



**ZEROFOX®**

*Your Intelligence Digest*

**It's a Digital World.  
Engage Securely.**

# Actor Claims Network Access To 6 High-Profile U.S.-Based Companies

New and positively trending threat actor “citrix” advertised network access to six different, high-profile U.S. companies on the Russian language Deep Web forum xss[.]is. This is significant as most network access brokers in the Russian underground have largely avoided targeting U.S.-based corporate networks since the war in Ukraine began in February 2022.

The actor claims to have remote desktop, VPN, and Citrix access to various companies, including:

- A financial organization that generates \$2 billion USD in revenue
- A healthcare provider that generates \$354 million USD in revenue
- A systems management company that generates \$281 USD million in revenue
- An insurance company that generates \$4 billion USD in revenue
- A manufacturer that generates \$800 million USD in revenue
- A healthcare provider that generates \$2 billion USD in revenue

The actor requires escrow for payment, indicating that they are more likely to possess the alleged access.

Additionally, the actor noted that they are looking for long-term partners. This suggests a renewed interest among threat actors in U.S.-based network access deals that will likely lead to an increase in cyber-attacks against U.S. companies in the coming months.

Original post and updates from threat actor "citrix" advertising network access to six different, high-profile U.S. companies

# Network Access To 6 High-Profile U.S.-Based Companies Cont.

1KKK+ Corps accesses

citrix · 09.05.2022

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧ

Новая сделка



**citrix**  
CD-диск

Пользователь

Регистрация: 03.05.2022  
Сообщения: 13  
Реакции: 3

09.05.2022

US,CA,EU accesses under RDP,VPN,Citrix Revenues from 3KK - 2KKK+ , I work % only / escrow.

Looking for long term cooperation  
PM jabber or tox

Жалоба

RichBitch, xperito и whitestein



**citrix**  
CD-диск

Пользователь

Регистрация: 03.05.2022  
Сообщения: 13  
Реакции: 3

10.05.2022

1.Rev \$2 Billion (finance,USA)....

2.Rev \$354 Million (healthcare , USA)....

3.Rev \$281 Million (sys management, USA)

updates  
toxin: 6119C34F573F133BCD06CEC711CF5B7332B7667757FF4621F679BFD7248B894798F1BA492CEB

Жалоба

xperito



**citrix**  
CD-диск

Пользователь

Регистрация: 03.05.2022  
Сообщения: 13  
Реакции: 3

Суббота в 15:42

4. Rev \$4 Billion (insurance,USA)

5. Rev \$800 Million (manufacturing,USA)

updates  
toxin: 6119C34F573F133BCD06CEC711CF5B7332B7667757FF4621F679BFD7248B894798F1BA492CEB

Жалоба



**citrix**  
CD-диск

Пользователь

Регистрация: 03.05.2022  
Сообщения: 13  
Реакции: 3

Сегодня в 04:25

6. Rev \$2 Billion (health,USA) (user, team workforce)

updates  
toxin: 6119C34F573F133BCD06CEC711CF5B7332B7667757FF4621F679BFD7248B894798F1BA492CEB

Жалоба

# Threat Actor Notes Potential Impact Of New OpenSSL Vulnerabilities

Well-regarded and established threat actor “r1z” recently posted about the potential impact of two new vulnerabilities in OpenSSL tracked as CVE-2022-1292 and CVE-2022-1473, on the predominantly Russian language Deep Web forum xss[.]is. The two new vulnerabilities enable unauthorized users to remotely execute code on a target machine and perform denial-of-service attacks, respectively.

The actor shared scan results from the Chinese mapper service fofa[.]info, showcasing more than 38.6 million vulnerable devices running the affected versions of OpenSSL worldwide, including more than 11.7 million devices in the U.S.

Based on the sheer quantity of vulnerable devices and the positive response the actor’s initial post has received from other forum members, ZeroFox researchers assess it is likely that threat actors will soon begin sharing exploits for the two vulnerabilities across the underground.

Impacted OpenSSL versions for the critical remote code execution vulnerability (CVE-2022-1292) include:

- 3.0.0,3.0.1,3.0.2
- 1.1.1-1.1.1n
- 1.0.2-1.0.2zd

Impacted OpenSSL versions for the high-level denial-of-service vulnerability (CVE-2022-1473) include:

- 3.0.0,3.0.1,3.0.2

Original post from threat actor “r1z” noting the potential impact of two new vulnerabilities in OpenSSL

# Potential Impact Of New OpenSSL Vulnerabilities Cont.

Remote OpenSSL Remote Code Execution & DDoS Vulnerability.

r1z · Вчера в 17:54 · cve-2022-1292 cve-2022-1473 ddos openssl openssl rce rce

Перейти к новому Отслеживать

Вчера в 17:54

 **r1z**  
(L2) cache  
Пользователь

Регистрация: 19.07.2019  
Сообщения: 311  
Реакции: 279

A [Tasty vulnerability](#) and critical one 9.8 of remote code execution vulnerability and denial of service vulnerability of OpenSSL will be in your hand soon.

**CVE-2022-1292 OpenSSL Code Execution Vulnerability**

Due to an issue where the c\_rehash script does not properly sanitize shell meta-characters, an unauthorized attacker could exploit the vulnerability to send a malicious request to execute a system command, resulting in remote code execution.

The vulnerability CVSS score: 9.8, hazard level: critical

**CVE-2022-1473 OpenSSL Denial of Service Vulnerability**

Due to memory resource management issues when decoding certificates, an unauthorized attacker could exploit this vulnerability to construct malicious requests, resulting in a denial of service.

The vulnerability CVSS score: 7.5, hazard level: high risk! a total of **38,623,336** related services are open to the world (app="OpenSSL"). The United States has the most with **11,727,666**; China is second with **2,994,966**; Germany is third with **2,288,855**; Japan is fourth with **2,229,943**; and France is fifth with **1,438,747**.

# Actor Looking For Developer To Build Web-Based Crypto Wallet For Fraud

Untested threat actor “heisen” is seeking a developer to build a web-based cryptocurrency wallet on the Russian language Deep Web forum exploit[.]in. ZeroFox researchers assess that this project will likely render a crypto wallet that steals funds from victims, based on the functionality the actor requested.

The actor specified that the wallet must have the following features:

- Supports various cryptocurrencies, including BTC and ETH
- Log all user data and actions
- Withdrawal requests for one-percent fee
- Editable withdrawal percentages
- Send fake transactions to users; labeled internal transactions
- Instantly rebrand website from web panel

Additionally, the actor specified that administrators must be able to send emails and custom popups to users. It is almost certain that the actor leverage social engineering methods to steal funds from victim, based on the requested features.

heisen

kilobyte

••



Paid registration

1

42 posts

Joined

21/21/22 (ID: 124569)

Activity

хакинг / hacking

Deposit

0.000259 B

Posted 8 hours ago (edited)

We are looking for someone to develop us a fake web wallet with the following features

**Budget - \$5000**

- 1. Users should be able to deposit to their wallet address and see the balance in cryptocurrency and fiat
- (Should support - BTC, ETH, USD, USDC)
- 2. Users should be able to edit account details, reset and change passwords. Reset password should be a
- 3. When a user's cryptocurrency deposit is confirmed 1 time on the blockchain, they should receive an email
- 4. Working support ticket system ( user should receive email notification whenever admin replies)
- 5. Users should be able to make withdrawal requests (1% withdrawal fee) and see pending requests on a
- 6. Admins should be able to view bitcoin address of any user, login location, edit their account details, clickable link leading to the blockchain.com look up of the bitcoin address
- 7. Admins should be able to see deposits in realtime along with the username, email address (of user), t
- 8. Admin ability to change withdrawal % of any user
- 9. Admin ability to send a fake transaction to an account in USD & Cryptocurrency value and this transaction have a label near them saying 'internal transaction'
- 10. Moderator accounts - no admin privileges and only ability is to see user pages and deposits (should)
- 11. Users should have the option to send from one fake wallet account to another fake wallet account
- 12. Instant rebranding feature Admin - Should be able to change domain name, logo (manual upload)
- 13. Admin panel - total money made in total (calculate total deposits of all users combined)
- 14. Ability to send email to all users at once (3rd party api can be used)
- 15. Automatic maintenance notice incase the site goes down
- 16. Admins should be able to send a custom popup like this to any user - <https://finbold.com/wp-content/uploads/2022/01/finbold-popup.png>

**Telegram - @heisen101**

DO NOT message me if you are a dropshipper or script seller. I will not buy your script.  
Not hiring developers from India, Nigeria, El Salvador, Ghana, Pakistan, Singapore for obvious reasons.

# Envoy Reboot Gains Popularity

Since its return in January 2022, after its initial 2020 shutdown, the Dark Web English language forum Envoy has gained popularity amongst threat actors. The new Envoy features a section for almost anything related to Deep Web activity, drugs (being the most popular thus far), hacking, cracking, pentesting, carding, and fraud have also been included as main topics of forum sections.

Researchers assess that this forum likely fills the need for a forum that contains high-profile information and is accessible to most common threat actors. This void was left by the closures of more reputable English language forums such as Torum and Torigon that both closed up shop in 2021. Although other forums have emerged that contain the high-profile topics and backdoor deals threat actors desire, such as KickAss, these remain largely inaccessible due to a high entry cost and require proof technical knowledge.

Researchers assess that drug sales, delivery methods, and vendors reviews are likely to dominate the content of the renewed Envoy. Due to the popularity of these sections so far and the well-regarded threat actor and administrator “Witchman” is discussing putting in a marketplace type functionality to facilitate this.

The serious cyber crime sections are currently either empty or feature basic method, and attack vectors, it is highly likely that these copied from other sources.



The home page of the new Envoy forum.

# Envoy Reboot Gains Popularity (Cont.)

envoy2vxtsbz63bik33yb6vka2ed4x5leeisfg2isd2gz2eg4skwmbyd.onion

envoy

Home Help Search Profile My Messages Members Logout

Envoy

### General

Unread Posts ↑

|                                                                                    |                                                                                                                                                   |                        |                                                                                                                      |
|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------|
|  | <b>Announcements</b><br>Admin-only posting board for announcements relating to the Envoy Project and its associates. Important stuff posted here! | 6 Posts<br>6 Topics    | <b>Last post</b> by Witchman05<br>in <a href="#">Contact the Admins.</a><br>on April 08, 2022, 02:09:45 pm           |
|  | <b>General Discussion</b><br>The main discussion board for the Envoy Forum. Say what thou wilt.                                                   | 764 Posts<br>98 Topics | <b>Last post</b> by plqqcs<br>in <a href="#">Re: I am looking for a s...</a><br>on <b>Today</b> at 06:18:03 am       |
|  | <b>Advertisements and Reviews</b><br>Drug, fraud and hacking reviews and ads. Verified vendors advertising only!                                  | 8 Posts<br>1 Topics    | <b>Last post</b> by MissGreenery<br>in <a href="#">!!!!NEW!!!! THC INFUSED DR...</a><br>on May 23, 2022, 01:49:32 pm |

Child Boards: [Drug Ads](#) NEW | [Drug Reviews](#) | [Fraud and Hacking Ads](#) NEW | [Fraud and Hacking Reviews](#) | [Other Ads](#)

### Drugs

Unread Posts ↑

|                                                                                      |                                                                                                                                                                                                              |                      |                                                                                                              |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|--------------------------------------------------------------------------------------------------------------|
|  | <b>The Opium Pipe</b><br>"I do not readily believe that any man having once tasted the divine luxuries of opium will afterwards descend to the gross and mortal enjoyments of alcohol." - Thomas de Quincey. | 16 Posts<br>4 Topics | <b>Last post</b> by fuckfckedup<br>in <a href="#">Re: m30 blues? US-US</a><br>on May 02, 2022, 07:10:41 pm   |
|  | <b>8 Ball</b><br>Cocaine: it's a hell of a drug.                                                                                                                                                             | 24 Posts<br>2 Topics | <b>Last post</b> by plqqcs<br>in <a href="#">Re: okay. how many types...</a><br>on May 21, 2022, 04:12:45 pm |

Child Boards: [Crack Cocaine](#)