Threat advisory: Cybercriminals compromise users with malware disguised as pro-Ukraine cyber tools

blog.talosintelligence.com/2022/03/threat-advisory-cybercriminals.html

This post is also available in:

Українська (Ukrainian)

Update March 17, 2022: Cisco Talos has updated the IOC section with additional hashes and ClamAV coverage.

Executive summary

- Opportunistic cybercriminals are attempting to exploit Ukrainian sympathizers by offering malware purporting to be offensive cyber tools to target Russian entities. Once downloaded, these files infect unwitting users rather than delivering the tools originally advertised.
- In one such instance, we observed a threat actor offering a distributed denial-of-service (DDoS) tool on Telegram intended to be used against Russian websites. The downloaded file is actually an information stealer that infects the unwitting victim with malware designed to dump credentials and cryptocurrency-related information.

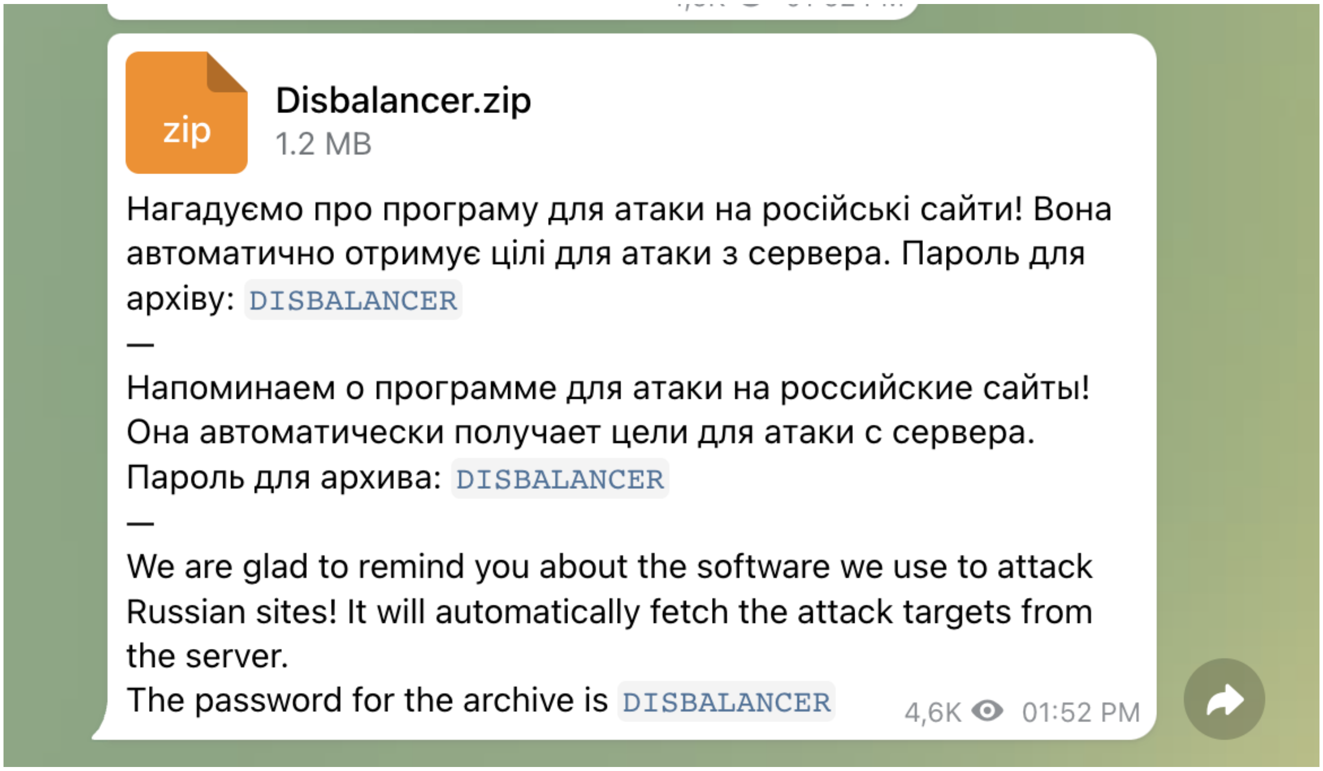
- These observations serve as reminders that users must be on heightened alert to increased cyber threat activity as threat actors look for new ways to incorporate the Russia-Ukraine conflict into their operations.
- Such activity could take the form of themed email lures on news topics or donation solicitations, malicious links purporting to host relief funds or refugee support sites, malware masquerading as defensive or offensive security tools, and more. We remind users to carefully inspect suspicious emails before opening them and validating software or other files before downloading them.

Campaign details

The ongoing situation in Ukraine has quickly changed the cyber threat landscape, introducing an influx of actors of varying skill and a variety of new threats to Cisco customers and users globally. 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 that Cisco Talos outlined in a recent blog.

In one of these new developments, we are seeing cybercriminals take advantage of the conflict by exploiting unwitting users seeking tools to carry out their own cyber attacks against Russian entities. A variety of these tools are advertised as ways to target Russian or pro-Russian websites and have quickly spread on various social media platforms over the last few days as the interest in crowdsourced attacks grows. A simple search for "Ukraine" or "Russia" on some popular open-source platforms returns a wide array of results. Most of the tools that have been released thus far are meant to disrupt various state-affiliated targets through distributed denial-of-service (DDoS) attacks. However, downloading any of these tools can be risky. In addition to the obvious potential legal implications of conducting a self-directed cyber attack, there is no way to know what other hidden features the tool may have or if it's going to operate in its advertised fashion.

One of the main ways we are seeing these types of offerings advertised and distributed is on the Telegram encrypted messaging app, which is extremely popular in eastern Europe and is heavily used by both Ukrainians and Russians. We've seen lots of communications from both sides, including links to Telegram channels associated with various sympathetic groups, such as the IT Army of Ukraine. During our ongoing monitoring of some of these spaces, we found the message shown below.



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

—

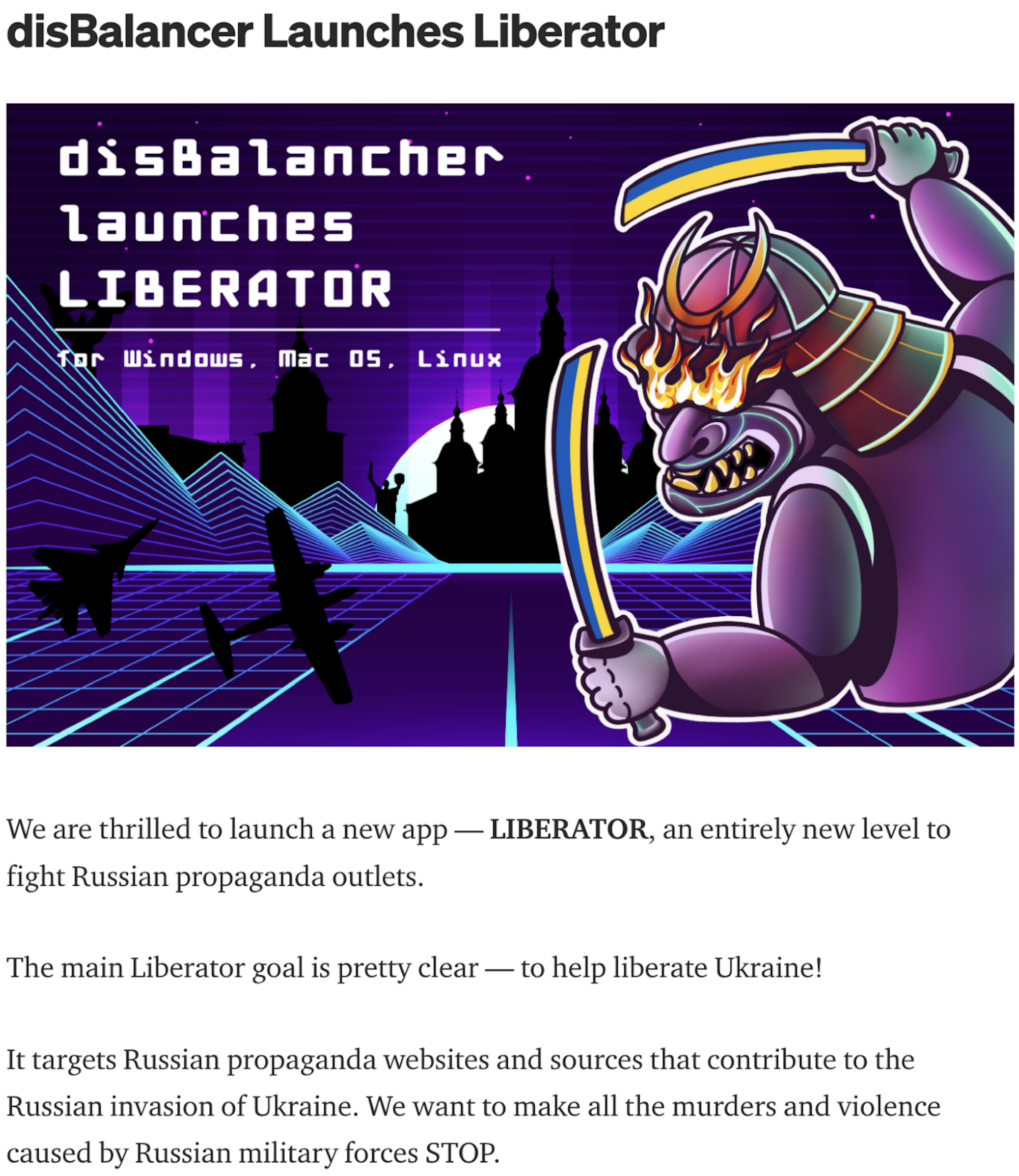
Напоминаем о программе для атаки на российские сайты! Она автоматически получает цели для атаки с сервера. Пароль для архива: DISBALANCER

—

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

Infostealer disguised as a Russian attack tool on Telegram.

There is a tool called "Liberator" that is produced by a group called disBalancer that we found relatively quickly. Liberator is advertised as a tool for performing DDoS attacks against "Russian propaganda websites." A quick look at disBalancer's website shows that the actor uses similar language to the malicious message on Telegram above and promises to target Russian sites with the stated goal of helping to "liberate" Ukraine. A spelling error can be seen in the below graphic from the site, where the group's name is misspelled 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.

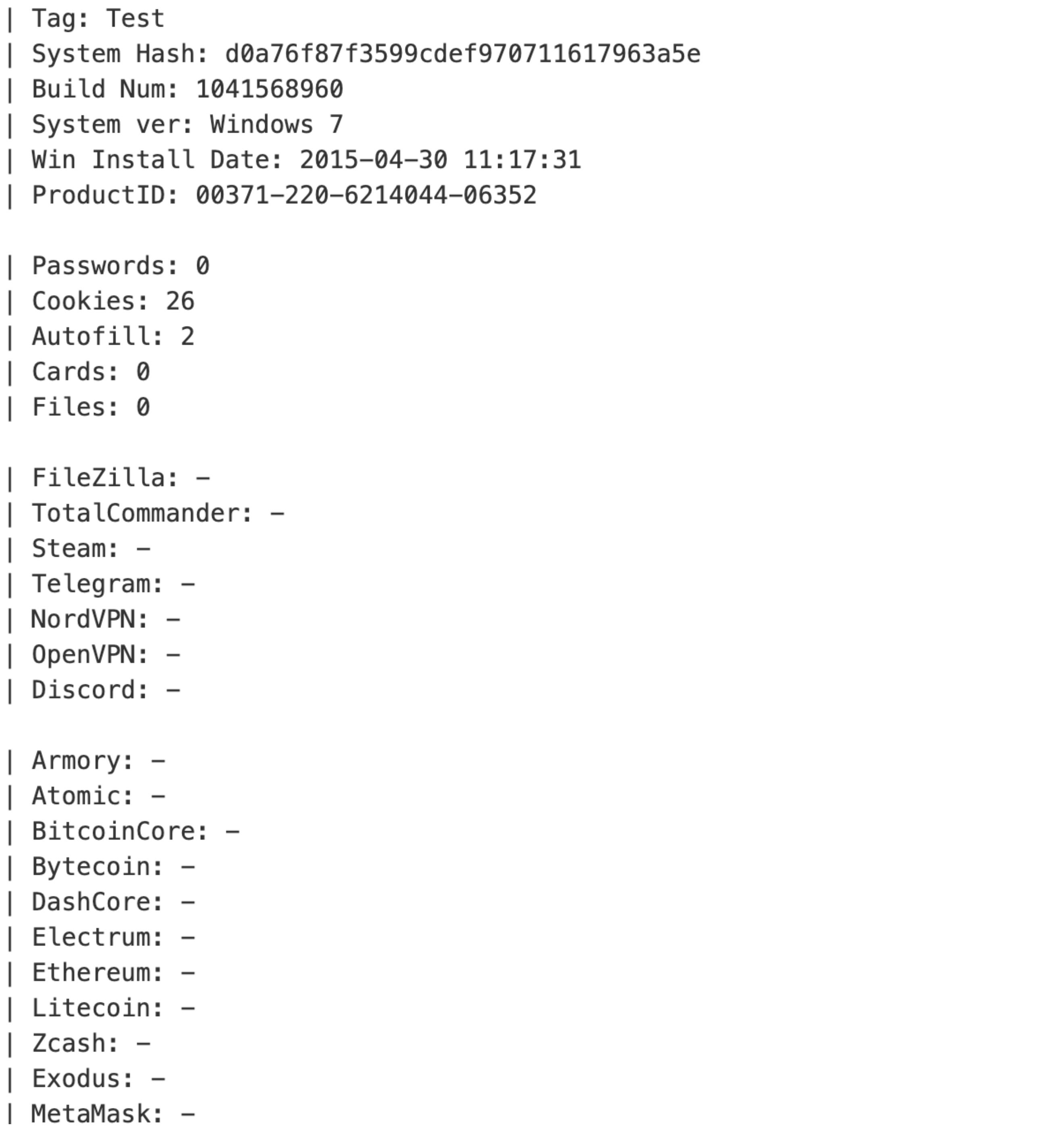
Cisco Talos did some quick analysis of the legitimate Disbalancer Liberator tool shown above and didn't find anything overtly malicious. However, it is effectively a DDoS client that, when used, launches attacks against a list of targets downloaded from a server, something that is potentially illegal. The file offered on the Telegram page ended up being malware, specifically an infostealer designed to compromise unwitting users. The malware in this case dumps a variety of credentials and a large amount of cryptocurrency-related information, including wallets and metamask information, which is commonly associated with non-fungible tokens (NFTs).

This is an example of one of the many ways opportunistic cybercriminals are attempting to take advantage of the Russian invasion by exploiting sympathizers on both sides of the conflict. 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. Users must carefully inspect suspicious emails before opening them and validate software or other files before downloading them.

Infostealer details

The campaign is based on a dropper disguised as the Disbalancer.exe tool. This dropper is protected with ASProtect, 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. 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 activity have been distributing infostealers since at least November 2021. This supports our belief that this is not the work of new actors, but existing actors taking advantage of the war in Ukraine. The ZIP file provided in the Telegram channel contains an executable, which is the infostealer. 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. This information is then sent to a remote IP address, in this case, a Russian IP — 95[.]142.46.35 — on port 6666. This particular IP/port pair has been distributing infostealers since at least November 2021. As shown in the deobfuscated screen capture below, the information, which is sent with a simple base64 encoding, shows the breadth of information being pulled off of the systems, including a large number of crypto wallets and MetaMask (a cryptocurrency wallet software) information. Following the summary, a ZIP file of the stolen data is also uploaded to the server, completing the compromise.



```
| 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 by infostealer.

This is the behavior of modern infostealers. They place increased focus on obtaining cryptocurrency information, as this can be quickly stolen and immediately monetized with a much lower threshold than other types of data that is being stolen, namely credentials themselves.

Pivoting on the sample itself has shown that it is being distributed through other means, using other names including peview.exe and ddos-reaper.exe. We also found other malware samples communicating with this command and control (C2) IP address.

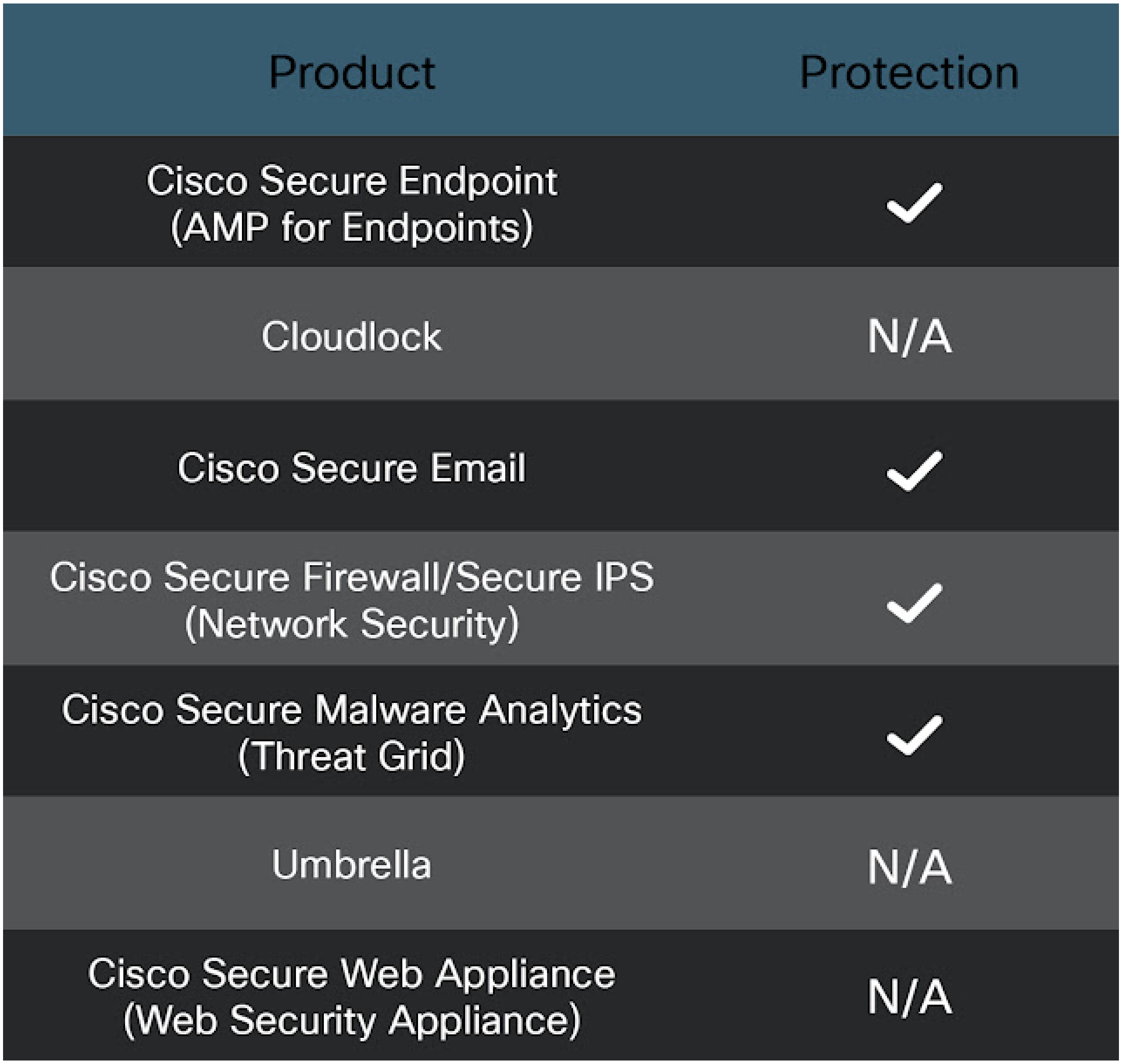
Conclusion

Cisco Talos constantly observes actors using any and all means to get their malware installed on systems, and the war in Ukraine is no exception. In this case, we found some cybercriminals distributing an infostealer, but it could have just as easily been a more sophisticated state-sponsored actor or privateer group doing work on behalf of a nation-state. We remind users to be wary of installing software whose origins are unknown, especially software that is being dropped into random chat rooms on the internet.

Cisco Talos expects this type of behavior to continue and diversify. 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.

Coverage

Ways our customers can detect and block this threat are listed below.



Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	N/A
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	N/A
Cisco Secure Web Appliance (Web Security Appliance)	N/A

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

ClamAV coverage

Win.Trojan.FakeDisbalancer-9941659-0
Win.Trojan.FakeDisbalancer-9941660-1
Win.Trojan.FakeDisbalancer-9941661-0
Win.Malware.Zusy-9812688-0

IOCs

Hashes

33e5d605c1c13a995d4a2d7cb9dca9facda4c97c1c7b41dc349cc756bfc0bd67
f297c69795af08fd930a3d181ac78df14d79e30ba8b802666605dbc66dffd994 (Added 3/10/2022)

Added 3/12/2022:

eca6a8e08b30d190a4956e417f1089bde8987aa4377ca40300eea99794d298d6 (EXE)

705380e21e1a27b7302637ae0e94ab37c906056ccbf06468e1d5ad63327123f9 (ZIP)

IP

95[.]142.46.35 - Port 6666