



| Flash |

New One-Time Purchase Ransomware Announced in Dark Web Forum

F-2024-05-30a

Classification: TLP:CLEAR

Criticality: Medium

**Intelligence Requirements: Deep and Dark Web, Ransomware, Threat
Actor**

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 09:00 AM (EDT) on May 30, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

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

> Key Findings

- 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.
- The announcement of SpiderX contributes to a broader upward trajectory in the number of both English-speaking and one-time purchase ransomware offerings observed in deep and dark web (DDW) marketplaces.
- 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 ransomware-as-a-service RaaS groups.

| Details

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, subscription-based RaaS offerings.

- SpiderX is almost certainly an upgraded version of the “Diablo” ransomware, which was released by phant0m in OmniForums in early 2023.
- While SpiderX lacks many of the features offered by 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
★★★★★
 — 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)

#1

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 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 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 increasingly 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 an 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.

Recommendations

- Develop a comprehensive incident response strategy, including the use of trusted third parties to assist with impact mitigation, communications, and ransom negotiations.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Implement secure password policies with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- 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.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system and ensure all business IT assets are updated with the latest software as quickly as possible.
- Proactively monitor for compromised accounts being brokered in DDW forums.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	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.	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	Clear
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.	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%