



| Flash |

Newly Identified “UBUD” Ransomware Product For Sale

F-2023-11-22b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Threat Groups, Ransomware, Deep and Dark
Web

November 22, 2023

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 November 22, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Newly Identified “UBUD” Ransomware Product For Sale

› Key Findings

- On November 17, 2023, positively trending threat actor “IsEmptyOrNull” announced the sale of a newly developed ransomware product dubbed “UBUD” on the Dark Web marketplace RAMP.
- Rather than a typical ransomware-as-a-service (RaaS) offering, UBUD is designed for solitary use and is a highly customizable product, with each payload build likely adapted for each deployment, making the detection and removal of the malicious code more difficult.
- Threat actors have demanded a very high price to purchase UBUD—2.5 BTC, or more than USD 90,000—more likely than not indicating that the ransomware has capabilities beyond those stated in the public description.
- UBUD’s appearance illustrates a trend in which entrepreneur-deployed ransomware is becoming more prolific and available. While most likely to be deployed in a limited number of targeted attacks, UBUD reflects the general trend whereby less-competent actors are increasingly able to deploy effective ransomware and digital extortion products as long as they have sufficient funds.

Details

On November 17, 2023, the positively trending threat actor "IsEmptyOrNull" announced on the ransomware-centered marketplace RAMP the sale of a newly developed ransomware product dubbed "UBUD." Rather than a typical RaaS offering—with an ongoing relationship between strain developers and deployers—UBUD is designed for solitary use; threat actors manage the entire extortion process of design, deployment, and negotiation without any recourse to the original developer.



RAMP post advertising the sale of UBUD Ransomware

Source: ZeroFox Collections

UBUD is written in C, a language prevalent amongst malicious payloads across the malware and ransomware landscape. C is fast and reliable, aids detection evasion, and payloads can be executed on systems without relying on pre-installed software.

Details included in the post indicate UBUD is a sophisticated and highly customizable product, with functions including:

- AES-256 file encryption
- RSA-4096 key encryption
- Customizable wallpapers and ransom notes
- Strong detection evasion capabilities.

- An encrypted binary stub that is allegedly only 25 KB in size.

A Command and Control (C2) server interface is also included as part of the purchase package, enabling threat actors to monitor the work of the client component of the ransomware and manage client builds. This includes the ability to track encryption success, manage IP and port settings, and customize decryption keys. Each payload build is likely customized for each deployment, making the detection and removal of the malicious code more difficult.

Threat actors have demanded a very high price to purchase UBUD—2.5 BTC, or more than USD 90,000—more likely than not indicating that the ransomware has capabilities beyond those stated in the public description. At the time of writing, ZeroFox has identified no instances of active deployment of UBUD against victims.

User Friendly server to monitor the success of the encryption :

- Login Page with your own profile.
- Choose IP PORT to listen.
- Start/Stop Server.
- Custom Key decryption.
- Customizable builder with RSA Keys Generator.

This is all the "simple" details about the program, for more technical details simply ask in PM.

Price : 2.5 BTC or % (with conditions)

Profile on neighbor forum : /profile/127684-isemptyornull/

AV ScanTime Result : <https://avcheck.net/id/3eEtJqCDuwxG>

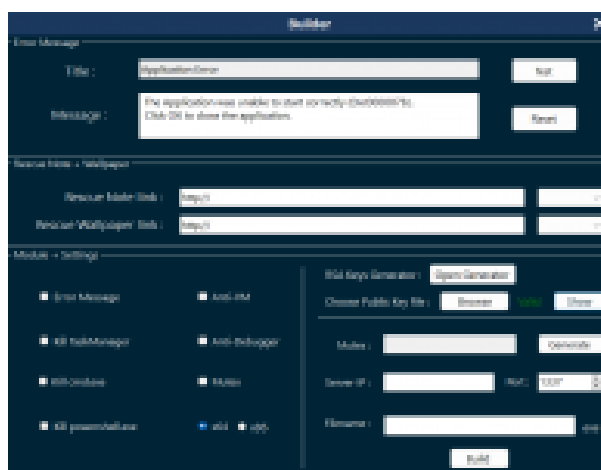
Further details of the UBUD Ransomware Offering

Source: ZeroFox Collections

The quality and prevalence of entrepreneur-type, non-RaaS products for sale on the Dark Web has increased in 2023. The standard of encryption, coverage, victim interaction, and ransomware preservation functionalities in these products is on an upward trajectory.

- Entrepreneur-type ransomware products have typically been less effective than RaaS offerings.

- Historically, the best-known ransomware product designed for solitary use was “Thanos.” After the Thanos developer was disrupted, a market niche opened, which was irregularly filled by a variety of low-sophistication ransomware products.
- This trend is likely shifting, with more and more sophisticated entrepreneur products advertised on the market, in some cases reaching parity with the sophistication of contemporary RaaS offerings.



Low-resolution screenshot provided by the threat actor showing the build generation panel on the server side of UBUD.

Source: ZeroFox Collections

UBUD’s appearance illustrates a trend in which entrepreneur-deployed ransomware is becoming more prolific and available. UBUD, more likely than not, has capabilities beyond those stated in the public description. It is too early to assess whether UBUD could turn out to be the new “Thanos” or surpass it in terms of functionalities. While most likely to be leveraged in a limited number of targeted attacks, UBUD represents a continuation of the general trend whereby less-competent actors are increasingly able to get their hands on highly effective products and services as long as they have sufficient funds.

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 MFA, complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform detection of Ransomware & Digital Extortion threats and 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.
- 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 deep and dark web 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%