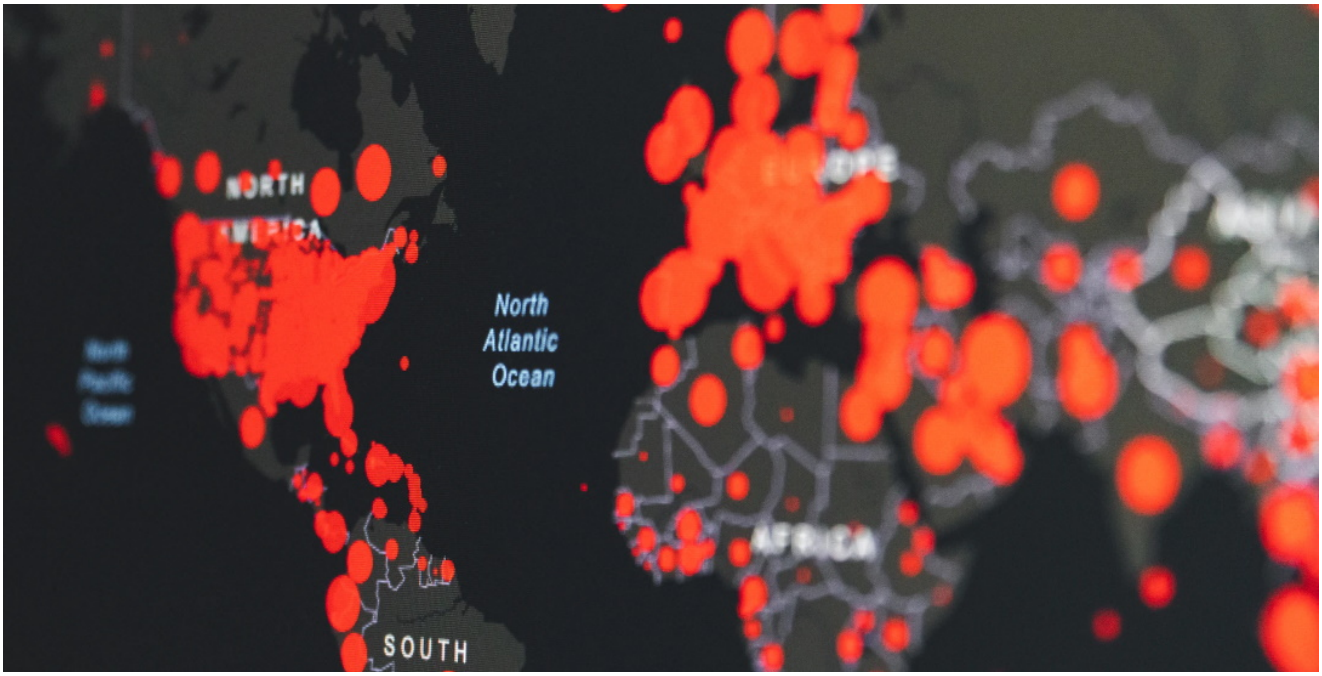
Phorpiex botnet shuts down, source code goes up for sale

therecord.media/phorpiex-botnet-shuts-down-source-code-goes-up-for-sale/

August 27, 2021



The operators of the Phorpiex malware have shut down their botnet and put its source code for sale on a dark web cybercrime forum, The Record has learned.

The ad, posted earlier today by an individual previously linked to the botnet's operation, claims that none of the malware's two original authors are involved in running the botnet, hence the reason they decided to sell its source code.

"As I no longer work and my friend has left the biz, I'm here to offer Trik (name from coder) / Phorpiex (name fomr AV firms) source for sell [sic]," the individual said today in a forum post spotted by British security firm Cyjax.

> The source code for the Phorpiex botnet is being sold on the darknet…👀 pic.twitter.com/GxBsnUacvh
>
> — Cyjax (@Cyjax_Ltd) August 27, 2021

Alexey Bukhteyev, a malware reverse engineer for security firm Check Point, helped *The Record* today confirm the ad's validity.

"The description of the malware is very similar to what we saw in the code," Bukhteyev told us.

The researcher, who previously analyzed the Phorpiex malware back in 2019, said that the malware's command and control (C&C) servers have not been active for almost two months.

Bukhteyev, who has been running a fake Phorpiex bot in order to spy on its activity, told *The Record* that the last command the bot received from the Phorpiex C&C servers was on July 6, 2021, and the command was a self-explanatory "SelfDeletion" instruction.

Since then, the botnet appears to have disappeared from open-source reporting.

"As we know, the source code is private and hasn't been sold before. Therefore, this [forum ad] looks really believable," Bukhteyev told *The Record*.

"However, we can be totally sure if we buy it. The binaries are quite straightforward, and we can easily confirm that the source code is for this bot indeed, if we get it," the researcher added.

"One thing that points to that the seller is likely a real author is: '***Main bot right now is FUD from windows defender***', because all the modules I know currently get AV detections on VT even if they are uploaded there for the first time."

Buyer gets access to all the Phorpiex infected systems too

However, Bukhteyev also warns that even if the botnet C&C servers are down, once someone buys the code, they can set up new ones and hijack all the previously infected systems.

"There are still a lot of infected machines = active bots. We can't definitely say how many, but we constantly see many hits on our gateways," the Check Point researcher added.

However, it is unclear if the botnet will be bought.

There's both an upside and a downside to operating the botnet.

The upside is that the botnet has a tried and tested history of generating profits, primarily through its spam module and cryptocurrency clipboard hijacking feature.

For example, the spam module has helped the botnet's authors generate more than $115,000 in profits from a classic sextortion scheme back in 2019.

The malware has also sold access to its infected bots to ransomware gangs, with the now-defunct Avaddon gang using Phorpiex bots to deploy their ransomware inside corporate networks last year.

"Also, the bot architecture allows the botmaster to passively earn some money from crypto-clipping (changing crypto-currency wallet addresses in the clipboard) even without any active C&C servers," Bukhteyev also said.

The downside is, however, a pretty big one. The botnet isn't as secure as other malware botnets and has often been hijacked by third parties to deploy their own payloads or issue rogue "uninstall" commands, something that may deter buyers.

Additional details on the Phorpiex malware are available on this Malpedia page. Some reports refer to the botnet as Phorpiex, the name given to it by antivirus companies, while others refer to it as Trik, is the name used by the botnet's authors.

The full text of the Phorpiex ad is below:

Hello,

as I no longer work and my friend has left the biz, I'm here to offer Trik

(name from coder) / Phorpiex (name fomr AV firms,) source for sell.

The Trik / Phorpiex botnet is no longer active.

Information about phorpiex:

https://www.microsoft.com/security/blog/2021/05/20/phorpiex-morphs-how-a-longstanding-botnet-persists-and-thrives-in-the-current-threat-environment/

https://research.checkpoint.com/2020/phorpiex-arsenal-part-i/

The main bot and all modules are coded in C++

Visual studio 2008 express projects, only PE infector is vs 2010

Everything is compiled with ignoring default libs and linking of msvcrt.lib

from w2k sdk, to reduce size and make it work on all WINOS

30kb

The bot nor modules trigger any firewall / UAC prompts

Bot works fine on 32 and 64 bit

Main bot right now is FUD from windows defender runtime, its easy to keep it

FUD runtime from windef, I can explain how

Tries to copy to %systemdrive% and create regkey @ HKLM, if this fails it

moves to %userprofile% and create regkey @ HKCU

> The main core of bot (one project) has the following
>
> Installer
>
> USB / rem drive spreader
>
> Loader
>
> Clipper
>
> USB / Remote drive spreader works with creating directory on drive, move all exisiting files from drive in the hidden folder, create shortcut with the name of the drive and drive icon when open the shortcut it will open the hidden folder with all files and the bot, so the user doesnt really notice something is wrong
>
> Clipper support those addresses
>
> LISK
>
> POLKADOT
>
> BITCOIN
>
> WAVES
>
> DASH
>
> DOGECOIN
>
> ETHEREUM
>
> LITECOIN
>
> RIPPLE
>
> BITTORRENT
>
> ZCASH
>
> TEZOS
>
> ICON
>
> QTUM

RAVENCOIN

NEM

NEO

SMARTCASH

ZILLIQA

ZCASH PRIVATE

YCASH

BITCOIN CASH

COSMOS

MONERO

CARDANO

GROESTLCOIN

STELLAR

BITCOIN GOLD

BAND PROTOCOL

PERFECT MONEY $ € BTC

PERFECT MONEY €

PERFECT MONEY BTC

The bot has no panel and checks for files every 30 minutes (can be changed), files 1 – 5

It comes with a signing tool for files, with your private key, bots execute

the files only if the key is right and they can decrypt the file, else it

simple is removed

Bot ddownload and execute the file only if its a new file and doesn't download

execute the same file multiple times

So the logic behind this is simply, you just need to sign the files with your

key and upload them to your websever, bot automatically download, decrypt and execute them

The signing tool has those options

-genkey, generate new keys

-sign, to sign file

-verify, to make sure the file is decrypted fine with current key

Modules:

Spambot

Possible to spam attachment or normal mail

Comes with a PHP script wich simple gives emails or emails with pass each request, the amount can be configured in the script

All you need is to upload the php script and your list to your server

Bot checks for connection on port 25, if connection is ok, it start download the mails in %temp%, read the list, split the mail, connect to MX server directly of the provider else [0.0.0.0] is used

After the list is spammed, the script will rename the list, and output "0" to

stops mailing

VNC Spreader and autoinfector

All you need todo is change direct link to exe in the source, everything else is automatically

Spreader gnerate random IPs, checks for port 5900, if port is open it start

bruteforce and if logged in, it downloads your file with powershell and bitsadmin

PE Infector

All you need to make your botnet bigger is to download it on whole botnet, it will scans all drives including USB and remote drives for .exe files and infect them with ddownload and exec shellcode

Infection works with 32 and 64 bit files

So those modules can be used to make botnet bigger

PE Infector

VNC spreader

Spambot

And it has the .LNK spreader in it

VNC spreader is also good for ransomware, as example alot of firms, schools are affected

The mailer can be used for sextortion and more

https://www.zdnet.com/article/phorpiex-botnet-made-115000-in-five-months-just-from-mass-spamming-sextortion-emails/

> With Trik you only can be richer and your botnet will never shrink
>
> The price for everything with source is 9k$
>
> Garant is no problem, proofs are no problem!
>
> I will fund my account here today too
>
> Kids, timewaster, stay away from me kthx.
>
> First contact – PM.

Tags

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.