



| Flash |

Introducing Wing, New Ransomware-as-a-Service

F-2024-01-30c

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware, Deep & Dark Web, Threat Actors

January 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 (EST) on January 30, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Introducing Wing, New Ransomware-as-a-Service

› Key Findings

- On January 28, 2024, positive-reputation English-speaking actor “blackhunt” announced a new Ransomware-as-a-Service (RaaS) operation known as Wing on the predominantly Russian-speaking dark web forum RAMP; it is the first RaaS launched on the forum in 2024.
- Wing is touted as a state-of-the art ransomware tool with multiple features designed to facilitate effective deployment and defense evasion.
- At the time of writing, ZeroFox has observed no instances of active deployment of the Wing ransomware strain, although victims are likely to emerge in the coming weeks.
- However, the announcement of the RaaS operation in English only is indicative of the trend observed in Q4 2023 whereby English-speaking actors are willing to enter the ransomware scene, which has been traditionally dominated by Russian-speaking operatives.

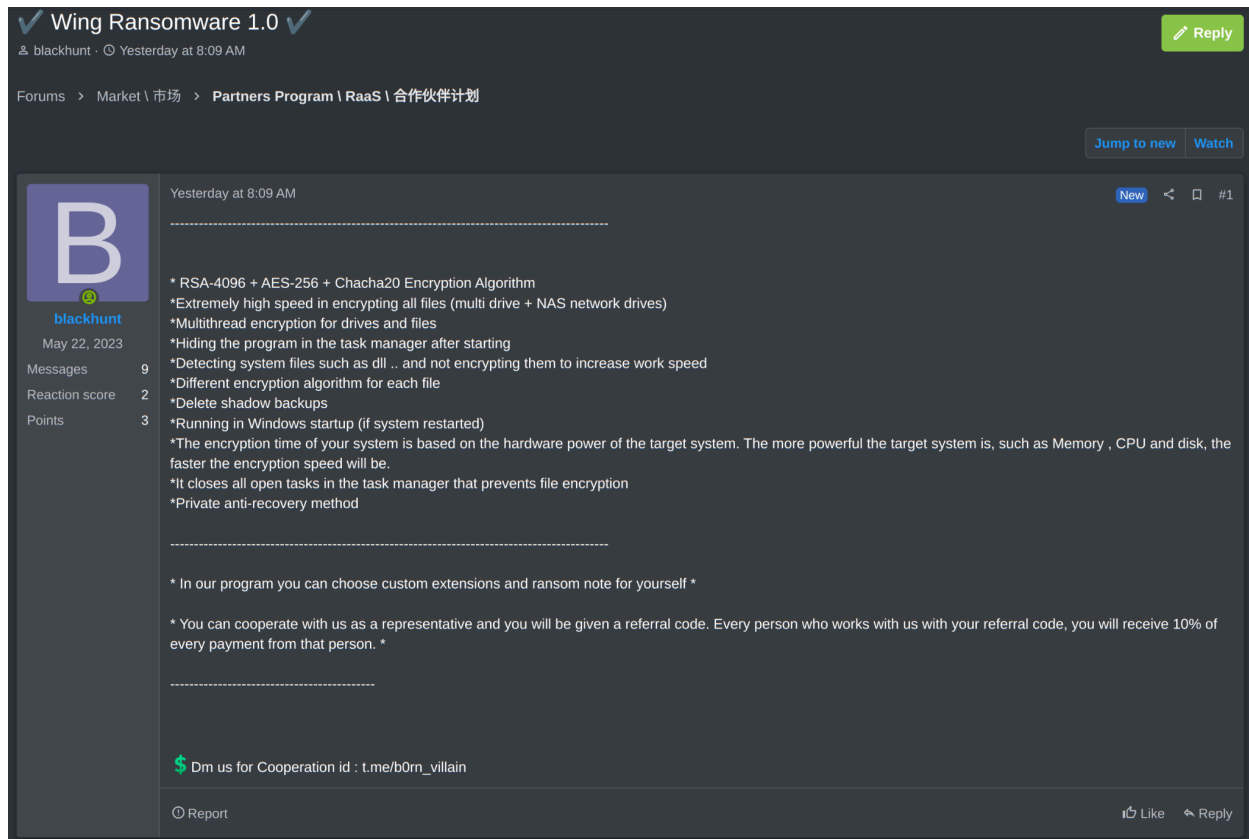
| Details

On January 28, 2024, positive-reputation English-speaking actor “blackhunt” announced a new RaaS operation known as Wing on the predominantly Russian-speaking dark web forum RAMP. This is the first RaaS operation launched on RAMP in 2024, following seven such operations launched in 2023. (Several additional operations were announced in 2023 implicitly under the call for affiliates or pentesters.)

Wing is touted as a state-of-the art ransomware tool with multiple features designed to facilitate effective deployment and defense evasion, including:

- Three modes of encryption (and a changing encryption algorithm for each file)
- Multithreading
- Lateral propagation
- Persistence mechanisms
- Destruction of backups
- A “private” anti-recovery implementation

The post also states that affiliates can customize their copy and their ransom note and can refer other affiliates to receive 10 percent of the profits of their successful extortions.



The screenshot shows a forum post on a dark-themed interface. At the top, the title "Wing Ransomware 1.0" is displayed with green checkmarks on either side. Below the title, the user "blackhunt" is listed with a timestamp of "Yesterday at 8:09 AM". A green "Reply" button is in the top right corner. The breadcrumb trail reads "Forums > Market \ 市场 > Partners Program \ RaaS \ 合作伙伴计划". On the right, there are buttons for "Jump to new" and "Watch". The post content is dated "Yesterday at 8:09 AM" and includes a "New" badge, a back arrow, and a "#1" indicator. The user's profile picture is a purple square with a white "B", and their name "blackhunt" is in blue. A sidebar on the left shows statistics: "May 22, 2023", "Messages 9", "Reaction score 2", and "Points 3". The post body contains a list of features in Chinese, followed by a referral code "t.me/b0rn_villain" and a Telegram link. At the bottom, there are "Report", "Like", and "Reply" options.

✓ Wing Ransomware 1.0 ✓

& blackhunt · Yesterday at 8:09 AM

Forums > Market \ 市场 > Partners Program \ RaaS \ 合作伙伴计划

Jump to new Watch

Yesterday at 8:09 AM

New < #1

B

blackhunt

May 22, 2023

Messages 9

Reaction score 2

Points 3

* RSA-4096 + AES-256 + Chacha20 Encryption Algorithm

*Extremely high speed in encrypting all files (multi drive + NAS network drives)

*Multithread encryption for drives and files

*Hiding the program in the task manager after starting

*Detecting system files such as dll .. and not encrypting them to increase work speed

*Different encryption algorithm for each file

*Delete shadow backups

*Running in Windows startup (if system restarted)

*The encryption time of your system is based on the hardware power of the target system. The more powerful the target system is, such as Memory , CPU and disk, the faster the encryption speed will be.

*It closes all open tasks in the task manager that prevents file encryption

*Private anti-recovery method

* In our program you can choose custom extensions and ransom note for yourself *

* You can cooperate with us as a representative and you will be given a referral code. Every person who works with us with your referral code, you will receive 10% of every payment from that person. *

\$ Dm us for Cooperation id : t.me/b0rn_villain

Report Like Reply

Post announcing the launch of the Wing Raas operation

Source: ZeroFox Intelligence

At the time of writing, ZeroFox has observed no instances of active deployment of the Wing ransomware strain, although victims are likely to emerge in coming weeks. The post indicates that 2024 will see continued diversification across the ransomware and digital extortion (R&DE) threat landscape with new operations emerging frequently, continuing the trend seen in 2023.

However, the announcement of the Raas operation in English only—suggesting the threat actor is unable to speak Russian—indicates a continuation of the trend observed in Q4 2023 suggesting that English-speaking actors are willing to enter the ransomware scene, which has traditionally been dominated by Russian-speaking operatives.

| Recommendations

- Implement secure password policies with phishing-resistant multi-factor authentication, complex passwords, and unique credentials.
- Configure ongoing monitoring for Compromised Account Credentials.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Leverage cyber threat intelligence to inform the detection of R&DE threats; their associated tactics, techniques, and procedures (TTPs); and Indicators of Compromise (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.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- 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.
- Should your organization be impacted by a data breach, utilize ZeroFox Incident Response Services to swiftly deploy IDX data breach products and services to mitigate the impact to you and your customers.

| 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%