



| Flash |

Network Access Sale Linked to Chandrayaan-3 Mission

F-2023-12-13a

Classification: TLP:CLEAR

Criticality: Medium

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

December 13, 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 9:00 AM (EST) on December 13, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Flash | Network Access Sale Linked to Chandrayaan-3 Mission

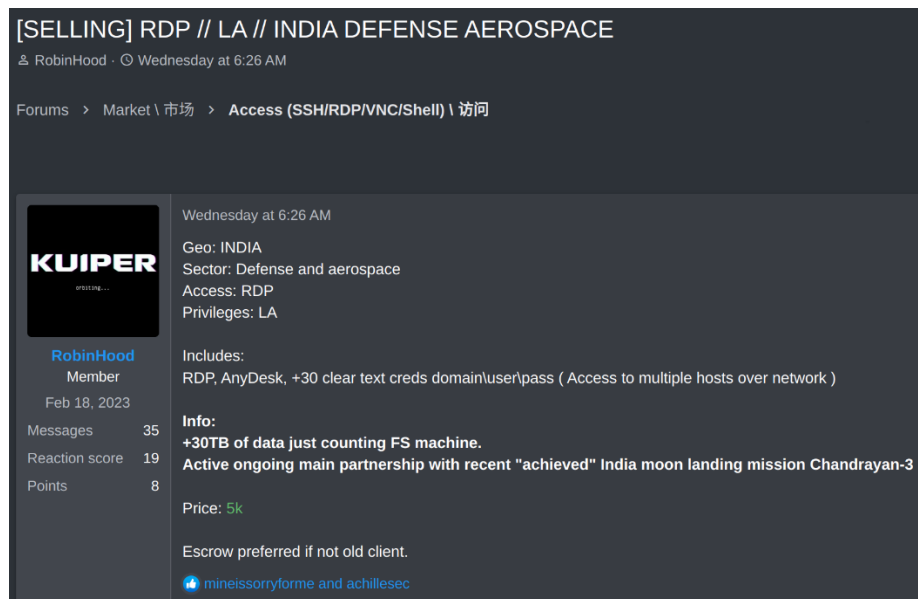
➤ Key Findings

- On December 6, 2023, well-regarded access broker “RobinHood” announced on Russian-language dark web forum RAMP the sale of likely network access to an unnamed India-based organization that has an ongoing partnership with India’s Chandrayaan-3 mission.
- Ransomware cartels frequently leverage RAMP to purchase such accesses from brokers; the post likely represents a legitimate network access sale, judging from RobinHood’s long-standing positive reputation.

Details

On December 6, 2023, network access broker RobinHood announced on Russian-language dark web forum RAMP the sale of likely network access to an unnamed India-based enterprise in the Defense and Aerospace sector. The compromised organization is alleged to have “active ongoing main partnership with recent [*sic*] achieved India moon landing mission Chandrayan-3.” The price requested is USD 5,000. The post states that access includes:

- Remote Desktop Protocol (RDP), AnyDesk, and user logins
- Over 30 terabytes of data



RAMP post advertising access to an Indian Defense and Aerospace Organization

Source: ZeroFox Collections

Judging from the long-standing positive reputation of RobinHood, the post likely represents a legitimate network access sale. RobinHood is also willing to accept escrow at the buyer's expense—a positive indicator of an actor's reliability. The advertised access is very likely designed to appeal to Russian ransomware and digital extortion collectives, as the forum was built and is dominated by Russian-speaking actors. High-profile targets on the network access market—particularly those with geopolitical implications—often draw widespread attention from extortion collectives.

- Russian ransomware cartels are very likely to deem the access sale affordable and to have a potentially high return on investment.
- The targeted company's partnership with Chandrayaan-3 will draw threat actors that are keen to hit back at organizations contributing to the success of Russia's competitors.
- The access broker RobinHood is very likely linked to the recently-announced Kuiper Ransomware-as-a-Service (Raas) operation.

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%