Phorpiex Breakdown - Check Point Research

By bferrite

Published: 2019-11-19 · Archived: 2026-04-05 12:42:29 UTC

Research by: Alexey Bukhteyev

Introduction

We recently wrote about the massive "sextortion" spam campaign carried out by the Phorpiex botnet. However, this is only a small part of this botnet's malicious activity. Capable of acting like both a computer worm and a file virus, Phorpiex is spread through exploit kits and with the help of other malware and has infected more than **1,000,000** Windows computers to date. By our assessment, the annual criminal revenue generated by Phorpiex botnet is approximately **half a million US dollars**.

Of course, to maintain such a large botnet, a reliable command and control (C&C) infrastructure is required. For malware with a small outreach, or if infected computers are not part of a single botnet, virtual private servers (VPS) are most often used. VPS hosting services can be purchased from legitimate companies. Many VPS hosting providers don't require identity verification, and the services can be paid for anonymously.

However, in the case of the Phorpiex botnet, a public VPS is not suitable. First of all, the C&C server for such a botnet would immediately attract attention with a large amount of malicious traffic: several million requests per day from more than 100,000 unique IP addresses are sent to the Phorpiex C&C servers. By our assessment, the monthly volume of the botnet's C&C traffic may exceed 70 TB. Therefore, Phorpiex doesn't use public VPS hosting services. Instead, it uses dedicated IP subnets registered to figureheads.

Botnet Architecture

Initially, the Phorpiex has been known as a botnet operated using IRC protocol (also known as Trik). However, recent Phorpiex campaigns have switched to modular architecture and got rid of IRC communication. We barely saw any of its IRC C&C servers online in 2019. However, our sinkholes still indicate many thousands of hosts infected with Trik. When we did spot IRC C&C servers online, we managed to capture a command for loading another malware to the infected machines:

Figure 1 – Trik C&C communication dump with the decrypted URL.

We assume that this malware, self-named Tldr (probably stands for "TrikLoader"), has currently become the core part of the Phorpiex botnet. Tldr is a downloader that uses HTTP protocol for communication with C&C servers. Its main purpose is to load another malware on the infected machines. Some Tldr samples have the functionality of a computer worm and can spread through removable drives. We also observed variants of the malware that act like a file virus infecting other software.

If necessary, malware actors can extend the functionality of the botnet by loading additional modules. The image below shows the infection flow and modular architecture of the current botnet.

Figure 2 – Phorpiex infection flow and architecture.

The purpose of Tldr, and modules such as the VNC Worm and the NetBIOS Worm, is to distribute the botnet as much as possible. The final goal of the Phorpiex operators is to gain profit, generally in crypto-currency.
The main ways the botnet is monetized:
– Sextortion spam.
– Crypto-jacking.
– Crypto-currency clipping.
– Providing services for loading other malware (Raccoon stealer, Predator The Thief), distributing ransomware.

Currently, the Phorpiex botnet doesn't load ransomware. After the termination of the GandCrab ransomware, the Phorpiex botnet completely switched to sending sextortion spam emails from the infected computers and loading data stealers there.
We should emphasize that almost all samples of Trik and Tldr include crypto-clipper functionality. Addresses of all crypto wallets consist of a long combination of digits and letters. The only way to transfer crypto-currency without additional devices is to copy the address to the clipboard and then insert it in a corresponding field in a wallet application. The malware alters crypto wallet addresses in a clipboard, and the money is transferred to the wallet that belongs to the malware operators. Crypto-clipper functionality allows malware operators to gain profits without any additional effort, even when C&C servers are offline. Bitcoin wallets used in both Trik and Tldr configurations continue to receive stolen Bitcoins and have collected more than 17 BTC so far.
Botnet capacity assessment
Phorpiex bots continuously scan domain names and IP addresses extracted from the configuration. Even if a valid C&C server responds, the malware continues to query other hosts. Therefore, after registering domains from different Tldr configurations, we started to receive a large number of connections from Phorpiex bots. This allowed us to assess the prevalence of the botnet.
During the past two months, we registered connections from more than 1,000,000 unique hosts. At any given time, an average of 15,000 bots is online, and up to 100,000 bots are active daily.

Figure 3 – Number of bots online hourly.

The botnet hosts are primarily located in Asia. The most significant parts of the botnet are located in India, China, Thailand, and Pakistan. There are also bots present in the US, Mexico, and many African countries. Europe is almost unaffected by the botnet.

Figure 4 – Phorpiex botnet global locations.

C&C Infrastructure

All Phorpiex modules use a hard-coded list of IP addresses and domain names for C&C communication. While most malware implements DGA, using hard-coded domain names doesn't impair the survival of the Phorpiex bots. We suppose the list of domain names is used as a precaution, to be able to regain control of the bots in case of the loss of C&C servers accessed by the IP address. The list of domain names is updated periodically. While monitoring the Phorpiex campaign during 2019, we discovered more than 4,000 different samples of Tldr, with approximately 300 configurations and 3297 domain names and IP addresses.
Tldr uses the same C&C servers that were used by the Trik IRC bot:

Figure 5 – Phorpiex C&C infrastructure.

Currently, the most active IP used by the botnet for its C&C servers is **185.176.27.132** and addresses from the subnet **92.63.197.0/24**.
We found that the subnet **92.63.197.0/24**, which hosts a lot of Phorpiex C&C servers, was also observed in other threats like Smoke Loader and Necurs, and used for sending phishing and spam emails, and for port scanning.

One more interesting fact regarding this subnet is that it is registered to an individual entrepreneur in the Ukraine:

> org-name: FOP HORBAN VITALII Anatoliyovich
> org-type: OTHER
> address: 62408, KHARKIV REGION, ELITE village, SCHOOL str. 25, AP. 26
> e-mail: vetalgorban@protonmail.com

We found the registration data for an individual entrepreneur called "FOP HORBAN VITALII Anatoliyovich."
His main activity is in food retail:

Figure 6 – Screenshot from the Directory of Companies of the Ukraine.

Therefore, we think "FOP HORBAN VITALII Anatoliyovich" is just a figurehead.
Almost the same situation appears if we search for data about another IP address used by the Phorpiex C&C server – **185.176.27.132**:

> org-name: IP Dunaev Yuriy Vyacheslavovich
> org-type: OTHER
> address: 420132, Kazan, Chuikova str, 69
> e-mail: dunaevyur@gmail.com

Dunaev Yuriy Vyacheslavovich is also an individual entrepreneur from Russia (Republic Tatarstan) whose main activity is transport services. As in the previous case, the activity of the entrepreneur is not related to the Internet or IT in any way.
Packets to this network are routed through Telehouse ISP, which is physically located in Bulgaria:

> 9 50 ms 49 ms 49 ms as50360.peer.telehouse.bg [178.132.83.102]
> 10 46 ms 46 ms 46 ms 192.168.244.2

> 11 51 ms 50 ms 50 ms 185.176.27.9
> 12 50 ms 46 ms 50 ms 185.176.27.132

Perhaps, what we are witnessing is cooperation between Phorpiex and another cybercrime group that obtains IP subnets from RIPE and provides services for hosting malicious C&C infrastructure.

Crypto-jacking campaign

Cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrency. One of the final payloads loaded to Phorpiex-controlled computers is XMRig mining software. The reward for crypto-currency mining using XMRig is paid in Monero (XMR). The Phorpiex XMRRig miner comes with the configuration embedded in the sample. It uses Phorpiex C&C servers as mining pools:

XMRig downloaded from	**Pool address**
hxxp://93.32.161[.]73/2 hxxp://185.176.27[.]132/2	193.32.161.73:7777
hxxp://185.176.27[.]132/2	185.176.27.132:4545
hxxp://193.32.161[.]77/2.exe	193.32.161.77:9595
hxxp://92.63.197[.]38/3.exe hxxp://92.63.197[.]60/2.exe hxxp://92.63.197[.]153/2.exe hxxp://94.156.133[.]65/55.exe	92.63.197.153:7575
hxxp://193.32.161[.]69/2.exe hxxp://193.32.161[.]77/2.exe	193.32.161.69:5555

Table 1 – Phorpiex C&C servers and XMRig mining pools.

In addition, we found XMR addresses for Phorpiex XMRig samples and found that they are the same as those used in the "sextortion" campaign. The wallets are stored in integrated format. This means that the address also contains the Payment ID. The Payment ID is usually used to identify transactions to merchants and exchanges. Given the intrinsic privacy features built into Monero, where a single public address is usually used for incoming transactions, the Payment ID is especially useful to tie incoming payments with user accounts. The XMR addresses extracted from the Phorpiex XMRig samples and used in sextortion campaigns differ only by the Payment ID:

Wallet from the XMRig sample (MD5): **36e824615d72d11a3f962ec025bfceba**	4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MR U4nUMXAHNFBEJhkTZV9HdaL4gfuNBxLPc3BeMk LGaPbF5vWtANQ**ujt72bSgzs7j6uNDV**
Wallet from the XMRig sample (MD5): **7f8880c0bc2dd024a3cf5261b6582313**	4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MR U4nUMXAHNFBEJhkTZV9HdaL4gfuNBxLPc3BeMk

	LGaPbF5vWtANQs**TC167gPTeRcVSaut**
Wallet from the sextortion spam module (MD5): **2c50efc0fef1601ce1b96b1b7cf991fb**	4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MR U4nUMXAHNFBEJhkTZV9HdaL4gfuNBxLPc3BeMk LGaPbF5vWtANQ**ubDtNq5uuC622w4we**

Table 2 – Phorpiex Monero wallets noticed in XMRig samples and sextortion campaign.

These facts leave no doubt that the Phorpiex botnet owners receive all the profit from mining.
Unfortunately for us, due to its privacy features, the Monero blockchain doesn't allow us to track transactions and view an individual's balance. However, we can estimate the profitability of the crypto-jacking campaign using the results of the botnet capacity assessment, the Monero mining profitability calculator, and other Monero benchmarks. Assuming that the average Phorpiex victim doesn't have top-level hardware, the basis of our calculation was a low hash rate of **100 H/s** which corresponds to INTEL I5-6500T CPU. At any given time, an average of **15,000** bots is online. Therefore, the total Monero mining hash rate provided by Phorpiex botnet is **1.5 MH/s**. Of course, Phorpiex actors don't pay for the electricity and pool fee as regular miners do, so we assume those values are equal to 0:

Figure 7 – Monero mining profitability calculation.

Therefore, by our assessment, the Phorpiex botnet must generate at least 3,122 XMR per year which currently is equivalent to about 21 Bitcoins (BTC) or $ 180,000.

Crypto-clipping campaign

We first saw transactions to the wallets observed in the Trik configuration in August 2016. This may be the time when crypto-clipping functionality was first added to Trik. Malware creators started their operations stealing Bitcoin only. In Tldr, they added support for a large number of virtual assets including Ethereum, Litecoin and even Perfectmoney.
Unlike Monero, the Bitcoin and Ethereum blockchains allow us to monitor all transactions. Therefore, we are able to assess how effective a particular crypto-clipping campaign is. We collected a large number of Trik and Tldr samples and the Bitcoin wallets extracted from them.
Bitcoin wallets extracted from Trik configurations received a total of more than 11 BTC in 376 transactions:

BTC Wallet	Amount	First Transaction Date	Last Transaction Date
1JWWZFUVAWvFNS2D5qwQQo4oSsseoD9kAn	0,04953613	14.08.2016	24.08.2016
1HewcqbrkXY5iqrDqjb4j4AHiaDeobpE6P	0,00030088	21.06.2017	21.06.2017
1KXZqR1fjAxcv1gvdmPfN2WsWsDwM7r2R2	0,0165661	18.06.2017	09.10.2018
1of6uEzx5qfStF1HrVXaZ1eE3X4ntnbsx	5,33347017	10.08.2017	02.09.2019

1LaVtKqJatoeAHkHEgp9UF2fJEarEdZPr9	0,37694525	13.09.2016	17.11.2016
1Kzhh4nqyjB3MAoQ5uH2Bcdz3qXWpnsMzd	3,39173817	19.12.2016	10.04.2017
1CpQYTKfiYj8ZoXUmz1DaohjJVsDzGpgbx	0,81380018	01.02.2017	11.09.2019
18qKrmaUXaEgbYEn6yMkGKNcqkYB3mSxNv	1,60713638	22.11.2016	04.08.2018
Total	11,58949326		

Table 3 – Phorpiex Trik crypto-clipper BTC wallets.

As we can see from the table, despite the fact that Trik bots don't receive updates and the C&C servers are offline, some wallets still continue to gain Bitcoins.
The table below contains Bitcoin wallets extracted from Tldr configurations:

BTC Wallet	Incoming Transactions	Amount	First Transaction Date
1DYwJZfyGy5DXaqXpgzuj8shRefxQ7jCEw	214	2,53308	31.05.2018
1BdhCwNFzNbWoJvxrok6V7z2af7xjJLS58	23	0,313455	29.04.2019
1Gx8oRKKczwdB32yiLzVx5hsjAze6g5HHw	13	0,286929	05.07.2019
14GJm9M5zaX6Zyojt5yxNZcdoouJ4WPAgT	10	0,109102	31.01.2019
1EN3bbs8UdVWA3i3ixtB9jQWvPnP9us4va	50	0,277109	21.02.2019
1C2SvtsUu8YZVUBbha4KiBGYRW5dwtrRvd	9	0,141692	30.06.2018
18bzpjFfo5JQ41GzzUNRMgcE7WwQwpqFrR	14	0,116484	12.09.2019
1Bn4JYKoVgQpZ73doWVFSNZBbwKj3cpJNR	23	0,192937	28.07.2019
1CUhtfNjsGMZziCVzZ4oVan9NCGriY4NDZ	14	0,139406	17.04.2019
1MaN4Me35n1kM6h7JVPNUQYqYgjasEQLzs	29	0,105204	08.06.2019
19mduWVW9QphW5W2caWF84wcGVSmASRYpf	8	0,016345	27.09.2019
1L6sJ7pmk6EGMUoTmpdbLez9dXACcirRHh	25	0,242939	18.07.2019
13cQ2H6oszrEnvw1ZGdsPix9gUayB8tzNa	33	0,286732	19.08.2019
19B5G1ftgXRrD6GiTzThL9BiySVdf1HJZy	27	0,718224	04.12.2018
1LdFFaJiM7R5f9WhUEskVCaVokVtHPHxL5	7	0,017085	30.10.2018
Total	499	5,49672513	

Table 4 – Phorpiex Tldr crypto-clipper BTC wallets.

Therefore, in the 3 year period, crypto-clipping campaigns allowed the malware operators to steal more than 17 BTC in 875 transactions, or about 5.6 BTC annually.
Ethereum crypto-currency wallets extracted from Trik and Tldr samples gained much less than Bitcoin wallets:

ETH Wallet	Incoming Transactions	Amount
0x8b7f16faa3f835a0d3e7871a1359e45914d8c344	2	0,163207
0xa9b717e03cf8f2d792bff807588e50dcea9d0b1c	2	0,1988
0xff0d45f3e2ec83de3b2e069300974732ba1c5d30	9	1,827462
0x373b9854c9e4511b920372f5495640cdc25d6832	2	0,096352
0x87f84b56fb061f51ca709f2ac3fc6e2d4b3b8f8f	5	4,139667
0xa5228127395263575a4b4f532e4f132b14599d24	3	0,092458
0x43e44151ad4d625d367376a6fd3ea44c82718777	3	7,294262
0x05F916216CC4BA6ac89b8093d474E2a1e6121c63	2	0,301865
0xc4e6e206ddc7f83a78582fc4e5536a8ed395c5e1	1	0,017308
0x74e4195d16e8887ebe6d6abde1aa38bc91e69976	2	0,039646
0x08a1f48df7b6847fe8276ee55068f6cf83340c9a	0	0
0xb6d8926bf0418de68a7544c717bbb4ea198769cc	9	1,240524
0xab1b250d67d08bf73ac864ea57af8cf762a29649	0	0
0xff8c5843e7abe2708037fc1acdca83b37466a299	11	1,911012
Total	40	17,32256

Table 5 – Phorpiex crypto-clipper ETH wallets

There are only 51 transactions, with a total amount of about 17 ETH, whose current value is much less than Bitcoin. However, those wallets are interesting to us for another reason. Services like etherescan.io can show if an Ethereum address belongs to a particular exchange or service. For the addresses from the table, all ETH are transferred to the address of the Cryptonator service:

Figure 8 – Ethereum transactions from the Phorpiex ETH address.

Therefore, we can conclude that the Ethereum addresses used in the crypto-clipping campaign are created in a Cryptonator wallet. Cryptonator requires a valid email address for registration and confirmation for each new IP

address and device by email. We think that the access logs of the Cryptonator service may store the real IP addresses of the Phorpiex actors.
Another interesting fact is that some of the Ethereum wallets have collected a large number of ERC-20 tokens:

Figure 9 – Ethereum ERC-20 tokens transactions to the Phorpiex ETH address.

However, the tokens can't be withdrawn from the wallets because Cryptonator doesn't support tokens based on the Ethereum blockchain. Most likely, this wasn't taken into account by the malware actors. Therefore, token transfers from victims are simply blackholed.
Comparison to the sextortion campaign
We've been observing the Phorpiex sextortion campaign for about half a year. During this period, we recorded transfers of more than 14 Bitcoins [update the numbers before publication] to the Phorpiex wallets related to this campaign. If the trend continues, the annual revenue of the sextortion campaign would be 28 Bitcoins.

Figure 10 – Comparison of the Phorpiex earnings from different malicious activities.

Sextortion appears to be a more profitable venture than crypto-currency clipping or mining using the botnet's computing power. However, those malicious activities complement each other, generating about 54.6 Bitcoins annually, which is currently about $500,000.

Conclusion

We inspected some of Darknet advertisements that provide prices for malware installation services. Usually infection services prices vary from $100 to $1000 per 1000 infections, depending on the victims' location. Phorpiex bots are mostly located in Asia – the region in which malware installation services are the cheapest. Therefore, to purchase malware infection services on the Darknet, the owners of the Phropiex botnet would pay about $100,000. However, in addition to purchasing infections through side services like the RIG exploit kit or the Smokeloader botnet, Phropiex also uses its own distribution techniques: the VNC worm module, NetBIOS worm module, and file virus functionality. But even with these costs, as we can see, the creation of such a botnet appears to be very profitable.
The tools used by Phorpiex are not too sophisticated. Obviously, not much time was spent on their development. This case shows us that such a massive botnet can be created by cybercriminals without a deep knowledge of system programming, cryptography, etc.
The ecosystem that currently exists in the Darknet makes it easy enough to implement almost any idea for cybercrime.

IOC

MD5	Description	Downloaded From
58198a2ebac604399c3e930207df47f1	Phorpiex Trik v5.0	

64990a45cf6b1b900c6b284bb54a1402	Phorpiex Tldr v3.0	
e5aea3b998644e394f506ac1f0f2f107	Phorpiex Tldr v2.0	
383498f810f0a992b964c19fc21ca398	Phorpiex Tldr v1.0	
afe348ff22ad43e98ee7ab19a851b817	Phorpiex Tldr mod2019 Dropped by Trik 2019-07-23	hxxp://92.63.197[.]59/lst.exe
d9e59a4295926df49c8d6484aa6b8305	Phorpiex Tldr Dropped by RIG EK 2019-05-29	hxxp://94.156.133[.]65/11.exe
051356bee1541f592d66969af46feb95	Phorpiex Tldr Dropped by SmokeLoader 2019-05-15	hxxp://ghjk78kjhb[.]net/ -> hxxp://94.156.133[.]65/11.exe
99a349f6b758c80e9a1b88d1895e7790	Sextortion DASH	hxxp://185.176.27[.]132/4
d85dcfd49b8e259f4135fa9f021f250a	Sextortion BTC	hxxp://thaus[.]top/7
2c50efc0fef1601ce1b96b1b7cf991fb	Sextortion XMR	hxxp://185.176.27[.]132/6
8f9b7c1c2b84b8c71318b6776d31c9af	XMRig miner	hxxp://185.176.27[.]132/2

C&C IP	**MD5**
112.126.94.107	2d33fd32d8ec7b7d0ed379b80a167ff4
123.56.228.49	2d33fd32d8ec7b7d0ed379b80a167ff4
172.104.40.92	2d33fd32d8ec7b7d0ed379b80a167ff4
185.176.27.132	f3dcf80b6251cfba1cd754006f693a73
193.32.161.69	a8ab5aca96d260e649026e7fc05837bf
193.32.161.73	a24bb61df75034769ffdda61c7a25926
193.32.161.77	cc89100f20002801fa401b77dab0c512
87.120.37.156	97835760aa696d8ab7acbb5a78a5b013
87.120.37.234	a0039fbc46f2e874f2e4151712993343
87.120.37.235	f0c7f0823de1a9303aa26d058c9951a0
92.63.197.106	e24b40197da64a4baa9a81cc735e839b
92.63.197.112	82eecd3b80caa7d0f51aba4ee8149c1a
92.63.197.153	20ef08bdae07f3494e20195e65d7b7f5

92.63.197.38	49d218a1a09ba212e187dc2de923ba62
92.63.197.48	1462114257a6fcc52a8782c2a2616009
92.63.197.59	c63a7c559870873133a84f0eb6ca54cd
92.63.197.60	82eecd3b80caa7d0f51aba4ee8149c1a
94.156.133.65	b69270ee30bd20694948dba6c09ead7f
95.81.1.43	5c79b524fb8d9bb4e9a3d79fe543c011
124.158.10.82	1727de1b3d5636f1817d68ba0208fb50
125.212.217.33	1727de1b3d5636f1817d68ba0208fb50
125.212.217.30	1727de1b3d5636f1817d68ba0208fb50
127.181.87.80	af1cf2281597aba08e40cf7c030d71a9
183.81.171.242	53cb3f1e57fbd596463d164d1ca79a14
185.189.58.222	aa0d8b2506376c95ba314e14f08a9b49
220.181.87.80	f8c110929606dca4c08ecaa9f9baf140
210.211.116.246	1727de1b3d5636f1817d68ba0208fb50

Check Point Anti-Bot blade provides protection against this threat:
Worm.Win32.Phorpiex.C
Worm.Win32.Phorpiex.D
Worm.Win32.Phorpiex.H

Source: https://research.checkpoint.com/2019/phorpiex-breakdown/