BREAKING CYBERSECURITY NEWS: BABUK 2.0 RANSOMWARE: THE TRUTH BEHIND THE ALLEGED COMEBACK

Vairav Cyber Security News Report

Date: April 03, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Babuk Locker, a ransomware strain that originally surfaced in 2021 before disbanding, appears to have resurfaced as Babuk Locker 2.0. However, in-depth analysis indicates that this is not a true revival of the original Babuk group but rather a rebranding of LockBit 3.0. Multiple underground forums and Telegram channels began discussing 'Babuk Locker 2.0,' with certain threat actors claiming responsibility for recent cyberattacks.

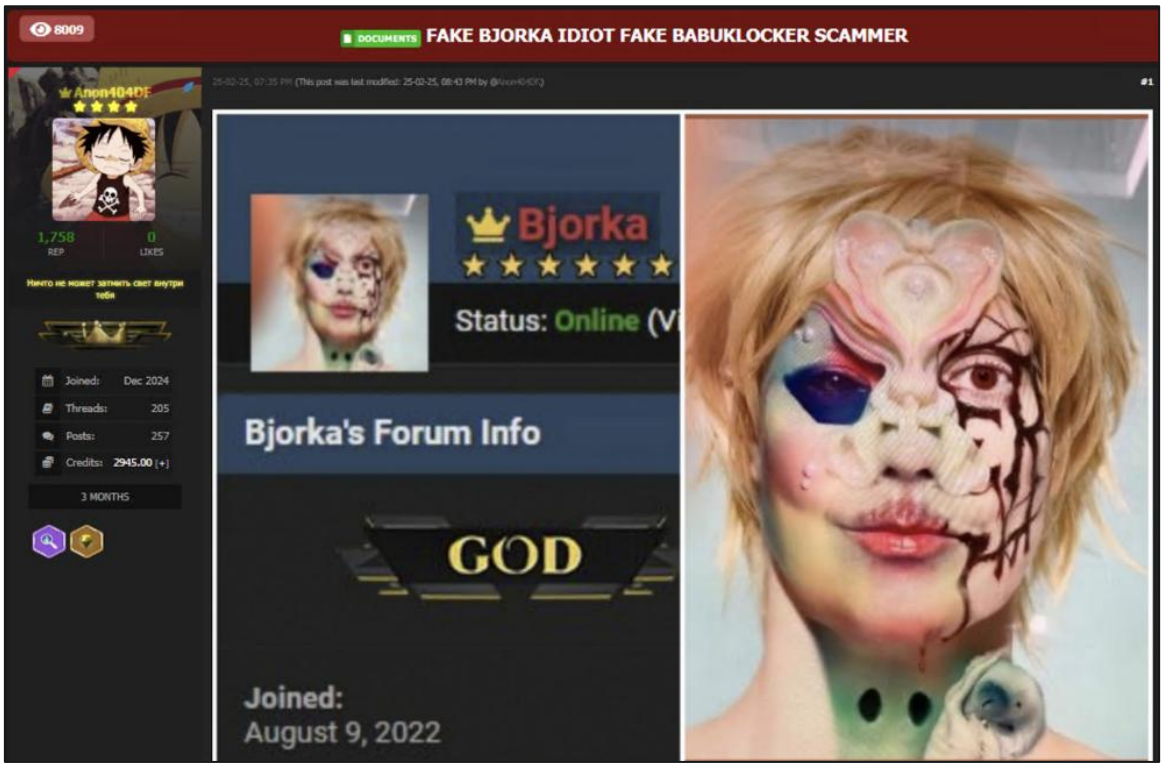

Figure 1: Online discourse against Bjorka as a scammer

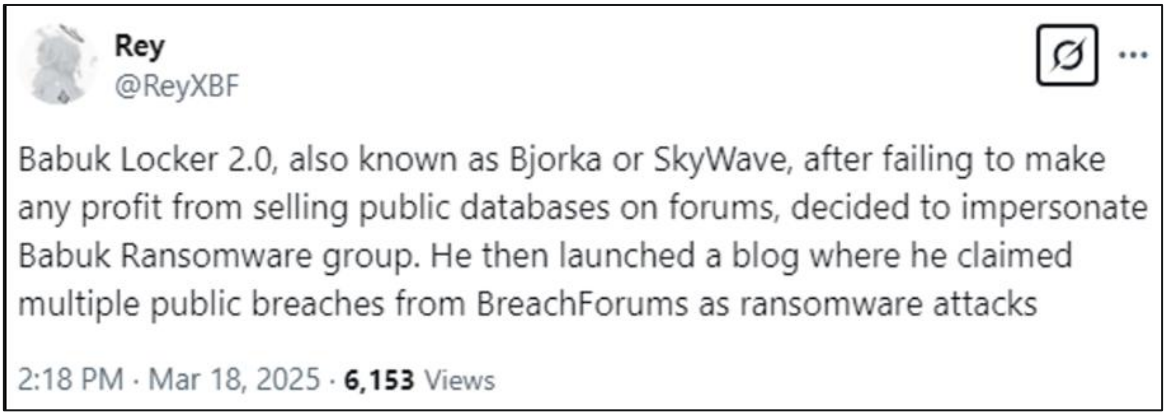

Figure 2: Online discourse against Bjorka and SkyWave as scammers

Cybercriminal groups Skywave and Bjorka have been identified as key players in promoting and operating Babuk Locker 2.0, using Telegram and dark web forums to claim responsibility for high-profile cyberattacks.

Figure 3: The 'Contact US' tab on the DLS of Babuk, showing the logos of Bjorka and Skywave

The investigation reveals that Babuk Locker 2.0 is not a new threat but a repackaged version of LockBit 3.0, continuing the trend of ransomware operators using rebranding strategies to deceive researchers, attract affiliates, and maintain relevance in the cybercrime ecosystem.

KEY FINDINGS

- Babuk Locker 2.0 is heavily linked to cybercriminal groups Skywave and Bjorka.
- The ransomware code used by Babuk 2.0 is identical to LockBit 3.0.
- Affiliates use the Babuk name to amplify their reputation and mislead security researchers.
- There is a significant overlap in victimology between Babuk 2.0 and other ransomware groups.
- The group relies on double extortion tactics, exfiltrating data before encrypting victim files and threatening to leak sensitive information.
- Threat actors use Telegram as a key communication and distribution platform, though many channels are quickly flagged as scams and removed.

OPERATORS: SKYWAVE AND BJORKA

SKYWAVE

Skywave is a relatively new cybercriminal group that targets high-profile organizations and government agencies. The group is known for operating multiple Telegram channels under different aliases, some of which have been flagged as scams.

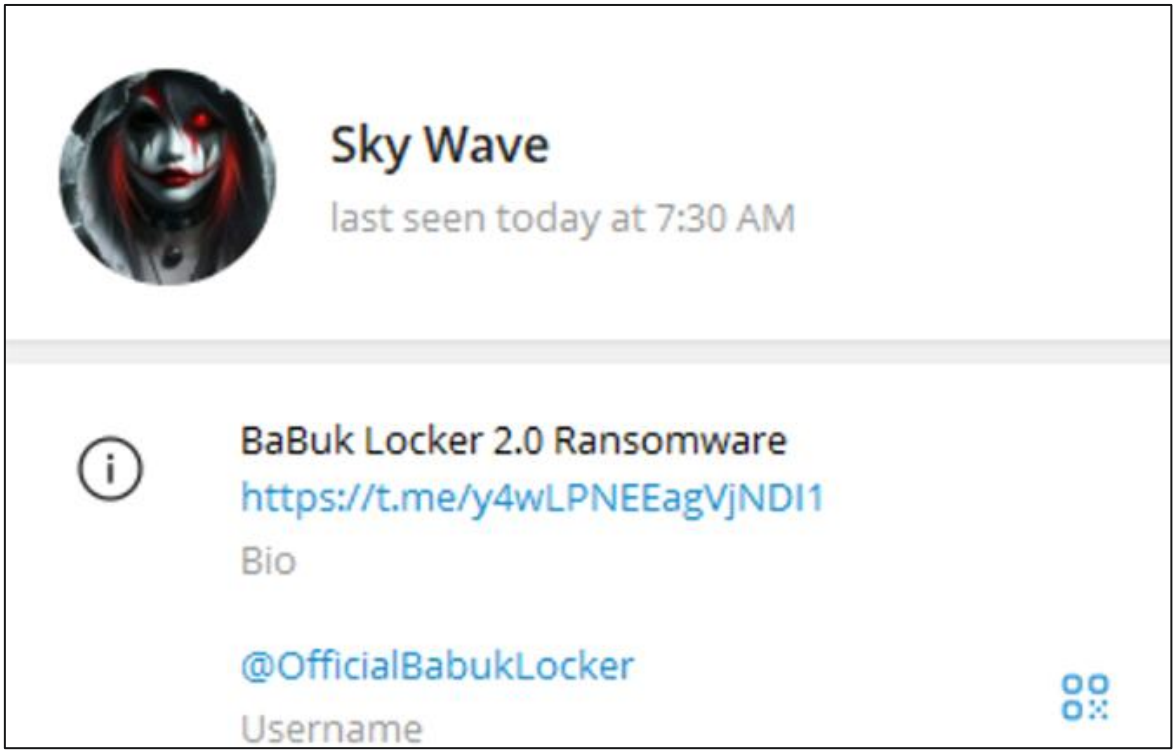

Figure 4: Telegram user of Skywave

- Skywave is suspected of running Babuk Locker 2.0's dark web leak site (DLS), where stolen data is published.
- The group claims responsibility for various cyberattacks and has leaked data from government agencies and major corporations.
- Their Tactics, Techniques, and Procedures (TTPs) remain unclear, but they likely use phishing campaigns and exploit known vulnerabilities.

BJORKA

Bjorka is a well-known threat actor, first gaining notoriety in 2022 for breaching Indonesian government databases and leaking sensitive information.

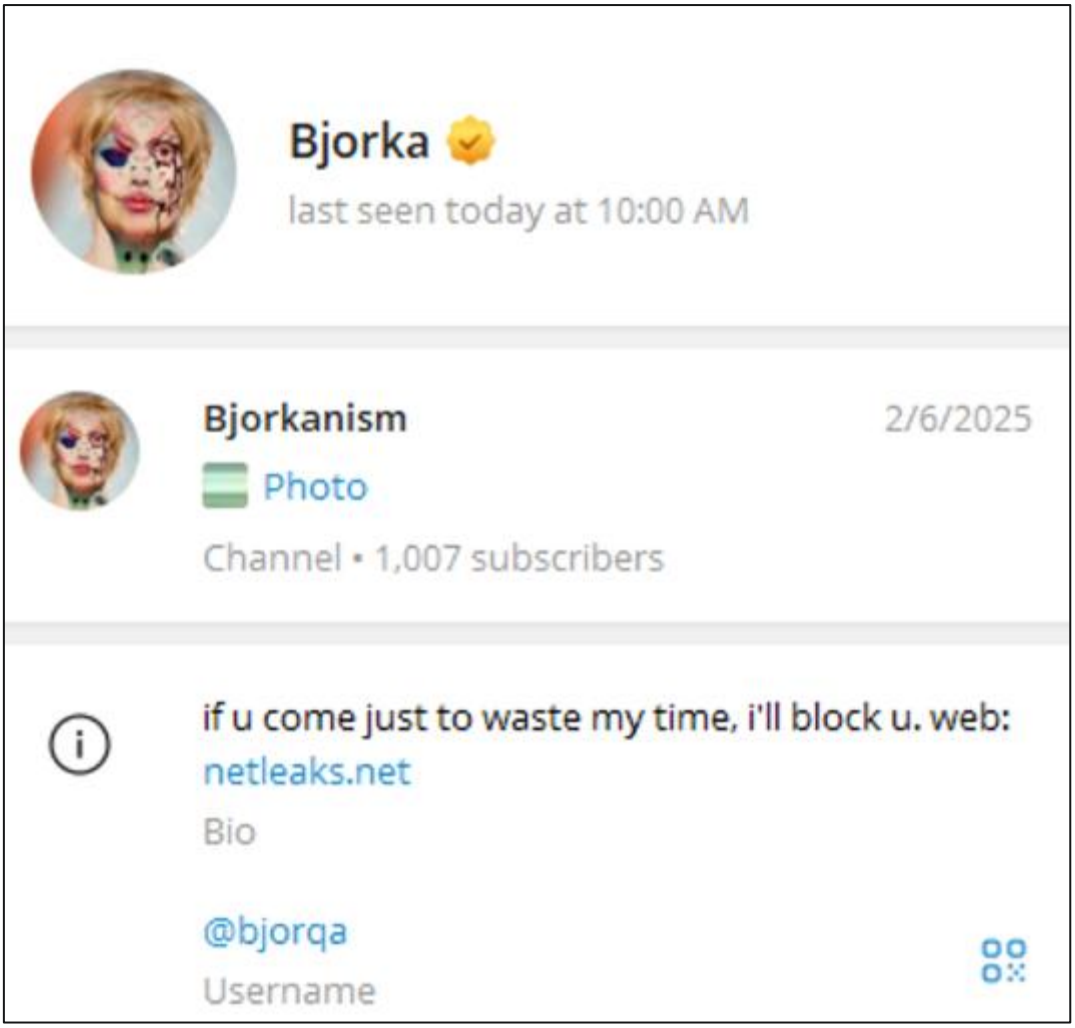

Figure 5: Telegram user of Bjorka

- Bjorka is active on BreachForums and Telegram, where they distribute stolen data.
- The group previously focused on hacktivism but has now shifted towards financially motivated ransomware operations.
- There is significant victim overlap between Bjorka and Babuk Locker 2.0, suggesting a possible affiliation.
- Their dark web presence and Telegram activity align closely with Babuk Locker 2.0 operations.

BABUK (BABUK 2.0 LOCKER)-BJORKA CONNECTION

Bjorka also amplified several Telegram channels promoting Babuk Locker 2.0 content. Victim analysis shows overlaps between Bjorka's previously claimed victims and Babuk Locker 2.0's newer targets. Babuk's dark web leak site (DLS) lists Bjorka and Skywave as affiliated groups, further supporting their collaboration.

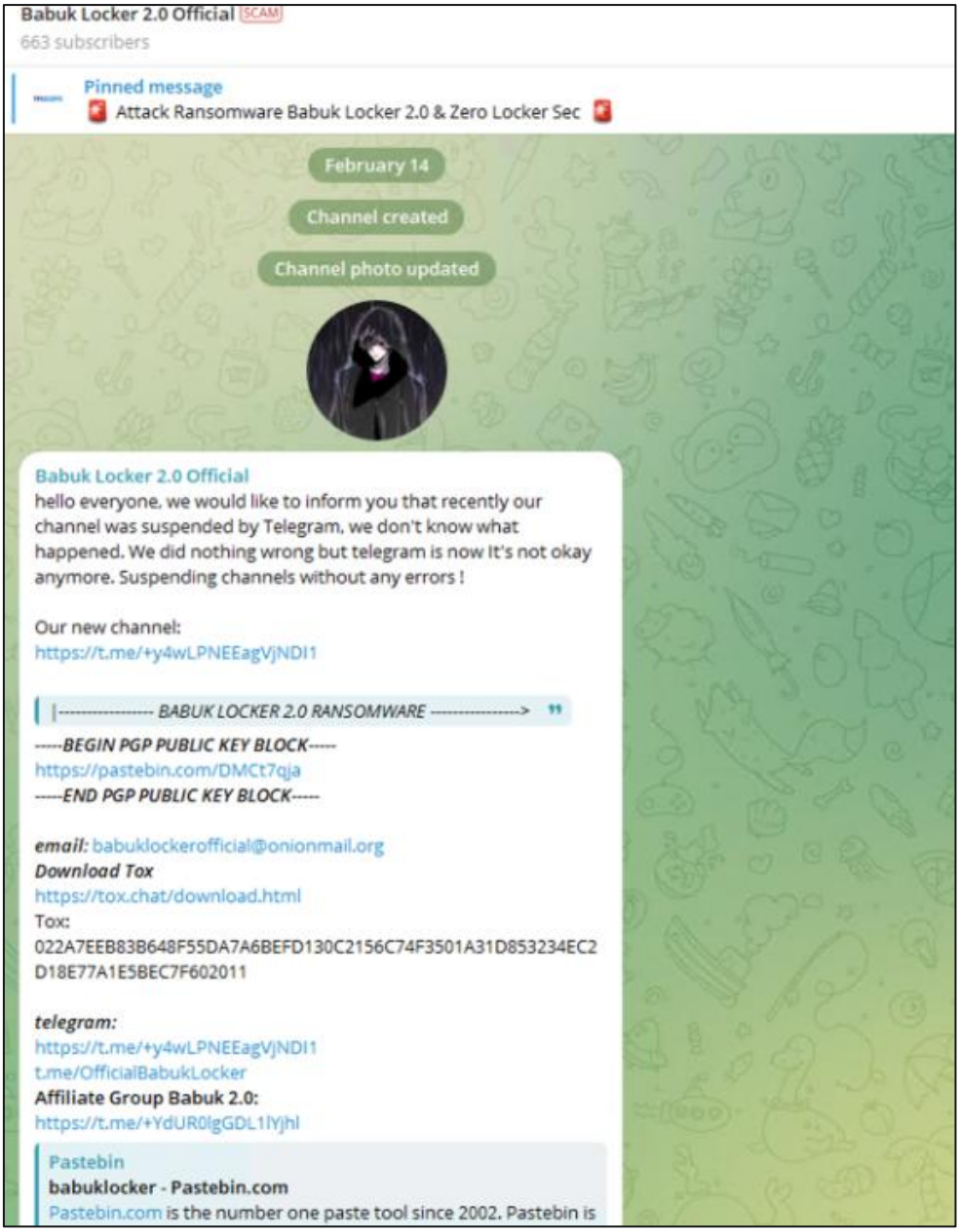

Figure 6: A Babuk Locker Telegram channel labeled as a scam by the platform

Figure 7: Overlap of victimology between Bjorka and Babuk 2.0

TECHNICAL ANALYSIS

A sample labeled *babuk.exe (SHA-256:3facc153ed82a72695ee2718084db91f85e2560407899e1c7f6938fd4ea011e9)* was found on the Telegram channel *"Babuk 2.0 Ransomware Affiliates"*.

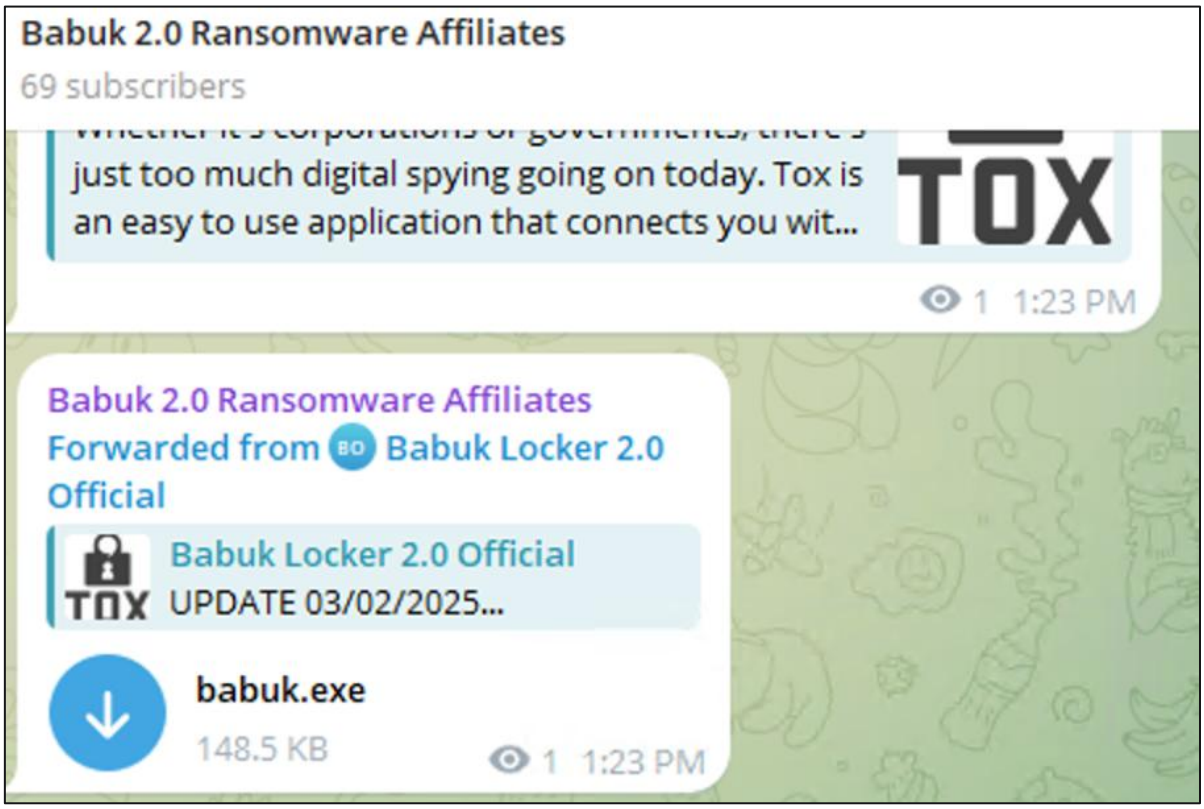

Figure 8: "Babuk" sample shared on Babuk 2.0 Affiliate Group Telegram channel

Upon analysis, it was revealed to be LockBit 3.0 (LockBit Black) rather than an actual Babuk variant, which confirms that Babuk Locker 2.0 is simply a renamed LockBit 3.0 campaign, a tactic often used by ransomware groups to deceive victims and security researchers.

ENCRYPTION METHODS USED

- Uses AES-256 and RSA-2048 encryption (standard for LockBit 3.0).
- Encrypts victim files and prevents recovery without the private key.

PROCESS & SERVICE TERMINATION

LockBit 3.0 (and by extension, Babuk Locker 2.0) terminates various system processes to maximize encryption efficiency and disable security tools.

Terminated Process	Terminated Services
sql, oracle, ocssd, dbsnmp, synctime, agntsvc, isqlplussvc, xfssvccon, mydesktopservice, ocautopds, encsvc, firefox, tbirdconfig, mydesktopqos, ocomm, dbeng50, sqbcoreservice, excel, infopath, msasccess, mspu, onenote, outlook, powerpnt, steam, thebat, thunderbird, visio, winword, wordpad,notepad, calc, wuauclt, onedrive	*vss, sql, svc, memtas mepocs, msexchange, sophos, veeam, backup, GxVss, GxBlr, GxFWD, GxCVD, GxCIMgr*

ACTIVE DIRECTORY ENUMERATION

The ransomware uses the logoncli_DsGetDcNameW API function for Active Directory enumeration, allowing attackers to escalate privileges and spread within a network.

Preloaded Base64-encoded username/password combinations found in the sample:

Username	Password
Bad.lab	*Qwerty*
Administrator	*123QWEqwe*
@#Admin2	*P@ssw0rd*
Administrator	*P@ssw0rd*
Administrator	*Qwerty*
Administrator	*123QWEqwe*
Administrator	*123QWEqweqwe*

RANSOM NOTE & BRANDING CONFUSION

The examined ransomware sample utilizes API harvesting, where API names from DLLs are hashed and compared against a predefined list of required functions.

```
v1 = result;
if ( result )
{
  result = (int (__stdcall *)(int, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD))hashed_API_sub_1D5AFC(1851803611);
  v2 = result;
  if ( result )
  {
    resolve_API_sub_1D5DB0(&unk_1F540C, dword_1D5EE8, v1, result);
    resolve_API_sub_1D5DB0(&unk_1F54FC, dword_1D5FDC, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F55EC, dword_1D60D0, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F568C, byte_1D6174, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F569C, dword_1D6188, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F56D4, dword_1D61C4, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F5728, dword_1D621C, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F573C, dword_1D6234, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F5764, dword_1D6260, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F579C, dword_1D629C, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F57B0, dword_1D62B4, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F57B8, dword_1D62C0, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F57CC, dword_1D62D8, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F57F8, dword_1D6308, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F5810, dword_1D6324, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F583C, dword_1D6354, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F584C, dword_1D6368, v1, v2);
    resolve_API_sub_1D5DB0(&unk_1F5858, dword_1D6378, v1, v2);
```

```
result = hashedAPI_4079A8(0xF80F18E8);
if ( result )
{
  result = (result)(266242, 0, 0, 0, 0, 0);   // RtlCreateHeap
  v1 = result;
  if ( result )
  {
    if ( ((*(result + 64) >> 28) & 4) != 0 )
      v1 = __ROL4__(result, 1);
    result = hashedAPI_4079A8(0x6E6047DB);    // RtlAllocateHeap
    v2 = result;
    if ( result )
    {
      resolveAPIs_407C5C(&unk_427408, dword_407DA4, v1, result);
      resolveAPIs_407C5C(&unk_4274F4, dword_407E94, v1, v2);
      resolveAPIs_407C5C(&unk_4275E4, dword_407F88, v1, v2);
      resolveAPIs_407C5C(&unk_427684, dword_40802C, v1, v2);
      resolveAPIs_407C5C(&unk_427694, dword_408040, v1, v2);
      resolveAPIs_407C5C(&unk_4276CC, dword_40807C, v1, v2);
      resolveAPIs_407C5C(&unk_427720, dword_4080D4, v1, v2);
      resolveAPIs_407C5C(&unk_427734, dword_4080EC, v1, v2);
      resolveAPIs_407C5C(&unk_42775C, dword_408118, v1, v2);
      resolveAPIs_407C5C(&unk_427794, dword_408154, v1, v2);
      resolveAPIs_407C5C(&unk_4277A8, dword_40816C, v1, v2);
```

Figure 9: LockBit 3.0's routine for API harvesting function comparison, the analyzed sample (left) vs. TrendMicro's reported sample (right)

This method, commonly used to obfuscate API calls and evade detection, closely resembles techniques observed in LockBit 3.0/Black and aligns with prior research by Trend Micro. Additionally, the XOR key *0x4803BFC7*, previously associated with LockBit 3.0 for renaming APIs, was also present in this sample and was reused multiple times throughout the code.

```
.text:0055125C
.text:0055125C loc_55125C:
.text:0055125C xor     dword ptr [ecx], 4803BFC7h
.text:00551262 not     dword ptr [ecx]
.text:00551264 nop
.text:00551265 add     ecx, 4
.text:00551268 dec     edx
.text:00551269 jnz     short loc_55125C
```

Figure 10: 0x4803BFC7 xor key observed in the analyzed sample

The ransom note generation process in this variant is identical to that seen in earlier LockBit 3.0/Black versions.

```
_WORD *__stdcall sub_DABACC(int a1)
{
  _WORD *v1; // ebx
  int readme[7]; // [esp+4h] [ebp-1Ch] BYREF

  v1 = (_WORD *)sub_DA6830(42);
  if ( v1 )
  {
    readme[0] = -1215348707;
    readme[1] = -1213317098;
    readme[2] = -1212333955;
    readme[3] = -1213120388;
    readme[4] = -1210957699;
    readme[5] = -1216069556;
    readme[6] = -1208205236;
    xor_with_key_4803BFC7h(readme, 7);          // Uf0SZw0ws.README.txt
    dword_DC5464(v1, readme, dword_DC5178 + 2);
    dword_DC5170 = hash_add_ror13(v1, -1);
  }
  return v1;
```

Figure 11: readme creation routine

Like past LockBit 3.0/Black samples, the analyzed variant modifies the desktop wallpaper to display a ransom message branded as “LockBit Black,” not Babuk. It also appends specific file extensions to encrypted data, alters their icons, and places a *.ico* file in the *%PROGRAMDATA%* directory, maintaining the standard LockBit operational approach. Furthermore, a ransom note references *“Orion Hackers”* and includes the TOX ID *32C12B278912E26E5EAC57AEBB3F4FF16F0E31603C7B9D46AC02E9D993EE14351CEC3AB5945C*.

Upon investigation, this TOX ID was linked to ransom demands posted in the Babuk 2.0 Affiliate Group on Telegram. Also, messages from this group were frequently reposted by a user named Bjorkanism, who has been actively distributing leaked LockBit 3.0 content under the guise of Babuk 2.0.

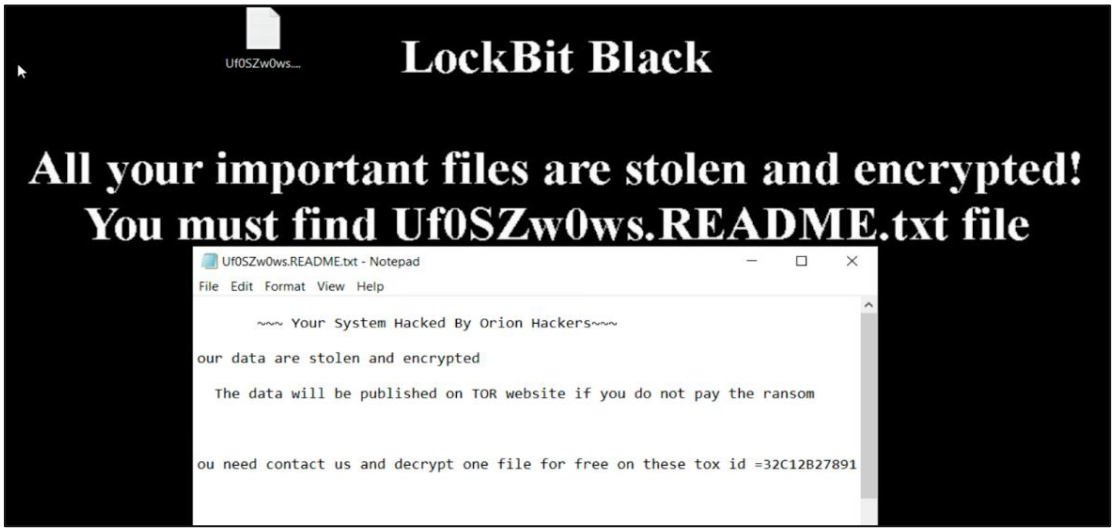

Figure 12: Lockbit3.0 wallpaper and ransom note

VICTIMOLOGY

Since January 2025, Babuk Locker 2.0 has claimed over 100 organizations as victims. High-profile targets include Amazon, Israeli Knesset, Sodexo, and Multiple government and energy sector organizations.

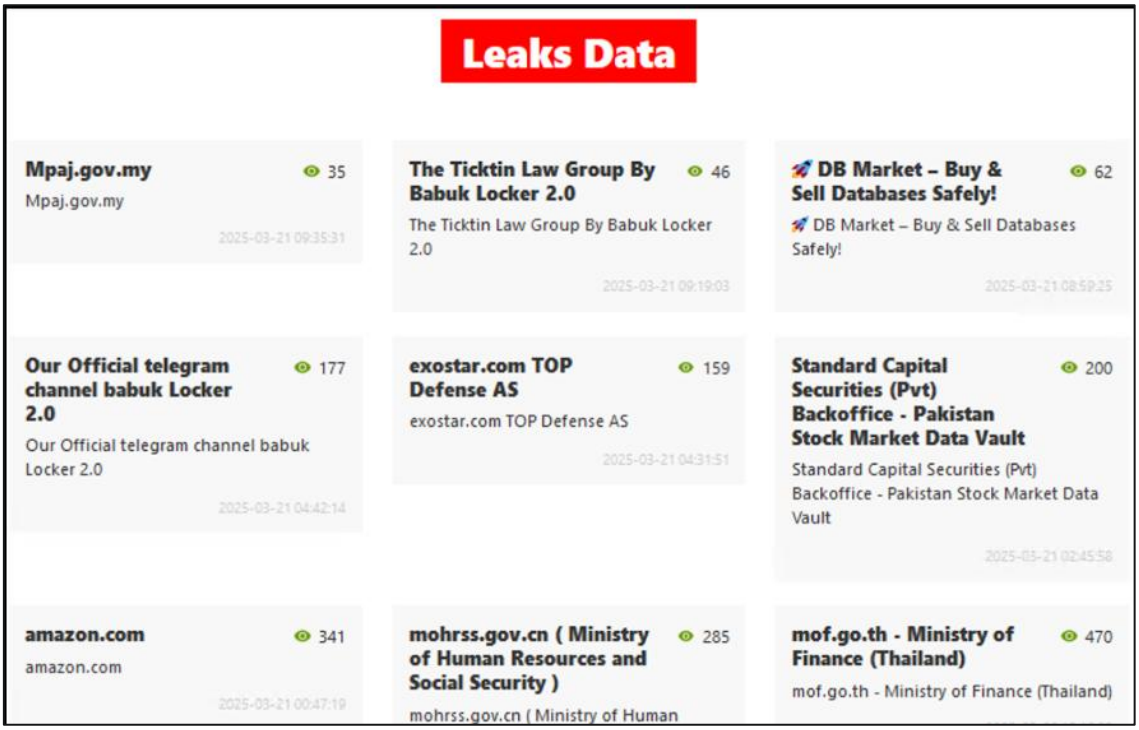

Figure 13: Victims listed on the Babuk Locker 2.0 DLS

Geographical Distribution: Babuk Locker 2.0 targets entities across multiple countries, with a strong presence in North America, Europe, and Asia.

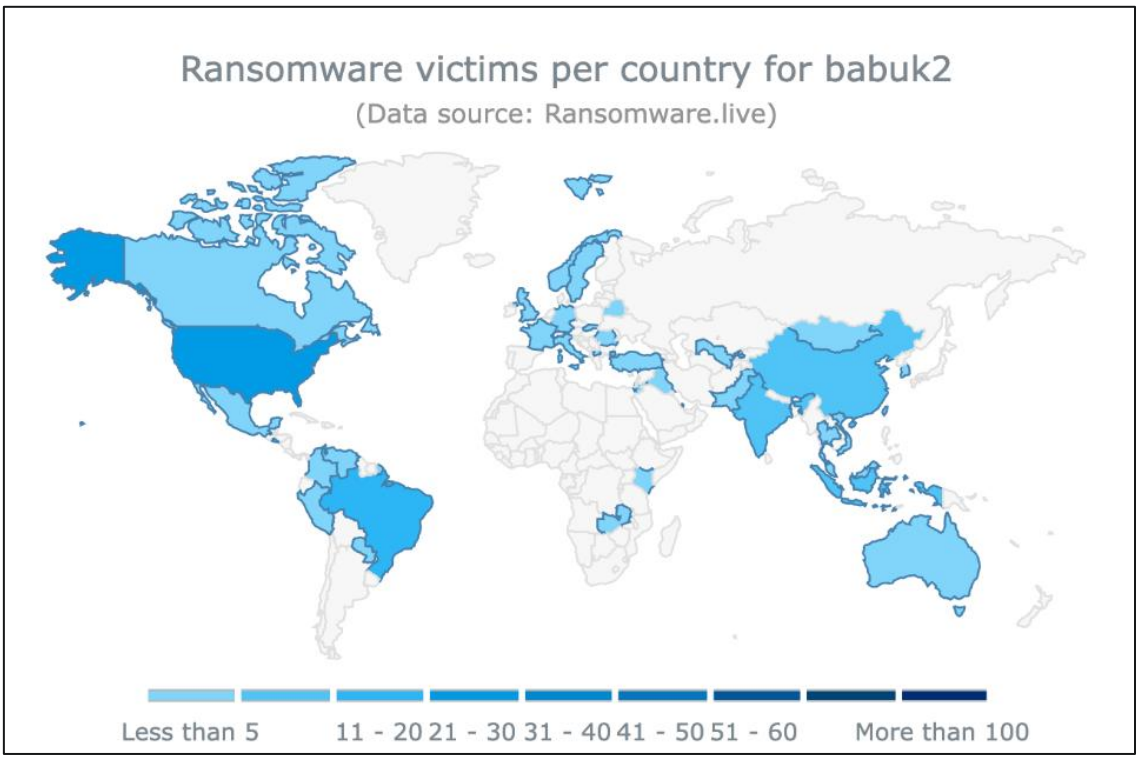

Figure 14: Babuk Locker 2.0 victims per county

VICTIM OVERLAP WITH OTHER RANSOMWARE GROUPS

Many Babuk 2.0's victims were already attacked by other groups, such as HellCat, RansomHub, and FunkSec. This suggests that Babuk 2.0 is exaggerating its victim count or reusing data from other attacks**.**

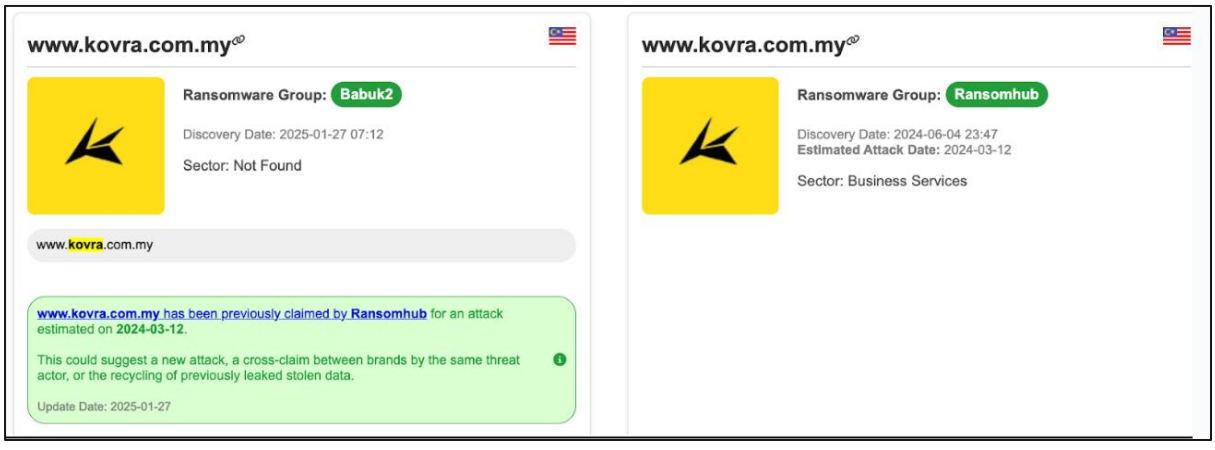

Figure 15: Babuk Locker 2.0 victims overlap with the RansomHub ransomware group

CONCLUSION

Babuk Locker 2.0 is not a true successor to the original Babuk ransomware but rather a LockBit 3.0 rebrand used by threat actors Skywave and Bjorka. Despite claiming numerous

high-profile attacks, many of these victims have already been targeted by other ransomware groups, raising doubts about the authenticity of Babuk 2.0's operations.

This case reinforces a familiar pattern in the ransomware landscape:

- Threat actors do not disappear, they rebrand, recycle code, and continue extortion under new names.
- Ransomware-as-a-Service (RaaS) is evolving, with multiple groups sharing attack infrastructure.
- Security teams must remain vigilant against rebranded threats that use deception to evade defenses.

INDICATORS OF COMPROMISE (IOCs)

Data Leak Sites (DLS) (.onion)

- *7dikawx73goypgfi4zyo5fcajxwb7agemmiwqax3p54aey4dwobcvcyd.onion*
- *imblth46g3x5oo444wkjn7umj4g26tnhmrlo53ovfqmmkmughdw4j2ad.onion*
- *bxwu33iefqfc3rxigynn3ghvq4gdw3gxgxna5m4aa3o4vscdeeqhiqad.onion*

Telegram Handles

- *@OfficialBabukLocker*
- *@BabukLockerRaasSHA1*
- *@BabukLockerRaas (inactive)*
- *@BGLocker*

Tox ID & Contact Information

Tox ID: *022A7EEB83B648F55DA7A6BEFD130C2156C74F3501A31D853234EC2D18E77A1E5BEC7F60201*

Email: *babuklockerofficial@onionmail.org*

YouTube Channel: youtube.com/@babuklocker

Ransomware Samples (SHA-256 Hashes)

- *3facc153ed82a72695ee2718084db91f85e2560407899e1c7f6938fd4ea011e9*
- *bdc482583a330a4682d13bfb7a0cf75b2fa350ac536064bce7b2bdd9d875de4a*
- *0192eaf2ea5a52fa9d2398b3a2f69c163d47b368cd131ccae60df0a98c1fa2ca*

RECOMMENDED ACTIONS

Given that Babuk Locker 2.0 is a rebranded LockBit 3.0 variant, organizations should implement security measures specifically targeting LockBit 3.0 tactics, techniques, and procedures (TTPs) to prevent infection, detect malicious activity, and respond effectively in case of an attack.

- Regularly update operating systems, software, and firmware to patch known vulnerabilities.
- Enforce MFA for administrative and remote access accounts.
- Implement role-based access control (RBAC) and monitor for privilege escalation attempts.
- Use network segmentation to separate critical infrastructure from user workstations.
- Implement firewalls and endpoint detection (EDR/XDR) solutions to monitor network traffic.
- Disable Office macros and PowerShell execution policies to prevent malicious scripts.
- Use Application Whitelisting (AWL) or AppLocker to block unauthorized scripts.
- Set alerts for file extensions commonly used by LockBit 3.0 (.lockbit, .babuk, .abcd, etc.).

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

https://www.rapid7.com/blog/post/2025/04/02/a-rebirth-of-a-cursed-existence-the-babuk-locker-2-0/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com