



Brief

The Underground Economist: Volume 4, Issue 11

B-2024-05-30b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Ransomware, Threat
Actors, Data Leaks, Hacktivism

May 30, 2024

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on May 30, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 11

| New One-Time Purchase Ransomware Announced in Dark Web Forum

On May 26, 2024, well-regarded actor “phant0m” announced a new ransomware tool named “SpiderX” on the English-speaking dark web forum “OnniForums.” The software, which quickly gained traction amongst other forum users, is available for a one-time purchase of USD 150. This is almost certainly perceived as inexpensive, particularly in comparison to more premium RaaS offerings.

- SpiderX is almost certainly an upgraded version of the “Diablo” ransomware, which was released by phant0m in OnniForums in early 2023.
- While SpiderX lacks many of the features expected from ransomware-as-a-service (RaaS) models, it does encompass features likely attractive to threat actors. These include a rarely seen feature that allows attackers to spread the tool via infected USB drives in the initial attack.

SpiderX Ransomware | reliable, undetectable, untraceable

**phant0m**
VIP
★★★★★


Posts: 67
Threads: 10
Joined: Sep 2023
Reputation:

Credits: 449.4 [Donate]

05-26-2024, 03:49 AM (This post was last modified: Yesterday, 03:56 AM by phant0m. Edit Reason: Forgot to add the file stealer option)

Introduction to the SpiderX Ransomware

Hi OnniForums,
After a few months of hard work, I would like to announce the release of my brand new SpiderX Ransomware. It will be successor of my Diablo which served its purpose really well but it is finally time to upgrade the things to a whole new level. SpiderX has all features of Diablo + some new extra which will be from a great advantage to you. The price is \$150. I accept Bitcoin and Monero.

Features of SpiderX:

- ChaCha20-256 encryption algorithm which is the fastest in the world and takes a lot less time than AES-256.
- SpiderX attacks not only the main user folders on the Windows drive, but also all the external partitions, drives, USBs etc. similar to Diablo
- No internet connection is required! Diablo works completely offline and it only needs to be executed then the victim loses all their files in just a few seconds.
- The custom wallpaper is embedded into the payload so this is not some basic script which just downloads all files from a server.
- The ransomware is written in C++ which provides a lot of benefits such as faster execution compared to all other languages like C#, Python etc.
- Very small sizes of the payloads (500-600 KB including the embedded wallpaper)
- Diablo will now be fully persistent and will continue to run silently in the background and will encrypt every new file + if a USB drive or any other external drive is connected after the initial attack, it will also get infected which will be a huge advantage for the attacker.
- Also unlike Diablo, SpiderX comes with a file stealer which will exfiltrate all data from target, compress all to zip and send it to your mega account and then cover all tracks as if the process never happened.

I hope you will like it even more than Diablo. If you have any questions, please let me know, share your opinion and I will be very glad to answer.
If you are interested, please send me a private message. We will be able to do the communication on whatever platform you please Jabber/XMPP, Telegram etc.

phant0m's post on OnniForums

Source: ZeroFox Intelligence

The announcement of SpiderX contributes to a broader upward trajectory in the number of English-speaking ransomware offerings observed in deep and dark web (DDW) marketplaces. This trend is very likely facilitating English-speaking actors who are unable to negotiate with larger, mostly Russian-speaking RaaS groups.

- So far in 2024, ZeroFox has observed the announcements of several new English-speaking ransomware offerings, including Diablo, "Nevermore," "Wing," and the prominent "RansomHub."
- Whilst some actors desire to work alone, some English-speaking actors are not able to negotiate with larger Russian-speaking RaaS groups. This is very likely due in part to low levels of trust amongst threat actors, as well as a perception of inferiority and incompetency.

As well as English-speaking ransomware offerings, one-time purchase models are also very likely on an upward trajectory in both English and Russian-speaking DDW forums. Due to the lower price, these options are very likely attractive to a higher number of would-be threat actors. However, compared to larger RaaS offerings, one-time ransomware purchases have significantly fewer capabilities and features. This very likely hinders many less technically competent actors from engaging in ransomware and digital extortion (R&DE) activity.

- The majority of prominent RaaS offerings contain customer-service features such as a support programme and instructions for use. Additionally, they offer more advanced software features, primarily surrounding secure encryption and exfiltration, and defense evasion measures.
- While the gap between subscription and one-time purchases remains significant, it is very likely to continue reducing as more options become available, and garner more interest, enabling further development. Furthermore, threat actors may be attracted to their low-profile approach, particularly in the wake of numerous 2024 law enforcement (LE) disruptions.

The proliferation of low-cost, one-time purchase ransomware models will very likely offer increased accessibility for English-speaking actors who wish to engage in R&DE activity outside of a large threat collective and away from the prominent Russian-speaking forums. This is very likely to contribute to the increasingly diverse R&DE threat landscape, the techniques, tactics, and procedures (TTPs) being observed, as well as a growing number of total ransomware incidents.

However, while threat actors leveraging this ransomware almost certainly pose a threat to organizations across regions and industries, they are almost certainly unable to conduct attacks at the frequency or scale of larger RaaS groups.

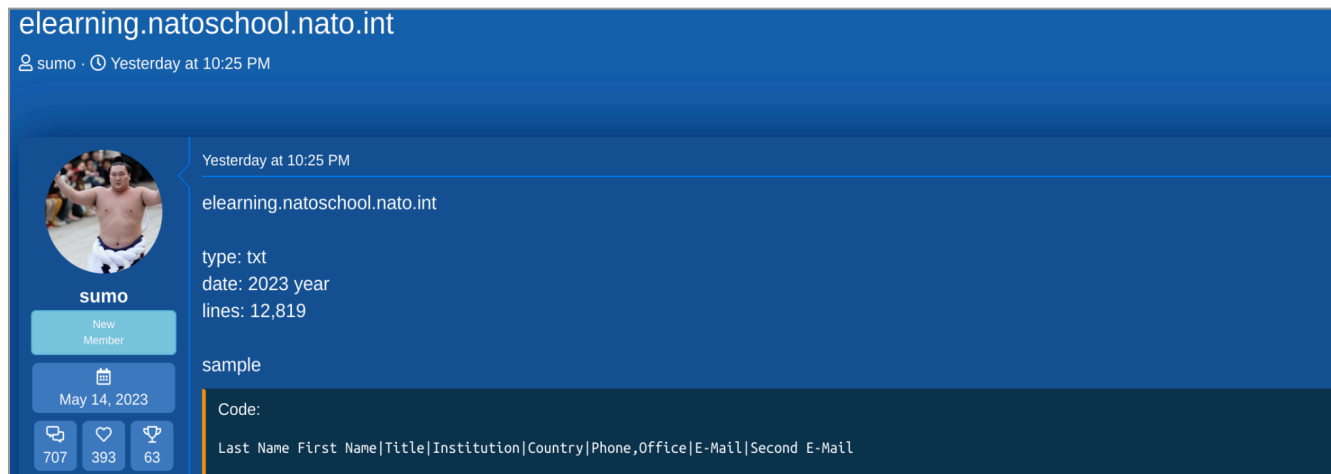
| NATO Data Leak Shared on Deep Web Forum

On May 19, 2024, threat actor “Sumo” announced a data leak pertaining to a NATO school’s e-learning platform on the Russian-speaking deep web forum “Cronos”. The data is available to all Cronos forum members who have paid for account privileges and could very likely be leveraged in various types of malicious social engineering activity.

- Sumo is a well-regarded, prolific distributor of data leaks in DDW forums, posting information stolen from both Western and Russian victims.
- The stolen data is primarily personally identifiable information (PII) such as names, titles, military ranks, institutions, countries, and contact information, likely pertaining to both military and civilian staff and e-learning students.

Cronos was created in 2022 and is focused on data breaches and hosting unique leaks, as well as republishing those from other forums. There is a roughly even chance that Cronos will increase its traffic and popularity following the recent closure of BreachForums.

- On May 15, 2024, the English-language DDW forum BreachForums was seized in an operation coordinated by multiple international LE agencies.
- Since mid-2023, BreachForums has been one of the most popular DDW marketplaces, hosting discussions surrounding the trading of illicitly-obtained goods.



Sumo's post on the forum Cronos

Source: ZeroFox Intelligence

It is likely that the data breach originated from an SQL injection vulnerability that was privately advertised for sale on Telegram in January 2024. The vulnerability allegedly implicated an unknown NATO entity.

- An SQL injection is a code injection technique used to attack data-driven applications that use SQL databases. It exploits security vulnerabilities in web applications that construct SQL statements from user input without properly sanitizing or validating that input.

It is very likely that the intended use of this data is social engineering and other fraudulent activity, with a likely chance it has already been leveraged in attacks by financially-motivated threat actors. There is also a smaller possibility that the information can be leveraged in geopolitically or ideologically-motivated espionage activity by state-associated actors.

| First Potential BreachForums Successor Announced

On May 16, 2024, threat actor “USDoD” announced on X their intent to launch a new, open-source data breach forum named “Breach Nation”. USDoD claimed that Breach Nation would use two separate domains, breachnation[.]io and databreached[.]io, with a planned launch date of July 4, 2024.

- USDoD has previously been referred to as “NetSec” in malicious forums and has allegedly been responsible for data breaches targeting numerous, primarily Western organizations.
- The actor had previously announced their retirement from cybercriminal activities in an April 21, 2024, DDW post.

My goal is to revive the community and provide opportunities for everyone. I am not affiliated with the old staff, but I promise to do a better job and keep the legacy alive.

I am not concerned with who is in charge at the Department of Justice or who the FBI director is. My focus is on keeping the system running.

Regarding the CDN with all databases, I have a plan. I cannot promise to have a full CDN at launch, but I am working on it.

At present, I am the sole admin and staff member. I am aware of individuals who were active previously, but for now, I do not plan to appoint anyone as staff for security reasons and due to a limited circle of trust.

I appreciate all the support and feedback. If a significant portion of the community dislikes the domain, I am open to providing a new one. Your feedback is crucial in every decision.

To make things right, I need the community on my side. You don't need to be staff to have a voice or to help us in this new phase. It will be a process, and everyone is welcome.

Best Regards, USDoD, a perpetual Threat Actor

USDoD announces the launch of Breach Nation

Source: [hXXps://x\[.\]com/EquationCorp/status/1791077909999886503](https://x[.]com/EquationCorp/status/1791077909999886503)

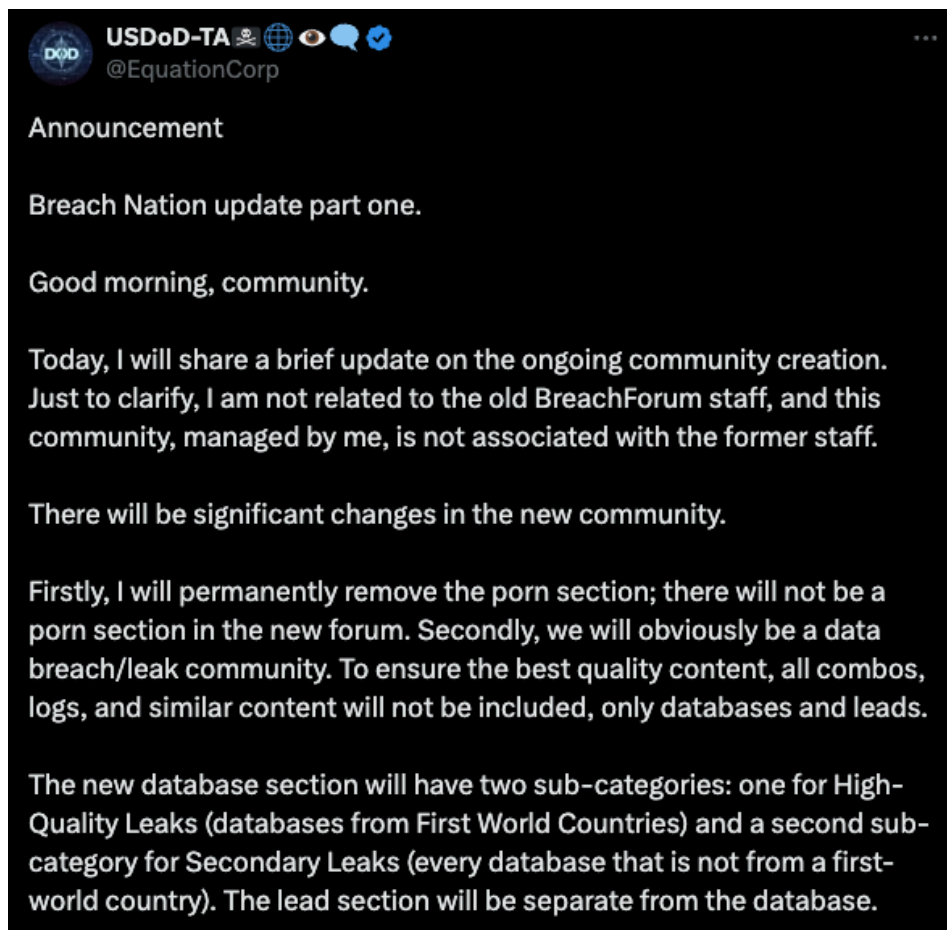
USDoD stated their intent for Breach Nation to serve as a successor to “BreachForums”, where USDoD was almost certainly a prominent figure—despite denying any affiliation with BreachForum moderators.

- BreachForums was a popular forum consisting of open source and DDW domains, as well as an instant messaging platform. It was severely disrupted on May 15, 2024, by a LE operation that seized the forum’s [.]st domain, a [.]onion domain, and a Telegram channel.
- ZeroFox observed unconfirmed reports that the platform’s moderator, known as “Bapohmet,” was arrested.

USDoD claims to be working alone on the production of the new forum, stating that they are not currently seeking to recruit moderators or other staff due to “a limited circle of trust.” This is very likely a reflection of uncertainty amongst DDW communities stemming from recent LE activity, as well as USDoD’s likely limited trusted network.

Further detail surrounding the structure, intent, and use of Breach Nation was provided in a second post on May 20, 2024. USDoD detailed two changes that they deemed significant. The post claimed that regular updates as to the forum’s status will be provided in subsequent X posts.

- Unlike BreachForums, Breach Nation will not include a pornography section.
- To ensure the “best quality” content, “combos, logs, and similar content” will not be allowed—only databases and “leads.” The data breach/leak section will be broken down into two sub-categories: one for high-quality leaks associated with first-world victims and one for all other victims.
- A market section will also be available once an escrow system is established, as well as a threat intelligence section that will reportedly use XenForo software.

**USDoD provides insight as to intended Breach Nation features**

Source: [hXXps://x\[.\]com/EquationCorp/status/1792571853904511048](https://x.com/EquationCorp/status/1792571853904511048)

USDoD stated that the first 200,000 individuals to become members will receive an upgraded member rank. It is not clear what privileges this will enable. Once the site has a “good amount” of users, the community will transition to an invite-only model. The criteria for granting a member this privilege is unclear at the time of writing.

There is a roughly even chance that Breach Nation will become a popular tool for threat actors seeking to discuss TTPs related to data breach attacks, publicize results, and sell stolen information. It is likely that, in the coming months, other BreachForums members, moderators, and staff will seek to capitalize upon its disruption by creating and advertising new forums.

| GhostSec Announces Return to Hacktivism

On May 15, 2024, “GhostSec” announced on its official Telegram channel its intention to abandon financially motivated cybercrime and resume hacktivism activities. According to the statement, the group’s current “services” and Telegram channel will be closed, as it has “obtained enough funding” to enable future hacktivism operations.

- GhostSec first came to prominence in 2015 as an offshoot of the “Anonymous” collective, with an initial aim of combating the Islamic State of Iraq and Syria (ISIS).

GhostSec has almost certainly been focused primarily on politically and ideologically motivated hacktivism activity since 2015.

- Since approximately Q3 2023, GhostSec has been conducting financially motivated cybercrime activities leveraging GhostLocker malware. This temporary shift in focus and tactics was almost certainly undertaken to amass enough funding to enable the group to eventually shift back to focusing on politically-motivated activity and resume targeting of its ideological opposition.
- In the statement, GhostSec alluded to its intention to provide an educational hacking course to forum members but appeared undecided on the content.

GhostSec

We'd like to announce GhostSec's leave from the financial motivation "CyberCrime" Scene. We as Ghosts have obtained enough funding through our times to continue funding our operations for a while we deem the cybercrime and ransomware we once promoted no longer necessary and will shift back to pure hacktivism what does this mean?

All this means is that we will not be providing services anymore therefore the Ghostsec services channel and services once provided will be closed, The ransomware Ghostlocker will be closed Though we will provide the entire code of V3 to Stormous and shift all buyers from GL to the new Stormous locker making it a clean exit without any exit scam. Five families will be taken over and Stormous will be in charge with the new associates involved in that organization resulting in our complete retirement from the "cybercrime" and ransomware scene!

What will remain? At the moment we will continue to keep our private channel and chat room available and will be running a discount from today until may 23rd, Get lifetime access to the private channel and chat room for \$400 \$250 ONLY until may 23rd. We may also plan soon to make and provide a hacking course/package though we are still debating on making this hack like a ghost course.

Thank you for your constant support, love and understanding. We are very excited to continue and put all focus into our work in changing the world to becoming a better place!

Fight for something you believe in and truly find it for yourself. Chase your own freedom, dreams and goals. Then Pass it on to the future.

Hack the planet!!
We Run Shit Cause We Can!
~GhostSec0

GhostSec announcement on its Telegram channel

Source: ZeroFox Intelligence

Since the outbreak of the Israel-Hamas war, GhostSec has been vocal in its support for Palestine, targeting Israeli critical national infrastructure and organizations.

- GhostSec conducted its first attack intended to harm Israel back in May 2022. Attacks have continued since then to the present.
- GhostSec has also conducted attacks against nations such as Russia, Iran, and France. The array of nations GhostSec has targeted shows no geopolitical trend, and it is very unlikely the group has any wider allegiance.



GhostSec announcing attacks conducted against Israel

Source: [hXXps://www.uptycs\[.\]com/blog/ghostlocker-ransomware-ghostsec](https://www.uptycs[.]com/blog/ghostlocker-ransomware-ghostsec)

GhostSec is a member of the “Five Families,” a collective of hacking groups that have conducted financially, ideologically, and politically motivated attacks against industries across the globe. Aside from GhostSec, the Five Families collective consists of the hacktivist groups “ThreatSec” and “SiegedSec” and the ransomware group “Stormous,” as well as “Blackforums,” a DDW forum used for illicit discussion and trading. In December 2023, SiegedSec was allegedly removed from the Five Families following the post of a statement appearing to promote pedophilia.

- The Five Families has conducted attacks against a diverse array of organizations across regions and industries. Despite their collaboration, the individual collectives are unlikely to be geopolitically or ideologically aligned.



GhostSec announce its intention to focus on hacktivism activities

Source: ZeroFox Intelligence

In the statement, GhostSec alleged that the “GhostLocker” malware, along with all associated affiliates, will be taken over by fellow Five Families member Stormous. According to GhostSec, this approach will ensure a “clean exit” with no exit scam activity.

- GhostLocker is a RaaS operation that came to prominence in late 2023 and is reportedly available for USD 269.99 per month. GhostLocker versions 2.0 and 3.0 have almost certainly been leveraged by the Stormous ransomware collective in past digital extortion attacks.

GhostSec's resumed focus on hacktivism is very likely enabled by its financial success in leveraging GhostLocker in R&DE activity. In the short to medium term, GhostSec is likely to attempt disruptive and undermining attacks against the Israeli government, as well as other state institutions that are politically and ideologically misaligned with the group.

| Recommendations

- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Implement secure password policies with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management process and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Proactively monitor for compromised accounts being brokered in DDW forums.
- Configure ongoing monitoring for Compromised Account Credentials.

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

Sources may use

TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

Amber

Sources may use

TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW MAY IT BE SHARED?

Recipients may NOT share

TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Recipients may ONLY share

TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that

TLP:AMBER+STRICT restricts sharing to the organization only.

Green

WHEN SHOULD IT BE USED?

Sources may use

TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

Clear

Sources may use

TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW MAY IT BE SHARED?

Recipients may share

TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

Recipients may share

TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%