New Erbium password-stealing malware spreads as game cracks, cheats

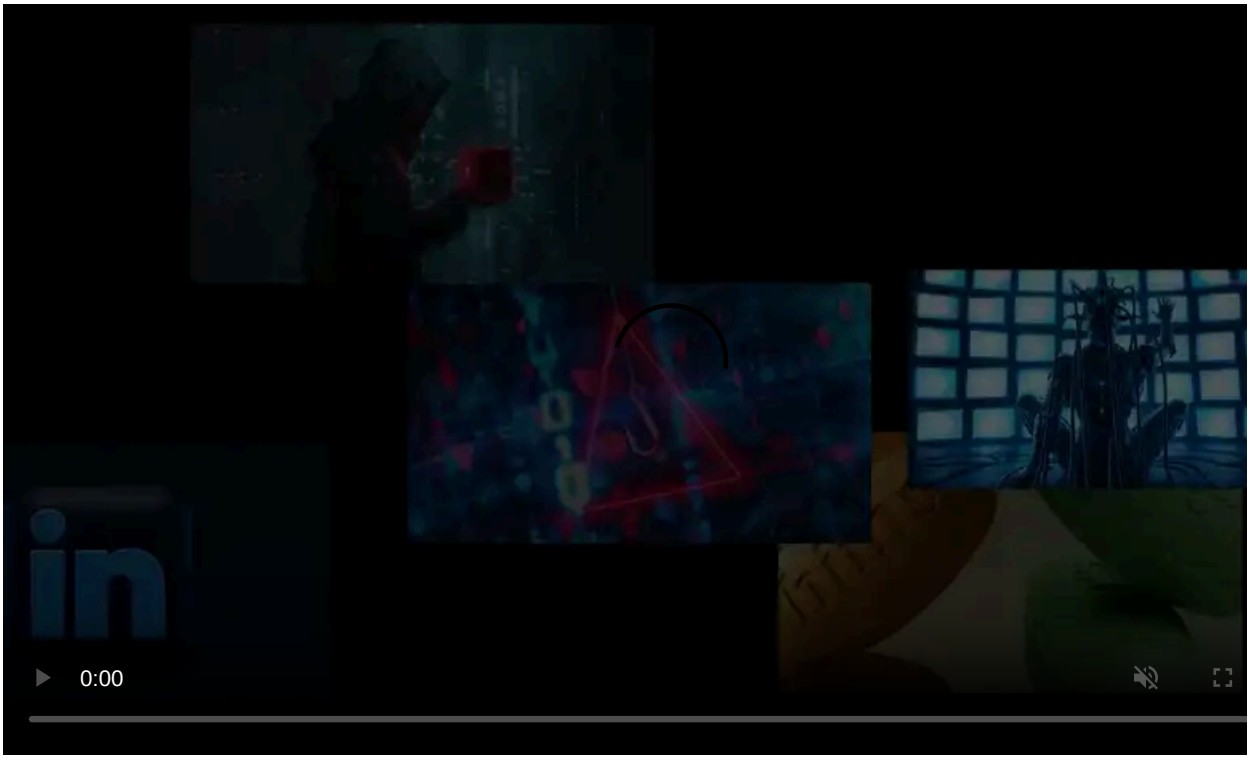
By Bill Toulas

Published: 2022-09-26 · Archived: 2026-04-05 18:45:28 UTC

The new 'Erbium' information-stealing malware is being distributed as fake cracks and cheats for popular video games to steal victims' credentials and cryptocurrency wallets.

Erbium is a new Malware-as-a-Service (MaaS) that provides subscribers with a new information-stealing malware that is gaining popularity in the cybercrime community thanks to its extensive functionality, customer support, and competitive pricing.

Researchers at Cluster25's team were the first to report on Erbium earlier this month, but a new report by Cyfirma shares further information on how the password-stealing trojan is distributed.


0:00

New Malware-as-a-Service operation

Erbium has been promoted on Russian-speaking forums since July 2022, but its actual deployment in the wild has been uncertain thus far.

Erbium initially cost $9 per week, but since its popularity rose in late August, the price went up to $100 per month or $1000 for a full-year license.

Compared to the "defacto" choice in the field, RedLine stealer, Erbium's cost is roughly one-third, so it's aiming to disrupt the market for malware commonly used by threat actors.

Like other information-stealing malware, Erbium will steal data stored in web browsers (Chromium or Gecko-based), such as passwords, cookies, credit cards, and autofill information.

The malware also attempts to exfiltrate data from a large set of cryptocurrency wallets installed on web browsers as extensions.

Extension ID	Crypto browser wallet	Extension ID	Crypto browser wallet
jojhfeoedkpkglbfimdfabpdfjaoolaf	Polymesh Wallet	afbcbjpbpfadlkmhmclhkeeodmamcflc	Math Wallet
hcflpincpppdclinealmandijcmnkbgn	KHC Wallet	fihkakfobkmkjojpchpfgcmhfjnmnfpi	BitApp Wallet
knccchdigobghenbbaddojjnnaogfppfj	iWallet	nanjmdknhkinifnkgdcggcfnhdaammmj	GuildWallet
ijmpgkjfkbfhoebgogflfebnmejmfbml	BitClip	kpfopkelmapcoipemfendmdcghnegimn	Liquality Wallet
bfnaelmomeimhlpmgjnjophhpkkoljpa	Phantom	aiifbnbfobpmeekipheeijimdpnlpgpp	Terra Station
cphhlgmgameodnhkjdmkpanlelnlohao	NeoLine	cnmamaachppnkjgnildpdmkaakejnhae	Auro Wallet
fnnegphlobjdpkhecapkijjdkgcjhkib	Harmony	aeachknmefphepccionboohckonoeemg	Coin98 Wallet
ffnbelfdoeiohenkjibnmadjiehjhajb	Yoroi	pdadjkfkgcafgbceimcpbkalnfnepbnk	KardiaChain
nkddgncdjgjfcddamfgcmfnlhccnimig	Saturn Wallet	acmacodkjbdgmoleebolmdjonilkdbch	Rabby
nhnkbkgjikgcigadomkphalanndcapjk	Clover Wallet	cgeeodpfagjceefieflmdfphplkenlfk	EVER Wallet
dmkamcknogkgcdfhhbddcghachkejeap	Keplr	fhbohimaelbohpjbbldcngcnapndodjp	Binance Chain Wallet
nlgbhdfgdhgbiamfdfmbikcdghidoadd	Byone	nkbihfbeogaeaoehlefnkodbefgpgknn	MetaMask
bcopgchhojmggmffilplmbdicgaihlkp	Hycon Lite Client	hpglfhgfnhbgpjdenjgmdgoeiappafln	Guarda
blnieiiffboillknjnepogjhkgnoapac	EQUA Wallet	amkmjjmmflddogmhpjloimipbofnfjih	Wombat
flpiciilemghbmfalicajoolhkkenfel	ICONex	mnfifefkajgofkcjkemidiaecocnkjeh	TezBox
infeboajgfhgbjpjbeppbkgnabfdkdafs	OneKey	cihmoadaighcejopammfbmddcmdekcje	LeafWallet
lkcjlnjfpbikmcmbachjpdbijejflpcm	Steem Keychain	jbdaocneiiinmjbjlgalhcelgbejmnid	Nifty Wallet
cjelfplplebdjjenllpjcblmjkfcffne	Jaxx Liberty	nlbmnnijcnlegkjjpcfjclmcfggfefdm	MEW CX
fnjhmkhhmkbjkkabndcnnogagogbneec	Ronin Wallet	fhmfendgdocmcbmfikdcogofphimnkno	Sollet
nknhiehlklippafakaeklbeglecifhad	Nabox Wallet	dkdedlpgdmmkkfjabffeganieamfklkm	Cyano Wallet
lodccjjbdhfakaekdiahmedfbieldgik	DAppPlay	onofpnbbkehpmmoabgpcpmigafmmnjhl	Nash Extension
klnaejjgbibmhlephnhpmaofohgkpgkd	ZilPay		

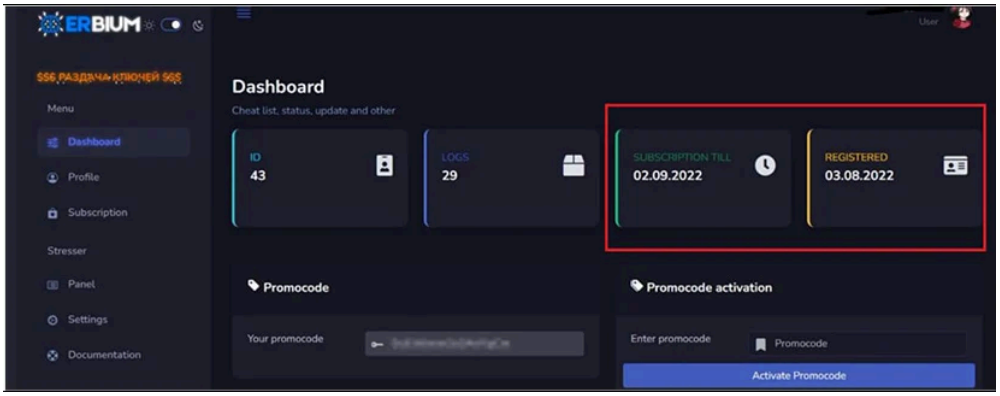
Targeted hot cryptocurrency wallets *(Cyfirma)*

Cold desktop wallets like Exodus, Atomic, Armory, Bitecoin-Core, Bytecoin, Dash-Core, Electrum, Electron, Coinomi, Ethereum, Litecoin-Core, Monero-Core, Zcash, and Jaxx are also stolen.

Erbium also steals two-factor authentication codes from Trezor Password Manager, EOS Authenticator, Authy 2FA, and Authenticator 2FA.

The malware can grab screenshots from all monitors, snatch Steam and Discord tokens, steal Telegram auth files, and profile the host based on the OS and hardware.

All data is exfiltrated to the C2 via a built-in API system, while the operators get an overview of what has been stolen from each infected host on a Erbium dashboard, shown below.

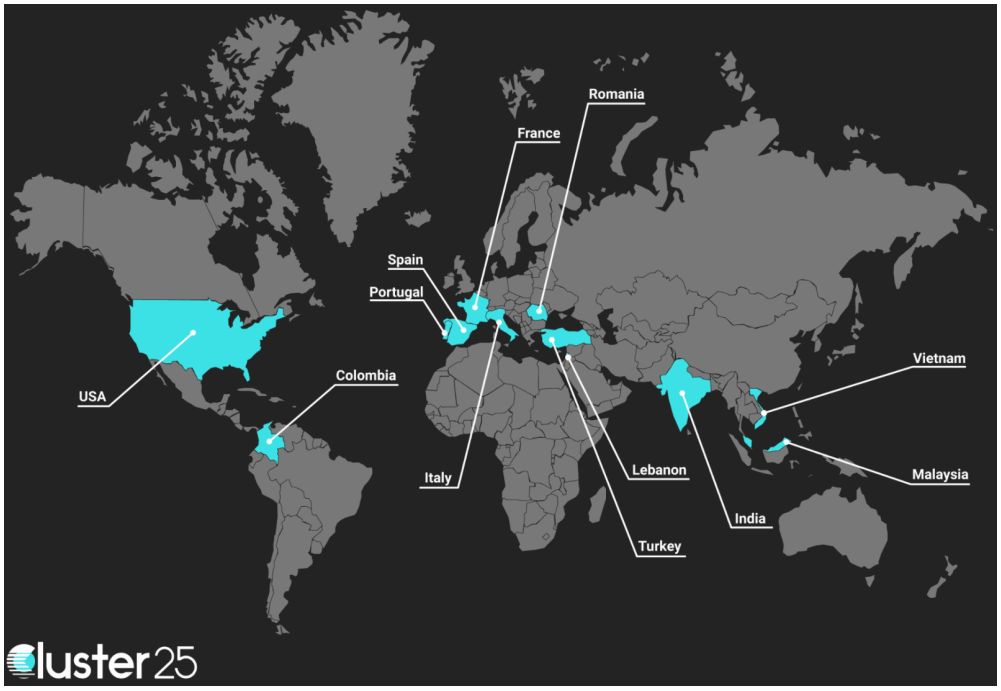


Erbium's dashboard *(Cyfirma)*

The malware uses three URLs for connecting to the panel, including Discord's Content Delivery Network (CDN), a platform that malware operators have heavily abused.

While Erbium is still a work in progress, users on hacker forums have praised the author's efforts and willingness to listen to client requests.

Cluster25 reported signs of Erbium infections worldwide, including in the USA, France, Colombia, Spain, Italy, India, Vietnam, and Malaysia.



Erbium distribution map *(Cluster25)*

While the first Erbium campaign uses game cracks as lures, the distribution channels could diversify significantly anytime, as buyers of the malware may choose to push it via different methods.

To keep the threat out of your system, avoid downloading pirated software, scan all downloaded files on an AV tool, and keep your software up to date by installing the latest available security patches.

Source: https://www.bleepingcomputer.com/news/security/new-erbium-password-stealing-malware-spreads-as-game-cracks-cheats/