Babuk ransomware's full source code leaked on hacker forum

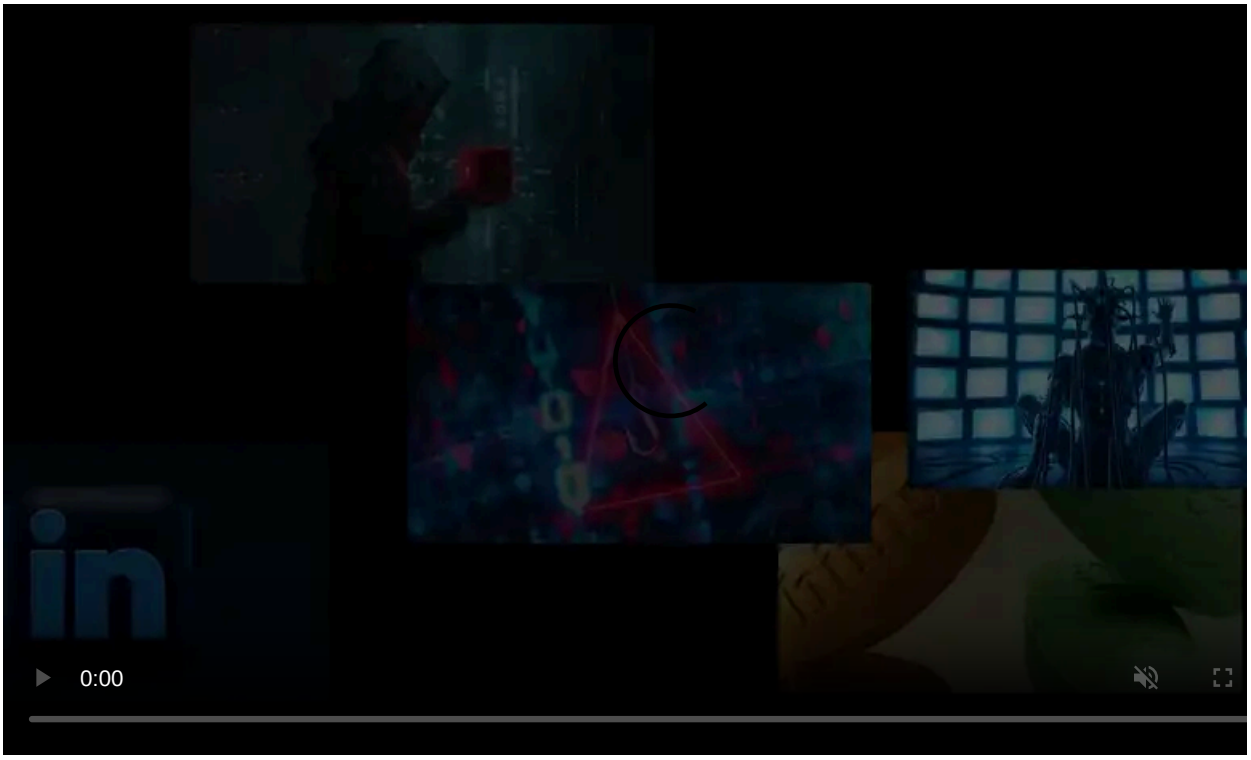
By Lawrence Abrams

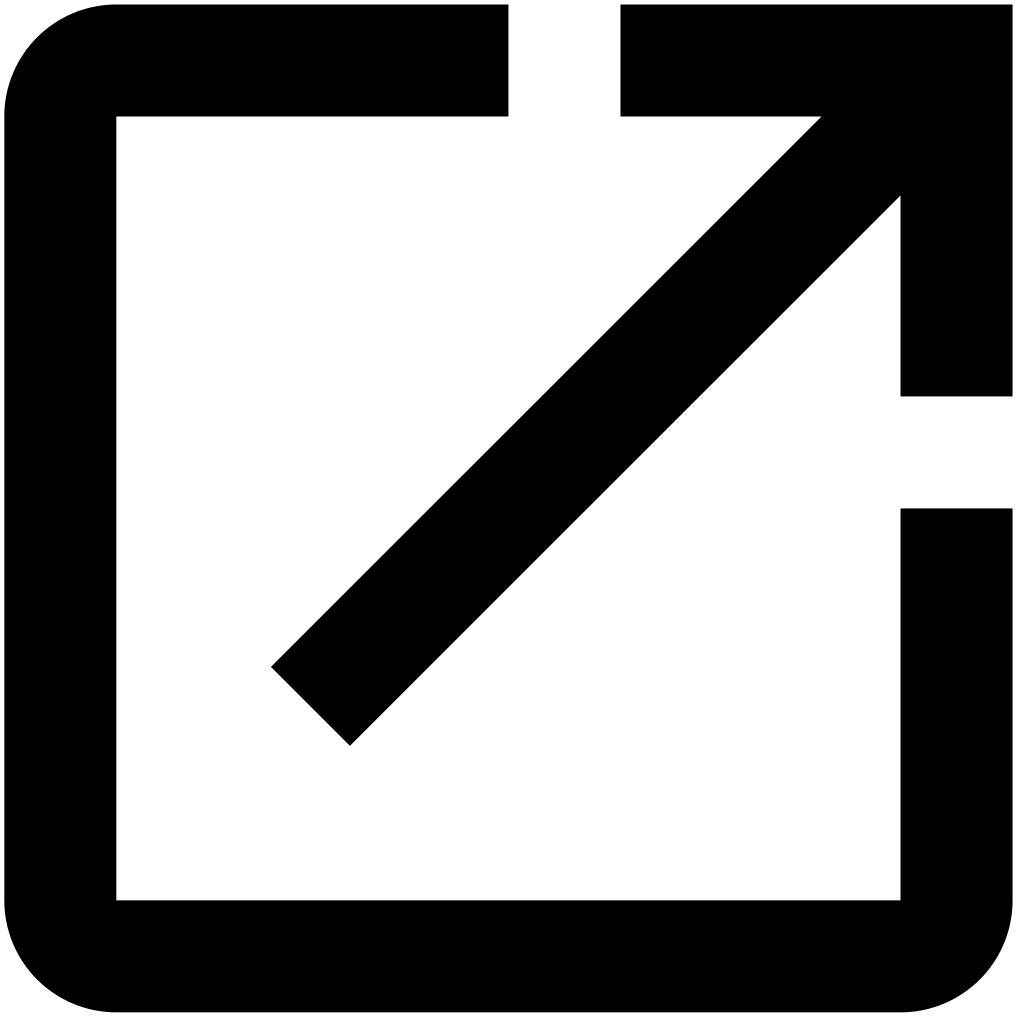
Published: 2021-09-03 · Archived: 2026-04-05 15:36:54 UTC

A threat actor has leaked the complete source code for the Babuk ransomware on a Russian-speaking hacking forum.

Babuk Locker, also known internally as Babyk, is a ransomware operation launched at the beginning of 2021 when it began targeting businesses to steal and encrypt their data in double-extortion attacks.

After attacking the Washinton DC's Metropolitan Police Department (MPD) and feeling the heat from U.S. law enforcement, the ransomware gang claimed to have shut down their operation.


0:00

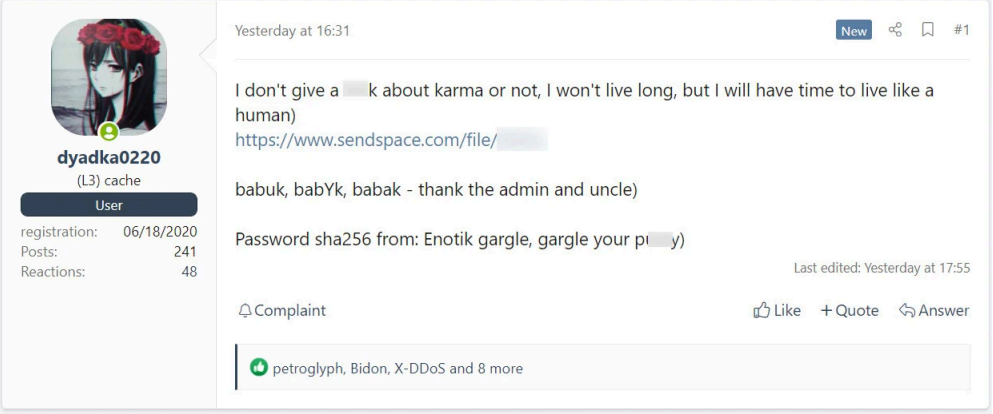


However, members of the same group splintered off to relaunch the ransomware as Babuk V2, where they continue to encrypt victims to this day.

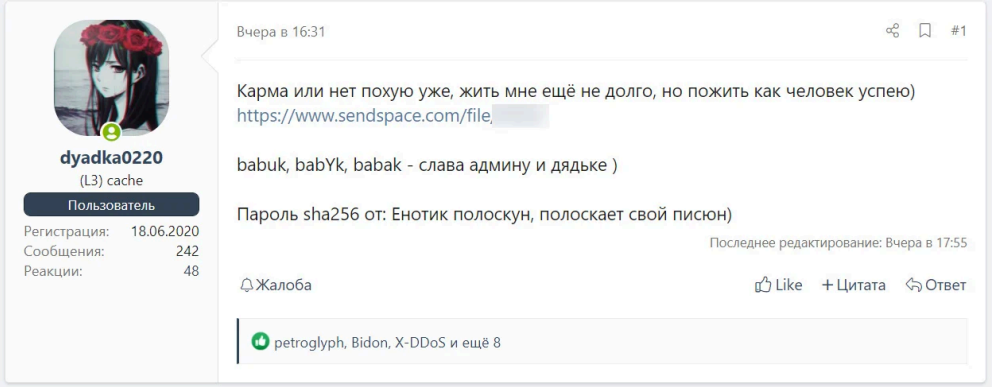
Source code released on a hacking forum

As first noticed by security research group vx-underground, an alleged member of the Babuk group released the full source code for their ransomware on a popular Russian-speaking hacking forum.

This member claimed to be suffering from terminal cancer and decided to release the source code while they have to "live like a human."



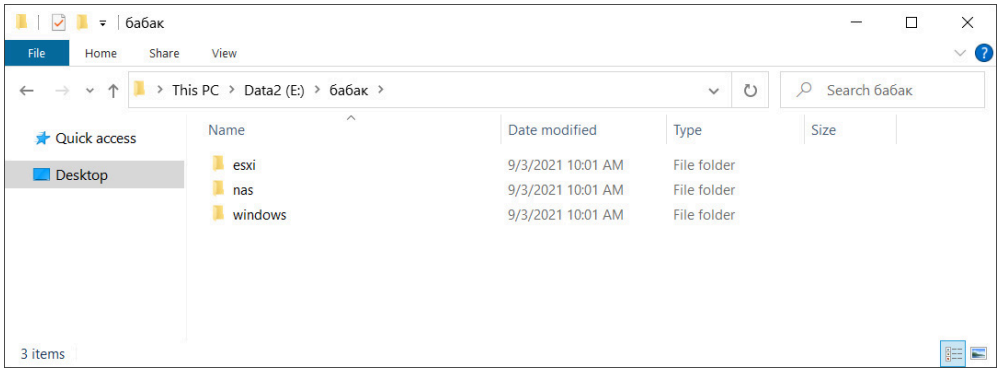
A translated forum post on a hacking forum



Original post in Russian

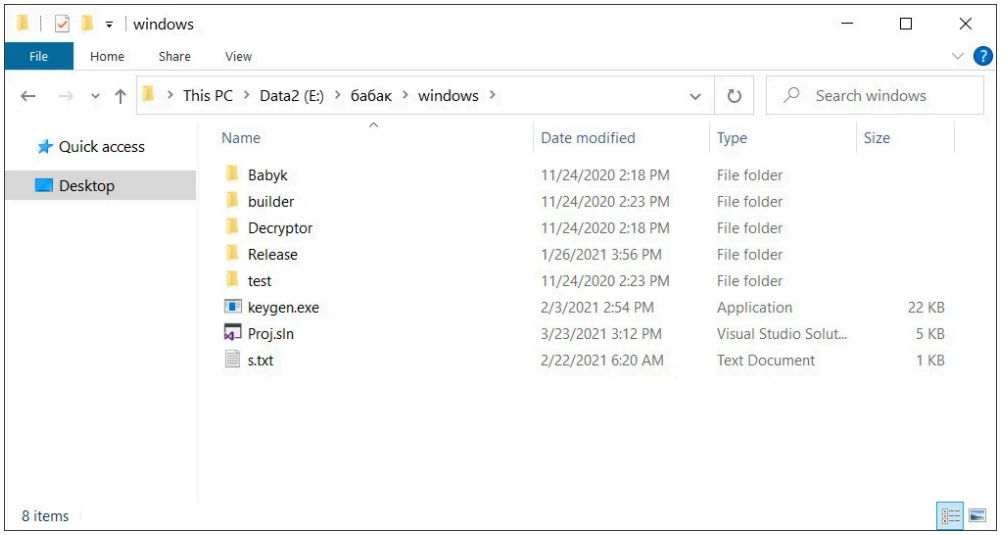
As the leak contains everything a threat actor needs to create a functional ransomware executable, BleepingComputer has redacted the links to the source code.

The shared file contains different Visual Studio Babuk ransomware projects for VMware ESXi, NAS, and Windows encryptors, as shown below.



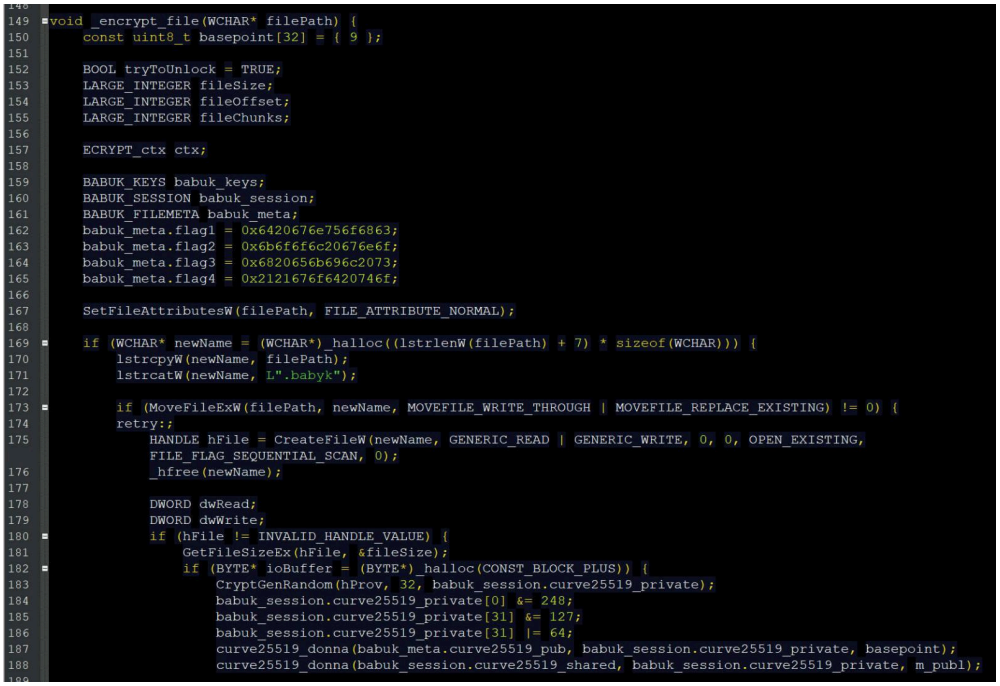
ESXi, NAS, and Windows Babuk ransomware source code

The Windows folder contains the complete source code for the Windows encryptor, decryptor, and what appears to be a private and public key generator.



Babuk Windows encryptor source code

For example, the source code for the encryption routine in the Windows encryptor can be seen below.



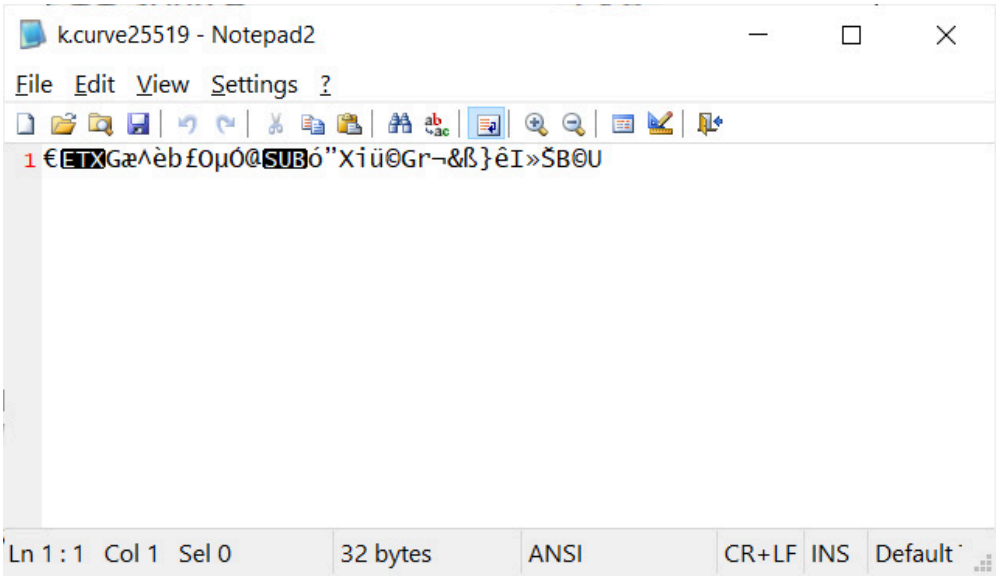
```
void _encrypt_file(WCHAR* filePath) {
    const uint8_t basepoint[32] = { 9 };

    BOOL tryToUnlock = TRUE;
    LARGE_INTEGER fileSize;
    LARGE_INTEGER fileOffset;
    LARGE_INTEGER fileChunks;

    ECRYPT_ctx ctx;

    BABUK_KEYS babuk_keys;
    BABUK_SESSION babuk_session;
    BABUK_FILEMETA babuk_meta;
    babuk_meta.flag1 = 0x6420676e756f6863;
    babuk_meta.flag2 = 0x6b6f6f6c20676e6f;
    babuk_meta.flag3 = 0x6820656b696c2073;
    babuk_meta.flag4 = 0x2121676f6420746f;

    SetFileAttributesW(filePath, FILE_ATTRIBUTE_NORMAL);

    if (WCHAR* newName = (WCHAR*)_halloc((lstrlenW(filePath) + 7) * sizeof(WCHAR))) {
        lstrcpyW(newName, filePath);
        lstrcatW(newName, L".babyk");

        if (MoveFileExW(filePath, newName, MOVEFILE_WRITE_THROUGH | MOVEFILE_REPLACE_EXISTING) != 0) {
        retry:;
            HANDLE hFile = CreateFileW(newName, GENERIC_READ | GENERIC_WRITE, 0, 0, OPEN_EXISTING,
            FILE_FLAG_SEQUENTIAL_SCAN, 0);
            _hfree(newName);

            DWORD dwRead;
            DWORD dwWrite;
            if (hFile != INVALID_HANDLE_VALUE) {
                GetFileSizeEx(hFile, &fileSize);
                if (BYTE* ioBuffer = (BYTE*)_halloc(CONST_BLOCK_PLUS)) {
                    CryptGenRandom(hProv, 32, babuk_session.curve25519_private);
                    babuk_session.curve25519_private[0] &= 248;
                    babuk_session.curve25519_private[31] &= 127;
                    babuk_session.curve25519_private[31] |= 64;
                    curve25519_donna(babuk_meta.curve25519_pub, babuk_session.curve25519_private, basepoint);
                    curve25519_donna(babuk_session.curve25519_shared, babuk_session.curve25519_private, m_publ);
```

Babuk encryption routine source code

Emsisoft CTO and ransomware expert Fabian Wosar and researchres from McAfee Enterprise have both told BleepingComputer that the leak appears legitimate. Wosar also stated that the leak may contain decryption keys for past victims.

Babuk ransomware uses elliptic-curve cryptography (ECC) as part of its encryption routine. Included in the leak are folders containing encryptors and decryptors compiled for specific victims of the ransomware gang.

Wosar told BleepingComputer that these folders also contain curve files that could be the ECC decryption keys for these victims, but this has not been confirmed yet.



ECC curve file for Babuk victim

In total, there are 15 folders with curve files containing possible decryption keys.

Of tales of betrayal and backstabbing

Babuk Locker has a sordid and public history involving betrayal and backstabbing that led to the group splintering.

BleepingComputer has learned from one of the Babuk ransomware gang members that the group splintered after the attack on the Washinton DC's Metropolitan Police Department (MPD).

After the attack, the 'Admin' allegedly wanted to leak the MPD data for publicity, while the other gang members were against it.

> **"We're not good guys, but even for us it was too much.)" - Babuk threat actor**

After the data leak, the group splintered with the original Admin forming the Ramp cybercrime forum and the rest launching Babuk V2, where they continue to perform ransomware attacks.

Soon after the Admin launched the Ramp cybercrime forum, it suffered a series of DDoS attacks to make the new site unusable. The Admin blamed his former partners for these attacks, while the Babuk V2 team told BleepingComputer that they were not responsible.

"We completely forgot about the old Admin. We are not interested in his forum," the threat actors told BleepingComputer.

To add to the group's controversy, a Babuk ransomware builder was leaked on a file-sharing site and was used by another group to launch their own ransomware operation.

It appears that Babuk is not alone with stories of backstabbing and betrayals.

After Wosar setup up a Jabber account for threat actors to contact him, he tweeted that he has received intel from threat actors who feel "wronged" by their partners and decided to leak information in revenge.

Wosar has told BleepingComputer that he has been able to use this intelligence to prevent ongoing ransomware attacks.

Update 9/3/21: McAfee Enterprise also confirmed that the source code is legitimate.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
