



| Flash |

Actor Seeks Access to Government and Critical Infrastructure Networks

F-2024-04-02a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware, Deep & Dark Web, Threat Actors

April 2, 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 PM (EDT) on April 2, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Actor Seeks Access to Government and Critical Infrastructure Networks

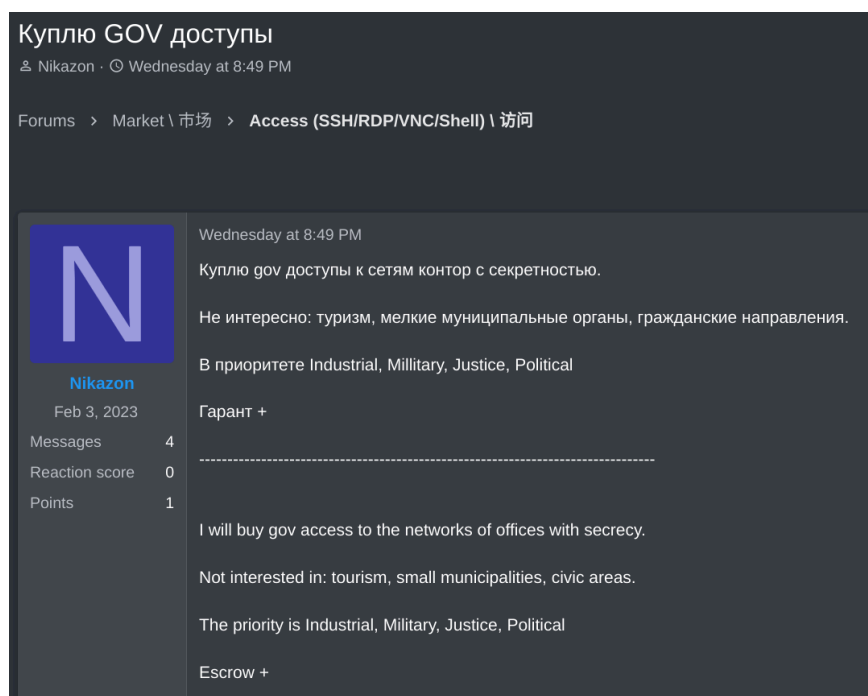
> Key Findings

- On March 27, 2024, untested threat actor “Nikazon” posted in the deep and dark web (DDW) forum RAMP advertising their search for affiliates able to provide illicit access to the networks of industrial, military, justice, and political targets.
- ZeroFox observed an approximately 55 percent increase in the number of ransomware and digital extortion (R&DE) attacks targeting organizations within the defense, government, and critical infrastructure sectors between Q1 2023 and Q1 2024.
- This advertisement is likely supportive of an ongoing shift in DDW norms manifested by financially-motivated R&DE threat actors punitively seeking victim organizations—the targeting of which would traditionally be frowned upon by other groups, affiliates, and platform moderators.

| Details

On March 27, 2024, untested threat actor Nikazon posted in DDW forum RAMP advertising their search for affiliates able to provide illicit access to the networks of industrial, military, justice, and political targets. The advertisement is posted in both Russian and English and offers use of the forum’s escrow service.

- The use of escrow is very likely indicative of legitimate services, offering opportunities to access brokers frequenting the forum.
- The inclusion of Russian and English languages is very likely intended to extend the advertisement's reach and secure as much market attention as possible.
- The overt advertisement for network access of this nature is unusual. It is very likely that the majority of R&DE actors that target these industries either source their own access via the leveraging of stolen credentials or vulnerability exploitation or procure access privately through instant messaging platforms.



RAMP post advertising Nikazon's search for access brokers

Source: ZeroFox Intelligence

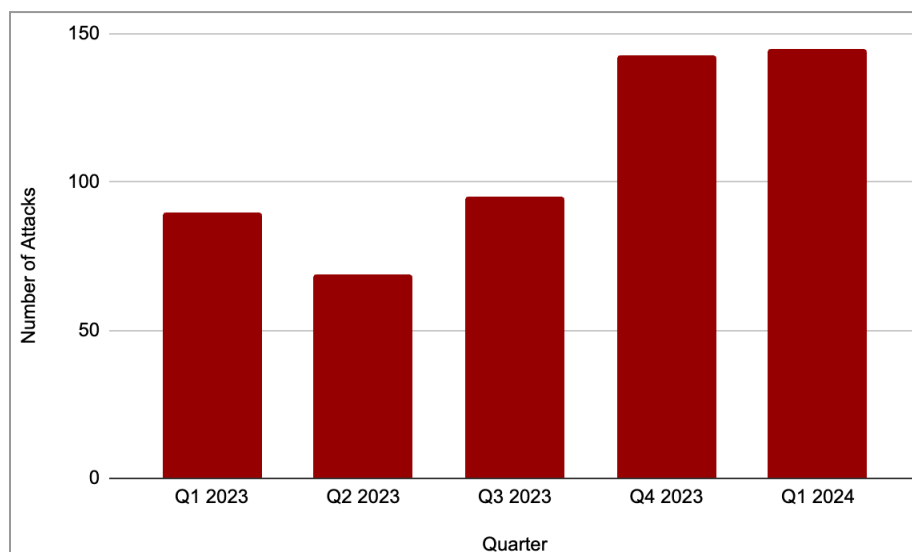
The requested industries outlined in the advertisement are highly diverse and composed of a wide array of organizations. However, it is likely that Nicazon is seeking access to the networks of specific organizations that are associated, directly or indirectly, with government entities and critical national infrastructure.

- The targeting of these industries, along with others such as healthcare and education, is generally considered bad practice and against the "norms" of DDW marketplaces. While in some cases these parameters may be an attempt to display empathy or exhibit professionalism, they very likely stem more often from

attempts to avoid additional law enforcement (LE) scrutiny—particularly given the abundance of organizations whose lucrative targeting is less likely to draw significant attention.

Despite them often contravening established norms, ZeroFox observed an approximately 55 percent increase in the number of R&DE attacks targeting organizations within the defense, government, and critical infrastructure sectors between Q1 2023 and Q1 2024.

- The proportion of these attacks targeting Europe and North America remained mostly consistent during this time period, while those targeting the Middle East and Africa increased by approximately 100 percent.
- There is a roughly even chance that this increase can be attributed, in part, to heightened international tensions correlating to several ongoing geopolitical disputes. Such turbulence is likely to entice politically or ideologically-motivated threat actors to conduct attacks against opposing government entities or the organizations perceived to support them.



R&DE attacks targeting the Defense, Government and Critical Infrastructure sectors globally between Q1 2023 and Q1 2024

Source: ZeroFox Intelligence

This advertisement is likely supportive of an ongoing shift in DDW norms manifested by financially-motivated R&DE threat actors punitively seeking victim organizations—the targeting of which would traditionally be frowned upon by other groups, affiliates, and platform moderators. These threat actors likely view ongoing geopolitical turbulence as

an opportunity to be capitalized upon, inflicting disruption and financial extortion on opposing organizations while minimizing the likelihood of LE intervention.

| 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 R&DE 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 DDW 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%