BASHE AKA APT73

RANSOMWARE

Vairav Advisory Report

27th January 2025

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 014441540
Mobile: +977-9820105900
Email: mail@vairavtech.com

EXECUTIVE SUMMARY

This report analyses the actions of the **Bashe Ransomware** group, which has received a lot of attention owing to its increasing targeting of businesses in a variety of industries. Bashe, previously known as Eraleign, is a ransomware group that emerged in early April 2024, adopting tactics like the LockBit group. Self-identifying as an "Advanced Persistent Threat" Bashe operates through a Tor-based Data Leak Site (DLS) to engage in double extortion, encrypting victims' files and threatening to release stolen data. The group primarily targets critical industries such as technology, financial services, customer services, and healthcare, in developed nations, including the United States, United Kingdom, Brazil, India, and France.

Key Points

- The report focuses on the Bashe ransomware group, an active and rapidly growing group that has experienced a surge in activity since 2024.
- Bashe encrypts sensitive files while threatening to leak data on their dark web data leak site (DLS) by leveraging double extortion tactics.
- The tactics and methods used by Bashe resemble established ransomware groups like LockBit, suggesting either emulation of LockBit or shared resources to gain credibility among cyber criminals.

The report highlights the importance of understanding the tactics, techniques, and procedures used by the Bashe ransomware group, as it enables it to enhance defense strategies and proactively protect against such ransomware attacks.

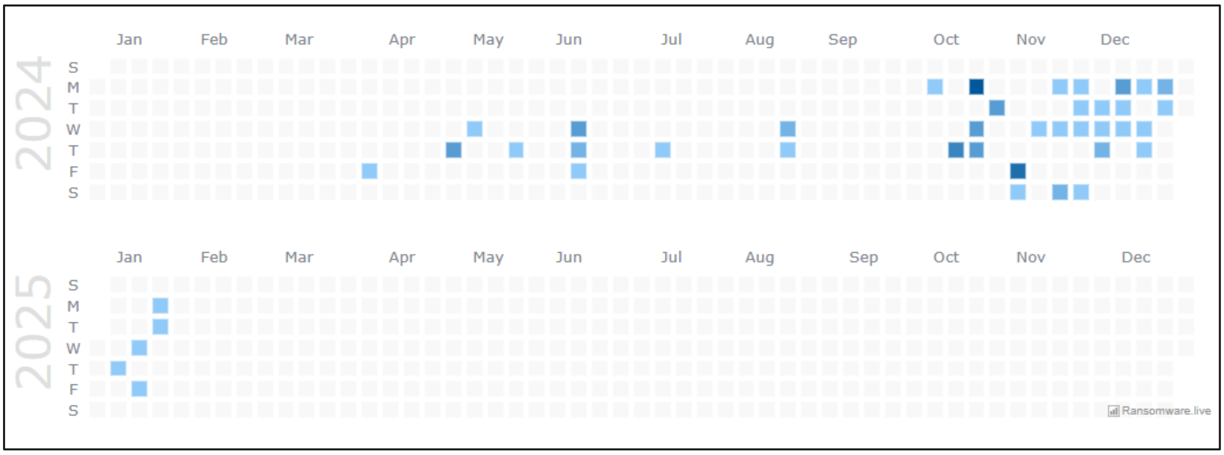


Figure 1: Bashe ransom group activity (2024-2025) Source: Ransomware.live.

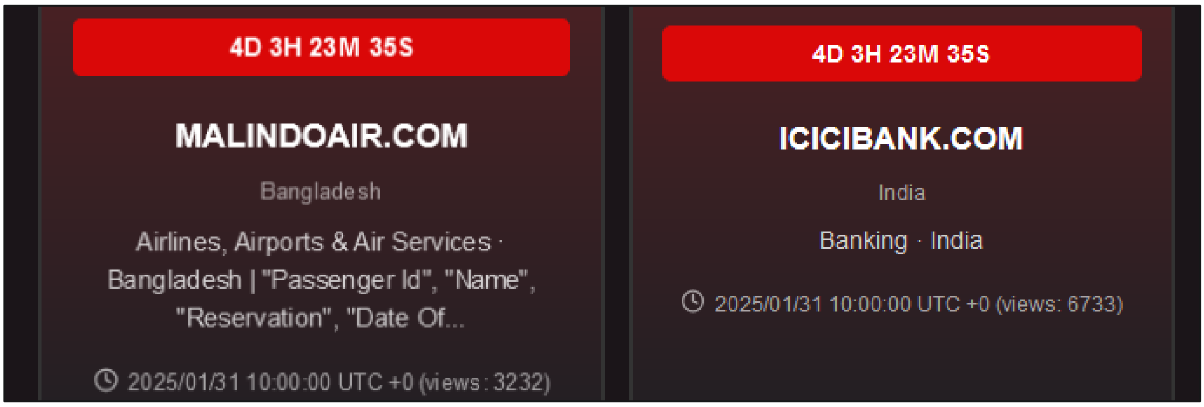
As of January 27th, the Bashe ransomware group has been linked to a total of **71 attacks**, predominantly targeting organizations in the United Kingdom, the United States, and Brazil. The group has launched a data leak site, where they self-identify as an **APT**.

Country	Number of Victims
UK	14
USA	13
Brazil	4
Switzerland	4
France	3
India	3

Table 1: Top 5 victim countries of Bache Group.

Recent Victims

Two recent victims of the Bashe attack group are MalindoAir.com from Bangladesh and ICICIBank.com from India. Both organizations have been given the option to pay to prevent further leaks.



4D 3H 23M 35S

MALINDOAIR.COM

Bangladesh

Airlines, Airports & Air Services · Bangladesh | "Passenger Id", "Name", "Reservation", "Date Of...

2025/01/31 10:00:00 UTC +0 (views: 3232)

4D 3H 23M 35S

ICICIBANK.COM

India

Banking · India

2025/01/31 10:00:00 UTC +0 (views: 6733)

Malindo Air: Operating in the airline and air services industry, has suffered a data breach exposing sensitive customer information, including Passenger IDs, names, reservation details, dates of birth, mobile numbers, passport details, and nationalities. The deadline for action to prevent further data exposure is set for January 31, 2025, at 10:00 UTC, with the breach already garnering 3,232 views.

ICICI Bank: A prominent banking institution in India, has experienced a breach of critical data, although the specific details of the exposed information are not mentioned. The deadline for this case is also January 31, 2025, at 10:00 UTC, with 6,733 views recorded so far.

TACTICS, TECHNIQUES, AND PROCEDURE

The Bashe ransomware aka APT73 acquires early access to their victims' systems in various ways, including phishing emails, Trojan infections, exploiting weaknesses in software purchased from peer-to-peer (P2P) networks, etc. APT73 primarily conducts its attacks through phishing campaigns, leveraging tactics to exploit vulnerabilities in public-facing applications.

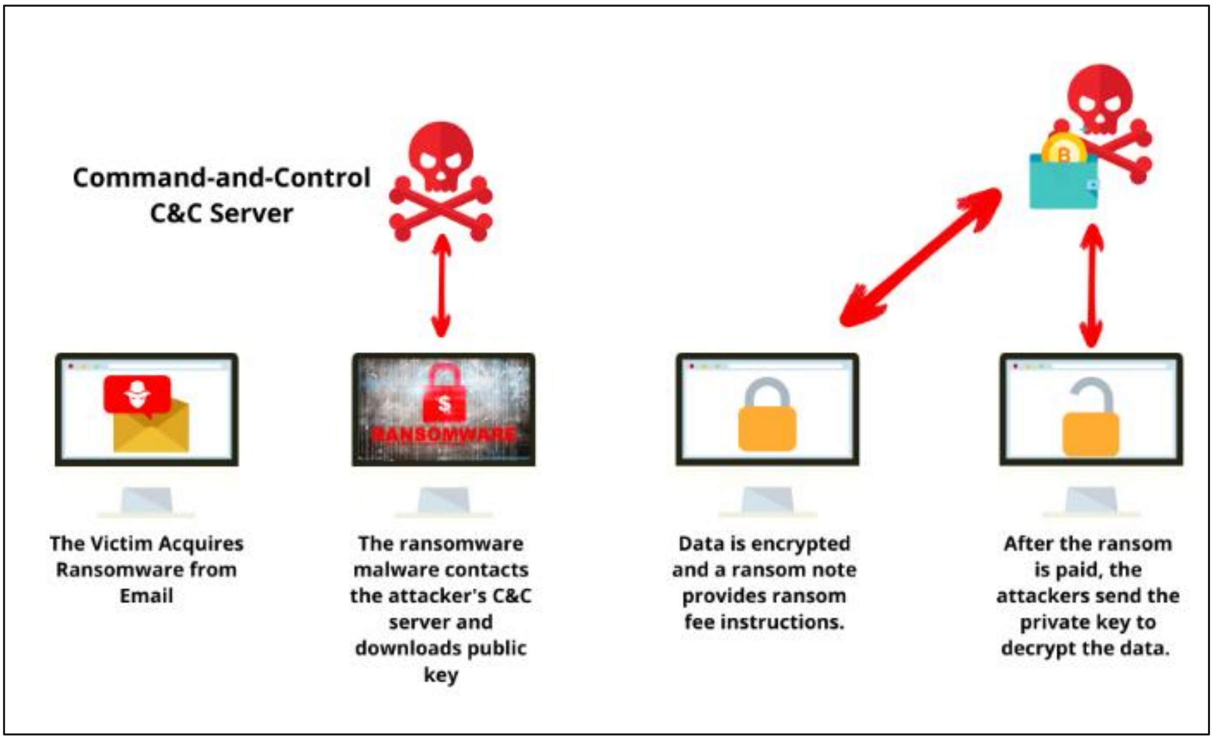
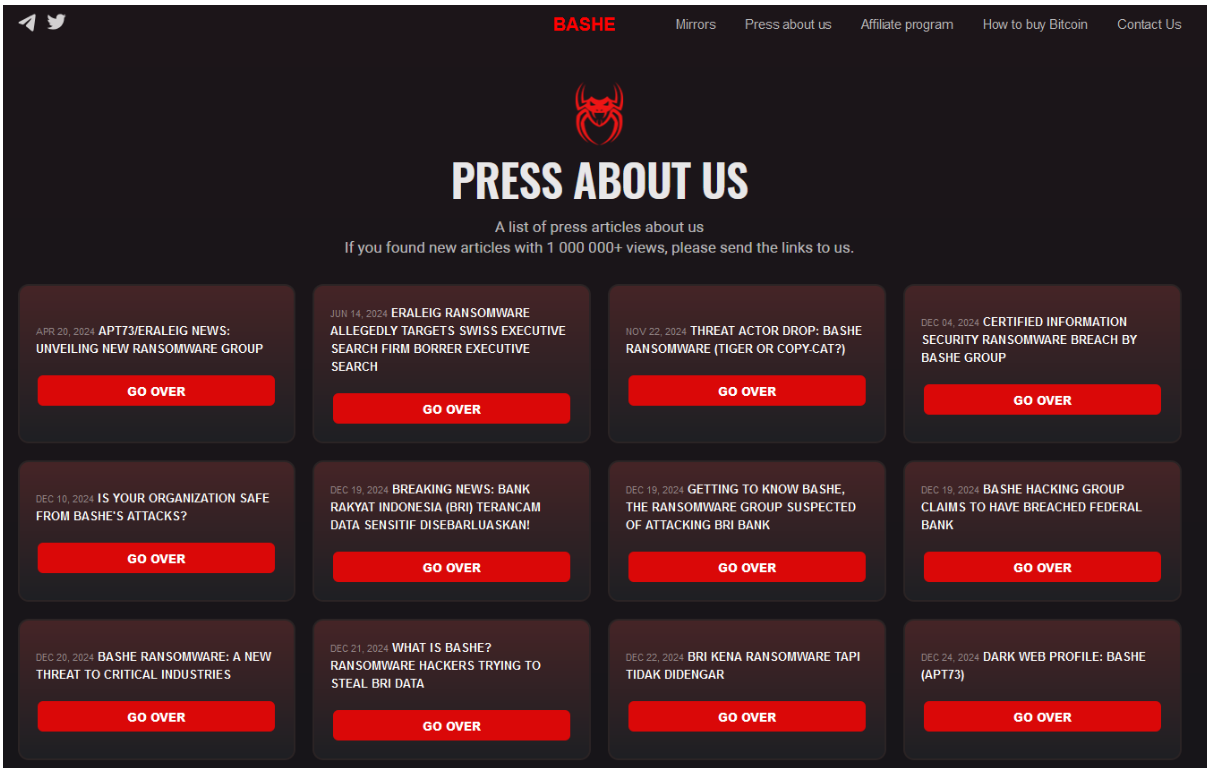

Command-and-Control
C&C Server
RANSOMWARE
The Victim Acquires Ransomware from Email
The ransomware malware contacts the attacker's C&C server and downloads public key
Data is encrypted and a ransom note provides ransom fee instructions.
After the ransom is paid, the attackers send the private key to decrypt the data.

Figure 2: Infection chain of Ransomware.

Once access is gained, Bashe typically proceeds with **data exfiltration** and **double extortion** tactics. After encrypting the victim's systems, the group exfiltrates sensitive data, which they use as leverage to further their extortion efforts. They threaten to release this stolen data on their dark website unless the ransom demands are met, combining encryption with the potential exposure of sensitive information to intensify pressure on the victim.

Bashe's data leak site (DLS) is hosted on the dark web and is only accessible via Tor. However, in contrast to more established ransomware groups like LockBit, the site remains in its early stages. It lacks active mirrors, and only a single victim's data has been publicly leaked so far, suggesting that Bashe is still in the initial phase of its ransomware operations.

The site features an "About Us" section, which includes multiple posts written by external security researchers.



PRESS ABOUT US

A list of press articles about us
If you found new articles with 1 000 000+ views, please send the links to us.

APR 20, 2024 APT73/ERALEIG NEWS: UNVEILING NEW RANSOMWARE GROUP
GO OVER

JUN 14, 2024 ERALEIG RANSOMWARE ALLEGEDLY TARGETS SWISS EXECUTIVE SEARCH FIRM BORRER EXECUTIVE SEARCH
GO OVER

NOV 22, 2024 THREAT ACTOR DROP: BASHE RANSOMWARE (TIGER OR COPY-CAT?)
GO OVER

DEC 04, 2024 CERTIFIED INFORMATION SECURITY RANSOMWARE BREACH BY BASHE GROUP
GO OVER

DEC 10, 2024 IS YOUR ORGANIZATION SAFE FROM BASHE'S ATTACKS?
GO OVER

DEC 19, 2024 BREAKING NEWS: BANK RAKYAT INDONESIA (BRI) TERANCAM DATA SENSITIF DISEBARLUASKAN!
GO OVER

DEC 19, 2024 GETTING TO KNOW BASHE, THE RANSOMWARE GROUP SUSPECTED OF ATTACKING BRI BANK
GO OVER

DEC 19, 2024 BASHE HACKING GROUP CLAIMS TO HAVE BREACHED FEDERAL BANK
GO OVER

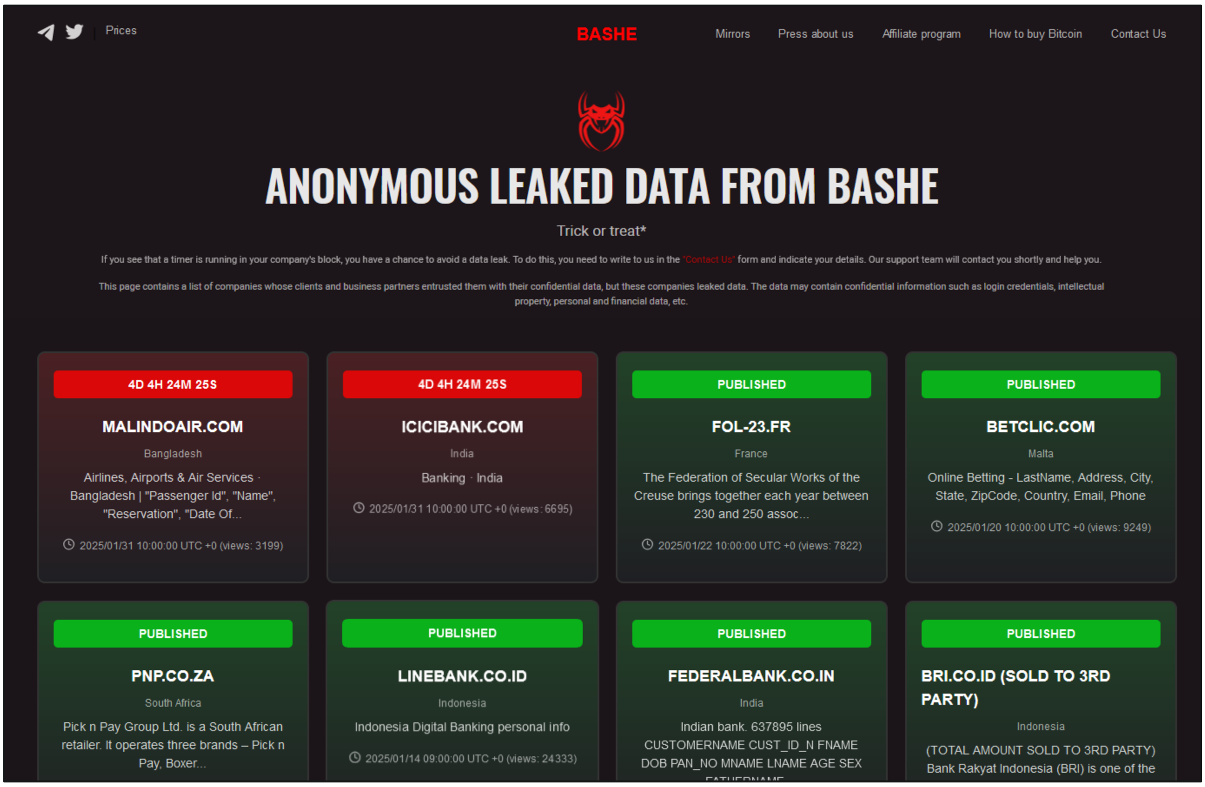
DEC 20, 2024 BASHE RANSOMWARE: A NEW THREAT TO CRITICAL INDUSTRIES
GO OVER

DEC 21, 2024 WHAT IS BASHE? RANSOMWARE HACKERS TRYING TO STEAL BRI DATA
GO OVER

DEC 22, 2024 BRI KENA RANSOMWARE TAPI TIDAK DIDENGAR
GO OVER

DEC 24, 2024 DARK WEB PROFILE: BASHE (APT73)
GO OVER

Additionally, the site lists the organizations they have compromised with, alongside data from those that have refused to comply with their ransom demands.



ANONYMOUS LEAKED DATA FROM BASHE

Trick or treat*

If you see that a timer is running in your company's block, you have a chance to avoid a data leak. To do this, you need to write to us in the "Contact Us" form and indicate your details. Our support team will contact you shortly and help you.

This page contains a list of companies whose clients and business partners entrusted them with their confidential data, but these companies leaked data. The data may contain confidential information such as login credentials, intellectual property, personal and financial data, etc.

4D 4H 24M 25S
MALINDOAIR.COM
Bangladesh
Airlines, Airports & Air Services · Bangladesh | "Passenger Id", "Name", "Reservation", "Date Of...
2025/01/31 10:00:00 UTC +0 (views: 3199)

4D 4H 24M 25S
ICICIBANK.COM
India
Banking · India
2025/01/31 10:00:00 UTC +0 (views: 6695)

PUBLISHED
FOL-23.FR
France
The Federation of Secular Works of the Creuse brings together each year between 230 and 250 assoc...
2025/01/22 10:00:00 UTC +0 (views: 7822)

PUBLISHED
BETCLIC.COM
Malta
Online Betting - LastName, Address, City, State, ZipCode, Country, Email, Phone
2025/01/20 10:00:00 UTC +0 (views: 9249)

PUBLISHED
PNP.CO.ZA
South Africa
Pick n Pay Group Ltd. is a South African retailer. It operates three brands – Pick n Pay, Boxer...

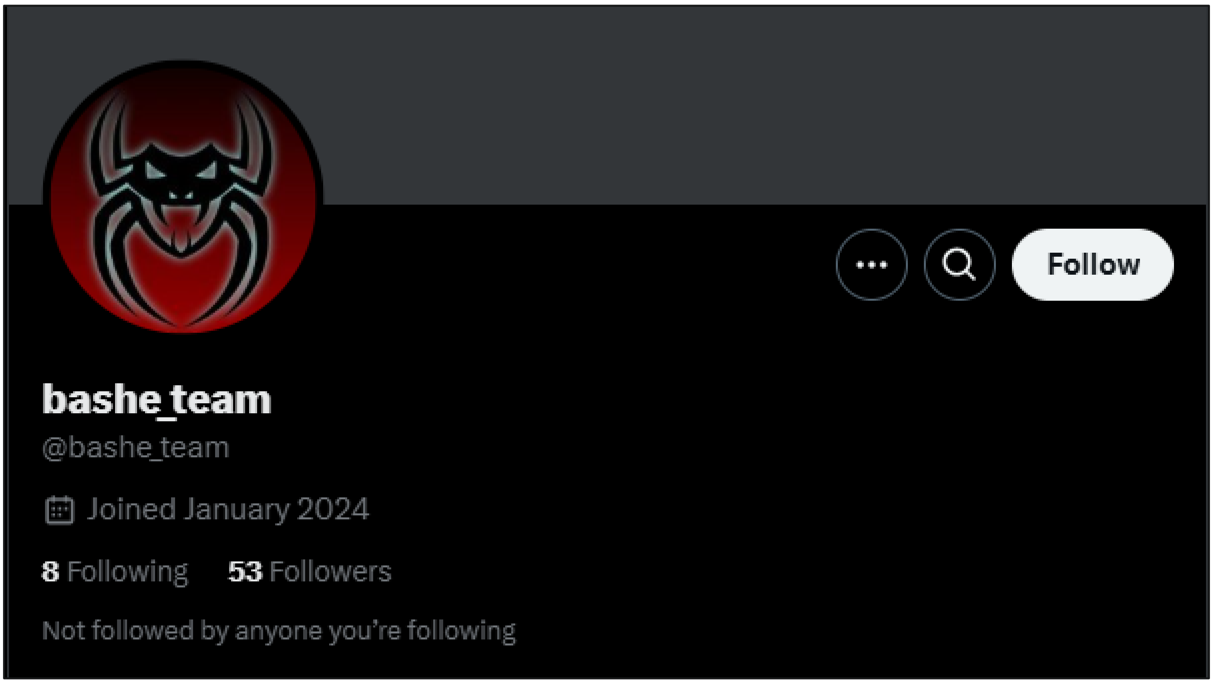
PUBLISHED
LINEBANK.CO.ID
Indonesia
Indonesia Digital Banking personal info
2025/01/14 09:00:00 UTC +0 (views: 24333)

PUBLISHED
FEDERALBANK.CO.IN
India
Indian bank. 637895 lines CUSTOMERNAME CUST_ID_N FNAME DOB PAN_NO MNAME LNAME AGE SEX FATHERNAME

PUBLISHED
BRI.CO.ID (SOLD TO 3RD PARTY)
Indonesia
(TOTAL AMOUNT SOLD TO 3RD PARTY) Bank Rakyat Indonesia (BRI) is one of the

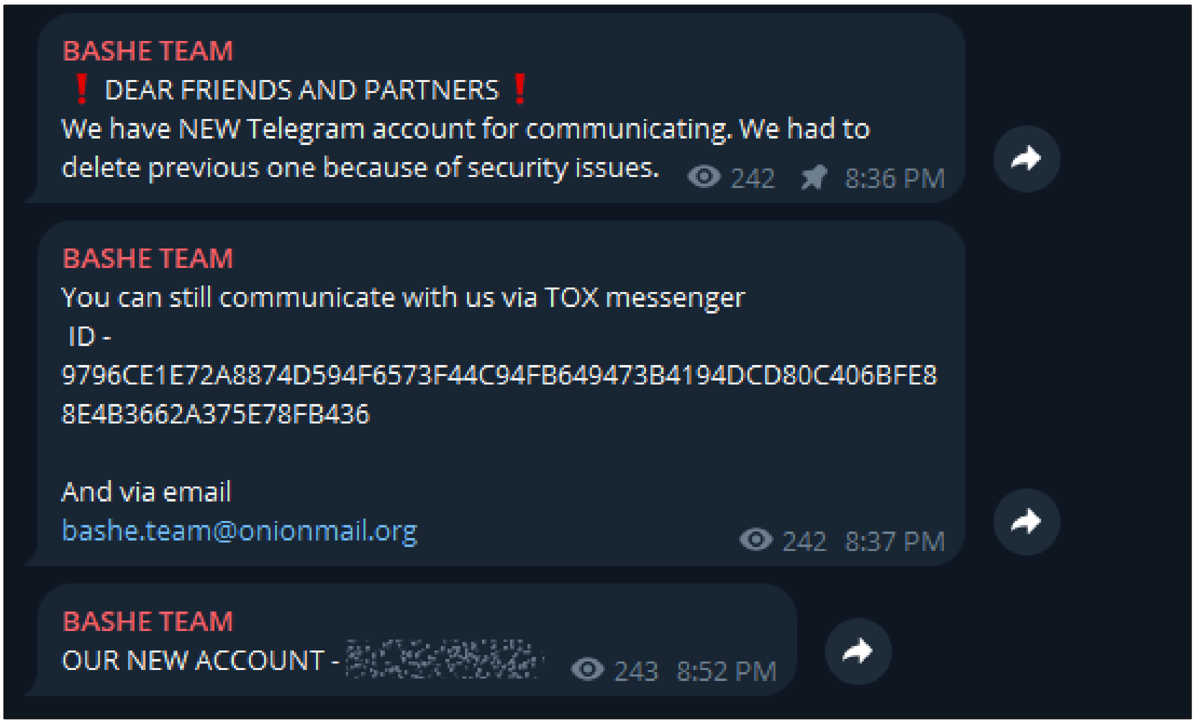
Figure 3: Bashe data leak site on the dark web.

The group has provided links to their Telegram and X (formerly Twitter) handles, which are as follows: [t.me/bashe_team_official] and [https://x.com/bashe_team].



bashe team
@bashe_team
Joined January 2024
8 Following **53** Followers
Not followed by anyone you're following

Figure 4: X (formerly Twitter) handle.



BASHE TEAM
❗ DEAR FRIENDS AND PARTNERS ❗
We have NEW Telegram account for communicating. We had to delete previous one because of security issues. 242 8:36 PM

BASHE TEAM
You can still communicate with us via TOX messenger
ID -
9796CE1E72A8874D594F6573F44C94FB649473B4194DCD80C406BFE88E4B3662A375E78FB436

And via email
bashe.team@onionmail.org 242 8:37 PM

BASHE TEAM
OUR NEW ACCOUNT - [redacted] 243 8:52 PM

Figure 5: Telegram handle.

From a technical perspective, Bashe's DLS is relatively rudimentary, reflecting the group's developmental stage. The platform is significantly less sophisticated than those of more established groups, with minimal data leaks and no active mirrors. The group relies extensively on the Tor network for hosting and data leaks, ensuring a high level of anonymity and complicating efforts to trace their activities.

When compared to LockBit, Bashe's tactics and methods show considerable similarities. Their DLS structure and attack techniques, including encryption and data exfiltration, mirror those used by LockBit. The two groups utilize similar layouts for their data leak sites, which may indicate that Bashe is either attempting to emulate LockBit or leveraging shared resources to establish credibility within the cybercriminal community.

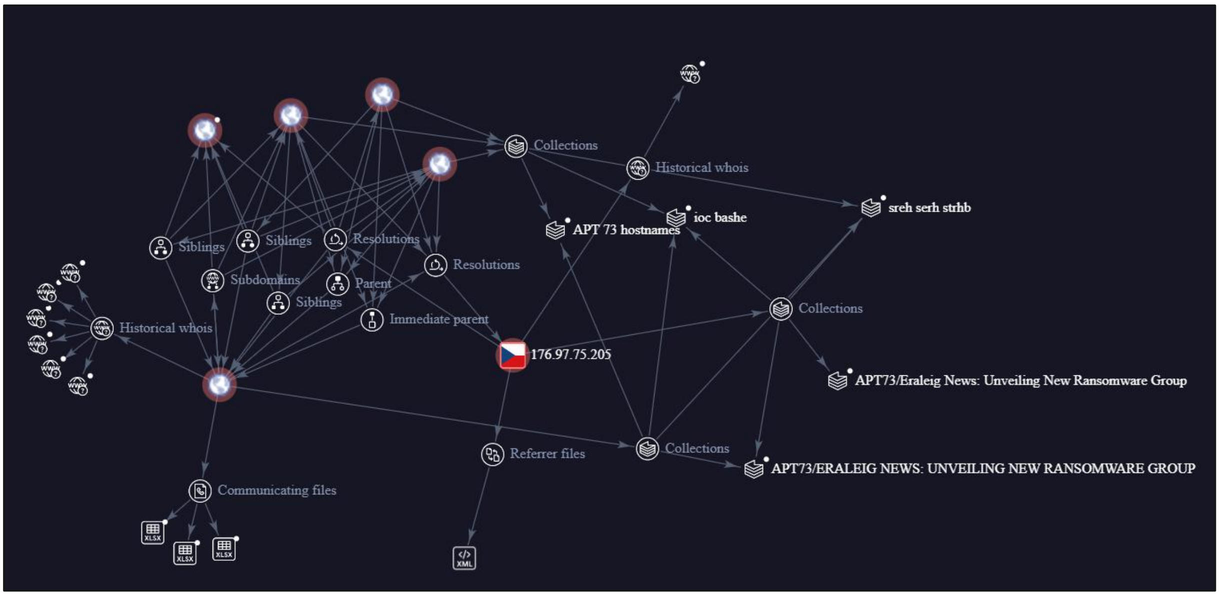


Table 2: Network Infrastructure.

MITRE ATT&CK TECHNIQUES

The Bashe ransomware gang makes the usage of various attack tactics, techniques, and procedures based on the MITRE ATT&CK framework to attack victimized users or organizations.

TACTIC	TECHNIQUE
Initial Access	Phishing (T1566) • Exploit Public-Facing Application (T1190)
Execution	Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) Exploitation for Client Execution (T1203)
Persistence	Scheduled Task/Job (T1053) • Scheduled Task (T1053.005) Boot or Logon AutoStart Execution (T1547) • Registry Run Keys (T1547.001)
Privilege Escalation	Exploitation for Privilege Escalation (T1068) Abuse Elevation Control Mechanism(T1548) • Bypass User Account Control (UAC) (T1548.002)
Defense Evasion	Process Injection (T1055) Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
Discovery	Remote System Discovery (T1018) File and Directory Discovery (T10183) Process Discovery (T1057)
Lateral Movement	Remote Services (T1021) • SMB/Windows Admin Shares (T1021.002)
Collection	Data from Local System (T1005) Data Staged (T1074) • Local Data Staging (T1074.001)

INDICATORS OF COMPROMISE (IOCS)

IOC	Type
176.97.75[.]205	**IP Address**
eraleignews[.]com	**Domains**
ns4.eraleignews[.]com	
ns3.eraleignews[.]com	
ns2.eraleignews[.]com	
ns1.eraleignews[.]com	
qcgv5tfer4f46ns6ohh72zeyyh5uavoiybypzpt3lmwk5ecyqykptgqd.onion	**TOR**
9796CE1E72A8874D594F6573F44C94FB649473B4194DCD80C406BFE88E4B3662A375E78FB436	**TOX**
f1a00e2fe86455b9d1a384d5e96185e016816acd1d7ef3460e232e9ecb9da794	**SHA-256**
94895ed0dc352981fbec38b5348ec3ae3be26371	**SHA-1**
6d170d36a4d6b47987f51445b24e587c	**MD5**

Table 3: List of IOCs related to Bashe Ransomware group.

DETECTION RULES

Office application-initiated network connection to non-local IP

```
title: Office Application Initiated Network Connection To Non-Local IP
id: 75e33ce3-ae32-4dcc-9aa8-a2a3029d6f84
status: test
description: |
    Detects an office application (Word, Excel, PowerPoint)  that initiates
a network connection to a non-private IP address.
    This rule aims to detect traffic similar to the one seen exploited in
CVE-2021-42292.
    This rule will require an initial baseline and tuning that is specific
to your organization.
References:
    - https://corelight.com/blog/detecting-cve-2021-42292
    - https://learn.microsoft.com/de-de/microsoft-365/enterprise/urls-and-
ip-address-ranges?view=o365-worldwide
author: Christopher Peacock '@securepeacock', SCYTHE '@scythe_io', Florian
Roth (Nextron Systems), Tim Shelton, Nasreddine Bencherchali (Nextron
Systems)
date: 2021-11-10
modified: 2024-07-02
Tags:
    - attack.execution
    - attack.t1203
log source:
    category: network_connection
    product: windows
Detection:
    Selection:
        Image|endswith:
            - '\excel.exe'
            - '\outlook.exe'
            - '\powerpnt.exe'
            - '\winword.exe'
            - '\wordview.exe'
        Initiated: 'true'
    filter_main_local_ranges:
        DestinationIp|cidr:
            - '127.0.0.0/8'
            - '10.0.0.0/8'
            - '172.16.0.0/12'
            - '192.168.0.0/16'
            - '169.254.0.0/16'
            - '::1/128'  # IPv6 loopback
            - 'fe80::/10'  # IPv6 link-local addresses
            - 'fc00::/7'  # IPv6 private addresses
    filter_main_msrange_generic:
        DestinationIp|cidr:
            - '20.184.0.0/13' # Microsoft Corporation
            - '20.192.0.0/10' # Microsoft Corporation
            - '23.72.0.0/13' # Akamai International B.V.
            - '40.76.0.0/14' # Microsoft Corporation
            - '51.10.0.0/15' # Microsoft Corporation
            - '51.103.0.0/16' # Microsoft Corporation
            - '51.104.0.0/15' # Microsoft Corporation
            - '51.142.136.0/22' # Microsoft Corporation -
https://ipinfo.io/AS8075/51.140.0.0/14-51.142.136.0/22
            - '52.160.0.0/11' # Microsoft Corporation -
https://ipinfo.io/AS8075/52.160.0.0/11
```

```
            - '204.79.197.0/24' # Microsoft Corporation
    filter_main_msrange_exchange_1:
        # Exchange Online
        # "urls": [
        #       "outlook.cloud.microsoft",
        #       "outlook.office.com",
        #       "outlook.office365.com"
        # ]
        DestinationIp|cidr:
            - '13.107.6.152/31'
            - '13.107.18.10/31'
            - '13.107.128.0/22'
            - '23.103.160.0/20'
            - '40.96.0.0/13'
            - '40.104.0.0/15'
            - '52.96.0.0/14'
            - '131.253.33.215/32'
            - '132.245.0.0/16'
            - '150.171.32.0/22'
            - '204.79.197.215/32'
            - '2603:1006::/40'
            - '2603:1016::/36'
            - '2603:1026::/36'
            - '2603:1036::/36'
            - '2603:1046::/36'
            - '2603:1056::/36'
            - '2620:1ec:4::152/128'
            - '2620:1ec:4::153/128'
            - '2620:1ec:c::10/128'
            - '2620:1ec:c::11/128'
            - '2620:1ec:d::10/128'
            - '2620:1ec:d::11/128'
            - '2620:1ec:8f0::/46'
            - '2620:1ec:900::/46'
            - '2620:1ec:a92::152/128'
            - '2620:1ec:a92::153/128'
        DestinationPort:
            - 80
            - 443
    filter_main_msrange_exchange_2:
        # Exchange Online
        # "urls": [
        #       "outlook.office365.com",
        #       "smtp.office365.com"
        # ]
        DestinationIp|cidr:
            - '13.107.6.152/31'
            - '13.107.18.10/31'
            - '13.107.128.0/22'
            - '23.103.160.0/20'
            - '40.96.0.0/13'
            - '40.104.0.0/15'
            - '52.96.0.0/14'
            - '131.253.33.215/32'
            - '132.245.0.0/16'
            - '150.171.32.0/22'
            - '204.79.197.215/32'
            - '2603:1006::/40'
            - '2603:1016::/36'
            - '2603:1026::/36'
            - '2603:1036::/36'
            - '2603:1046::/36'
            - '2603:1056::/36'
            - '2620:1ec:4::152/128'
            - '2620:1ec:4::153/128'
            - '2620:1ec:c::10/128'
            - '2620:1ec:c::11/128'
            - '2620:1ec:d::10/128'
            - '2620:1ec:d::11/128'
            - '2620:1ec:8f0::/46'
            - '2620:1ec:900::/46'
            - '2620:1ec:a92::152/128'
            - '2620:1ec:a92::153/128'
        DestinationPort:
            - 143
            - 587
            - 993
            - 995
        Protocol: 'tcp'
    filter_main_msrange_exchange_3:
        # Exchange Online
        # "urls": [
        #       "*.protection.outlook.com"
        #  ]
        DestinationIp|cidr:
            - '40.92.0.0/15'
            - '40.107.0.0/16'
            - '52.100.0.0/14'
            - '52.238.78.88/32'
            - '104.47.0.0/17'
            - '2a01:111:f400::/48'
            - '2a01:111:f403::/48'
        DestinationPort: 443
    filter_main_msrange_exchange_4:
        # Exchange Online
        # "urls": [
        #       "*.mail.protection.outlook.com",
        #       "*.mx.microsoft"
        #  ]
        DestinationIp|cidr:
            - '40.92.0.0/15'
            - '40.107.0.0/16'
            - '52.100.0.0/14'
            - '52.238.78.88/32'
            - '104.47.0.0/17'
            - '2a01:111:f400::/48'
            - '2a01:111:f403::/48'
        DestinationPort: 25
    filter_main_msrange_sharepoint_1:
        # SharePoint Online and OneDrive for Business",
        # "urls": [
        #       "*.sharepoint.com"
        # ]
        DestinationIp|cidr:
            - '13.107.136.0/22'
            - '40.108.128.0/17'
            - '52.104.0.0/14'
            - '104.146.128.0/17'
            - '150.171.40.0/22'
            - '2603:1061:1300::/40'
            - '2620:1ec:8f8::/46'
            - '2620:1ec:908::/46'
            - '2a01:111:f402::/48'
        DestinationPort:
            - 80
            - 443
        Protocol: 'tcp'
    filter_main_msrange_office_1:
        # Microsoft 365 Common and Office Online",
        # "urls": [
        #       "*.officeapps.live.com",
        #       "*.online.office.com",
        #       "office.live.com"
        # ],
        DestinationIp|cidr:
            - '13.107.6.171/32'
            - '13.107.18.15/32'
            - '13.107.140.6/32'
            - '52.108.0.0/14'
            - '52.244.37.168/32'
            - '2603:1006:1400::/40'
            - '2603:1016:2400::/40'
            - '2603:1026:2400::/40'
            - '2603:1036:2400::/40'
            - '2603:1046:1400::/40'
            - '2603:1056:1400::/40'
            - '2603:1063:2000::/38'
            - '2620:1ec:c::15/128'
            - '2620:1ec:8fc::6/128'
            - '2620:1ec:a92::171/128'
            - '2a01:111:f100:2000::a83e:3019/128'
            - '2a01:111:f100:2002::8975:2d79/128'
            - '2a01:111:f100:2002::8975:2da8/128'
            - '2a01:111:f100:7000::6fdd:6cd5/128'
            - '2a01:111:f100:a004::bfeb:88cf/128'
        DestinationPort:
            - 80
            - 443
        Protocol: 'tcp'
    filter_main_msrange_office_2:
        # Microsoft 365 Common and Office Online
        # "urls": [
        #       "*.auth.microsoft.com",
        #       "*.msftidentity.com",
        #       "*.msidentity.com",
        #       "account.activedirectory.windowsazure.com",
        #       "accounts.accesscontrol.windows.net",
        #       "adminwebservice.microsoftonline.com",
        #       "api.passwordreset.microsoftonline.com",
        #       "autologon.microsoftazuread-sso.com",
        #       "becws.microsoftonline.com",
        #       "ccs.login.microsoftonline.com",
        #       "clientconfig.microsoftonline-p.net",
        #       "companymanager.microsoftonline.com",
        #       "device.login.microsoftonline.com",
        #       "graph.microsoft.com",
        #       "graph.windows.net",
        #       "login-us.microsoftonline.com",
        #       "login.microsoft.com",
        #       "login.microsoftonline-p.com",
        #       "login.microsoftonline.com",
        #       "login.windows.net",
        #       "logincert.microsoftonline.com",
        #       "loginex.microsoftonline.com",
        #       "nexus.microsoftonline-p.com",
        #       "passwordreset.microsoftonline.com",
        #       "provisioningapi.microsoftonline.com"
        # ]
        DestinationIp|cidr:
            - '20.20.32.0/19'
            - '20.190.128.0/18'
            - '20.231.128.0/19'
            - '40.126.0.0/18'
            - '2603:1006:2000::/48'
            - '2603:1007:200::/48'
            - '2603:1016:1400::/48'
            - '2603:1017::/48'
            - '2603:1026:3000::/48'
            - '2603:1027:1::/48'
            - '2603:1036:3000::/48'
            - '2603:1037:1::/48'
            - '2603:1046:2000::/48'
            - '2603:1047:1::/48'
            - '2603:1056:2000::/48'
            - '2603:1057:2::/48'
        DestinationPort:
            - 80
            - 443
        Protocol: 'tcp'
    filter_main_msrange_office_3:
        # Microsoft 365 Common and Office Online
        #  "urls": [
        #       "*.compliance.microsoft.com",
        #       "*.protection.office.com",
        #       "*.security.microsoft.com",
        #       "compliance.microsoft.com",
        #       "defender.microsoft.com",
        #       "protection.office.com",
        #       "security.microsoft.com"
        #  ]
        DestinationIp|cidr:
            - '13.107.6.192/32'
            - '13.107.9.192/32'
            - '52.108.0.0/14'
            - '2620:1ec:4::192/128'
            - '2620:1ec:a92::192/128'
        DestinationPort: 443
        Protocol: 'tcp'
    condition: selection and not 1 of filter_main_*
falsepositives:
    - You may have to tune certain domains out that Excel may call out to,
such as Microsoft or other business use case domains.
    - Office documents commonly have templates that refer to external
addresses, like "sharepoint.ourcompany.com" which may have to be tuned.
    - It is highly recommended to baseline your activity and tune out
common business use cases.
level: medium
```

Threat Summary	
Name	Bashe Ransomware
Threat Type	Ransomware
Detection Names	Bashe, APT73
Symptoms	The affected computer is unable to open files that were previously accessible. A message demanding ransom appears on the desktop, insisting on payment (usually in bitcoins) to regain access to the files.
Additional Information	Their DLS structure and attack techniques mirror those used by LockBit.
Distribution methods	Infected email attachments (macros), torrent websites, and malicious ads.
Damage	The encryption of all files renders them inaccessible until a ransom is paid. Alongside the ransomware infection, there is a possibility of additional installations of password-stealing Trojans and malware infections.
Malware Removal (Windows)	Conduct a thorough computer scan using trusted antivirus software.

VAIRAV RECOMMENDATIONS

We strongly advise applying the following complete procedures to properly mitigate and prevent ransomware attacks:

1. Implement Regular Data Backups

Regular data backups are essential because they provide an effective way of restoring the data in the event of a ransomware attack. Backing up vital data regularly ensures that even if the files are encrypted by ransomware, one can restore them from a safe backup source. Offline or isolated network storage methods are advised to keep backups safe during an attack.

2. Develop an Incident Response Plan

It is critical to have a well-defined incident response strategy in place before reacting to a ransomware attack. The strategy should outline specific processes and responsibilities for isolating affected systems, alerting key stakeholders, and beginning the recovery process. Organizations that have an established and rehearsed response strategy can reduce downtime, limit the attack, and swiftly resume operations.

3. Restrict Execution of Files from Untrusted Sources

Ransomware frequently penetrates organizations via malicious email attachments, untrustworthy website downloads, or illegal software. Implementing strict security measures, such as application whitelisting or sandboxing solutions, to prohibit the execution of files from untrusted sources, aids in the prevention of harmful code execution. This gives an extra layer of defense and lowers the risk.

4. Keep Systems and Software Updated

Regularly upgrading operating systems, software programs, and firmware is critical because it helps to fix security weaknesses that ransomware attackers can exploit. Updates and patches are released by software manufacturers to address known vulnerabilities, therefore staying up to date is critical for ensuring a safe computer environment.

5. Implement the Least Privilege Principle

The principle of least privilege guarantees that employees are only provided the access rights and privileges required to carry out their job tasks. Organizations may lower the attack surface for ransomware by restricting access to essential systems and sensitive data.

In the case of a successful ransomware outbreak, limiting user rights can reduce the damage and prevent lateral network migration.

6. Use Robust Antivirus and Anti-Malware Solutions:

Using trusted antivirus and anti-malware software adds an extra layer of protection against ransomware. These technologies aid in detecting and preventing harmful files and actions, including known ransomware incidents. Maintaining them ensures that you have the most recent virus definitions to identify and prevent new threats.

7. Implement Multi-factor Authentication (MFA)

Multi-factor authentication strengthens the security of your organization's systems and accounts. MFA helps prevent unwanted access even if a user's credentials are compromised by requiring multiple authentication factors, such as a password and a unique verification code. This greatly decreases the possibility of attackers obtaining control of important systems and data.

8. Enable Firewall and Intrusion Detection/Prevention Systems

Firewalls serve as a line of defense between the internal network and external threats. Configuring firewalls to filter incoming and outgoing network traffic aids in the prevention of intrusion and suspicious connections. It monitors network traffic for malicious activity signals and responds quickly to prevent possible ransomware attacks.

It is important to remember that the cyber adversaries behind ransomware gangs are likely to constantly evolve their methods, tools, and techniques to evade detection and continue to be successful in their attacks. Therefore, organizations and individuals must stay informed about the latest TTPs of the 8Base ransomware gang and take proactive steps to protect themselves.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4441540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Website: https://vairavtech.com