



| Brief |

The Underground Economist: Volume 5, Issue 4

B-2025-02-27b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

February 27, 2025

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 February 27, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 5, Issue 4

Network Access to Large Manufacturing Company Advertised

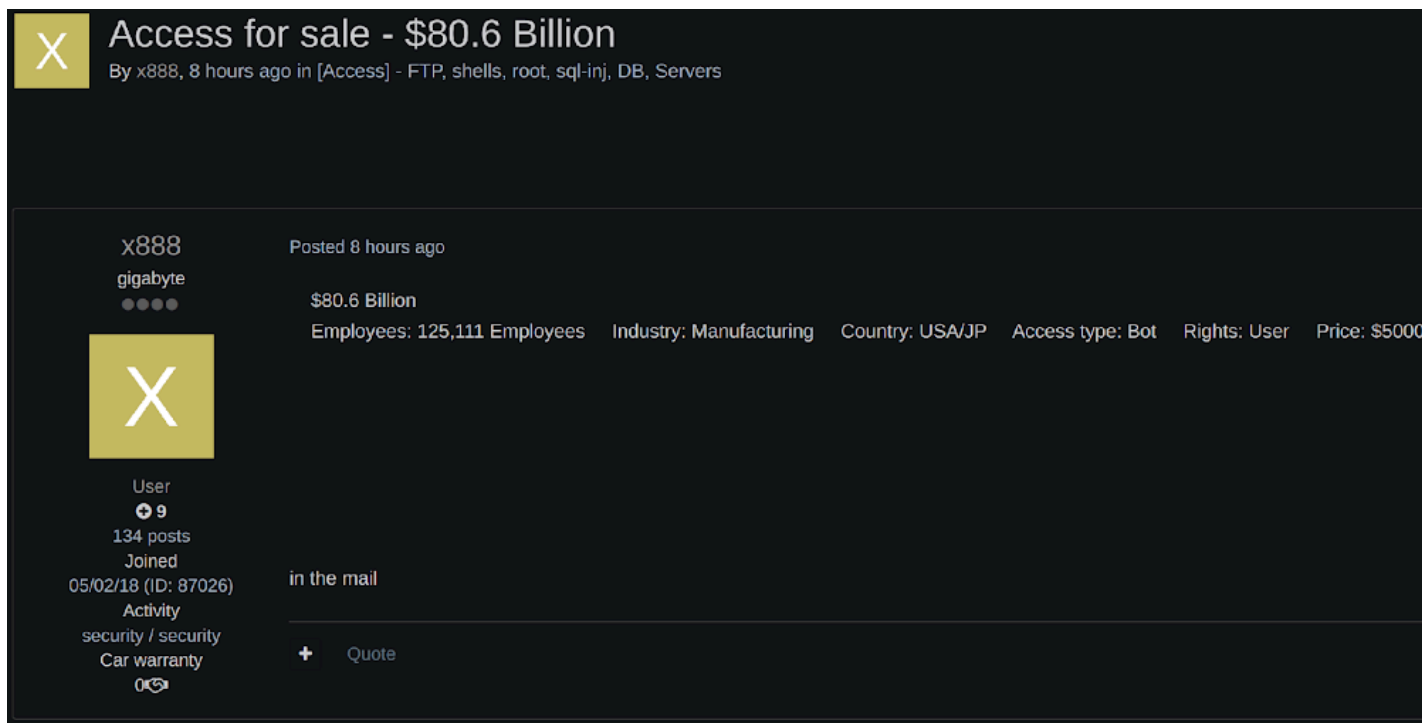
On February 25, 2025, Russian-speaking actor “x888” posted in the dark web forum Exploit, advertising network access to a large manufacturing organization. According to x888, the target entity has approximately 125,000 employees and an annual revenue of over USD 80 billion. The alleged access is enabled by a bot and grants the buyer user-level privileges.

- Across operating systems, user-level accounts/logins are among the least privileged.
- In an appropriately configured network, these users are typically enabled only to access the areas, tools, and information required to perform their daily functions. Functions such as amending security protocol, user accounts, installed software, or system settings are unlikely to be permitted.
- While critical areas of the network are unlikely to be accessible, an attacker would likely be able to access data such as personally identifiable information (PII), personal financial information (PFI), and information relating to partners and supply chains.

While illicit network access with user-level privileges does pose a threat to the organization and would likely be an appealing purchase to an array of threat actors,

there is a likely chance that any buyer would seek to escalate privileges in order to establish persistence or access more sensitive information. This could be accomplished via the exploitation of software flaws, misconfigured security infrastructure, or stolen PII.

The asking price for the alleged network access is USD 5,000. Despite no visible replies or interaction at the time of writing, x888's positive reputation in the forum and the relatively low asking price will likely result in actors such as digital extortion collectives perceiving the alleged access as legitimate and potentially lucrative.



The screenshot shows a forum post with a dark theme. At the top, a yellow square with a white 'X' icon is next to the title "Access for sale - \$80.6 Billion". Below the title, it says "By x888, 8 hours ago in [Access] - FTP, shells, root, sql-inj, DB, Servers". The post content area shows the user profile for "x888" with a yellow square icon containing a white 'X'. The profile includes the text "gigabyte", "User", "134 posts", "Joined 05/02/18 (ID: 87026)", and "Activity security / security Car warranty". To the right of the profile, it says "Posted 8 hours ago" and "\$80.6 Billion". Below this, it lists "Employees: 125,111 Employees", "Industry: Manufacturing", "Country: USA/JP", "Access type: Bot", "Rights: User", and "Price: \$5000". At the bottom of the post content area, there is a "Quote" button.

x888's Exploit post advertising illicit network access

Source: Exploit

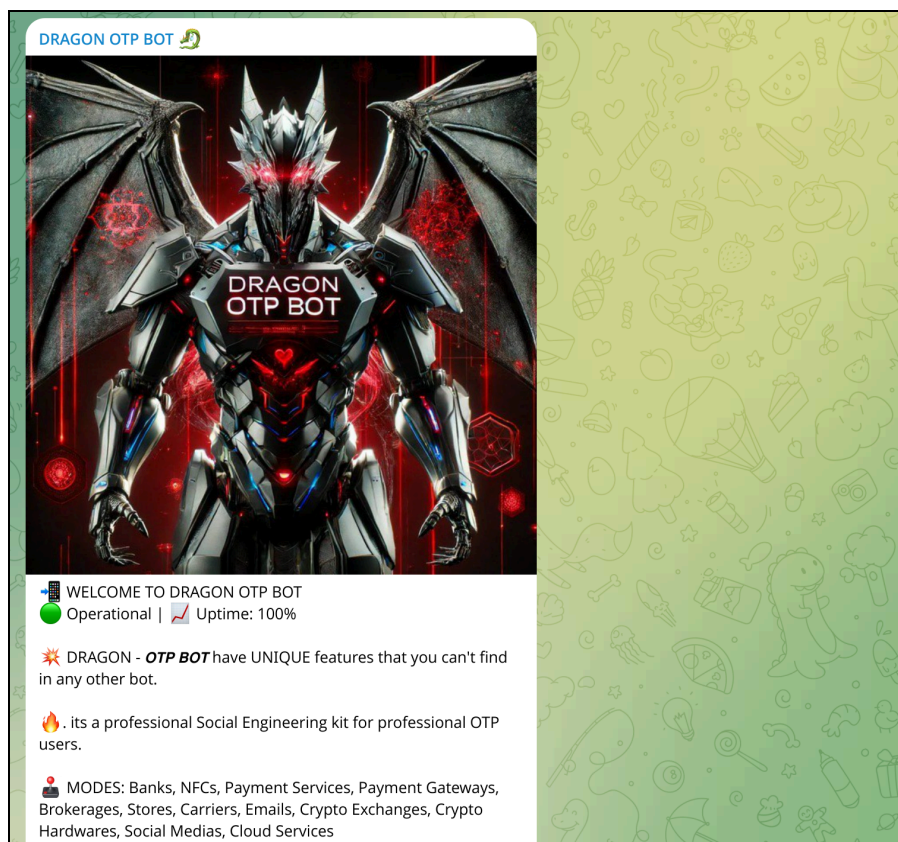
| Novel One-Time Password Bot Service Announced on Telegram

On February 15, 2025, threat actors announced the launch of a one-time password (OTP) bot service dubbed "Dragon OTP Bot" on Telegram. The actors claimed that the bot is a professional kit which leverages social engineering techniques against legitimate users, enabling threat actors to obtain active OTP codes. The bot was offered with various

subscriptions, with prices including USD 60 for one day, USD 130 for one week, and USD 300 per month. The actors allege the bot enables users to receive OTP codes to authenticate logins to:

- Banks
- Near Field Communication (NFC)
- Payment Services
- Payment Gateways
- Brokerages
- Stores
- Carriers
- Emails
- Crypto Exchanges
- Crypto Hardware
- Social Media
- Cloud Services

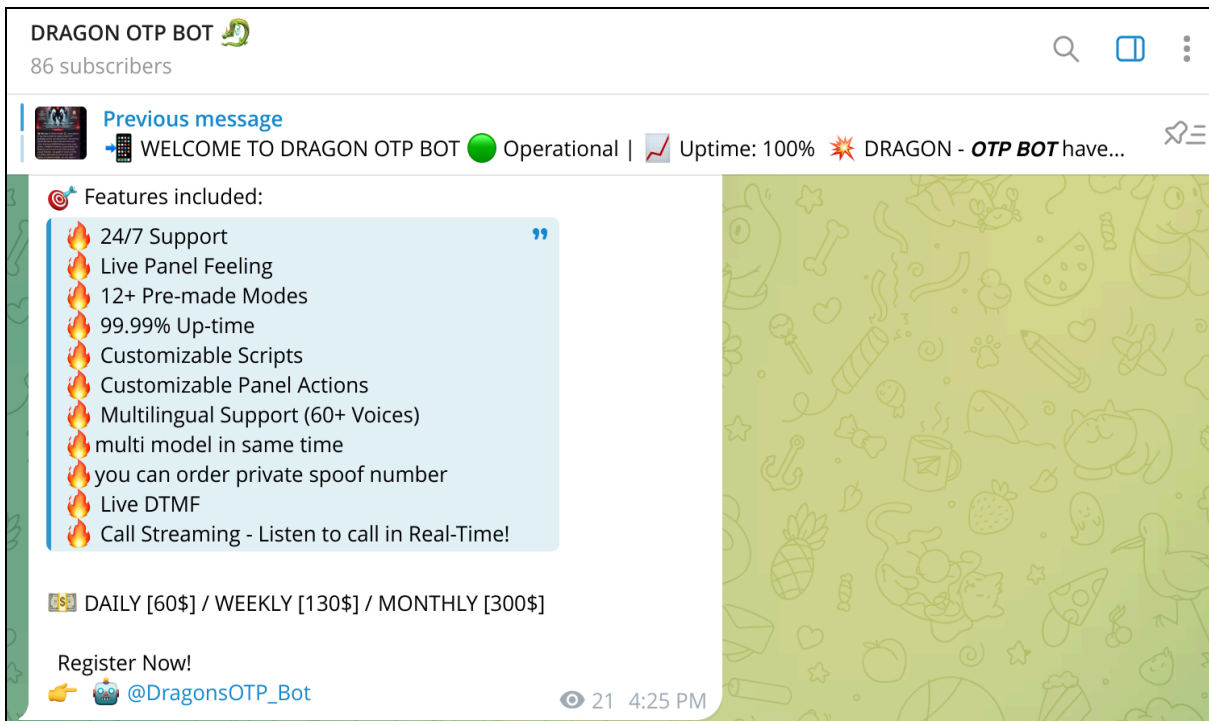
As of writing, the bot service has not yet been tested by ZeroFox, and there is little information available as to the quality or authenticity of the service. There is also very limited detail provided about how the social engineering component of the service works.



Dragon OTP bot service announced on Telegram (Part 1)

Source: Telegram

Numerous Telegram-based OTP bots claim to send valid OTP codes to threat actors to grant access to compromised victim accounts; however, the alleged use of social engineering techniques makes Dragon OTP Bot relatively novel in comparison with other market offerings. Currently, one of the largest obstacles to threat actors being able to leverage the ever-growing database of compromised digital assets belonging to victims is the presence of two-factor authentication (2FA). The availability of valid OTP codes is one method to bypass these restrictions, but many are not as reliable as claimed. If legitimate, the use of social engineering could enable threat actors to hijack OTP codes in near-real time, facilitating 2FA bypass and posing a substantial risk to victim organizations.

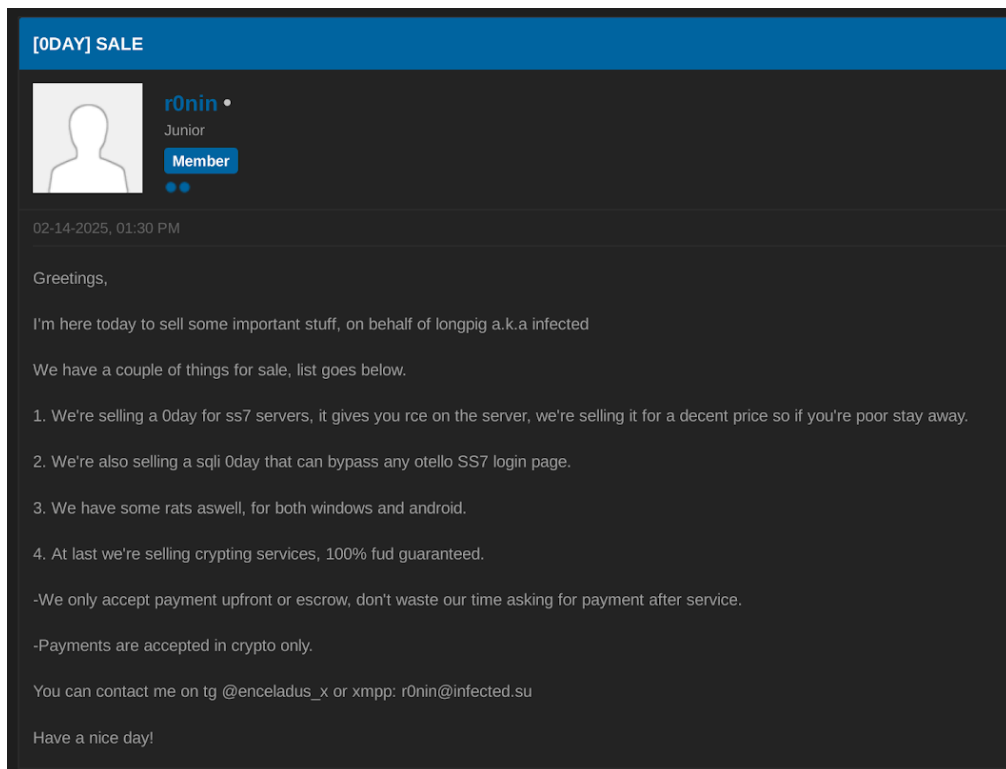


Dragon OTP bot service announced on Telegram (Part 2)

Source: Telegram

Zero-Day Allegedly Affecting Signaling System 7 Protocol and Servers Advertised for Sale

On February 14, 2025, the English-speaking actor "r0nin" advertised a zero-day vulnerability affecting the Signaling System 7 (SS7) protocol and servers on the dark web forum CryptBB. The seller claims the vulnerability grants remote code execution (RCE) on an unspecified server. A zero-day vulnerability in the SS7 system that grants attackers RCE poses a critical security risk. If successfully exploited, attackers could potentially manipulate 2FA and other telecom-related services.



r0nin's original post on the CryptBB dark web forum

Source: CryptBB

The price for the zero-day was not disclosed, but the actor advises those who cannot afford it to “stay away”. R0nin stated that they would only accept payments upfront or through escrow.

- R0nin joined the CryptBB forum in January 2024 and currently has a reputation score of zero.
- R0nin has been observed advertising malware development services, corporate network access, and zero-day exploits.

In addition to this zero-day, r0nin also claimed to be selling:

- A Structured Query Language injection (SQLi) zero-day that can bypass any OTello SS7 login page
- Remote Access Trojans (RATs) working on Windows and Android
- Crypting services which are guaranteed 100 percent fully undetectable

The OTello SIP/SS7 Gateway is a telecommunications device designed to bridge modern IP-based networks using the Session Initiation Protocol (SIP) with traditional Public Switched Telephone Networks (PSTN) that utilize SS7. This integration facilitates seamless communication between Voice-over-Internet-Protocol (VoIP) services and legacy telephony systems.

A potential SQLi zero-day could lead to the exfiltration of user databases. This would likely enable attackers to exploit sensitive credentials belonging to telecommunications carriers that use the Otello Gateway.

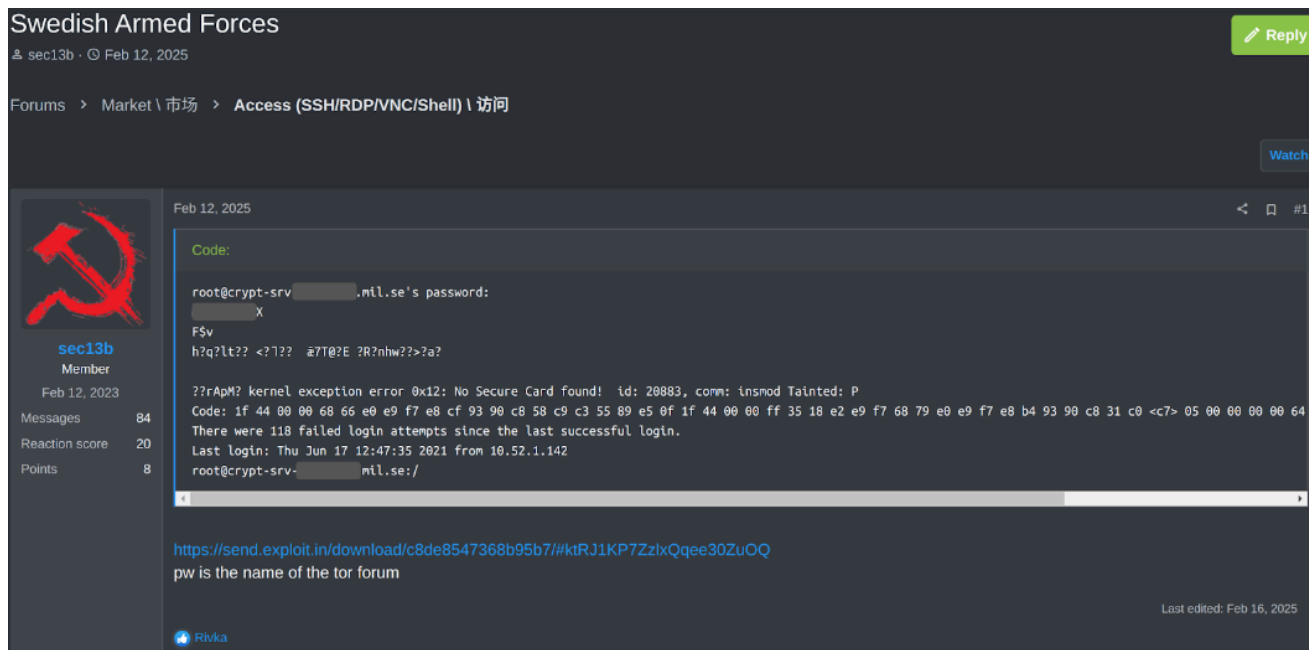
It is likely the actor r0nin is associated with CryptBB forum administrator "LongPig," who has been identified advertising SS7 access multiple times in recent years. However, forum members have accused LongPig of scams. While this advertisement is likely fraudulent, ZeroFox can neither confirm nor deny this.

| Root Access Allegedly Related to the Swedish Armed Forces Discussed

On February 12, 2025, the actor "sec13b" shared details of a root login attempt to a server likely associated with the Swedish Armed Forces on the dark web forum RAMP. After failing to access sensitive resources of the Swedish Armed Forces, the actor shared the file containing all server details and credentials with forum users, who may attempt to exploit the access.

Sec13b provided a file containing server details and login credentials for the exposed server. Although the actor successfully guessed the root password for "root@crypt-srv-0214[.]fra[.]mil[.]se", the authentication attempt failed due to a missing security card.

- The Secure Card module refers to a hardware or software component responsible for security-related functions involving a secure card, such as a smart card, cryptographic card, or other security modules.



sec13b's original post discussing root access to the Swedish Armed Forces. Some details have been obfuscated by ZeroFox.

Source: RAMP

The post garnered the attention of several RAMP users. The well-regarded threat actor “Rivka” stated that any potential attack would require a zero-day exploit to gain access to the resources. Sec13b responded, agreeing that it was possible but noted that not everyone has the time or resources to obtain such an exploit. Another vetted user, “achillesec”, stated that it is likely only governments would be interested in such a vulnerability, as most RAMP forum members seek quick financial gain.

This initial phase of access into a NATO country's infrastructure poses a serious risk of sensitive data leakage if exploited. While the barriers to successful exploitation would very likely deter (and exceed the capability of) the majority of forum users, highly capable threat actors—including adversarial nation state actors—could leverage such access to cause significant reputational and operational damage to a perceived enemy.

| Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- 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.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

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.

Amber

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

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.

Clear

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%