



**| Flash |**

# **Access to U.S. Web Hosting Organization Advertised in Deep and Dark Web Forum**

**F-2024-04-15a**

**Classification: TLP:CLEAR**

**Criticality: Medium**

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

**April 15, 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 April 15, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

## **| Flash | Access to U.S. Web Hosting Organization Advertised in Deep and Dark Web Forum**

### **> Key Findings**

- On April 8, 2024, untested threat actor “synthetic” posted in deep and dark web (DDW) platform RAMP advertising access to a U.S.-based web hosting organization that has an annual revenue of approximately USD 16 million.
- Synthetic claims that the buyer will receive administrative access to all hosted web pages, which could number in the hundreds of thousands and belong to hundreds to thousands of separate organizations.
- The asking price for the initial access was USD 80,000, which is significantly higher than the typical price tag for initial access to an organizational network. This is almost certainly due to the notably high potential financial return for the successful exploitation of such significant access.
- Synthetic is not an active user in RAMP, but the advertisement indicates that sales will take place using the forums escrow service—significantly increasing the credibility of both the sale and the actor.

## Details

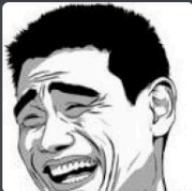
On April 8, 2024, untested threat actor synthetic posted in the DDW platform RAMP advertising access to a U.S.-based web hosting organization that has an annual revenue of approximately USD 16 million. According to the post, the victim organization is in the “General Telecommunications Hosting” industry and currently hosts over 120,000 web domains.



**synthetic**  
Jan 18, 2024  
Messages 2  
Reaction score 0  
Points 1

Yesterday at 10:37 PM

Websites - +120k domains registered  
Access - Root, Admin Panel  
Rev - ~16M  
All .tld available  
+ Info  
All sites can be accessed through admin panel to cpanels/whm/vnc  
Data: +50TB  
Price: 80,000\$  
Garant!



**BinLangRen91**  
Member  
Nov 18, 2021  
Messages 38  
Reaction score 11  
Points 8

Today at 3:13 AM

country?

 Report



**synthetic**

Today at 3:53 AM

**BinLangRen91 said:** 

country?

US

**RAMP posts advertising initial access and specifying the victim region**

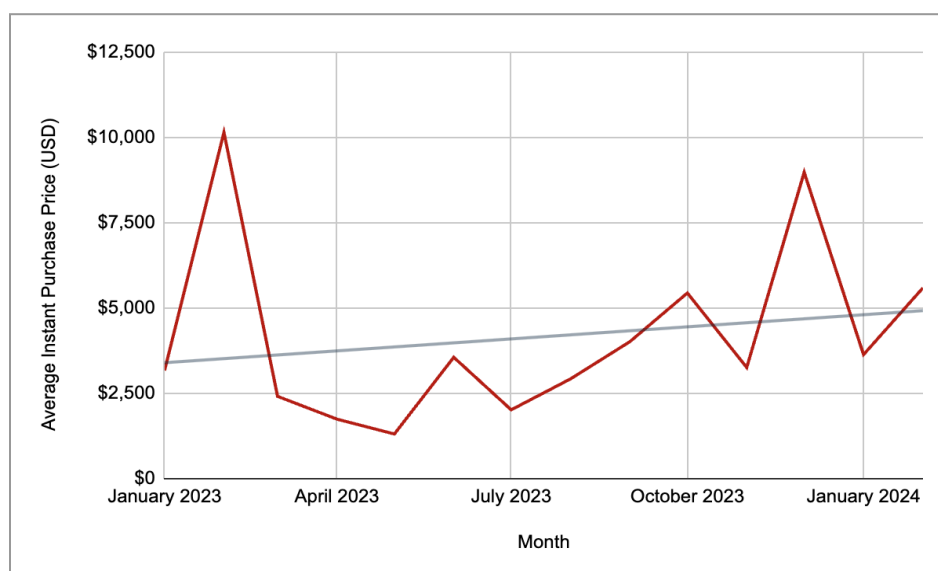
Source: ZeroFox Intelligence

Synthetic claims that the buyer will receive administrative access to all hosted web pages, which could number in the hundreds of thousands and belong to hundreds to thousands of separate organizations. The access is enabled through web hosting tools cPanel, WebHost manager (WHM), and Virtual Network Computing (VNC).

Fifty terabytes of data are also included in the sale, which very likely includes personally identifiable information and personal financial information of employees and customers extracted from the hosted web pages.

The asking price for the initial access is USD 80,000, which is significantly higher than the typical price tag for initial access to an organizational network. This is almost certainly due to the notably high potential financial return for the successful exploitation of such significant access.

- Between January 2023 and April 2024, the average asking price for illicit initial access sales publicized in DDW forums xss, Exploit, and RAMP was approximately USD 8,000.
- The requested asking price of initial access is a reflection of the potential lucrativeness of the network access. This almost certainly takes into account factors such as the victim organization's annual revenue, the type of access (virtual private network, remote desktop protocol, etc.), and any associated privileges that enable faster exploitation.



**Average instant purchase price of initial access sales**

Source: ZeroFox Intelligence

The description included in the advertisement suggests there is a likely chance that the victim is a web or cloud hosting organization with access to significant quantities of customer data.

Privileged access to the web hosting tools of an organization's website can enable a threat actor to conduct an array of subsequent malicious activity.

- The victim organization could be targeted in a digital extortion attack, whereby the buyer leverages ransomware to extract significant payment in exchange for the alleged deletion of the data. This would likely cause financial, operational, and reputational damage.
- The threat actor may target the victim's clients and associates by leveraging techniques such as cross-site scripting or SQL injection against their hosted web pages. The attacker could then move laterally toward the organizations' own servers, putting them at risk of data theft or phishing attacks.
- The end users of the compromised web pages' services could also be targeted, resulting in phishing, impersonation attacks, or fraudulent activity. Their stolen information could also be used to extort the web page owners in large-scale ransomware attacks, leveraging techniques similar to those enacted by threat group CI0p during 2023 campaigns.<sup>1</sup>

Synthetic is not an active user in RAMP, but the advertisement indicates that sales will take place using the forum's escrow service—significantly increasing the credibility of both the sale and the actor. Due to their limited exposure and the nature of the advertised access, there is a roughly even chance that synthetic is an insider and selling information gained through implicit access and trust.

---

<sup>1</sup> [hXXps://zf-dashboard-media.s3.amazonaws.com/intel/d4545937-a245-4dcd-ad06-1b2dc46860e8](https://zf-dashboard-media.s3.amazonaws.com/intel/d4545937-a245-4dcd-ad06-1b2dc46860e8)

## **Recommendations**

- Organizations should implement training for employees focusing on awareness of contemporary threats, phishing vigilance, social engineering resilience, and basic cybersecurity hygiene.
- Organizations should ensure their web pages and other online content are protected by using secure coding practices and updated security plugins and subjecting them to regular website security audits.
- Websites should be monitored to prevent irrelevant keywords or hidden data from being inserted.
- Implement secure password policies with phishing-resistant multi-factor authentication, complex passwords, and unique credentials.
- Proactively monitor for compromised accounts being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of ransomware and digital extortion (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, and implement network segmentation to separate resources.
- 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.

## | Appendix A: Traffic Light Protocol for Information Dissemination

|                         | Red                                                                                                                                                                                          | Amber                                                                                                                                                                                                                                                                                                                  |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WHEN SHOULD IT BE USED? | Sources may use <b>TLP:RED</b> 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 <b>TLP:AMBER</b> 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 <b>NOT</b> share <b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                              | Recipients may <b>ONLY</b> share <b>TLP:AMBER</b> 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.<br><b>Note that</b> <b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                         | Green                                                                                                                                                                                        | Clear                                                                                                                                                                                                                                                                                                                  |
| WHEN SHOULD IT BE USED? | Sources may use <b>TLP:GREEN</b> 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 <b>TLP:CLEAR</b> 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 <b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | Recipients may share <b>TLP:CLEAR</b> 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%         |