Blaze's Security Blog

Personal blog about internet & malware threats.

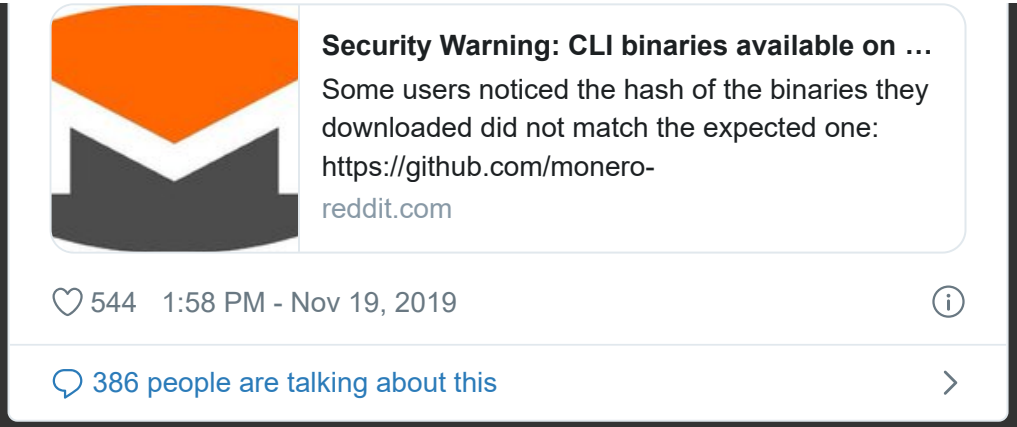
Tuesday, November 19, 2019

Monero download site and binaries compromised

Introduction

Earlier this evening I saw a tweet appear which claimed Monero has been hacked and a malicious binary (instead of the real one) has been served:

> **dark.fail**
> @DarkDotFail
>
> Warning Monero users: If you downloaded Monero in the past 24 hours you may have installed malware. Monero's official website served compromised binaries for at least 30 minutes during the past 24 hours. Investigations are ongoing. reddit.com/r/Monero/comme…



Post on Reddit:
https://www.reddit.com/r/Monero/comments/dyfozs/security_warning_cli_binaries_available_on/

Github issue:
https://github.com/monero-project/monero/issues/6151

Linux binary

Thanks to user nikitasius I was able to retrieve the malicious binary:
https://github.com/monero-project/monero/issues/6151#issuecomment-555511805

This binary is an ELF file with the following properties:

- MD5: d267be7efc3f2c4dde8e90b9b489ed2a
- SHA-1: 394bde8bb86d75eaeee69e00d96d8daf70df4b0a
- SHA-256: ab9afbc5f9a1df687558d570192fbfe9e085712657d2cfa5524f2c8caccca31
- File type: ELF
- Magic: ELF 64-bit LSB shared object, x86-64, version 1 (GNU/Linux), dynamically linked (uses shared libs), for GNU/Linux 3.2.0, from 'x)', not stripped
- File size: 27.63 MB (28967688 bytes)

When comparing the legitimate file and this ELF file, we notice the file size is different, and a few new functions have been added:

cryptonote::simple_wallet::send_seed

Subscribe To

Posts

Comments

This function is immediately called after either opening or creating a new wallet, as can be seen in Figure 1 and 2 below.

```
local_40 = *(long *)(in_FS_OFFSET + 0x28);
success_msg_writer(SUB81(local_1e8,0));
                    /* try { // try from 0078b7ea to 0078b835 has its CatchHandler @ 0078b979 */
__ostream_insert<char,std::char_traits<char>>(local_1d0,"\n",1);
cVar2 = multisig((wallet2 **)(this + 0x450),(bool *)0x0,(uint *)0x0,(uint *)0x0);
if (cVar2 == '\0') {
                    /* try { // try from 0078b93f to 0078b943 has its CatchHandler @ 0078b979 */
  local_2f0 = tr("25 words");
}
else {
  local_2f0 = tr("string");
}
pcVar4 = (char *)tr(
                    "NOTE: the following %s can be used to recover access to your wallet. Write
                    them down and store them somewhere safe and secure. Please do not store them
                    in your email or on file storage services outside of your immediate control.\
                    );
```

Figure 1 - Create wallet (legitimate)

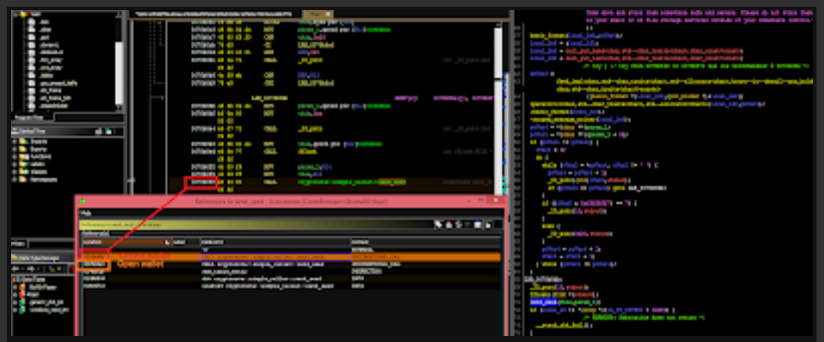


Figure 2 - Call new seed function

The seed will be sent to: node.hashmonero[.]com.

cryptonote::simple_wallet::send_to_cc

As you may have guessed, this function will send data off to the CC or C2 (command and control) server - this will be stolen funds.

```
                    LAB_0078b28d                                    XREF[1]:    0078b06c(j)
0078b28d 48 8d 9d       LEA         RBX=>local_1b8,[-0x1b0 + RBP]
         50 fe ff ff
0078b294 48 8d 35       LEA         param_1,[s_45.9.148.65_011ec193]             = "45.9.148.65"
         f8 0e a6 00
0078b29b 48 89 df       MOV         this,RBX
```

Figure 3 - Send to cc

Blog Archive

▼ 2019 (3)
▼ November (1)
Monero download site and binaries compromised
► March (2)
► 2018 (12)
► 2017 (16)
► 2016 (12)
► 2015 (7)
► 2014 (9)
► 2013 (23)
► 2012 (14)
► 2011 (15)
► 2010 (13)

Twitter

FOLLOW ME ON twitter

Popular Posts

Malware spreading via Steam chat

If you're only interested in how to remove this malware from your machine or other tips and prevention advise, click here . In case you ...

Satan ransomware adds EternalBlue exploit

Today, MalwareHunterTeam reached out to me about a possible new variant of Satan ransomware. Satan ransomware itself has been around si...

Sending funds to the C2 is handled using an HTTP POST request to the following C2 servers:

- node.xmrsupport[.]co
- 45.9.148[.]65

As far I can see, it doesn't seem to create any additional files or folders - it simply steals your seed and attempts to exfiltrate funds from your wallet.

Windows binary

The C2 server 45.9.148[.]65 also hosts a Windows binary with the following properties:

- MD5: 72417ab40b8ed359a37b72ac8d399bd7
- SHA-1: 6bd94803b3487ae1997238614c6c81a0f18bcbb0
- SHA-256: 963c1dfc86ff0e40cee176986ef9f2ce24fda53936c16f226c7387e1a3d67f74
- File type: Win32 EXE
- Magic: PE32+ executable for MS Windows (console) Mono/.Net assembly
- File size: 65.14 MB (68302960 bytes

The Windows version is essentially doing the same things as the Linux version - stealing your seed and wallet funds - the function names are just different,
e.g. **_ZN10cryptonote13simple_wallet9send_seedERKN4epee15wipeable_stringE**.

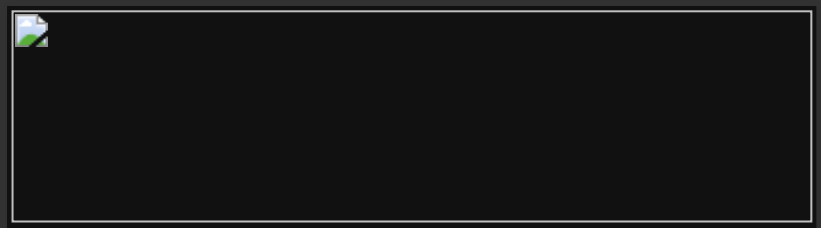
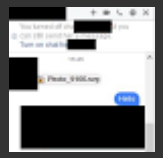


Figure 4 - Send to cc

Note: this doesn’t mean the official Windows binary was also compromised - it simply means there’s also a compromised Windows binary out there. Only the Monero team can confirm if other

Free Riot codes scam
Below you can find a list of confirmed phishing and scam websites. In the conclusion (end of this post or click) you'll be able to fin...

Notes on Linux/Xor.DDoS
In this post we'll be focusing on a certain kind of malware: Linux/Xor.DDoS (also known as DDoS.XOR or Xorddos). As usual, we'll b...



Nemucod downloader spreading via Facebook
Earlier today, a friend of mine notified me of something strange going on with his Facebook account; a message containing only an image (an...

Reddit

Translate

Google Translate

English to Chinese BETA
English to French
English to German
English to Italian
English to Japanese BETA
English to Korean BETA
English to Russian BETA

binaries (besides the Linux one mentioned in this blog) have been compromised.

Detection

- If you have a firewall or proxy, whether hardware or software, verify if you had any network traffic or connections to;
  - node.hashmonero[.]com
  - node.xmrsupport[.]co
  - 45.9.148[.]65
  - 91.210.104[.]245
- Remove all the binaries listed in this blog post;
- Verify the hashes of your Monero setup or installer file. Guides to do that here;
  - Beginner: https://src.getmonero.org/resources/user-guides/verification-windows-beginner.html
  - Advanced: https://src.getmonero.org/resources/user-guides/verification-allos-advanced.html
  - Note: hashes list is available here: https://web.getmonero.org/downloads/hashes.txt.

Note: What is a hash? A hash is a unique identifier. This can be for a file, a word, ... It is preferred to use SHA256 hashes for file integration checks.

You may also use the following Yara rule to detect the malicious or compromised binaries: Monero_Compromise.yar
Download Yara (and documentation) from:
https://github.com/VirusTotal/yara

Recommendations

- Install an antivirus, and if possible, use a firewall (free or paid is of less importance);
- If you already use an antivirus: it may be a good idea to not exclude a specific folder in your antivirus when using Monero (or other miners), and if needed, only do so **after** the hashes have been verified;
- Restore your seed or account;

    - How to restore your account: https://web.getmonero.org/resources/user-guides/restore_account.html
    - Recovering wallet using the mnemonic seed: https://monero.stackexchange.com/questions/10/how-can-i-recover-a-wallet-using-the-mnemonic-seed
- Monitor your account/wallet for the next days and verify there have been no fraudulent transactions. Contact the Monero team for support.

Note: Especially go through the steps if at any point you downloaded, used or installed new binaries between these dates: Monday 18th 1:30 AM UTC and 5:30 PM UTC. Download the latest version from: https://web.getmonero.org/downloads/.

Monero team statement

The Monero team has issued a statement as follows:

Warning: The binaries of the CLI wallet were compromised for a short time: https://web.getmonero.org/2019/11/19/warning-compromised-binaries.html

I expect this statement to be updated the following days, so monitor it as well.

Conclusion

Monero is not the first, nor will it likely be the last cryptocurrency (in this case, its website and binaries) that gets compromised.

Follow the steps in this blog post to protect yourself and always watch your online accounts closely, especially those where you have financially invested in. Use strong passwords, use MFA (or 2FA) where possible and always be vigilant. Verify hashes when a new version is available.

Note: this blog post is not intended to be a full analysis, but rather a quick report on the facts, including recommendations. Questions or feedback? Happy to hear it!

Let me know in the comments below or on Twitter.

Indicators

Indicator type	Indicator
FileHash-SHA256	7ab9afbc5f9a1df687558d570192fbfe9e085712657d2cfa5524f2c8caccca31
FileHash-SHA256	963c1dfc86ff0e40cee176986ef9f2ce24fda53936c16f226c7387e1a3d67f74
hostname	www.hashmonero.com
hostname	node.xmrsupport.co
hostname	node.hashmonero.com
FileHash-MD5	d267be7efc3f2c4dde8e90b9b489ed2a
FileHash-MD5	72417ab40b8ed359a37b72ac8d399bd7
FileHash-SHA1	6bd94803b3487ae1997238614c6c81a0f18bcbb0
FileHash-SHA1	394bde8bb86d75eaeee69e00d96d8daf70df4b0a
IPv4	91.210.104.245
IPv4	45.9.148.65
domain	hashmonero.com
domain	xmrsupport.co

On AlienVault:

https://otx.alienvault.com/pulse/5dd4574fc7c82cddbdcb8d12

Posted by Bart at 10:18 PM

Labels: getmonero compromised, getmonero hack, Monero, Monero hack, Monero project compromised

3 comments:

Paul November 20, 2019 at 10:50 AM

Thanks for your analysis! Can you please tell which software you used to decompile the functions?

Reply

Replies

Anonymous November 20, 2019 at 2:03 PM

ghidra

Bart November 20, 2019 at 6:08 PM

Thanks Paul! It's indeed Ghidra - get it from here: https://ghidra-sre.org/

Reply

Enter your comment...

Comment as: joanna07246@ ▼ Sign out

Publish Preview Notify me

Links to this post

Create a Link

Home Older Post

Subscribe to: Post Comments (Atom)

Follow by Email