



BASHE (APT73)

THREAT **REPORT**

CERTMH_CTI_2025_12

2025

.....

TABLE OF CONTENTS

▶ Introduction	03
▶ Background	04
▶ Objectives	04
▶ MITRE ATT&CK TTPs	05
▶ Attack Campaign	06
▶ Targeting Preferences	07
▶ Attribution & Analysis	10
▶ News & Recent Developments	12
▶ Mitigation Strategies	17
▶ Conclusion	19
▶ References	20

INTRODUCTION

BASHE



APT73, also known as Bashe, is a ransomware group that emerged in March 2024, self-identifying as an Advanced Persistent Threat (APT). The group has been linked to the LockBit ransomware variant, adopting similar operational tactics and utilizing a TOR-based data leak site for extortion purposes. APT73 has targeted various industries, including finance and technology. In June 2024, the group claimed responsibility for a ransomware attack on AlphaNovaCapital, a boutique investment firm based in Hong Kong. The attack resulted in the exfiltration and leakage of sensitive documents, highlighting the vulnerabilities of financial institutions to cyber threats.

APT73's tactics include phishing attacks to gain initial access, followed by data exfiltration and encryption. The group employs a TOR-based data leak site to publish stolen data, pressuring victims into paying ransoms to prevent public exposure. Organizations are advised to implement robust cybersecurity measures, including regular data backups, system updates, and employee training, to mitigate the risk of falling victim to such ransomware campaigns.

- **Aliases:** Eraleig



BACKGROUND

APT73, also known as Bashe, is a ransomware group that surfaced in March 2024. It operates using double extortion tactics, encrypting victim data while also stealing and threatening to leak it unless a ransom is paid. The group has primarily targeted finance, IT services, and consumer sectors in India, exploiting vulnerabilities in organizations handling sensitive information. APT73's operations closely resemble those of the LockBit ransomware gang, raising speculation that it could be a spinoff or an affiliate. Their dark web leak site structure and ransom negotiation tactics mirror LockBit's approach, suggesting a shared playbook or direct inspiration.

OBJECTIVES

APT73's objectives align with those of most ransomware groups, focusing on financial gain and disruption. Its key goals include:

- **Data Encryption & Extortion** – Encrypting victim data and demanding ransom payments for decryption keys.
- **Double Extortion** – Stealing sensitive data and threatening to leak it if the ransom is not paid.
- **Targeting High-Value Sectors** – Focusing on finance, IT services, and consumer industries to maximize impact.
- **Reputation Building** – Establishing credibility in the cybercriminal ecosystem by mimicking well-known groups like LockBit.
- **Attracting Affiliates** – Potentially exaggerating attack claims to draw in cybercriminal collaborators.

These objectives indicate that APT73 aims to enhance its standing among ransomware groups while profiting from cyber extortion.

MITRE ATT&CK TTPs



Initial Access:

- **Phishing (T1566):** APT73 uses phishing emails to gain initial access to target systems.

Execution:

- **Command and Scripting Interpreter: PowerShell (T1059.001):** Utilizes PowerShell scripts to execute malicious commands.
- **Exploitation for Client Execution (T1203):** Exploits vulnerabilities in client applications to execute code.

Persistence:

- **Scheduled Task/Job: Scheduled Task (T1053.005):** Creates scheduled tasks to maintain persistence on compromised systems.
- **Boot or Logon Autostart Execution: Registry Run Keys (T1547.001):** Adds entries to registry run keys for automatic execution upon system startup.

Impact:

- **Data Encrypted for Impact (T1486):** Encrypts data on target systems to disrupt operations and demand ransom.

Lateral Movement:

- **Remote Services: SMB/Windows Admin Shares (T1021.002):** Uses SMB and admin shares to move laterally within the network.


Privilege Escalation:

- **Exploitation for Privilege Escalation (T1068):** Exploits system vulnerabilities to gain higher-level privileges.
- **Abuse Elevation Control Mechanism: Bypass User Account Control (UAC) (T1548.002):** Bypasses UAC to execute tasks with elevated privileges

Defense Evasion:

- **Process Injection (T1055):** Injects malicious code into legitimate processes to evade detection.
- **Impair Defenses: Disable or Modify Tools (T1562.001):** Disables or modifies security tools to avoid detection.

ATTACK CAMPAIGNS



ANONYMOUS LEAKED DATA FROM APT73

Trick or treat

<p>PUBLISHED</p> <p>WWW.TRIFECTA.COM</p> <p>Information: Trifecta is a trusted advisor for some of the most widely recognized and successful companies in the world. Brands choose Trifecta bas...</p> <p>🕒 2024/04/05 07:37:45 UTC +0</p>	<p>PUBLISHED</p> <p>MELTING-MIND.DE</p> <p>German company melting-mind.de. IT systems company operating throughout Europe and offering a wide range of services in all areas of information te...</p> <p>🕒 2024/06/03 08:00:00 UTC +0</p>	<p>PUBLISHED</p> <p>WWW.CREDIO.EU</p> <p>Czech company Credio. IT consulting, electronic document management. Credits to internal systems. 11 MB</p> <p>🕒 2024/05/09 11:00:00 UTC +0</p>	<p>PUBLISHED</p> <p>WWW.SERVICEPOWER.COM</p> <p>Large software development company Service Power. Great Britain. Documents of internal systems, credits to internal resources. 328 MB</p> <p>🕒 2024/05/09 10:00:00 UTC +0</p>
<p>PUBLISHED</p> <p>FORTIFY.PRO</p> <p>The Canadian company has been developing high-quality and reliable software for corporate needs since 2015. They are renowned professionals of soft...</p> <p>🕒 2024/05/18 10:00:00 UTC +0</p>	<p>PUBLISHED</p> <p>BRIGHTWAYCONSULTANTS.CO.UK</p> <p>Brightway Consultants Ltd is a chartered surveying firm based in London. They offer comprehensive surveying services tailored to clients' individua...</p> <p>🕒 2024/06/04 10:00:00 UTC +0</p>	<p>PUBLISHED</p> <p>AMI GLOBAL ASSISTANCE</p> <p>Your trusted partner for personalized, timely, and reliable medical support services worldwide.</p> <p>https://x.com/AMIGlobalAssist Personal data, pas...</p> <p>🕒 2024/06/21 10:10:00 UTC +0</p>	<p>PUBLISHED</p> <p>ALPHANOVACAPITAL</p> <p>Private limited Company 272KB</p> <p>🕒 2024/06/21 10:10:00 UTC +0</p>
<p>PUBLISHED</p> <p>APEX.UK.NET</p> <p>Apex Engineering Service has established itself as a leading supplier of technical services to the construction industry worldwide. Passwords, int...</p> <p>🕒 2024/06/21 10:10:00 UTC +0</p>	<p>PUBLISHED</p> <p>WWW.BIGALSFOODSERVICE.CO.UK</p> <p>Our foodservice roots trace all the way back to a butchers shop in Dublin city centre in 1966. Kepak Foodservice specialise in creating innovative,...</p> <p>🕒 2024/06/24 10:00:00 UTC +0</p>	<p>PUBLISHED</p> <p>BORRER EXECUTIVE SEARCH</p> <p>Borrer Executive Search is an AESC accredited boutique search and selection firm based in Lausanne, Switzerland. Internal documents, agreements ...</p> <p>🕒 2024/06/24 10:00:00 UTC +0</p>	<p>PUBLISHED</p> <p>WWW.GANNONS.CO.UK</p> <p>Gannons Commercial Law Limited Catherine Gannon, then a tax solicitor at a large US law firm, looks out from their ivory tower and spots a gap in ...</p> <p>🕒 2024/06/25 10:00:00 UTC +0</p>
<p>4D 3H 55M 1S</p> <p>GLOBACAP.COM</p> <p>Globacap is an innovative private markets ecosystem that allows you to</p>	<p>4D 3H 55M 1S</p> <p>WWW.PINDROPHEARING.CO.UK</p> <p>We're specialists in the diagnosis and treatment of hearing conditions, but</p>	<p>4D 3H 55M 1S</p> <p>RYLANDPETERS.COM</p> <p>Ryland Peters & Small and CICO Books is an independent, illustrated publisher</p>	

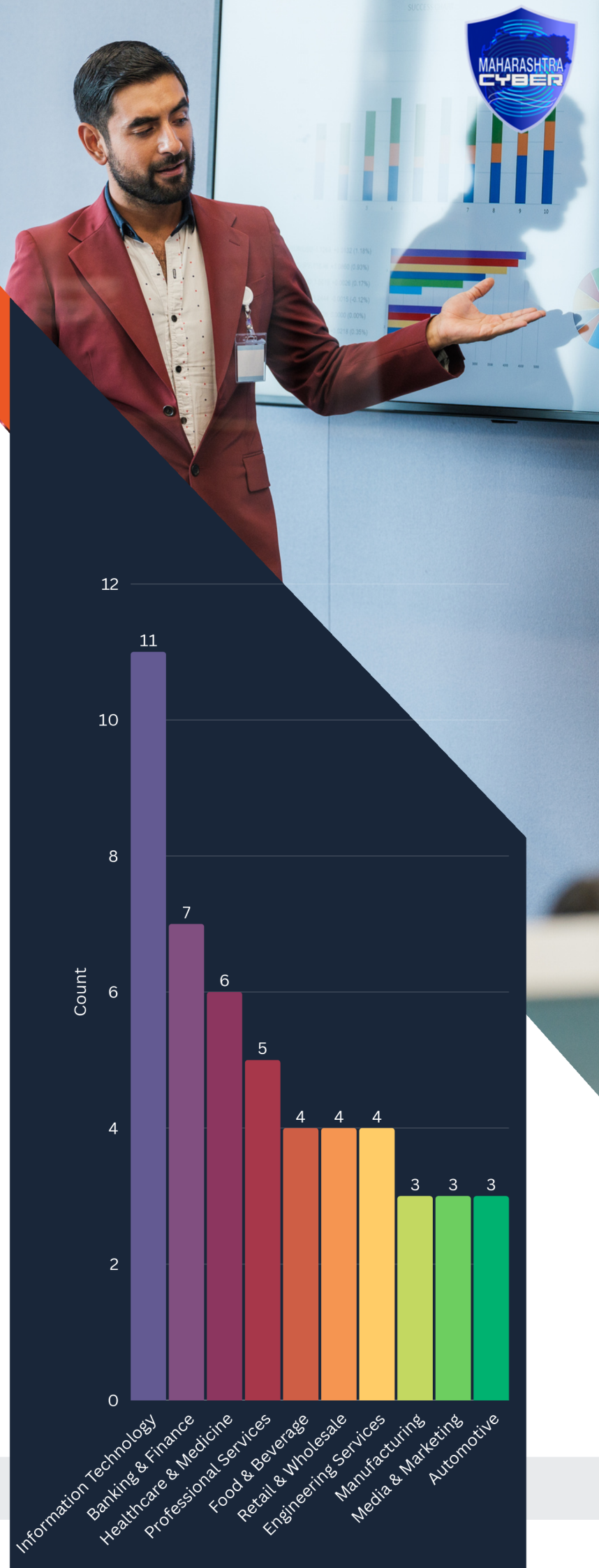
Bashe APT73's attacks typically begin with a highly targeted spear-phishing campaign. Emails are crafted to appear legitimate, often impersonating trusted individuals or organizations. These emails contain malicious attachments (e.g., weaponized Word documents or PDFs) or links to compromised websites. Once the initial foothold is established, the group deploys custom malware and utilizes various techniques to move laterally, escalate privileges, and exfiltrate data. Threat actors may also abuse Google Ads.

TARGETING PREFERENCES

INDUSTRY WISE

APT73 has demonstrated a strategic approach to its ransomware campaigns, focusing mostly on developed nations and industries where data sensitivity and operational disruption are most impactful. By leveraging double extortion tactics, the group not only encrypts victims' files but also threatens to expose stolen data on its DLS to maximize financial gain and coerce compliance.

APT73's industry-specific focus underscores its methodical approach to victim selection. Technology companies are targeted for their valuable intellectual property, healthcare organizations for critical patient data, and financial institutions for sensitive records and transactional data. The group also disrupts supply chains in manufacturing and logistics, exploits operational systems in transportation, and capitalizes on large-scale investments in construction projects.

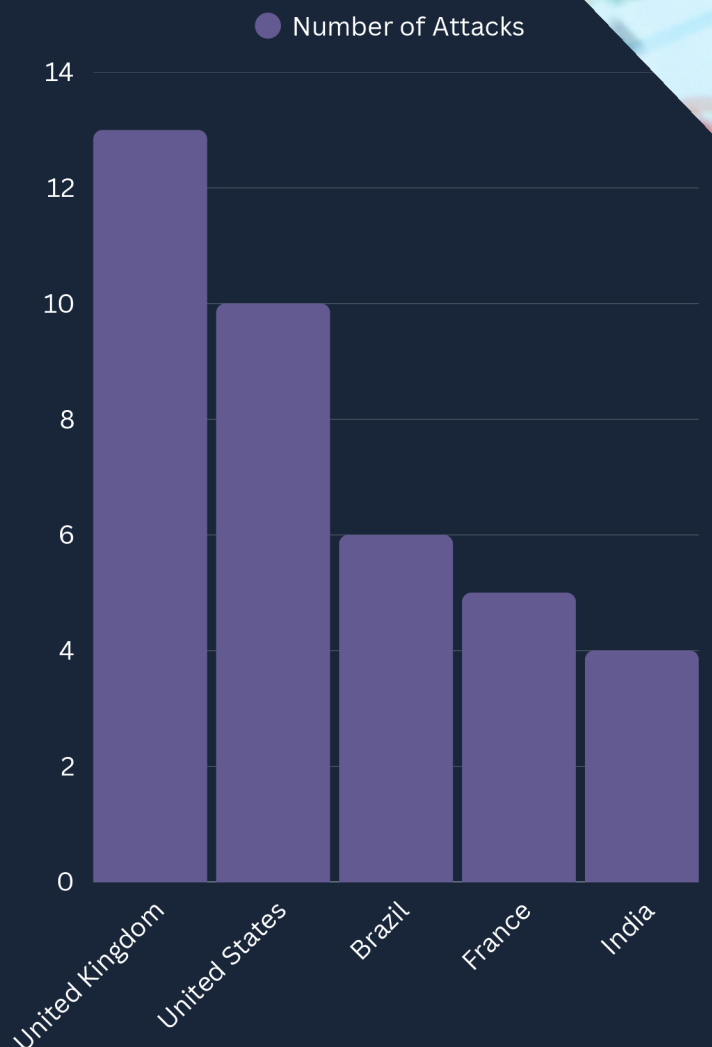


COUNTRY WISE

The group's operations span several countries, with victims identified in the United States, United Kingdom, France, Germany, India, and Australia. In the United States, APT73 has primarily targeted the technology, healthcare, and financial services sectors, exploiting their reliance on sensitive data and operational continuity.

Insights:

- UK (13 attacks) & US (10 attacks) are the top targets, possibly due to their economic impact.
- India (4 attacks) is emerging as a key target, especially in banking, media, and government sectors.
- Brazil, France, and Canada (6, 5, and 4 attacks respectively) indicate growing ransomware activity in South America and Europe.

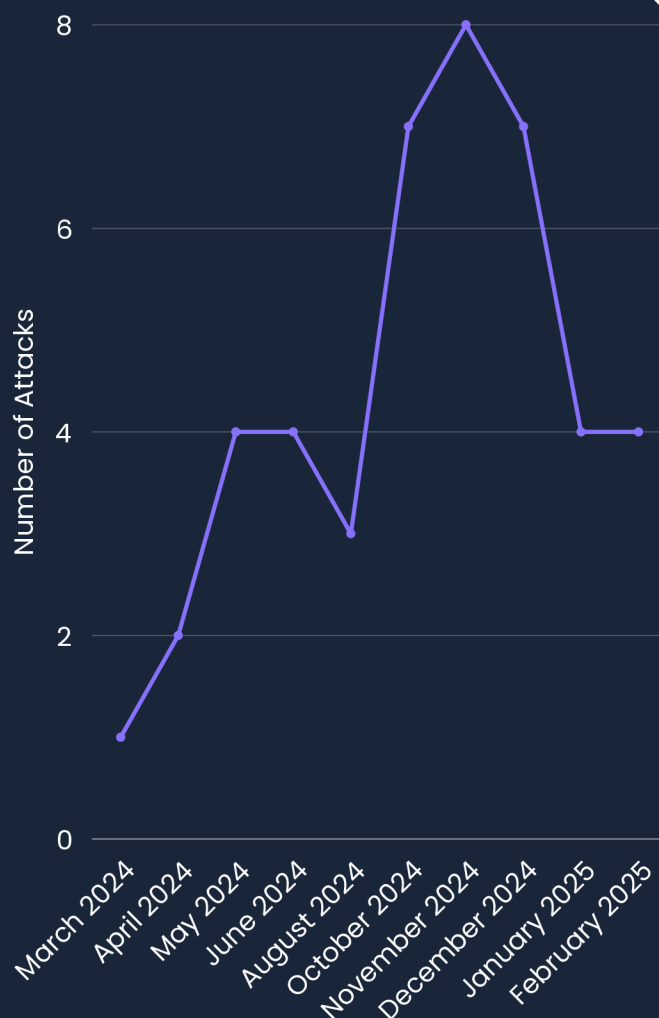


MONTHLY TRENDS IN ATTACK

The group's operations span several countries, with victims identified in the United States, United Kingdom, France, Germany, India, and Australia. In the United States, APT73 has primarily targeted the technology, healthcare, and financial services sectors, exploiting their reliance on sensitive data and operational continuity.

Insights:

- Attack activity increases in Q4 (October–December), indicating a possible preference for financial quarter closings.
- November 2024 saw the highest attacks (8 incidents), possibly exploiting end-of-year vulnerabilities.
- March–June sees moderate activity, possibly targeting budget cycles or financial reporting periods.



ATTRIBUTION & ANALYSIS



EXTORTION TYPES

Direct Extortion

Double Extortion

Free Data Leaks

COMMUNICATION

Medium	Identifier
Email	apt73[.]group@onionmail[.]org
Email	bashe[.]team@onionmail[.]org
Telegram	https://t.me/apt73_official
Telegram	https://t.me/bashe_admin
Telegram	https://t.me/bashe_team_official
Tox	9796CE1E72A8874D594F6573F44C94FB649473B4 194DCD80C406BFE88E4B3662A375E78FB436
Twitter X	https://x.com/bashe_team



FILE SERVER

File Servers

http[:]//7bbqrijcds5sgji3kiwo5o5qgxfgoyufykhzfd06xl3qbdes2e7tdyad[.]
onion

http[:]//bashe4aec32kr6zbifwd5x6xgjsmhg4tbowrbx4pneqhc5mqooyif
pid[.]onion

http[:]//bashed52orwi7qoyvmcfkdnuagta4inpojfd6cthzkp4qpsq64ux4ad[.]onion

http[:]//bashedl53memptddxzb4kr5mnkzse4fmhpeqeq7jb4srndswar46
nofid[.]onion

http[:]//bashefe5uezp2jtxpk24b2pyfnnfyguicgrgqufgu57mfluegotbeay
d[.]onion

http[:]//bashei5oy4zvmf2letnupwhgprdkjyssm3zxj2oyr6wfezkf3elehzqd[.]onion

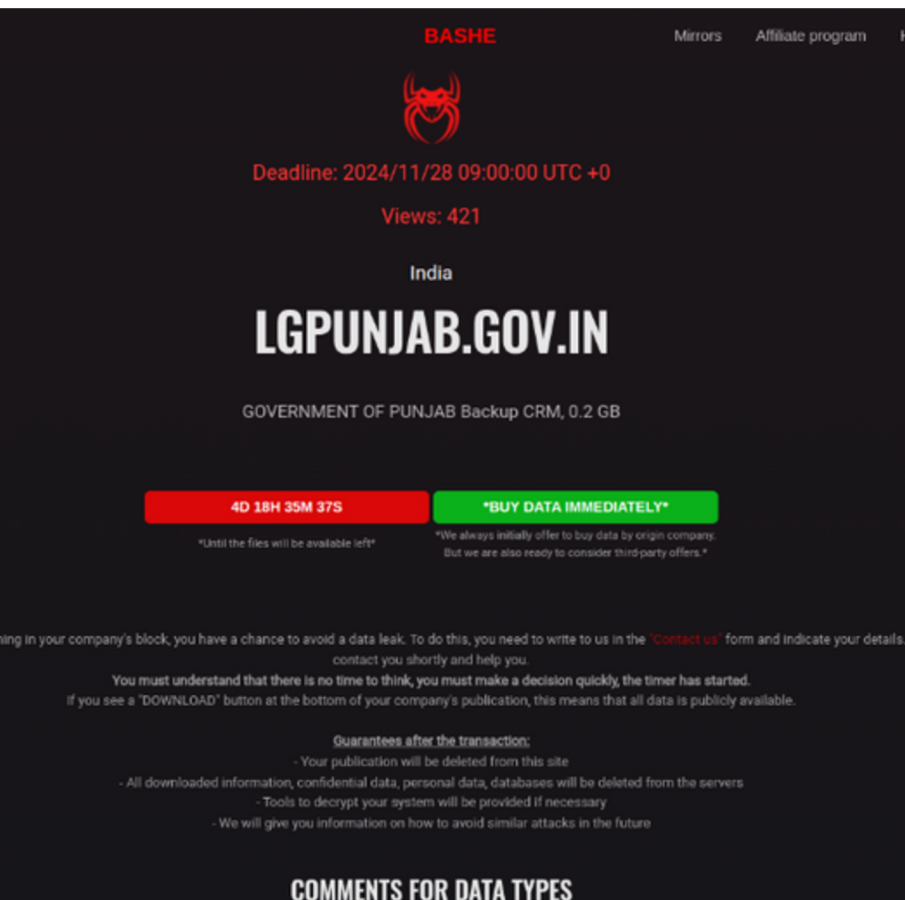
http[:]//qku4reiyfcs2vqq5tow2uprhyqhweo56lrgs6457svr3ej4ton5frkad[
.]onion

In October 2024, the ransomware group APT73, also known as Bashe, claimed responsibility for a cyberattack on filmai.in, an Indian movie streaming service. The breach reportedly involved the exfiltration of approximately 645,000 records containing user data such as email addresses, usernames, and passwords.

- * Estimated Data Stolen:
Around 645,000 user records (including email addresses, usernames, and passwords).
- * Estimated Ransom Demand/Data Sale Price:
Between \$50,000 to \$100,000, based on typical ransomware extortion tactics for similar breaches.

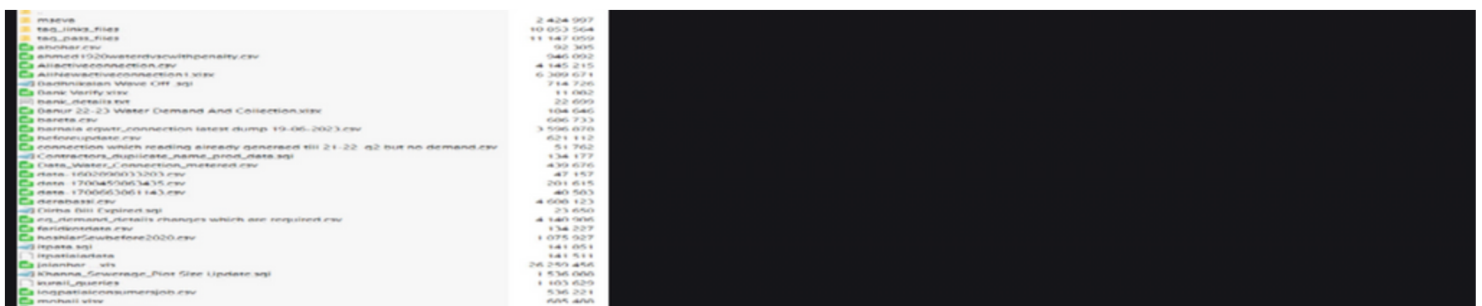
12

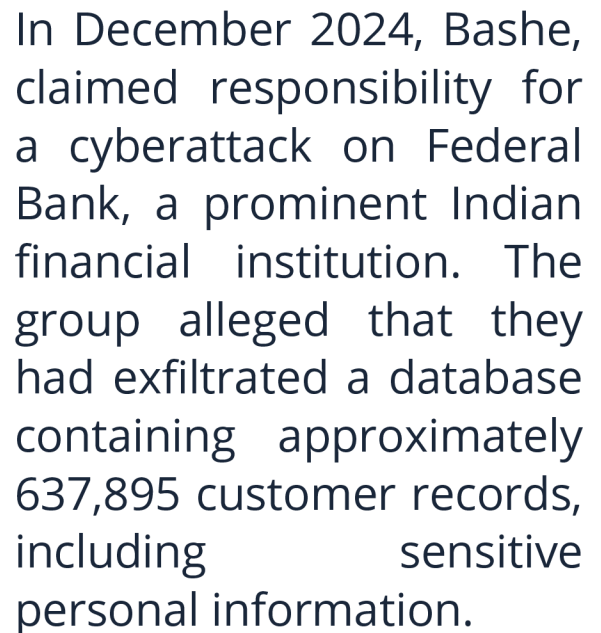
23th Nov 2024 – Bashe attack on GOVERNMENT OF PUNJAB Backup CRM



In November 2024, the ransomware group APT73, claimed responsibility for a cyberattack on the Government of Punjab's Backup CRM 2.0 system. The group alleged that they had exfiltrated approximately 0.2 GB of data from the system.

- * The Department of Local Government Punjab is responsible for directing, supervising, and controlling the functioning of all the Municipal Corporations, Municipal Councils, Nagar Panchayats, and Improvement Trusts in the state.

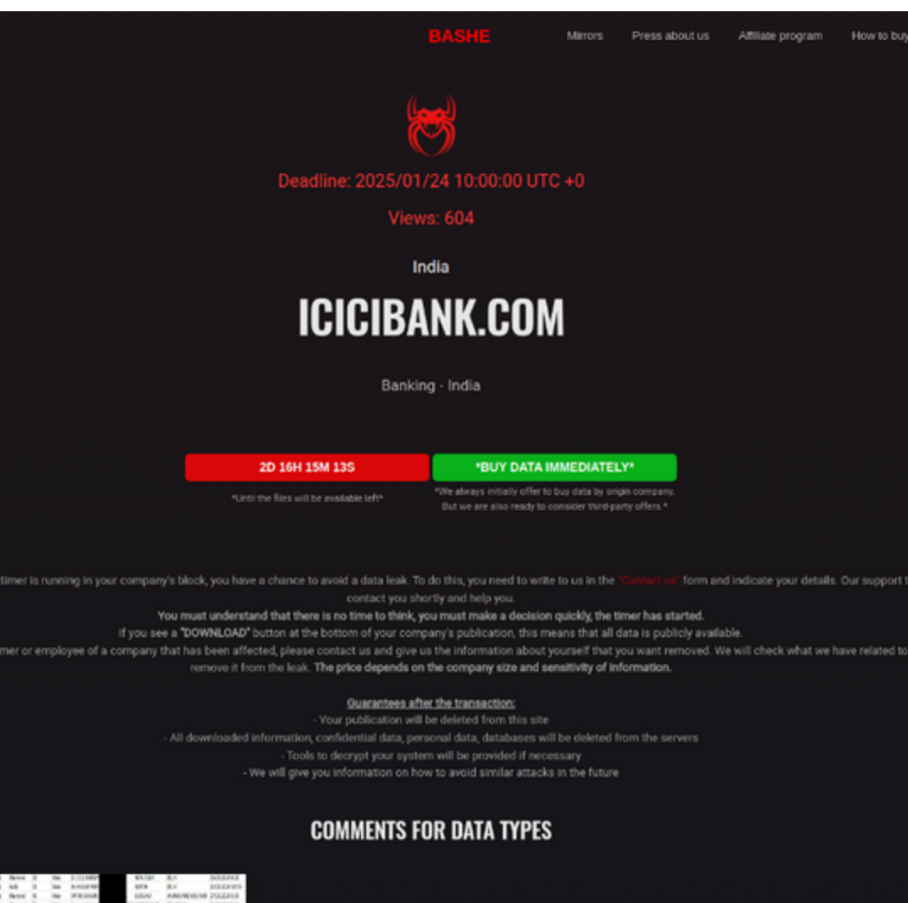




- ✱ APT73 claimed responsibility for the cyberattack on Federal Bank, alleging the theft of sensitive customer data, include: Customer Names, Customer IDs, Addresses, Dates of Birth, Mobile Numbers, PAN Numbers, Driving License Numbers, Passport Numbers, UID (Aadhaar) Numbers, Voter ID Information.

14

21st Jan 2025 – Bashe attack on ICICI Bank

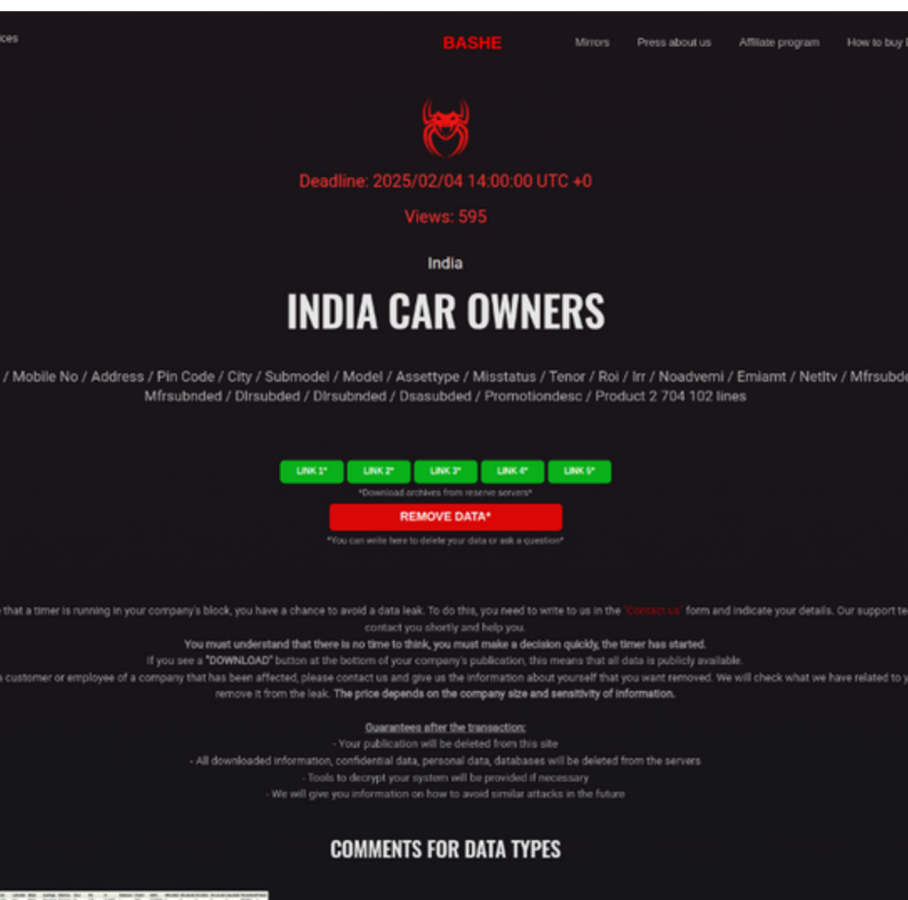


In January 2025, BASHE, claimed responsibility for a cyberattack on ICICI Bank, one of India's leading financial institutions. The group alleged that they had breached the bank's internal systems and exfiltrated sensitive data, including information related to approximately 63,778 employees, 40,686 users, and interactions with 392 third-party entities across 116 distinct domains.

- ❖ BASHE set an initial ransom deadline of January 24, 2025, threatening to release the stolen data if their demands were not met. However, reports indicate that the deadline was extended to January 31, 2025, with no files leaked as of that date.

[illegible]

2nd Feb 2025 – APT73 attack on India Car Owners



In February 2025, APT73, claimed responsibility for a cyberattack targeting Indian car owners. The group alleged that they had exfiltrated sensitive personal data, including names, mobile numbers, addresses, pin codes, city names, and specific vehicle details such as model and asset type.

- * This incident is part of a broader trend of ransomware attacks targeting the automotive industry. In early 2025, a surge of such attacks was observed, affecting various sectors within the automotive industry, including parts manufacturers, dealerships, and service providers.



MITIGATION STRATEGIES

To defend effectively against ransomware attacks like those executed by APT73, organizations must implement a multi-layered security strategy. Below are key measures to minimize the risk of such attacks:

Preventing Initial Access

- **Patch Management:** Regularly update and patch systems, particularly public-facing applications, to address vulnerabilities attackers might exploit.
- **Network Segmentation:** Isolate sensitive systems and critical data to limit lateral movement within the network.
- **Access Controls:** Use firewalls, Intrusion Prevention Systems (IPS), and secure VPNs to monitor and control access to remote services.

Strengthening Identity Security

- **Multi-Factor Authentication (MFA):** Implement MFA across critical systems to protect against unauthorized access and brute-force attacks.
- **Strong Password Policies:** Enforce complex, unique passwords that are rotated regularly and managed securely with password managers.
- **Employee Training:** Educate users on phishing risks and secure password practices to prevent credential-based attacks.

Monitoring and Protecting Credentials

- **Dark Web Monitoring:** Regularly track credential dumps and leaks on the Dark Web to identify exposed data early.
- **Account Lockouts:** Set thresholds for failed login attempts to prevent brute-force attacks and unauthorized access.



Preventing Malware Execution

- **Endpoint Detection and Response (EDR):** Deploy tools that can detect unauthorized activities, including suspicious behaviors and new account creations.
- **Application Whitelisting:** Only allow approved applications to run within the network to reduce the chances of malware execution.
- **Behavioral Analytics:** Use behavioral monitoring tools to detect anomalous activities indicative of ransomware behavior.

Limiting Persistence and Lateral Movement

- **Principle of Least Privilege (PoLP):** Regularly review and limit user privileges to minimize attack surfaces.
- **Harden Remote Services:** Disable unnecessary services like Remote Desktop Protocol (RDP) and restrict Server Message Block (SMB) access.
- **Network Traffic Monitoring:** Monitor network traffic for signs of lateral movement or command-and-control communications.

Mitigating Ransomware Impact

- **Data Backup:** Ensure regular offline backups and regularly test restoration procedures to maintain business continuity during an attack.
- **Isolated Backup Systems:** Keep backups isolated from the main network to protect them from being encrypted during a ransomware attack.
- **Incident Response Plan:** Develop and maintain an incident response plan to quickly contain, communicate, and recover from ransomware attacks.

Post-Incident Recovery

- **Ransomware Decryption Tools:** Check for available decryption tools from trusted sources like No More Ransom to recover encrypted files.
- **Forensics and Logging:** Analyze attack logs to identify attack vectors and improve future defenses.
- **Law Enforcement Collaboration:** Report ransomware incidents to authorities for broader threat intelligence efforts.





CONCLUSION

The APT73 (Bashe) attack on Indian car owners serves as a stark reminder of the increasing cyber threats targeting the automotive sector and personal data security. With sensitive information, including personal details and vehicle data, allegedly compromised, the incident raises serious concerns about data privacy and misuse. Such attacks not only endanger individual privacy but also pose risks to financial security and identity theft. As cybercriminals continue to evolve their tactics, organizations handling consumer data must implement robust security measures, including encryption, multi-factor authentication, and continuous monitoring. Meanwhile, individuals should stay alert, regularly update their credentials, and be cautious of phishing attempts. Strengthening cybersecurity frameworks and fostering awareness will be crucial in mitigating such threats in the future.

REFERENCES

Watchguard

- <https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/apt73>

SOCRadar

- <https://socradar.io/dark-web-profile-bashe-apt73/>

CloudSek

- <https://www.cloudsek.com/blog/unmasking-media-hungry-ransomware-groups-bashe-apt73>

Breach Sense

- <https://www.breachsense.com/breaches/departement-of-local-government-punjab-data-breach/>

RedHot Cyber

- <https://www.redhotcyber.com/post/gli-hacker-criminali-di-bashe-rivendicano-un-attacco-informatico-allo-stadio-san-siro/>

Cyber News

- <https://cybernews.com/security/bashe-ransomware-gang-claims-icici-bank/>