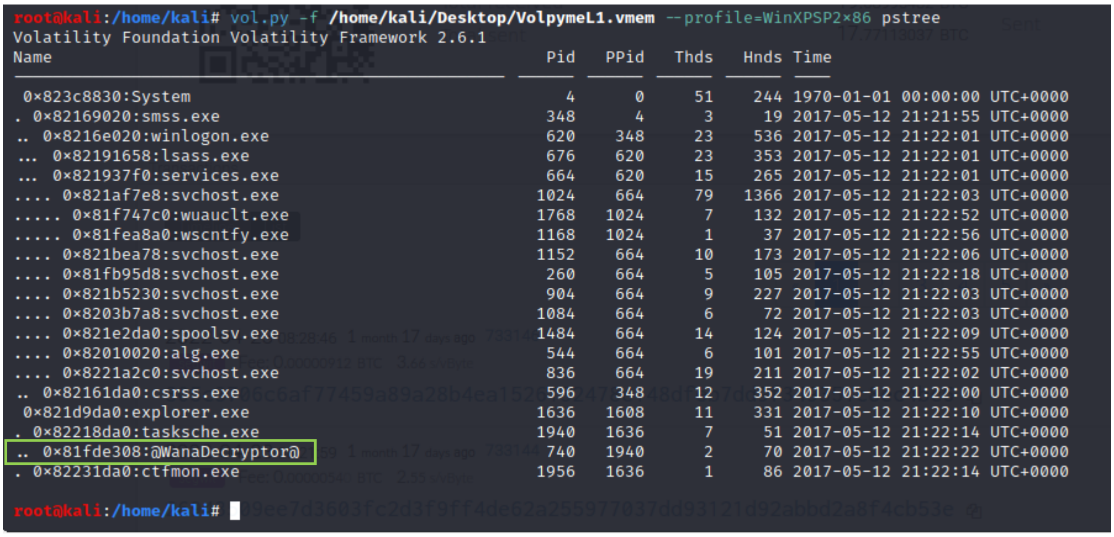
I have installed the Volatility framework in my kali machine

In order to investigate a memory (RAM) file to find a ransomware attempt

That has been going.

To be specific to find the "wallet address of the bitcoin" demand.

First we searched inside Volatility framework on kali to see any evidence of ransomware with basic pstree command and we found the next result:



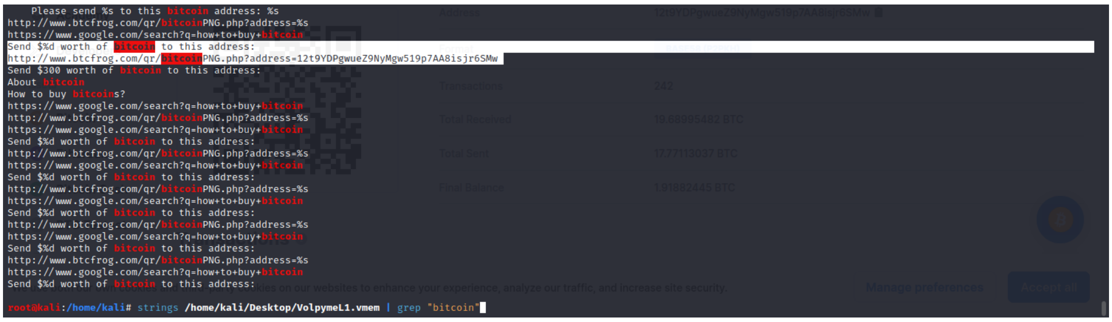
```
root@kali:/home/kali# vol.py -f /home/kali/Desktop/VolpymeL1.vmem --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c8830:System                                      4      0     51    244 1970-01-01 00:00:00 UTC+0000
. 0x82169020:smss.exe                                 348      4      3     19 2017-05-12 21:21:55 UTC+0000
.. 0x8216e020:winlogon.exe                            620    348     23    536 2017-05-12 21:22:01 UTC+0000
... 0x82191658:lsass.exe                              676    620     23    353 2017-05-12 21:22:01 UTC+0000
... 0x821937f0:services.exe                           664    620     15    265 2017-05-12 21:22:01 UTC+0000
.... 0x821af7e8:svchost.exe                          1024    664     79   1366 2017-05-12 21:22:03 UTC+0000
..... 0x81f747c0:wuauclt.exe                         1768   1024      7    132 2017-05-12 21:22:52 UTC+0000
..... 0x81fea8a0:wscntfy.exe                         1168   1024      1     37 2017-05-12 21:22:56 UTC+0000
.... 0x821bea78:svchost.exe                          1152    664     10    173 2017-05-12 21:22:06 UTC+0000
.... 0x81fb95d8:svchost.exe                           260    664      5    105 2017-05-12 21:22:18 UTC+0000
.... 0x821b5230:svchost.exe                           904    664      9    227 2017-05-12 21:22:03 UTC+0000
.... 0x8203b7a8:svchost.exe                          1084    664      6     72 2017-05-12 21:22:03 UTC+0000
.... 0x821e2da0:spoolsv.exe                          1484    664     14    124 2017-05-12 21:22:09 UTC+0000
.... 0x82010020:alg.exe                               544    664      6    101 2017-05-12 21:22:55 UTC+0000
.... 0x8221a2c0:svchost.exe                           836    664     19    211 2017-05-12 21:22:02 UTC+0000
.. 0x82161da0:csrss.exe                               596    348     12    352 2017-05-12 21:22:00 UTC+0000
 0x821d9da0:explorer.exe                             1636   1608     11    331 2017-05-12 21:22:10 UTC+0000
. 0x82218da0:taskche.exe                             1940   1636      7     51 2017-05-12 21:22:14 UTC+0000
.. 0x81fde308:@WanaDecryptor@                         740   1940      2     70 2017-05-12 21:22:22 UTC+0000
. 0x82231da0:ctfmon.exe                              1956   1636      1     86 2017-05-12 21:22:14 UTC+0000

root@kali:/home/kali# 
```

We found an IOC of a "WannaCry" ransomware attempt.

Then I moved more to find more details about the ransomware and searched the file

For some "bitcoin" demand with the search command "strings" and "grep"

The outcome:

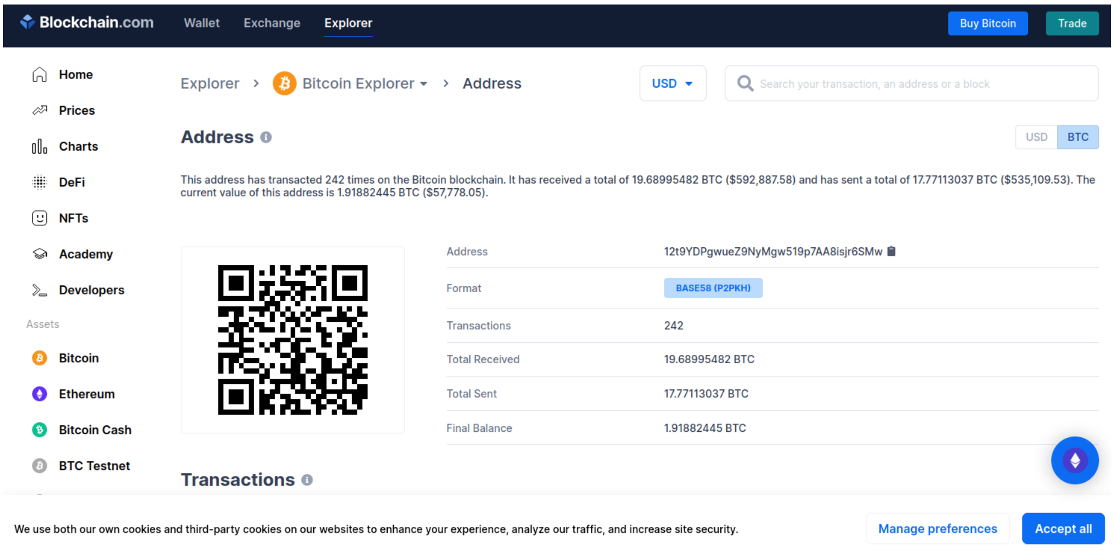


```
    Please send %s to this bitcoin address: %s
http://www.btcfrog.com/qr/bitcoinPNG.php?address=%s
https://www.google.com/search?q=how+to+buy+bitcoin
Send $%d worth of bitcoin to this address:
http://www.btcfrog.com/qr/bitcoinPNG.php?address=12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Send $300 worth of bitcoin to this address:
About bitcoin
How to buy bitcoins?
https://www.google.com/search?q=how+to+buy+bitcoin
http://www.btcfrog.com/qr/bitcoinPNG.php?address=%s
https://www.google.com/search?q=how+to+buy+bitcoin
Send $%d worth of bitcoin to this address:
http://www.btcfrog.com/qr/bitcoinPNG.php?address=%s
https://www.google.com/search?q=how+to+buy+bitcoin
Send $%d worth of bitcoin to this address:
http://www.btcfrog.com/qr/bitcoinPNG.php?address=%s
https://www.google.com/search?q=how+to+buy+bitcoin
Send $%d worth of bitcoin to this address:
http://www.btcfrog.com/qr/bitcoinPNG.php?address=%s
https://www.google.com/search?q=how+to+buy+bitcoin
Send $%d worth of bitcoin to this address:
http://www.btcfrog.com/qr/bitcoinPNG.php?address=%s
https://www.google.com/search?q=how+to+buy+bitcoin
Send $%d worth of bitcoin to this address:

root@kali:/home/kali# strings /home/kali/Desktop/VolpymeL1.vmem | grep "bitcoin"
```

We can see that we found the ransomware demand, and the "bitcoin wallet address"

Which is : "12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw"

And to verify it exists I want to search the web for that address, and this is the results:



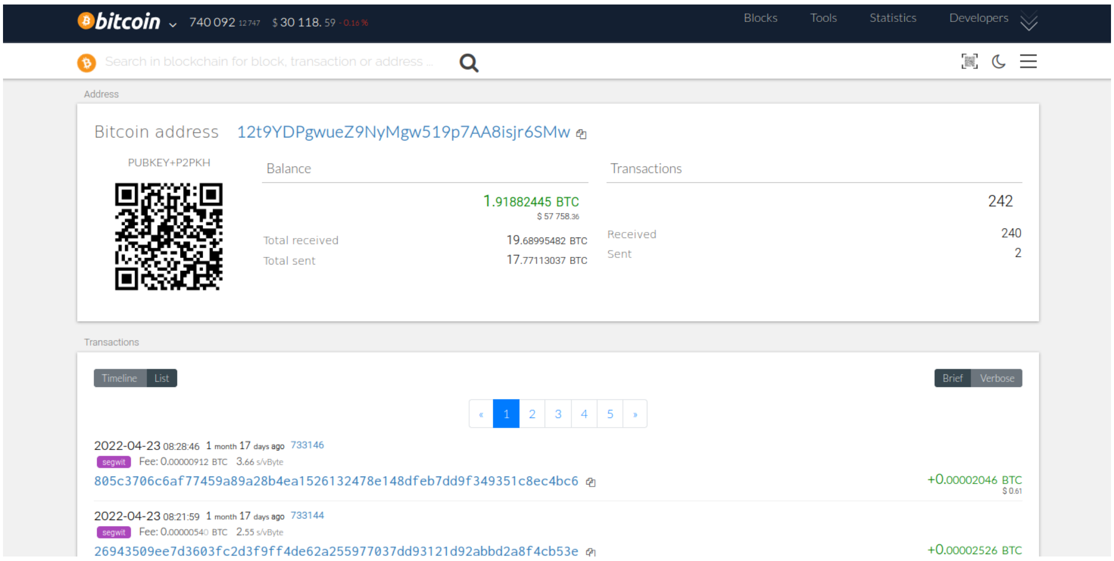
Address

This address has transacted 242 times on the Bitcoin blockchain. It has received a total of 19.68995482 BTC ($592,887.58) and has sent a total of 17.77113037 BTC ($535,109.53). The current value of this address is 1.91882445 BTC ($57,778.05).

Address	12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Format	BASE58 (P2PKH)
Transactions	242
Total Received	19.68995482 BTC
Total Sent	17.77113037 BTC
Final Balance	1.91882445 BTC

Transactions

We use both our own cookies and third-party cookies on our websites to enhance your experience, analyze our traffic, and increase site security.



Address

Bitcoin address 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

PUBKEY+P2PKH

Balance

1.91882445 BTC
$ 57 758.36

Total received	19.68995482 BTC
Total sent	17.77113037 BTC

Transactions

242

Received	240
Sent	2

Transactions

2022-04-23 08:28:46 1 month 17 days ago 733146
segwit Fee: 0.00000912 BTC 3.66 s/vByte
805c3706c6af77459a89a28b4ea1526132478e148dfeb7dd9f349351c8ec4bc6 +0.00002046 BTC
$ 0.61

2022-04-23 08:21:59 1 month 17 days ago 733144
segwit Fee: 0.00000540 BTC 2.55 s/vByte
26943509ee7d3603fc2d3f9ff4de62a255977037dd93121d92abbd2a8f4cb53e +0.00002526 BTC