

## Leaked Babuk Locker ransomware builder used in new attacks

By Lawrence Abrams

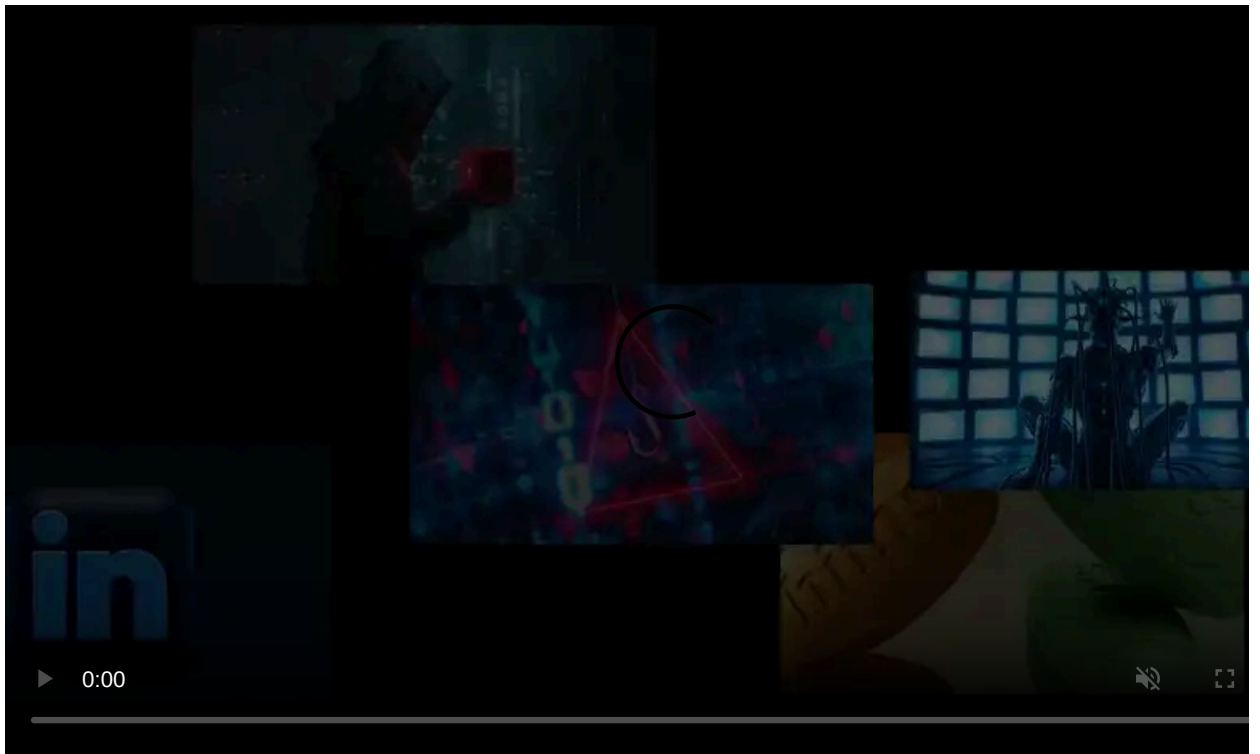
Published: 2021-06-30 · Archived: 2026-04-05 17:01:10 UTC



A leaked tool used by the Babuk Locker operation to create custom ransomware executables is now being used by another threat actor in a very active campaign targeting victims worldwide.

Babuk Locker was a ransomware operation that [launched at the beginning of 2021](#) when it began targeting corporate victims and stealing their data in double-extortion attacks.

After performing an [attack on Washinton DC's Metropolitan Police Department](#) (MPD) and feeling the pressure from law enforcement, the ransomware gang shut down in April and [switched to a non-encrypting data extortion model](#) under the name PayLoad Bin.



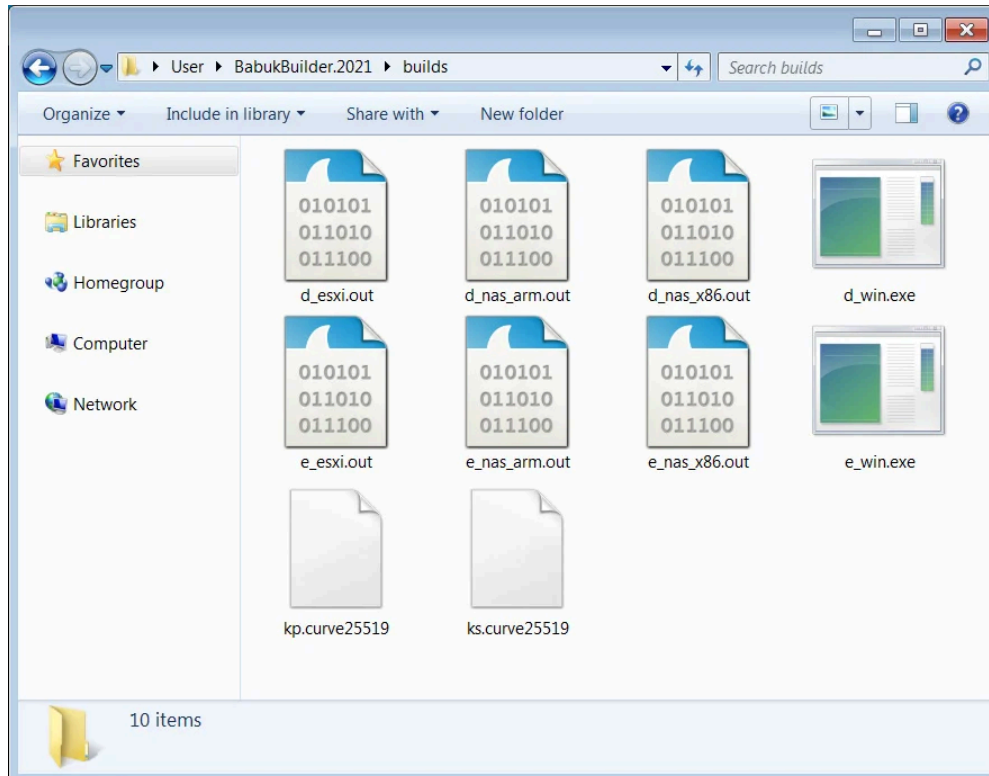
Visit Advertiser website [GO TO PAGE](#)

## Babuk Locker builder leaked

Last week, security researcher [Kevin Beaumont discovered](#) that someone uploaded the Babuk operation's ransomware builder to VirusTotal.

When BleepingComputer tested the builder, it was simplistic to generate a customized ransomware.

All a threat actor has to do is modify the enclosed ransom note to include their own contact info, and then run the build executable to create customized ransomware encryptors and decryptors that target Windows, VMware ESXi, Network Attached Storage (NAS) x86, and NAS ARM devices.



**Using the builder to create a customized Babuk ransomware**

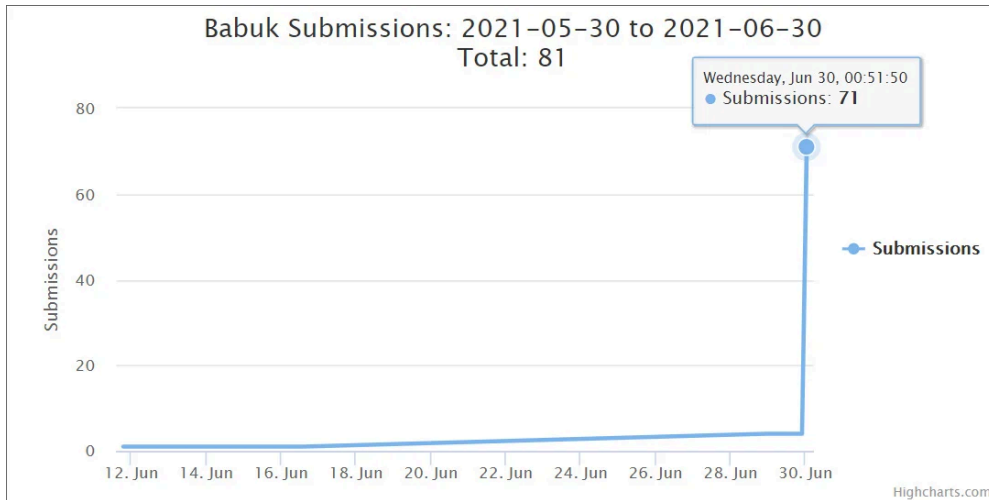
Source: [BleepingComputer.com](#)

## Babuk builder used to launch new attacks

Soon after the builder was leaked online, a threat actor began using it to launch a very active ransomware campaign.

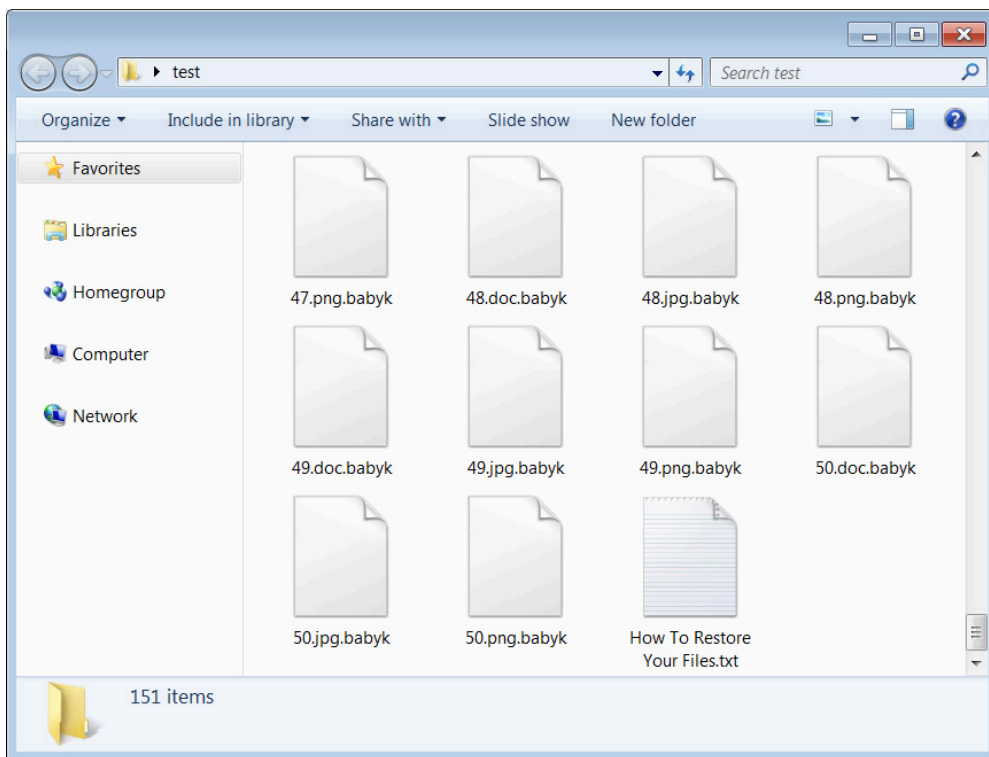
Starting on Tuesday, a victim [reported](#) on Reddit that they were hit by ransomware calling itself 'Babuk Locker.'

Security researcher [MalwareHunterTeam](#) also told BleepingComputer that ID Ransomware received a sharp spike in Babuk Locker submissions starting on June 29th. These victims are from all over the world, and the submitted ransom notes all contained the email address of the threat actor.



### A sharp spike in Babuk Ransomware submissions to ID Ransomware

Like the original operation, this ransomware attack adds the **.babyk** extension to encrypted file names and drops a ransom note named **How To Restore Your Files.txt**.



### Files encrypted by Babuk Locker

Source: *BleepingComputer*

Compared to the original Babuk Ransomware operation that demanded hundreds of thousands, if not millions, of dollars to recover their files, this new threat actor is only asking for .006 bitcoins or approximately \$210 from their victims.

```
1 ----- Hello -----
2
3 *** By BABUCK LOCKER ***
4
5 Your computers and servers are encrypted, and backups are deleted.
6 We use strong encryption algorithms, so no one has yet been able to decrypt their files without our
7 participation.
8 The only way to decrypt your files is to purchase a universal decoder from us, which will restore all the
9 encrypted data and your network.
10 Follow our instructions below, and you will recover all your data:
11
12 1) Pay 0,006 bitcoin to [redacted]
13 2) Send us message with transaction id to babuckransom@tutanota.com
14 3) Launch decryptor.exe, which our support will send you through email
15
16 What guarantees?
17 -----
18 We value our reputation. If we will not do our work and liabilities, nobody will pay us. This is not in our
19 interests.
20 All our decryption software is tested by time and will decrypt all your data.
21 -----
22 !!! DO NOT TRY TO RECOVER ANY FILES YOURSELF. WE WILL NOT BE ABLE TO RESTORE THEM!!!
23
```

### Ransom note from new Babuk ransomware attack

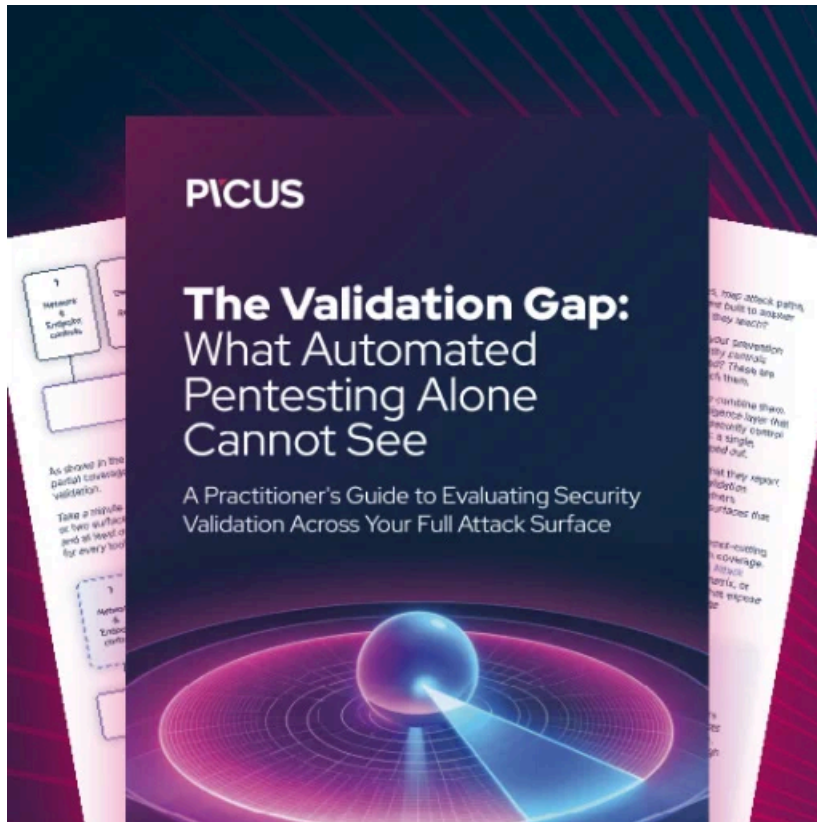
Source: *BleepingComputer*

The new threat actors also misspelled Babuk by adding a 'C' to 'Babuck Locker' in the ransom note.

Another noticeable change is that the original Babuk Locker operation utilized a dedicated Tor payment site used to negotiate with victims. However, the new attacks are using email to communicate with victims through a [babuckransom@tutanota.com](mailto:babuckransom@tutanota.com) email address.

It is unclear how the ransomware is being distributed, but we have created a dedicated [Babuck Locker support topic](#) that victims can use to share more information about the attack.

If anyone pays the ransom demand for this new ransomware campaign, please let us know as we would like to ask you some private questions.



### [Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

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

---

Source: <https://www.bleepingcomputer.com/news/security/leaked-babuk-locker-ransomware-builder-used-in-new-attacks/>