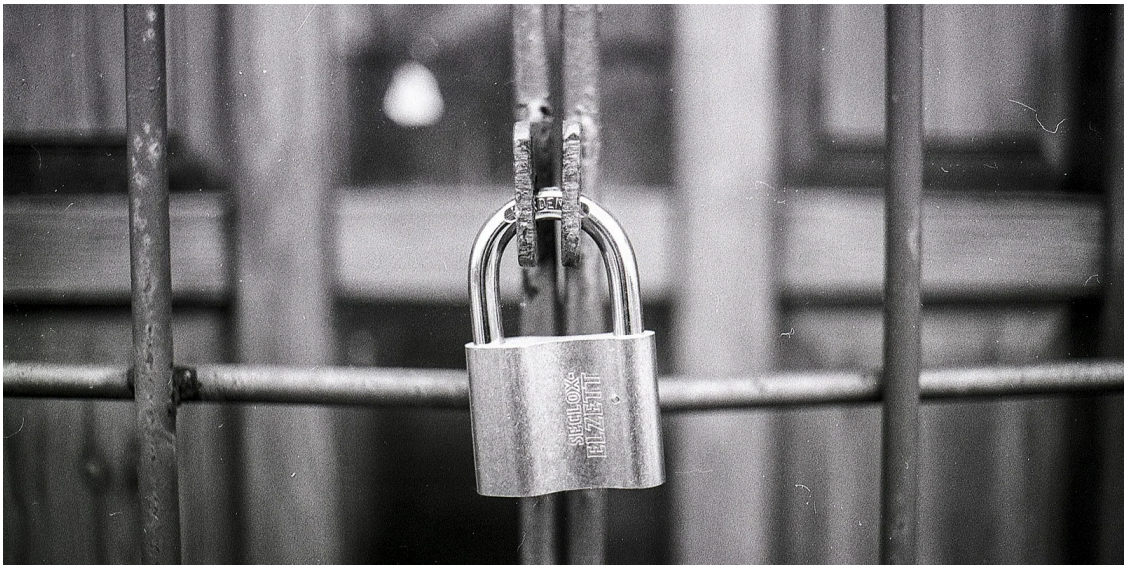
Babuk Locker is the first new enterprise ransomware of 2021

By Lawrence Abrams

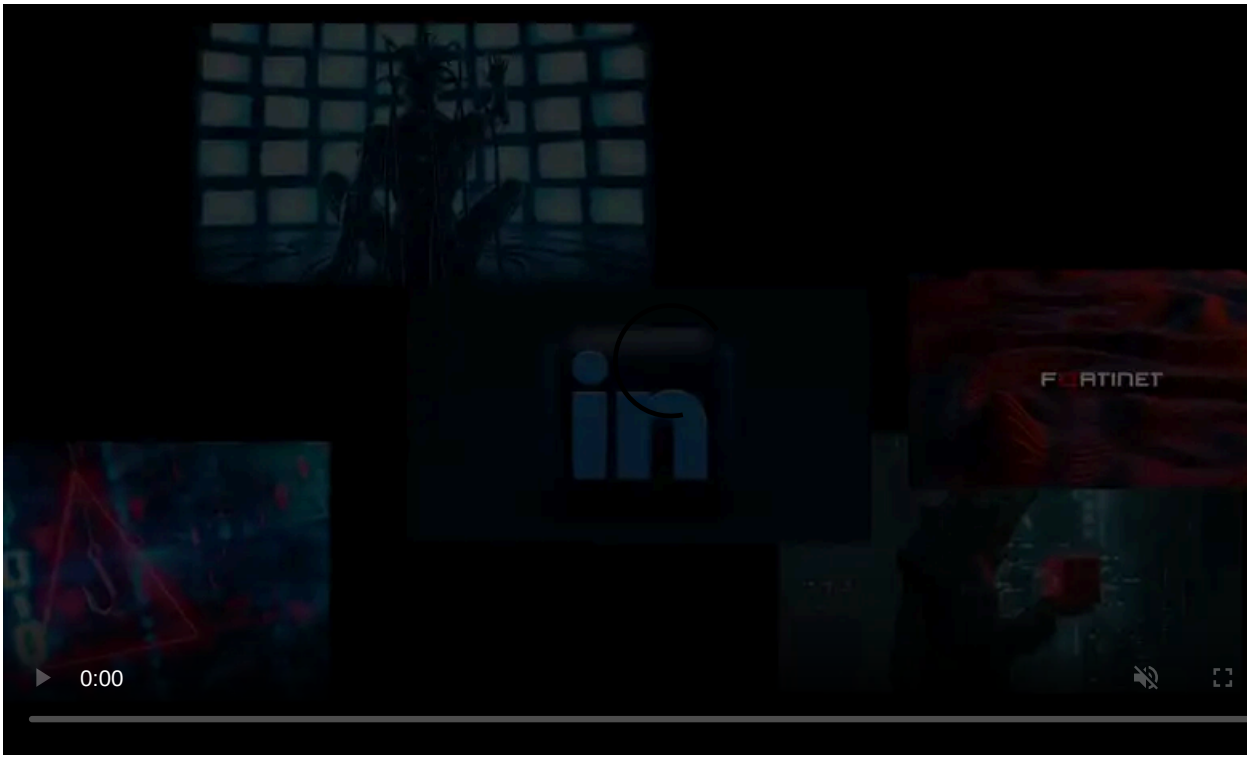
Published: 2021-01-05 · Archived: 2026-04-05 19:28:00 UTC

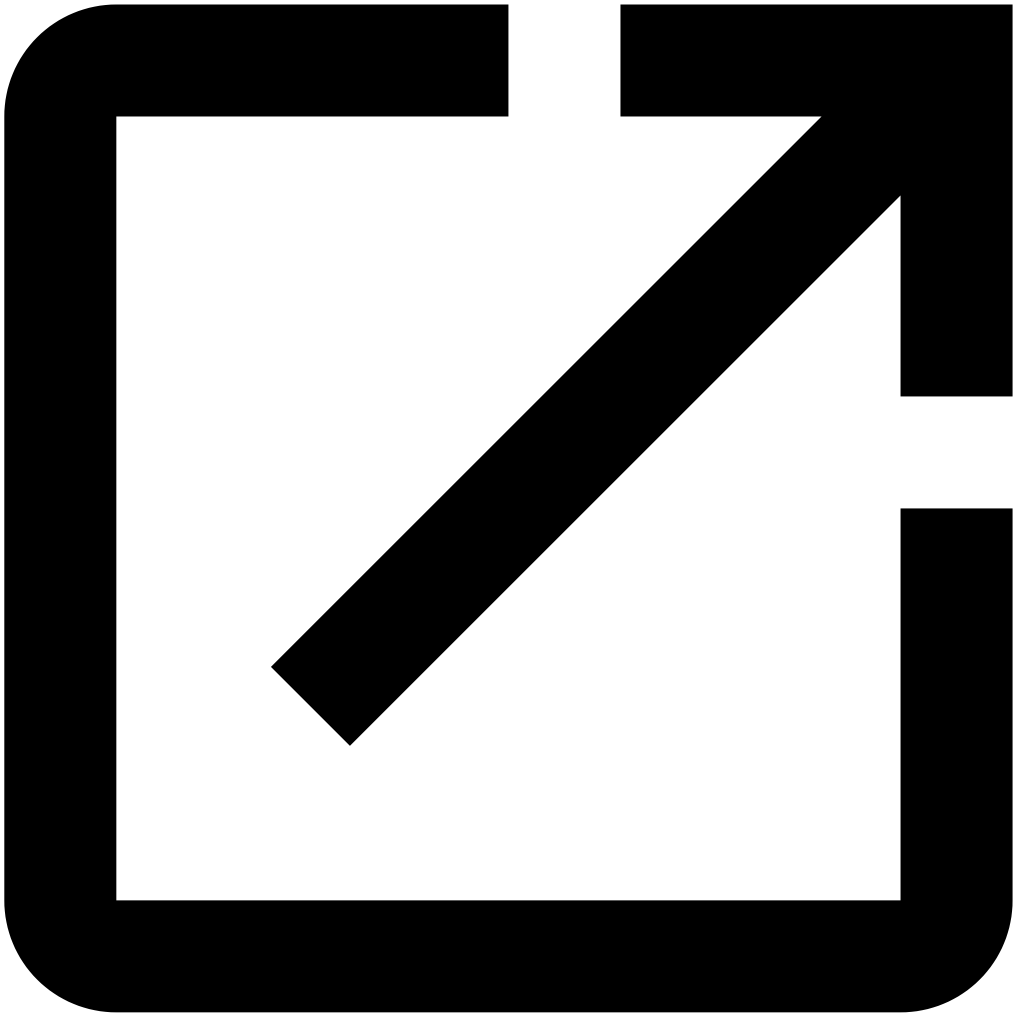


It's a new year, and with it comes a new ransomware called Babuk Locker that targets corporate victims in human-operated attacks.

Babuk Locker is a new ransomware operation that launched at the beginning of 2021 and has since amassed a small list of victims from around the world.

From ransom negotiations with victims seen by BleepingComputer, demands range from $60,000 to $85,000 in Bitcoin.


0:00



How the Babuk Locker encrypts devices

Each Babuk Locker executables analyzed by BleepingComputer has been customized on a per-victim basis to contain a hardcoded extension, ransom note, and a Tor victim URL.

According to security researcher Chuong Dong who also analyzed the new ransomware, Babuk Locker's coding is amateurish but includes secure encryption that prevents victims from recovering their files for free.

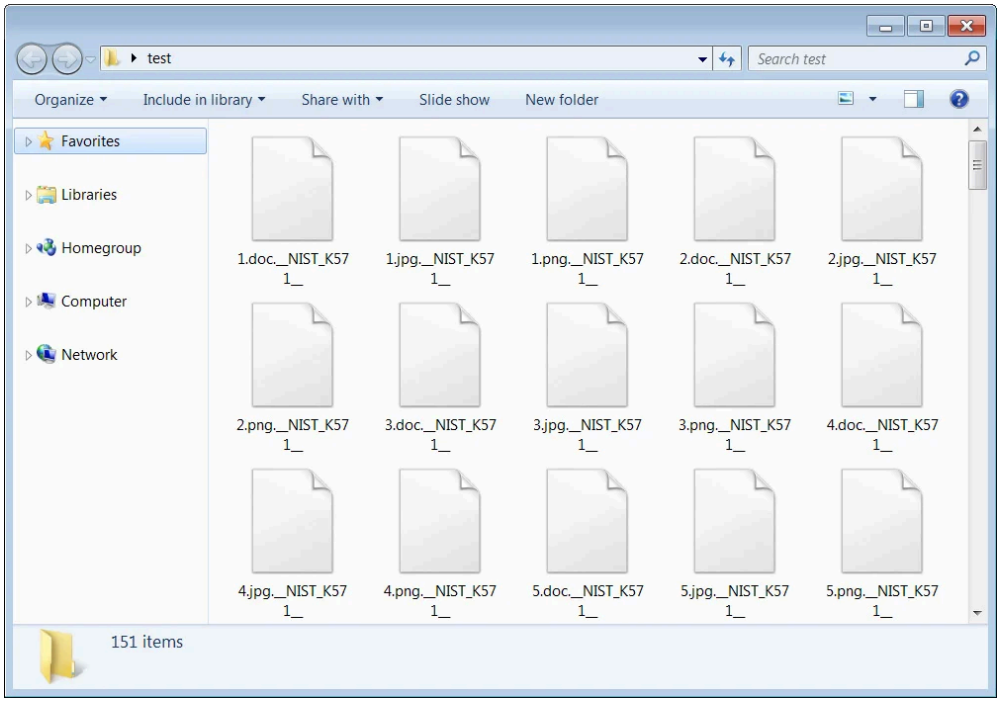
"Despite the amateur coding practices used, its strong encryption scheme that utilizes Elliptic-curve Diffie–Hellman algorithm has proven effective in attacking a lot of companies so far," Dong stated in his report.

When launched, the threat actors can use a command-line argument to control how the ransomware should encrypt network shares and whether they should be encrypted before the local file system. The command-line arguments that control this behavior are listed below:

```
 -lanfirst
-lansecond
-nolan
```

Once launched, the ransomware will terminate various Windows services and processes known to keep files open and prevent encryption. The terminated programs include database servers, mail servers, backup software, mail clients, and web browsers.

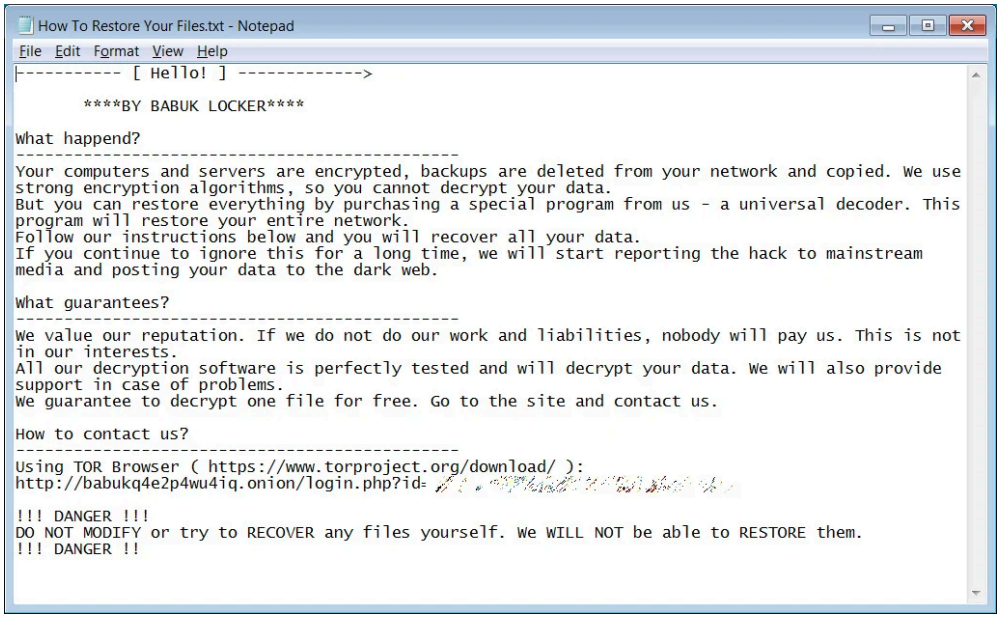
When encrypting files, Babuk Locker will use a hardcoded extension and append it to each encrypted file, as shown below. The current hardcoded extension used for all victims so far is **.__NIST_K571__**.



Babuk Locker encrypted files
Source: BleepingComputer

A ransom note named **How To Restore Your Files.txt** will be created in each folder. This ransom note contains basic information on what happened during the attack and a link to a Tor site where the victim can negotiate with the ransomware operators.

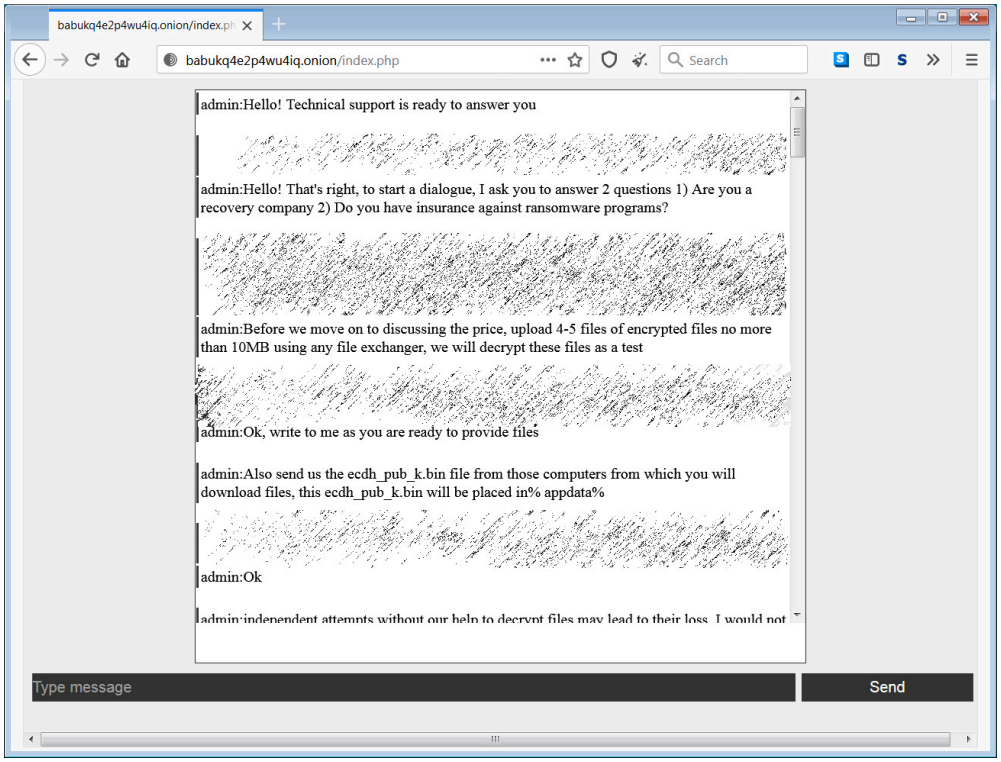
One of the ransom notes seen by BleepingComputer contains the victim's name and links to images proving that the threat actors stole unencrypted files during the attack.



Babuk Locker ransom note

Source: BleepingComputer

The Babuk Locker Tor site is nothing fancy and simply contains a chat screen where the victim can talk to the threat actors and negotiate a ransom. As part of the negotiation process, the ransomware operators ask their victims if they have cyber insurance and are working with a ransomware recovery company.



Babuk Locker Tor chat with a victim

Source: BleepingComputer

The ransomware operators will also ask victims for the **%AppData%\ecdh_pub_k.bin** file, which contains the victims' public ECDH key that allows the threat actors to perform test decryption of victim's files or provide a decryptor.

Unfortunately, Dong says that the ransomware's use of ChaCha8 and Elliptic-curve Diffie–Hellman (ECDH) makes the ransomware secure and not decryptable for free.

Uses hacker forum to leak stolen data

A common ransomware tactic is to steal unencrypted data from a victim before encrypting the network's devices. The threat actors use the stolen data in a double-extortion strategy, where they threaten to leak the data if a ransom is not paid.

Most ransomware operations that utilize this tactic have created public ransomware data leak sites to publish stolen data.

However, Babuk Locker is currently using a hacker forum to leak their stolen data. Babuk Locker currently has five known victims from around the world, including:

- An elevator and escalator company
- An office furniture manufacturer
- A car parts manufacturer
- A medical testing products manufacturer
- An air conditioning and heating company in the USA

At least one of the victims has agreed to pay the ransom, which was for $85,000.

In a post to the hacker forum, the Babuk Locker representative states that they will soon launch a dedicated leak site.
