



| Flash |

New Ransomware-as-a-Service Operation Claims Innovative Features

F-2024-04-25a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware, DDoS, Threat Actor Activity

April 25, 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 12:00 PM (EDT) on April 24, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | New Ransomware-as-a-Service Operation Claims Innovative Features

> Key Findings

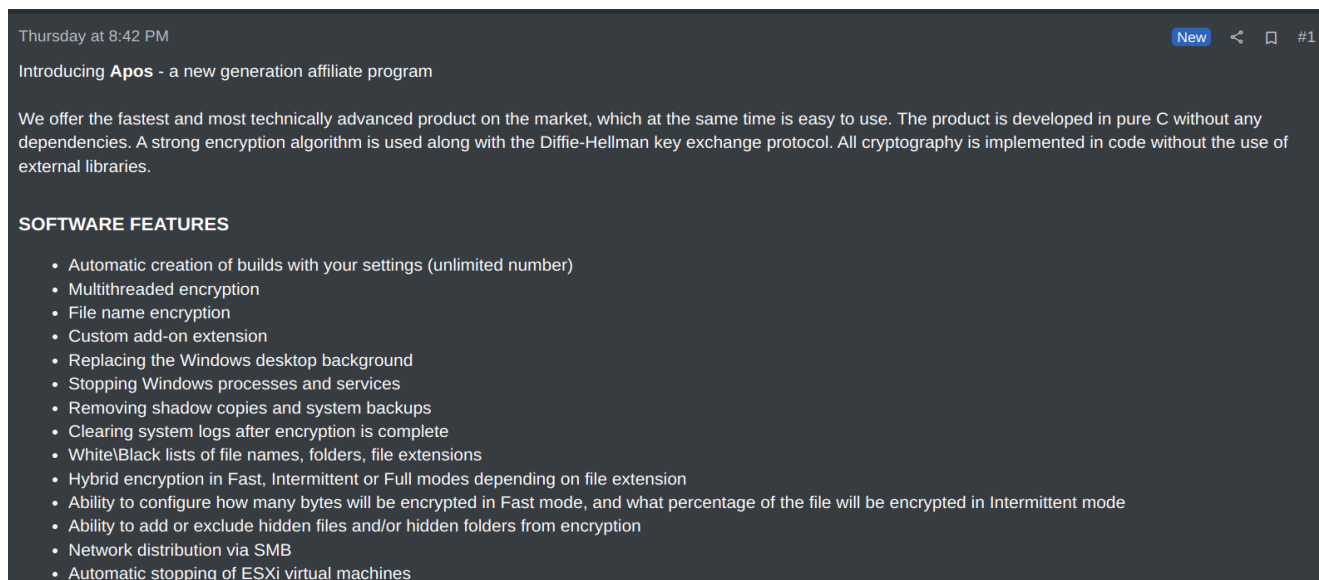
- On April 19, 2024, positive-reputation threat actor “Bezzle” announced a new ransomware-as-a-service (Raas) operation named “Apos” in the Russian-speaking deep and dark (DDW) community RAMP. Bezzle proclaims Apos is the “fastest” and “most technically advanced” product on the market.
- Apos purportedly has many software features that are typically only observed amongst the more advanced Raas offerings. The service also includes highly uncommon capabilities, which is very likely indicative of an attempt to separate the Apos service from its competition and appeal to potential affiliates.
- Raas offerings are very likely to become increasingly competitive during 2024, with collectives offering affiliates more software features, better technical support and digital infrastructure, higher payouts, and loyalty incentives.

| Details

On April 19, 2024, positive-reputation threat actor Bezzle announced a new Raas operation named Apos in the Russian-speaking DDW community RAMP. Bezzle proclaims Apos is the “fastest” and “most technically advanced” product on the market.

Similar to other RaaS offerings, Apos offers a bespoke victim negotiation platform, a dedicated victim leak site, and support from Bezzle. The post claims that affiliates are able to retain 90 percent of any ransom payouts, with Bezzle taking 10 percent. While 90 percent is almost certainly higher than average RaaS offerings, this has become more common during 2024, particularly amongst newer RaaS collectives.

- Bezzle further specifies that any affiliate able to generate USD 1 million will be able to negotiate more favorable terms, though details are not specified. Such affiliates will also be authorized to leverage Apos infrastructure to conduct denial-of-service (DoS) attacks.



RAMP post by Bezzle advertising Apos software features

Source: ZeroFox Intelligence

The announcement specifies a list of software features and capabilities supposedly included in the service, many of which, while not necessarily innovative, are almost certainly offered primarily by more advanced Raas platforms that are designed to compromise Windows-based systems. These features include:

- The software being written entirely in the programming language C
- No dependencies or external library requirements
- An unlimited, automatic creation of builds with customizable user settings
- The removal of shadow copies and system backups

- The ability to stop Windows process and services

- Ability to add a note to specific folders, even if they do not contain encrypted files
- Customizable process name displayed in Task Manager
- Work in the background (without any visual elements)
- Protection against re-encryption of already encrypted files
- Encrypting Windows builds to bypass Antivirus solutions*

Encryption modes :

Fast mode encrypts the first N bytes of the file.

Intermittent mode encrypts a specified percentage of all bytes in a file, distributing encrypted stripes evenly throughout the file with a specified segmentation.

Full mode encrypts the entire file.

Command line arguments allow you, if necessary, to overwrite some of the settings specified when creating the build. You will find a more detailed description of all product features in the User Guide.

Supported platforms :

Windows XP - 11 (x86 and x64)

Windows Server 2003 - 2022 (x86 and x64)

All x64 Linux distributions, and all major x86 Linux distributions

All x64 ESXi, BSD and NAS

Continuation of RAMP post by Bezzle advertising Apos software features

Source: ZeroFox Intelligence

Some of the claimed features are less common, however, and are very likely indicative of an attempt to separate the Apos service from its competition and appeal to potential affiliates. The first of these is Network distribution via SMB. This very likely refers to the attacker's ability to conduct lateral movement within the target network by exploiting vulnerabilities within Microsoft Windows Server Message Block, enhancing persistence.

The “protection against re-encryption of already encrypted files” is also a feature rarely seen in new Raas offerings. This is almost certainly intended to serve as a safeguard against competing ransomware and digital extortion (R&DE) operatives, as well as any other threat actors who have gained simultaneous illicit access to the victim's network. There are numerous ways in which this could occur, with the following being the most likely:

- The threat actor buys illicit network access from an initial access broker (IAB) in a DDW forum. In some cases, a threat actor can ensure that they are the sole buyer of the access, paying an often-premium price to ensure that the access is subsequently removed from the market. In the majority of cases, however, these sales are not limited to a single buyer, with the attack becoming a “first come, first served” opportunity.

- A software vulnerability that enables illicit network access becomes common knowledge within DDW forums, enabling numerous R&DE affiliates to conduct attacks. However, it is very likely that the majority of these instances do not result in the same networks being targeted but, rather, different organizations operating the same vulnerabilities.

CONDITIONS

- All payments are made to your wallet
- Leak site
- A platform for communicating with companies. You can negotiate on your own or with our help
- 24/7 support
- Until reaching \$1M we take 10%

After reaching the total amount of \$1M, the following services will become available to you:

- DDoS attacks
- Ringing

All conditions are individual and subject to change.

Spoiler: ONE

Apos Security

RAMP post by Bezzle advertising Apos

Source: ZeroFox Intelligence

There is a very likely chance that these circumstances will arise more frequently within DDW forums over the coming months, due primarily to the instability that ensued following the disruption of both ALPHV and LockBit in Q4 2023 and Q1 2024, respectively. The cessation of their operations is almost certain to have led to the increasing number of active R&DE collectives observed by ZeroFox and to growing competition between both RaaS offerings and affiliates caused by an increasingly fragmented R&DE ecosystem.

It is very likely that RaaS operators anticipate a void in the R&DE marketplace where ALPHV—and to a lesser extent LockBit, which continues to conduct limited activity—used to dominate. RaaS offerings are very likely to become increasingly competitive during 2024 as a result, with collectives offering affiliates more software features, better technical support and digital infrastructure, and higher payouts and loyalty incentives. At

the time of writing this report, ZeroFox has observed no Indicators of Compromise (IoCs) associated with Apos ransomware.

| Recommendations

- 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.
- Leverage cyber threat intelligence to inform detection of R&DE threats and their associated tactics, techniques, and procedures (TTPs) and IOCs.
- 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 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.
- Configure ongoing monitoring for Compromised Account Credentials.

| 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%