



2025



BABUK RANSOMWARE GROUP THREAT REPORT



CERTMH_CTL_2025_13

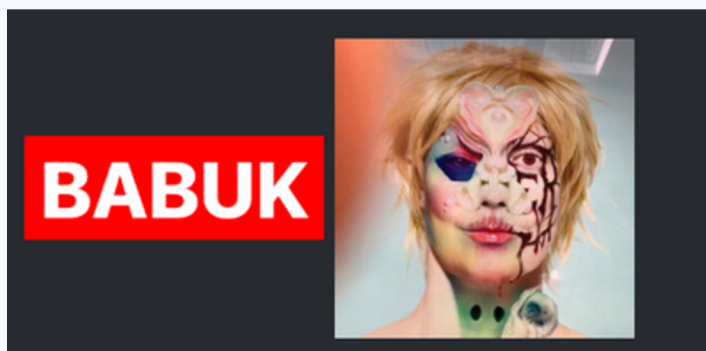
TABLE OF CONTENTS

• Introduction	3
• Background	4
• Objectives	4
• MITRE ATT&CK TTPs	5
• Attack Campaign	7
• Targeting Preferences	8
• Attribution & Analysis	11
• News & Recent Developments	13
• Mitigation Strategies	17
• Conclusion	21
• References	22

INTRODUCTION

Babuk is a ransomware group that emerged in early 2021 as part of the growing Ransomware-as-a-Service (RaaS) ecosystem. Unlike Advanced Persistent Threat (APT) groups, which focus on espionage and long-term infiltration, Babuk was financially motivated, targeting organizations to encrypt their data and demand ransom payments.

Babuk gained notoriety for double extortion tactics, where attackers not only encrypted files but also stole sensitive data and threatened to leak it if the ransom was not paid. One of its most high-profile attacks targeted the Washington D.C. Metropolitan Police Department, where officers' personal data was exposed.



:-)
Welcome to Leaks site
created by **Babuk ransomware**

We do not audit
next categories of organizations



Hospitals

Plastic surgery



Non-Profit

Any non-profitable charitable



Schools

Except the major universities

BACKGROUND AND OBJECTIVES

BACKGROUND

On January 26th, Babuk's dedicated leak site (DLS) was "relaunched". Bjorka is the current administrator. Upon launch, the DLS was populated mainly by victims previously claimed by other groups such as RansomHub, Lockbit3, and Funksec. At this current time there is no apparent connection to the original Babuk operation besides reusing the Babuk site template and logos. The group is also known as Babuk2 by other trackers.

Aliases: • **Babuk2** • **Babuk-Bjork** • **Bjork Indonesia** • **SkyWave**
• **Indonesia Cyber** • **Bjorkanesia**

OBJECTIVES

- **Ransom-Based Extortion** – Encrypting victims' files and demanding cryptocurrency payments.
- **Double Extortion Tactics** – Stealing sensitive data and threatening to leak it if ransom was not paid.
- **Ransomware-as-a-Service (RaaS)** – Providing ransomware tools to affiliates for a share of the profits.
- **Targeting High-Value Organizations** – Attacking government agencies, police departments, and enterprises.
- **Disrupting Victim Operations** – Deleting backups and encrypting critical servers to increase pressure.

MITRE ATT&CK

TTPs



Initial Access

- **T1078** - Valid Accounts → Use of compromised credentials to gain access.
- **T1133** - External Remote Services → Exploiting RDP, VPN, or exposed admin panels.



Execution

- **T1204** - User Execution → Using phishing emails or malicious attachments.
- **T1569.002** - System Services: Service Execution → Running ransomware payloads via Windows services.



Persistence

- **T1547.001** - Registry Run Keys/Startup Folder → Adding Babuk's payload to startup for persistence.
- **T1505.003** - Web Shell → Installing web shells on compromised servers.



Privilege Escalation

- **T1068** - Exploitation for Privilege Escalation → Exploiting system vulnerabilities for admin privileges.
- **T1134** - Access Token Manipulation → Impersonating system processes to escalate access.



Defense Evasion

- **T1027** - Obfuscated Files or Information → Encrypting payloads to evade detection.
- **T1070.004** - File Deletion → Deleting logs and forensic traces.
- **T1562.001** - Disable Security Tools → Disabling antivirus and EDR solutions.



Credential Access

- **T1003** - OS Credential Dumping → Using tools like Mimikatz to extract passwords.
- **T1555** - Credentials from Password Stores → Stealing credentials from browser and OS storage.



Discovery

- **T1083** - File and Directory Discovery → Identifying valuable files for exfiltration.
- **T1018** - Remote System Discovery → Mapping the network for lateral movement.



Lateral Movement

- **T1021.001** - Remote Desktop Protocol (RDP) → Using RDP for internal system movement.
- **T1570** - Lateral Tool Transfer → Moving Babuk payloads across systems.



Collection & Exfiltration

- **T1560.001** - Archive Collected Data: Archive via Utility → Compressing stolen data before exfiltration.
- **T1048** - Exfiltration Over Alternative Protocol → Sending data to external servers using encrypted tunnels.



Impact (Final Stage)

- **T1486** - Data Encrypted for Impact → Encrypting victim files for ransom.
- **T1490** - Inhibit System Recovery → Deleting backups and shadow copies.
- **T1531** - Account Access Removal → Locking out users post-compromise.

ATTACK CAMPAIGN

Bjorka's initial activities focused on leaking databases from Indonesian organizations, often accompanied by taunts and criticisms of the Indonesian government. The actor quickly gained a following among some Indonesians, who viewed them as a "folk hero" exposing government incompetence and corruption. This popularity, however, has been accompanied by copycat activity and concerns about the exposure of sensitive personal data.

The campaign typically follows these steps:

- **Initial Access** – Gaining entry via stolen credentials, RDP exploits, or phishing.
- **Data Exfiltration** – Stealing sensitive data before deploying ransomware.
- **Double Extortion** – Encrypting files and threatening to leak stolen data if ransom isn't paid.

This attack pattern disrupts victims' operations and pressures them into paying ransoms to avoid data exposure.

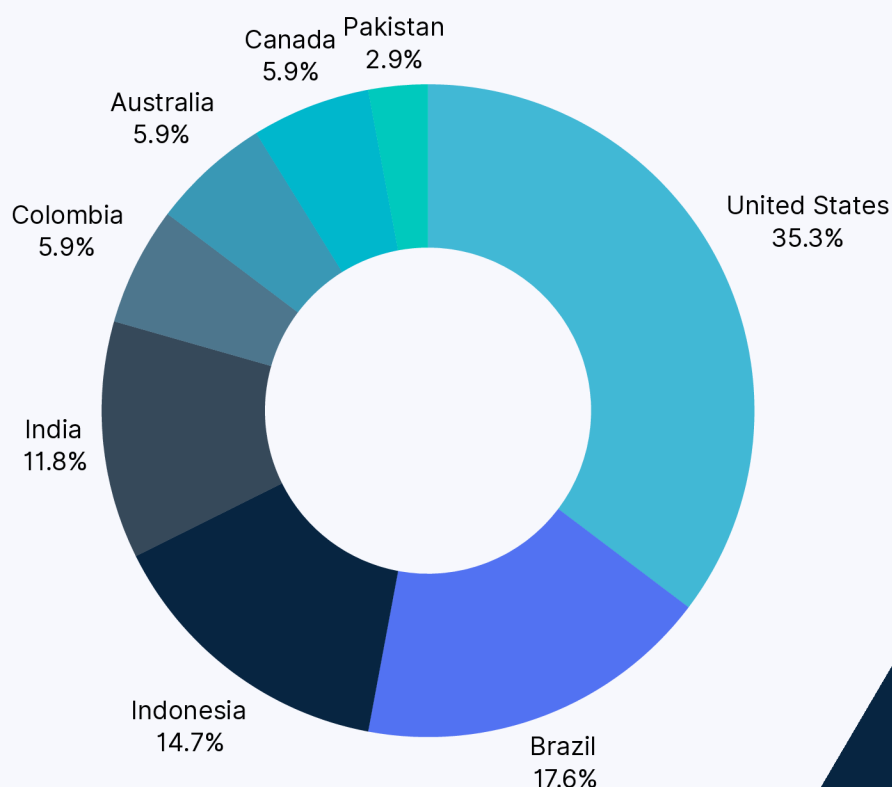
Leaks Data

<p>ER 2003</p> <p>ER IDENTIFICATION</p> <p>2025-01-28 22:13:01</p>	<p>MYINDIHOME TELKOM INDONESIA by (Babuk Locker)</p> <p>MYINDIHOME TELKOM INDONESIA</p> <p>2025-01-28 17:26:09</p>	<p>Hello! w Locker)</p> <p> ----- BABUK LO</p>
<p>RTAMINA NESIA</p> <p>ERTAMINA INDONESIA</p> <p>2025-01-28 08:06:03</p>	<p>www.scadea.com 1105</p> <p>www.scadea.com</p> <p>2025-01-27 20:40:04</p>	<p>www.co www.comp</p>
<p>kovra.com.my 940</p> <p>com.my</p> <p>2025-01-27 20:29:00</p>	<p>www.lapastina.com 1157</p> <p>www.lapastina.com</p> <p>2025-01-27 20:29:41</p>	<p>www.ind 1458 www.indus</p>
<p>1345</p> <p>2025-01-27 20:29:07</p>	<p>www.constelacion.com.sv 1368</p> <p>www.constelacion.com.sv</p> <p>2025-01-27 20:29:07</p>	<p>www.ag www.agor</p>

TARGETING PREFERENCES

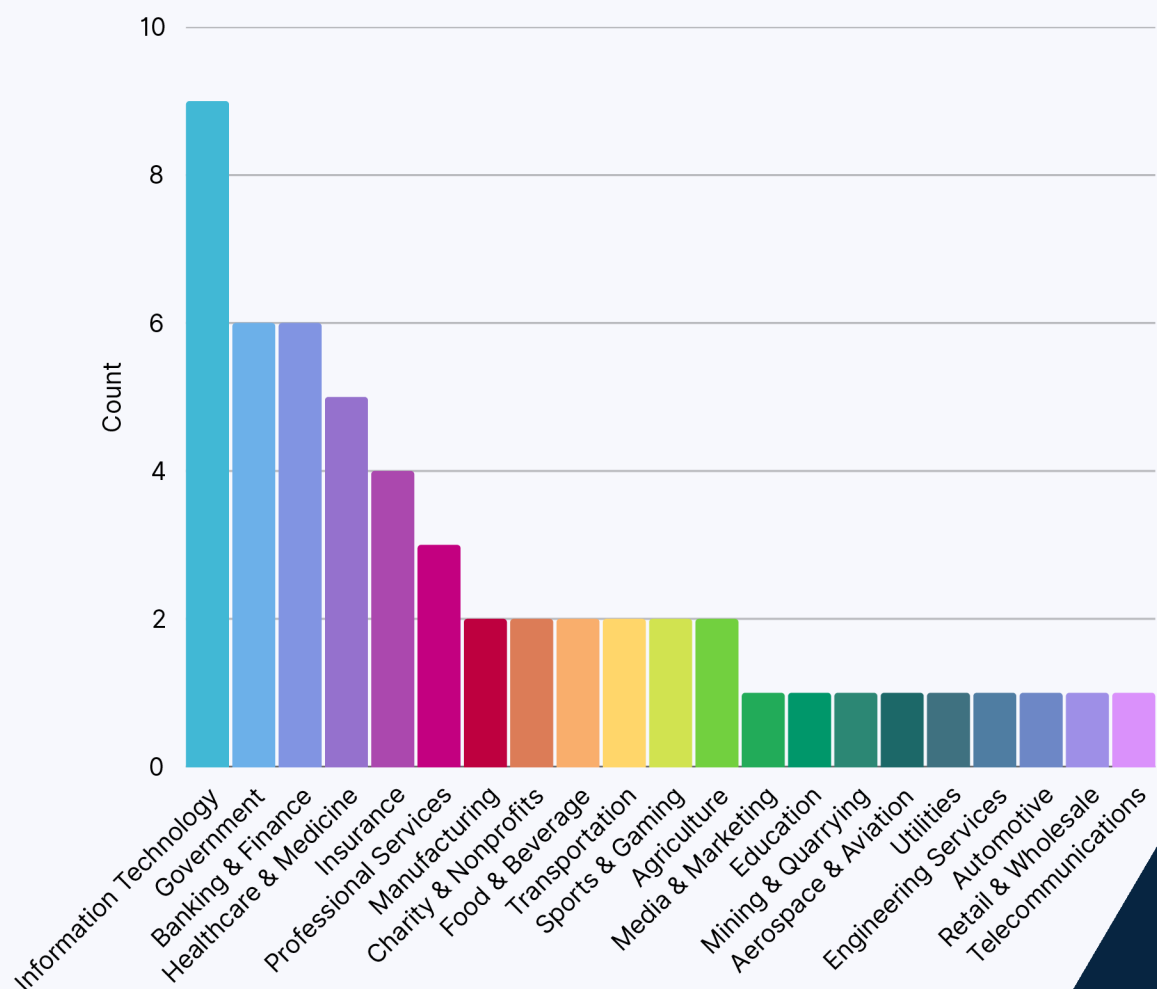
COUNTRY WISE

Babuk-Bjorka primarily targeted the United States, Brazil, and Indonesia, with a mix of developed and developing nations. The U.S. faced the highest number of attacks, likely due to its large corporations and government agencies. Brazil and Indonesia were also major targets, possibly due to cybersecurity gaps in growing digital sectors. Other countries saw fewer attacks, but the spread indicates a broad global reach, targeting both high-value entities and weaker defenses.



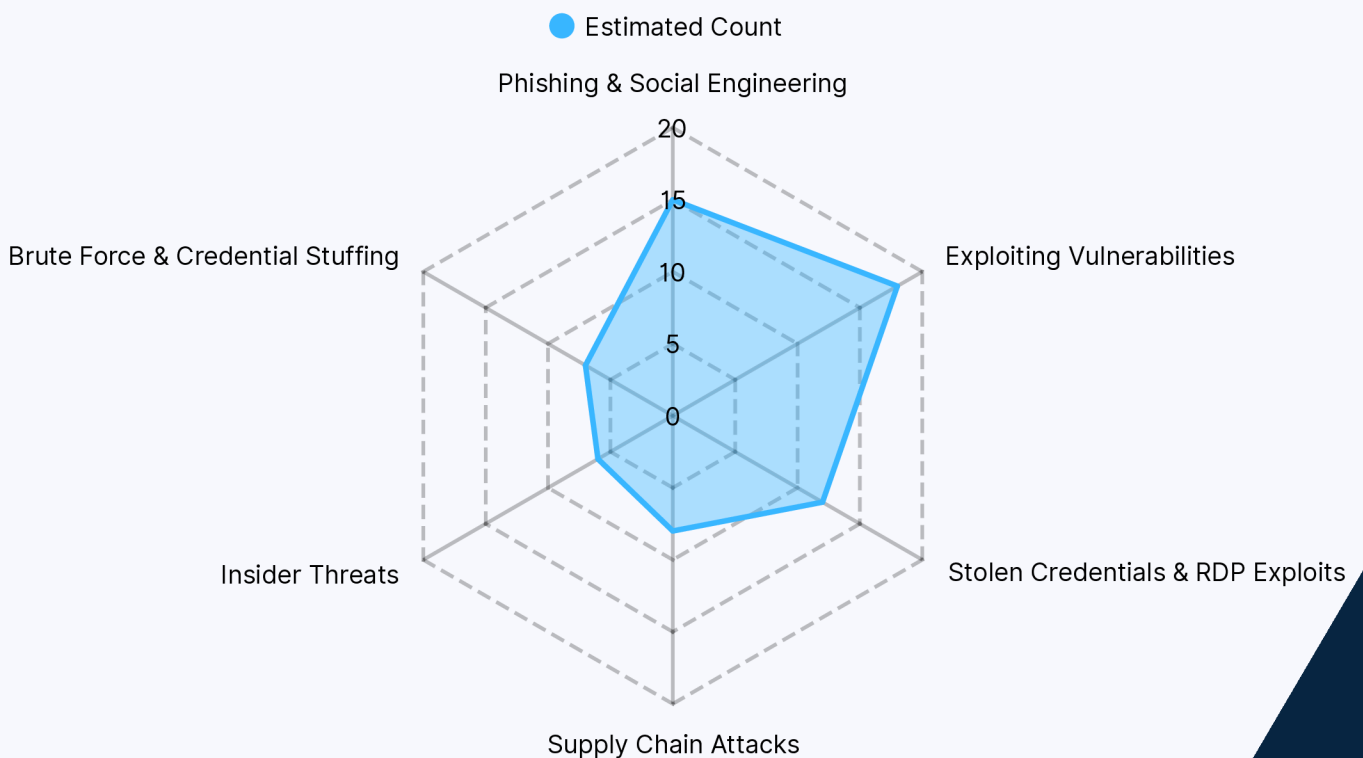
INDUSTRY WISE

Babuk-Bjorka targeted Information Technology, Government, and Banking & Finance sectors the most, likely due to their high-value data and critical operations. Healthcare & Medicine was also a key target, as ransomware attacks can disrupt essential services. Other affected industries included Insurance, Manufacturing, and Professional Services, showing a broad attack surface across both public and private sectors.



ATTACK VECTOR WISE

Babuk-Bjorka used a mix of technical exploits and human-based tactics to infiltrate systems. It primarily relied on exploiting vulnerabilities, phishing attacks, and stolen credentials to gain access. The group also targeted supply chains, leveraged brute force attacks, and, in some cases, used insider threats to bypass security measures. This diverse approach allowed them to compromise organizations across multiple industries and regions.



ATTRIBUTION & ANALYSIS

Mail	locksupport@onionmail.org
-------------	---------------------------

Telegram	@babuklockberOffice
	@bjorkanesiaaaa

Tox	022A7EEB83B648F55DA7A6BEFD130C215 6C74F3501A31D853234EC2D18E77A1E5BE C7F602011
	552653D2E9A5701EA30612EAE77345293F 2E35C5D29DB196BB62395BE71BB25F

Dark Web Link	http://7dikawx73goypgfi4zyo5fcajxwb7agemmiwqax3p54aey4dwobcvcyd[.]onion
	http://bxwu33iefqfc3rxigynn3ghvq4gdw3gxgxna5m4aa3o4vscdeeqhiqad[.]onion

Wallet	BTC: 1JdvS63gBEFH3auYStgeSB3Q2xMdi5cZiF
	XMR: 84aZsdYquVxDCVn49UDS8K89bhKyRzAqB Mef4XxZ7QQ7eSuSPxnpD1oKbhZpE6pqPSG25V 6Z3oRNkfXLuxqxYPzYL4xQPKV
	ETC:0xFd8Cd01BAB931c9aF6a99A5F969a9052b Bee6fd7
	ETH:0x9e2f075d3fff657695dc4661f42115588ee1 3263

File servers	http[:]//gtmx56k4hutn3ikv[.]onion
	<a href="http://xeuvs5poflczn5i5kbynb5rupmidb5zj
uza6gaq22uqsdp3jvkjkciqd.onion">http[:]//xeuvs5poflczn5i5kbynb5rupmidb5zj uza6gaq22uqsdp3jvkjkciqd.onion
	<a href="http://fpwwt67hm3mkt6hdavkfyqi42oo3v
kaggvjj4kxdr2ivsbzyka5yr2qd[.]onion">http[:]//fpwwt67hm3mkt6hdavkfyqi42oo3v kaggvjj4kxdr2ivsbzyka5yr2qd[.]onion
	<a href="http://57mphyfkxoj5lph2unswd23akewz3jt
j7mb6wignwmyto32ghp2visid[.]onion">http[:]//57mphyfkxoj5lph2unswd23akewz3jt j7mb6wignwmyto32ghp2visid[.]onion

NEWS & RECENT DEVELOPMENT

27TH JAN 2025 – BABUK CLAIMED ATTACK ON INDIAN AREOSPACE & ENGINEERING

Claimed data size: 2 GB
Sample Data Attached: 300 MB

Indian Aerospace & Engineering in Mumbai is a top institute for Aircraft Maintenance Engineering, part of Sha Shib Group, the largest in South Asia for AME training.

In December 2024, the cybercriminal group Funksec claimed responsibility for a data breach involving Indian Aerospace & Engineering. Details about the breach, including the volume and nature of the compromised data, have not been publicly disclosed.

It's important to note that Funksec is distinct from the Babuk ransomware group. While both are involved in cybercriminal activities, there is no evidence linking Babuk to this particular incident. Additionally, some ransomware groups have been known to falsely claim responsibility for attacks or recycle data from previous breaches to enhance their notoriety.



BABUK

indianaerospaceandengineering.com

indianaerospaceandengineering.com



Greetings!

Today we are posting here the new company - indian aerospace and engineering.com

The database contains documents size above 2GB. sample free 300MB enjoy
About indian aerospace and engineering.com

Established in 2006, Indian Aerospace and Engineering, Mumbai is managed by Sha-Shib Group of Institutions. It is recognized by the Directorate General of Civil Aviation, Ministry of Civil Aviation, Government of India, and complies with CAR-147 (Basic rules)

Contact Us

Tox ID Support

Tox ID Support

Download links:

5GM0lo

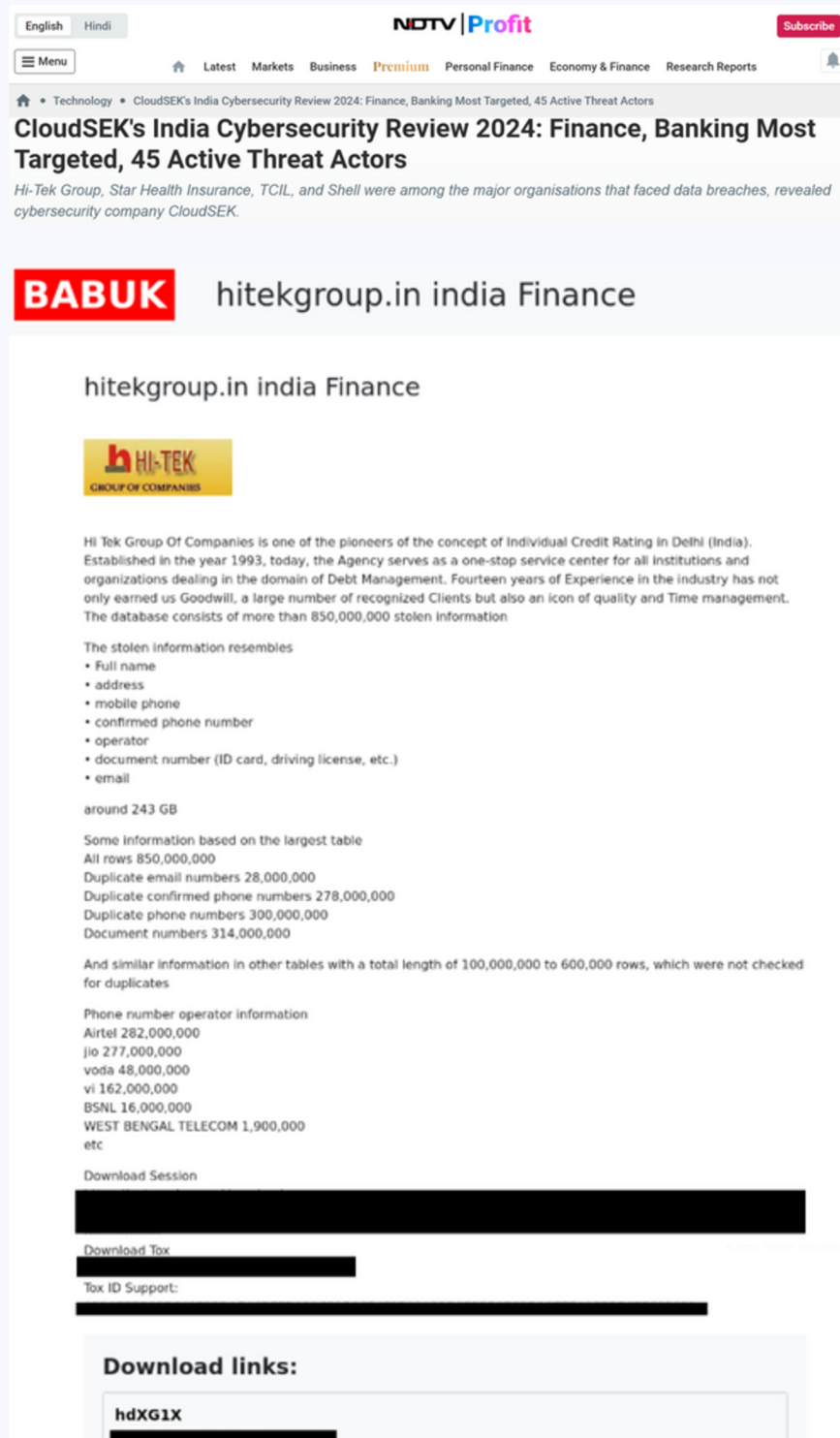
12TH MAR 2025 – BABUK CLAIMED ATTACK ON HITEK FINANCE GROUP & LEAKING PII

Claimed data size: 243 GB

Stolen Data include Full Name, Address, Mobile number, operator details, document number (ID Card, driving license, etc.), email

Hi Tek Group of Companies is one of the pioneers of the concept of individual Credit Rating in Delhi. Established in the year 1993, today, the Agency serves as a one-step service center for all institutions and organizations dealing in the domain of Debt Management. Fourteen Years of Experience in the industry has not only earned Goodwill, a large number of recognized Clients but also an icon of quality and time management.

While the exact ransom amount and volume of stolen data remain undisclosed, the attackers allegedly exfiltrated sensitive financial records and internal documents. The attack on HitekGroup highlights the continued targeting of financial institutions by ransomware groups, aiming for data theft, extortion, and operational disruption.

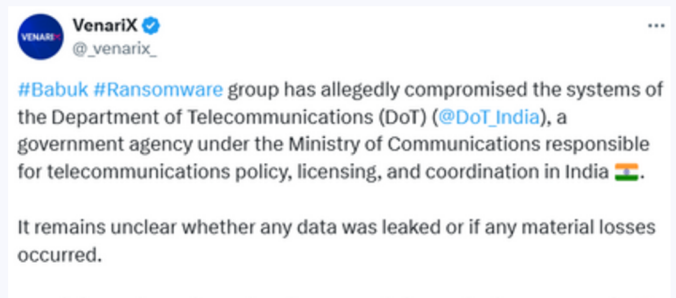


The image shows a screenshot of a news article from NDTV Profit titled "CloudSEK's India Cybersecurity Review 2024: Finance, Banking Most Targeted, 45 Active Threat Actors". The article mentions that Hi-Tek Group, Star Health Insurance, TCIL, and Shell were among the major organizations that faced data breaches. Below the article is a screenshot of the Babuk ransomware site, which displays the Hitekgroup.in logo and a list of stolen information, including full names, addresses, mobile numbers, confirmed phone numbers, operator details, document numbers (ID cards, driving licenses, etc.), and email addresses. The site also mentions a data size of around 243 GB and provides a list of phone numbers for various operators, including Airtel, Jio, Vodafone, Vi, BSNL, and West Bengal Telecom. The site includes a "Download Session" button and a "Download links" section with a link labeled "hdXG1X".

12TH MAR 2025 – BABUK CLAIMED ATTACK ON INDIA'S TELECOMMUNICATION NETWORK

Claimed data size: 1.8 TB

Stolen Data include Subscriber name, mobile number, address, national id number, photo, relative name, etc.



In March 2025, the Babuk2 ransomware group claimed responsibility for an attack on India's telecommunication network. The attack allegedly targeted a major telecom company, compromising sensitive customer data, internal documents, and network infrastructure details.

The breach reportedly affected critical communication services, posing risks to data security and operational continuity. However, specific details regarding the extent of the stolen data, ransom demands, or impact on services have not been publicly disclosed.

ABUK India's telecommunication network

India's telecommunication network Companies Indian



India's telecommunication network
Information Company:

India's telecom network is the second largest in the world by number of telephone users (both fixed and mobile) with over 1.19 billion subscribers as of September 2024. Its call rates are among the lowest in the world, made possible by the large number of large telecom operators and intense competition among them. India has the second largest internet user base in the world with over 949.21 million broadband internet subscribers as of September 2024.

Country: indian

Information: This dataset offers comprehensive mobile network consumer information for around 750 million individuals in India, which covers 85% of the population.

Stolen information

- person name: subscriber name
- phone number: mobile number
- alternate number: secondary contact number
- address: residential address
- national id number: national identification number (e.g. Aadhaar number)
- photo id number: government-issued photo identification number
- relative name: family member name

around 750 Million user information we have stolen

Compressed data size 600GB

Uncompressed data size 1.8TB

Download Session

Download Tox

Tox ID Support:

Download links:

ekYAH5

14TH MAR 2025 – BABUK CLAIMED ATTACK ON DRDO SERVERS LEAKING TOP SECRET DATA

Claimed data size: 20 TB

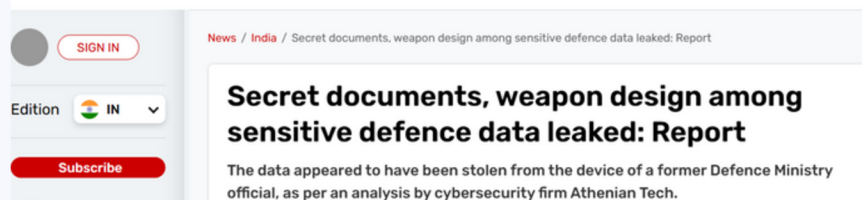
The claimed Stolen Data include secret documents regarding Indian Navy, Missile Systems, Employee details, Defense Technology, borders, troops, etc.

In March 2025, the ransomware group Babuk Locker 2.0 claimed to have exfiltrated 20 terabytes (TB) of sensitive data from India's Defence Research and Development Organisation (DRDO). The group released a 753 MB sample of the alleged data, which reportedly included:

- Weapon designs, such as engineering schematics for the T9 Bhishma Tank upgrade.
- Procurement plans and details of India's defense collaborations with countries like Finland, Brazil, and the United States.
- Evacuation protocols for high-profile officials, including the President and Prime Minister, in case of aerial threats.

However, analyses by cybersecurity firm Athenian Tech suggest that the breach likely originated from the personal device of Puneet Agarwal, a former Joint Secretary in the Defence Ministry (2019-2021). The compromised data included his Aadhaar details, financial records, and personal travel documents, indicating that DRDO's core IT infrastructure may not have been directly breached.

INDIA TODAY



MITIGATION STRATEGIES

Protecting against threat actors like Babuk-Bjorka requires a multi-faceted approach that combines proactive security measures with robust incident response capabilities:

BASIC AND IMMEDIATE SECURITY MEASURES

- Enforce Multi-Factor Authentication (MFA) for all users, especially those with privileged access.
- Deploy Endpoint Detection and Response (EDR) tools for real-time anomaly detection.
- Conduct employee awareness programs on phishing and social engineering.
- Implement dark web monitoring to detect early signs of data exposure.

ADVANCED PREVENTIVE PRACTICES

- Adopt a Zero Trust Architecture (ZTA)—no user or device is trusted by default.
- Regularly patch all systems and third-party tools to close known vulnerabilities.
- Perform Red Team vs. Blue Team exercises to evaluate and improve cyber defenses.
- Limit access based on the principle of least privilege (PoLP).
- Restrict or monitor the use of personal devices for official work.
- Apply network segmentation to reduce lateral movement in case of a breach.
- Encrypt all sensitive data at rest and in transit.

ORGANIZATION-SPECIFIC MITIGATIONS

SIEM Implementation & Monitoring

- Deploy and configure a robust SIEM solution (e.g., Splunk, Elastic, Wazuh).
- Integrate logs from endpoints, servers, firewalls, AD, and VPNs for real-time correlation.
- Enrich SIEM with threat intelligence feeds for contextual awareness.

Proactive Threat Hunting & Red Teaming

- Hunt for persistence mechanisms like scheduled tasks, service modifications, or registry changes.
- Scan for MITRE techniques like Masquerading (T1036) and Impair Defenses (T1562).
- Simulate attack paths used by Babuk in controlled environments to test detection and response.

Behavioral & Network Monitoring

- Enable DNS logging to detect tunneling behavior.
- Monitor RDP usage, especially from unexpected geolocations or outside office hours.
- Track privilege escalation attempts and sudden permission changes in user accounts.

Endpoint & Server Hardening

- Disable execution from temporary directories and user profile folders.
- Use application allowlisting to restrict execution of unauthorized binaries.
- Regularly audit Group Policy settings and restrict administrative privileges.

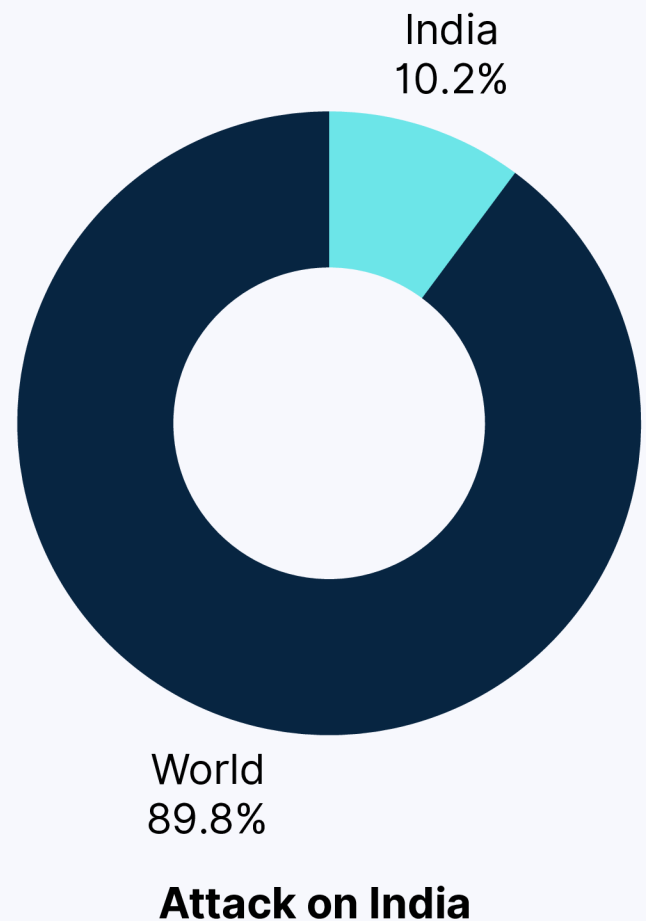
Custom SIEM Detection Rules

- Alert on unusual login patterns or lateral movement activities.
- Detect execution of dual-use tools such as PowerShell, PsExec, and RAR archivers.
- Trigger alerts on outbound data transfer anomalies, especially to external IPs over encrypted channels.

CONCLUSION

Babuk-Bjorka has emerged as a persistent and evolving cyber threat, leveraging sophisticated ransomware tactics to target organizations across multiple sectors worldwide. With a focus on financial extortion, data theft, and operational disruption, the group has demonstrated adaptability by shifting from encryption-based ransomware to data leak extortion.

Its attacks have primarily impacted industries such as finance, healthcare, government, and critical infrastructure, emphasizing the growing risks posed by ransomware-as-a-service (RaaS) operations. While law enforcement efforts have disrupted Babuk's original operations, variants and successor groups continue to pose a significant threat. The rise of Babuk-Bjorka highlights the need for robust cybersecurity defenses, including proactive threat intelligence, incident response planning, and strong access controls. Organizations must stay vigilant, adopt zero-trust architectures, and strengthen their data protection mechanisms to mitigate the risks of ransomware attacks.



REFERENCES

Watchguard

- <https://www.watchguard.com/wgrd-ransomware/babuk>
- <https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/bjorkanism>

RansomLook

- <https://www.ransomlook.io/group/babuk-bjorka>

SOCRadar

- <https://socradar.io/what-is-babuk-the-ransomware-gang-you-should-know-about>

RedPacket Security

- <https://www.redpacketsecurity.com/babuk2-ransomware-victim-hitekgroup-in-india-finance>

Breach Sense

- <https://www.breachsense.com/breaches/indian-aerospace-engineering-data-breach/>

Ransomware Live

- <https://www.ransomware.live/group/babuk2>

India Today

- <https://www.indiatoday.in/india/story/secret-documents-weapon-design-among-sensitive-defence-data-leaked-report-2700673-2025-03-28>