Malware Posing as Russia DDoS Tool Bites Ukraine Hackers

blackhatethicalhacking.com/news/malware-posing-as-russia-ddos-tool-bites-ukraine-hackers/

March 11, 2022

by | Mar 11, 2022 | News

Reading Time: 2 Minutes

Malware disguised as a pro-Ukraine cyber-tool could turn around and bite you instead, researchers are warning.

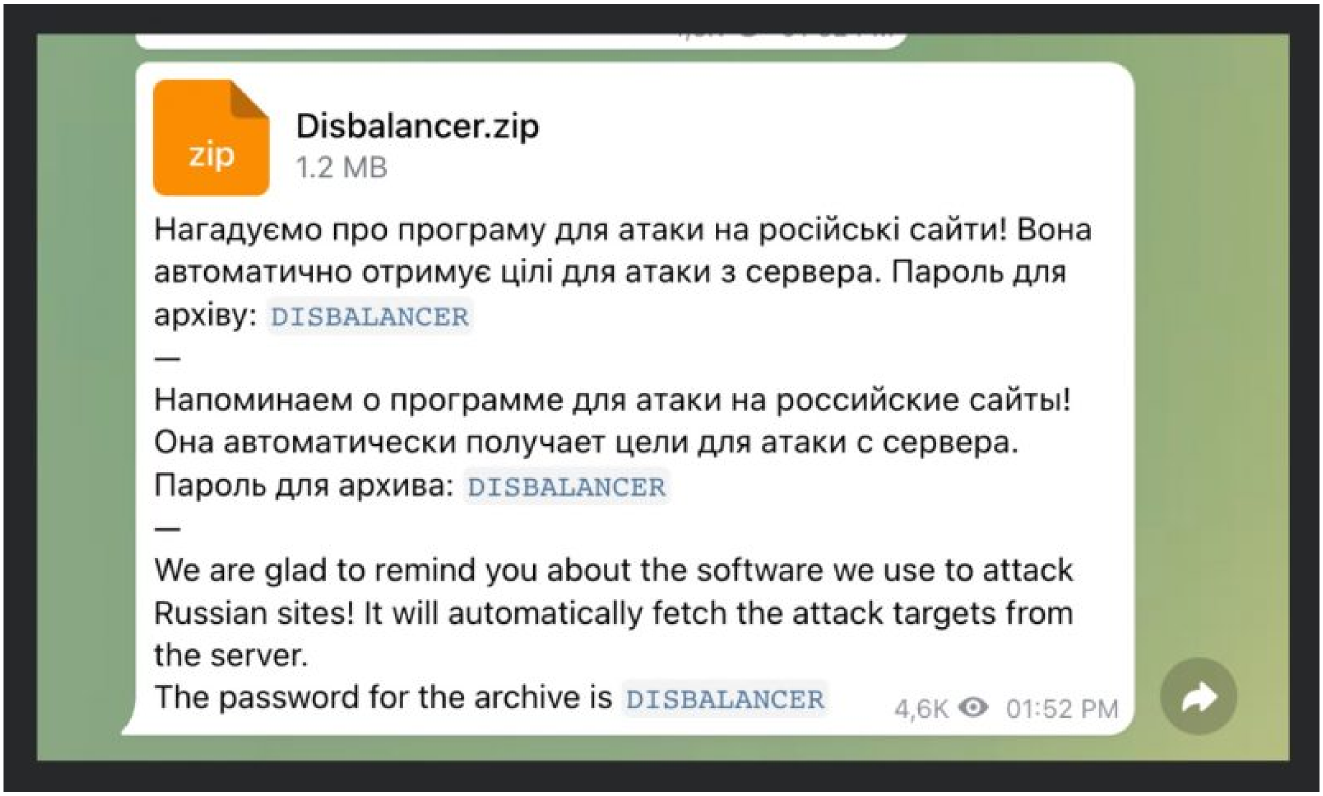
In a Wednesday threat advisory, Cisco Talos described a campaign it's observed in which a threat actor was offering a supposed distributed denial-of-service (DDoS) tool on Telegram, that's purportedly meant to pummel Russian websites.

In truth, the file is actually the Phoenix infostealer that's after credentials and cryptocurrency info, according to researchers.

Phoenix is a keylogger that emerged in the summer of 2019 and which had, within months, turned into a full-fledged infostealer with powerful anti-detection and anti-analysis modules.

Phoenix is a keylogger that emerged in the summer of 2019 and which had, within months, turned into a full-fledged infostealer with powerful anti-detection and anti-analysis modules.

Researchers shared one such Telegram come-on, shown below:



Disbalancer.zip
1.2 MB

Нагадуємо про програму для атаки на російські сайти! Вона автоматично отримує цілі для атаки з сервера. Пароль для архіву: `DISBALANCER`

—

Напоминаем о программе для атаки на российские сайты! Она автоматически получает цели для атаки с сервера. Пароль для архива: `DISBALANCER`

—

We are glad to remind you about the software we use to attack Russian sites! It will automatically fetch the attack targets from the server.
The password for the archive is `DISBALANCER`

4,6K 01:52 PM

Infostealer disguised as a Russian attack tool on Telegram. Source: Cisco Talos.

See Also: Complete Offensive Security and Ethical Hacking Course

“We are glad to remind you about the software we use to attack Russian sites!” the message burbled, waiting to jump on unsuspecting users so as to bleed them of cryptocurrency stored in wallets and MetaMask (a cryptocurrency wallet software commonly associated with non-fungible tokens [NFTs]).

Cyber-Warzone Flooded with New Threats, Hacker Newbies

The malware dressed in sheep’s clothing is just one more wrinkle in the cyber-threat landscape – a landscape that been undergoing seismic shifts leading up to and during Russia’s invasion of Ukraine. The crisis has brought both new threats and an influx of actors “of varying skill,” Cisco said.

For example, the cyber-warzone has entailed the Conti ransomware gang's secrets getting spilled (including a decryptor and TrickBot code) by a pro-Ukrainian member; furious phishing campaigns launched against Ukraine and those aiding Ukrainian refugees; the novel FoxBlade trojan; DDoS attacks against Ukraine's military and economy; campaigns using multiple destructive wipers; hackers affiliating themselves with the Anonymous collective hijacking Russian cameras; and more.

"Many of these changes have been brought about by the rise in attacks being outsourced to sympathetic people on the internet, which brings about its own unique challenges and threats," Cisco outlined. The threat advisory referenced a tweet exhorting people to join an IT army to fight on the cyber-front.

> We are creating an IT army. We need digital talents. All operational tasks will be given here: https://t.co/Ie4ESfxoSn. There will be tasks for everyone. We continue to fight on the cyber front. The first task is on the channel for cyber specialists.
>
> — Mykhailo Fedorov (@FedorovMykhailo) February 26, 2022

See Also: Kali Linux 2022.1 Release with Visual Updates, New Tools, Legacy SSH

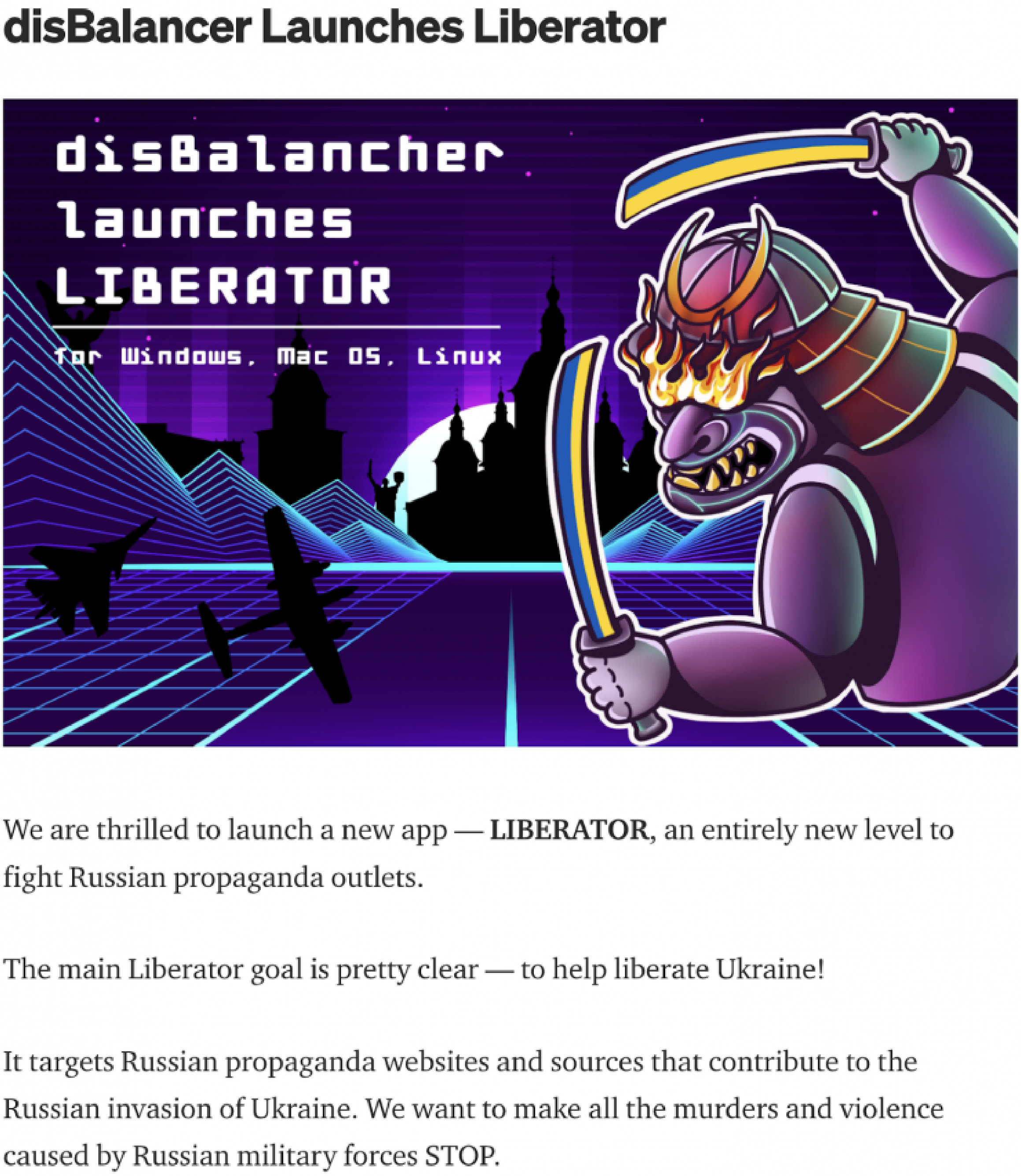
Soldiers on the frontlines get shot at, of course, and soldiers on the cyber-frontlines run the risk of getting arrested. After all, no matter how noble the hacking cause, it's still potentially illegal, Cisco pointed out.

'Legitimate' Disbalancer Liberator DDoS Tool

The malware in the Telegram message brands itself as a "Disbalancer" .ZIP file. There is, in fact, a group called "disBalancer" that distributes a "legitimate" DDoS attack tool called, ironically enough, Liberator, Cisco found – a tool for waging cyberwar against "Russian propaganda websites."

"A quick look at disBalancer's website shows that the actor uses similar language to the malicious message on Telegram…and promises to target Russian sites with the stated goal of helping to 'liberate' Ukraine," according to Cisco's writeup.

The security company offered a screenshot of the brandjacking Disbalancer Liberator website, shown below. As Cisco pointed out, there's a typo in the group's name, which is rendered as "disBalancher."



disBalancer Launches Liberator

We are thrilled to launch a new app — **LIBERATOR**, an entirely new level to fight Russian propaganda outlets.

The main Liberator goal is pretty clear — to help liberate Ukraine!

It targets Russian propaganda websites and sources that contribute to the Russian invasion of Ukraine. We want to make all the murders and violence caused by Russian military forces STOP.

Screenshot from Disbalancer Liberator website. Source: Cisco Talos.

disBalancer's tool – Disbalancer.exe – is sincerely meant to DDoS Russia. The infostealer campaign, on the other hand, is based on a dropper disguised as that tool. It's protected with ASProtect, Cisco said, a known packer for Windows executables.

"If a researcher tries to debug the malware execution, it will be confronted with a general error. The malware, after performing the anti-debug checks, will launch Regsvcs.exe, which is included along with the .NET framework," according to the writeup. "In this case, the regsvcs.exe is not used as a living off the land binary (LoLBin). It is injected with the malicious code, which consists of the Phoenix information stealer."

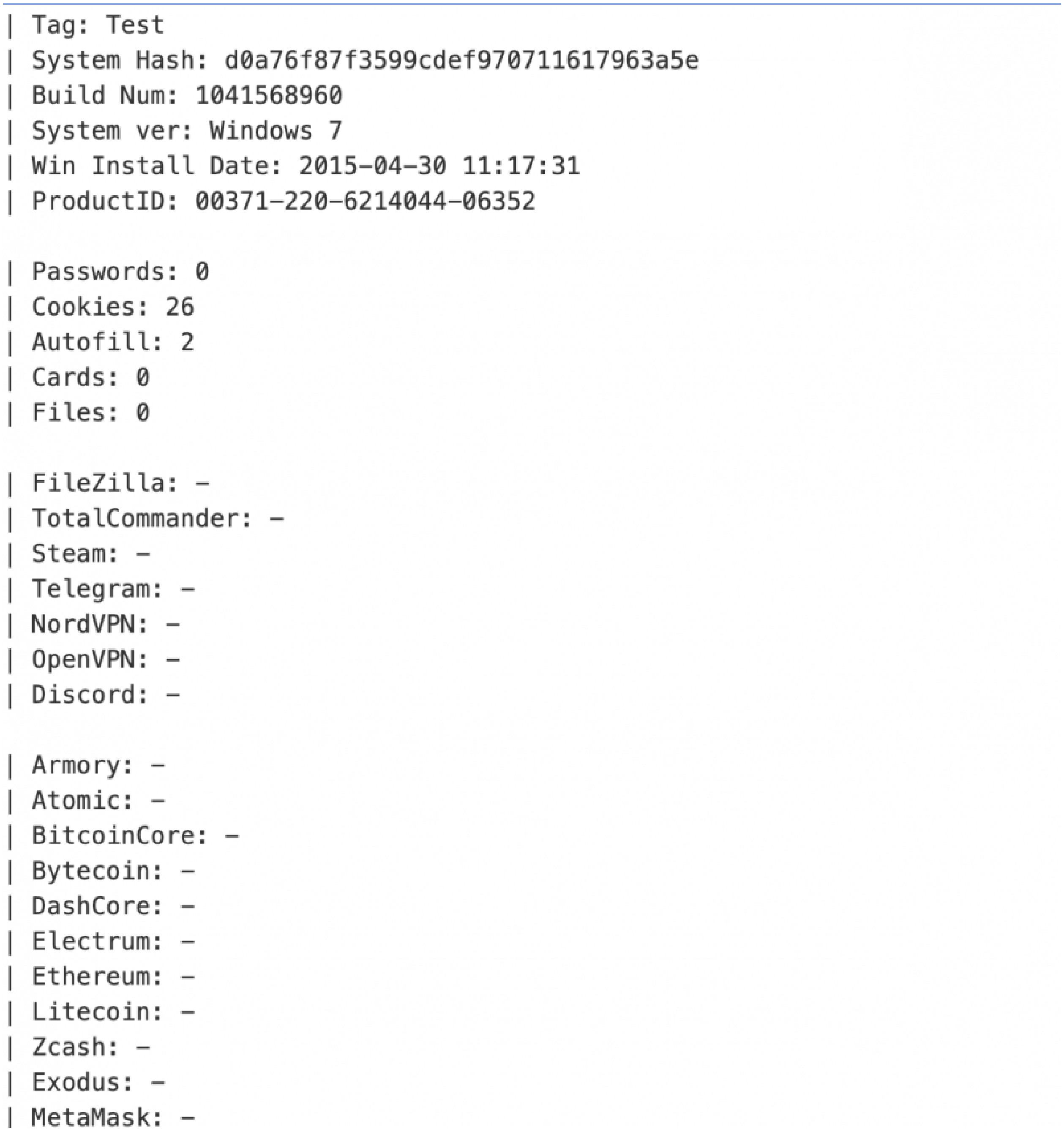
The actors behind this campaign aren’t the newbies flocking to the front lines. Rather, evidence shows that they’ve been distributing infostealers since at least November, Cisco said, as evidenced by the fact that the infostealer exfiltrates stolen info to a remote IP address – in this case, a Russian IP — 95[.]142.46.35 — on port 6666.

That IP/port pair “has been distributing infostealers since at least November 2021,” researchers said. The longevity of the pairing enforces researchers’ belief that these are experienced actors at work, taking advantage of the Ukraine calamity, rather than threat actors new to the scene.

The infostealer is hoovering up a broad array of information, Cisco said. “The .ZIP file provided in the Telegram channel contains an executable, which is the infostealer,” according to the report. “The infostealer gathers information from a variety of sources, including web browsers like Firefox and Chrome and other locations on the filesystem for key pieces of information.”

See Also: Offensive Security Tool: Scapy

The researchers provided a deobfuscated screen capture, replicated below, showing how the pilfered info is sent with a simple base64 encoding. The screen grab shows the breadth of information being pulled off of infected systems, including a large number of crypto wallets and information on MetaMask. “A .ZIP file of the stolen data is also uploaded to the server, completing the compromise,” Cisco said.



```
| Tag: Test
| System Hash: d0a76f87f3599cdef970711617963a5e
| Build Num: 1041568960
| System ver: Windows 7
| Win Install Date: 2015-04-30 11:17:31
| ProductID: 00371-220-6214044-06352

| Passwords: 0
| Cookies: 26
| Autofill: 2
| Cards: 0
| Files: 0

| FileZilla: -
| TotalCommander: -
| Steam: -
| Telegram: -
| NordVPN: -
| OpenVPN: -
| Discord: -

| Armory: -
| Atomic: -
| BitcoinCore: -
| Bytecoin: -
| DashCore: -
| Electrum: -
| Ethereum: -
| Litecoin: -
| Zcash: -
| Exodus: -
| MetaMask: -
```

Sample data exfiltrated to server. Source: Cisco Talos.

Don’t Eat That: You Don’t Know Where It’s Been

The infostealer masquerading as a DDoS tool to attack Russian targets is just one example of the many ways cybercriminals are milking the invasion for social-engineering sustenance, exploiting sympathizers on both sides. “Such activity could take the form of themed email lures on news topics or donation solicitations, malicious links purporting to host relief funds or refugee support sites, malware masquerading as security defensive or offensive tools, and more,” researchers suggested.

In this case, cybercriminals were distributing an infostealer in an apparently profit-motivated campaign. It could have been worse, though, according to the report: “It could have just as easily been a more sophisticated state-sponsored actor or privateer group doing work on behalf of a nation-state.”

Expect this type of situational exploitation to continue and to diversify, Cisco predicted: “The global interest in the conflict creates a massive potential victim pool for threat actors and also contributes to a growing number of people interested in carrying out their own offensive cyber operations.”

Cisco reminded users to essentially avoid eating food that’s been dropped on the floor. You don’t know where that stuff’s been, researchers warned, so be wary of installing software “whose origins are unknown, especially software that is being dropped into random chat rooms on the internet.”

As always, carefully inspect suspicious emails before opening attachments, Cisco advised, and validate software or other files before downloading.

See Also: Hacking stories: MafiaBoy, the hacker who took down the Internet

Source: threatpost.com

Source Link

HACK W/ STYLE
BLACKHAT
ETHICAL HACKING
RED/TEAM
FRONT
BACK
HACKING THE WORLD AND MAKING IT SAFER!
store.blackhatethicalhacking.com