



| Flash |

Mass Access Brokering Event Impacting Corporate Citrix VPN Users

F-2023-11-28a

Classification: TLP:CLEAR

Criticality: Medium

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

November 28, 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 11:00 AM (EST) on November 28, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Flash | Mass Access Brokering Event Impacting Corporate Citrix VPN Users

› Key Findings

- On November 26, 2023, highly regarded threat actor “Punktir” announced that they are selling at least 711 compromised Citrix Virtual Private Network instances with verified credentials on the Russian-speaking forum exploit[.]in.
- Targets included in the access sale are alleged to have a revenue of over USD 5 million and are all based in either Europe or the United States.
- Ransomware cartels—which frequently leverage exploit[.]in to purchase access from brokers—are very likely to deem the access sale affordable and to have a potentially high return on investment.
- The emergence of corporate access checkers on the deep and dark web has driven an increase in bulk access sales in 2023.

Details

On November 26, 2023, highly regarded threat actor “Punktir” announced the auction of access to at least 711 compromised Citrix Virtual Private Network (VPN) instances with verified credentials on the Russian-speaking forum exploit[.]in. Since 2020, Citrix VPN has

been one of the most widely-exploited products used by access brokers to gain a foothold into corporate networks.

The post very likely represents a legitimate mass access brokering event; the threat actor has a strong reputation and states that they will accept escrow at the buyer's expense. The post alleges that:

- There are no two-factor authentication (2FA) protected instances.
- There are no duplicates of previously-sold login portal links.
- The auction has a starting bid of USD 700, and it is USD 35,000 for a "blitz" or "buy now" price to acquire the total package without waiting for the auction to expire.

P

711 citrix with revenue >5kk and PC login, starting at \$10 per line

By Punktir, 21 hours ago in Auctions

Start new topic

Punktir

gigabyte

●●●●

P

Seller

34

143 posts

Joined

02/18/21 (ID: 114266)

Activity

virology / malware

Posted 21 hours ago

There are 711 lines in the list with verified logins and passwords on request /VPN/ (citrix)

The list includes only sites with a revenue of more than 5 million, no gov, no edu, no schools and universities, no CIS, no sites with 2fa, **no empty web entrances**

Not a single line from the list overlaps with my previous lots

The login and password to enter the request + **connect to the PC** in each line were checked!

Each line is a unique domain, there are no duplicates in the list Nothing was torn out or taken away, us, europe, com everything is in place (**us more than 400 lines in the list**)

Work is available through a guarantor at your expense

Start 7000\$ Step 1000\$ Blitz 35000\$

tg <https://t.me/wctrlshift>

tox E54D9131BB82D918C341747AC162FDC4F3334F6EE61B72F8A2EFE66411981E098A098C9FF849

Translated exploit[.]in post advertising the mass access brokering event

Source: ZeroFox Collections

Ransomware cartels—which frequently leverage exploit[.]in to purchase access from brokers—are very likely to deem the access sale affordable and to have a potentially high return on investment.

Organizations included in the access sale have an alleged revenue over USD 5 million—a figure that typically satisfies the criterion used by ransomware collectives. No government, education, or Commonwealth of Independent States (CIS)-based entities

are included. The targets are all Europe and U.S.-based, with U.S. targets allegedly accounting for more than 400 entries.

The emergence of corporate access checkers on the deep and dark web has driven an increase in bulk access sales in 2023.

- A corporate login checker (such as the Multi Network Checker) was likely leveraged in this instance to verify the list of targets given the high volume of compromised Citrix VPN portals and the claim that the credentials were checked.
- The target list was likely prepared prior to obtaining access and likely based on manual research supplemented by scanning via pentesting tools.

Use of these tools is expected to continue on an upward trajectory as corporate checkers become more readily available to potential attackers.

| 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 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.
- 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.

| 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%