Leaked Babuk Locker ransomware builder used in new attacks

bleepingcomputer.com/news/security/leaked-babuk-locker-ransomware-builder-used-in-new-attacks/

Lawrence Abrams

By
Lawrence Abrams

- June 30, 2021
- 07:01 PM
- 2

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.

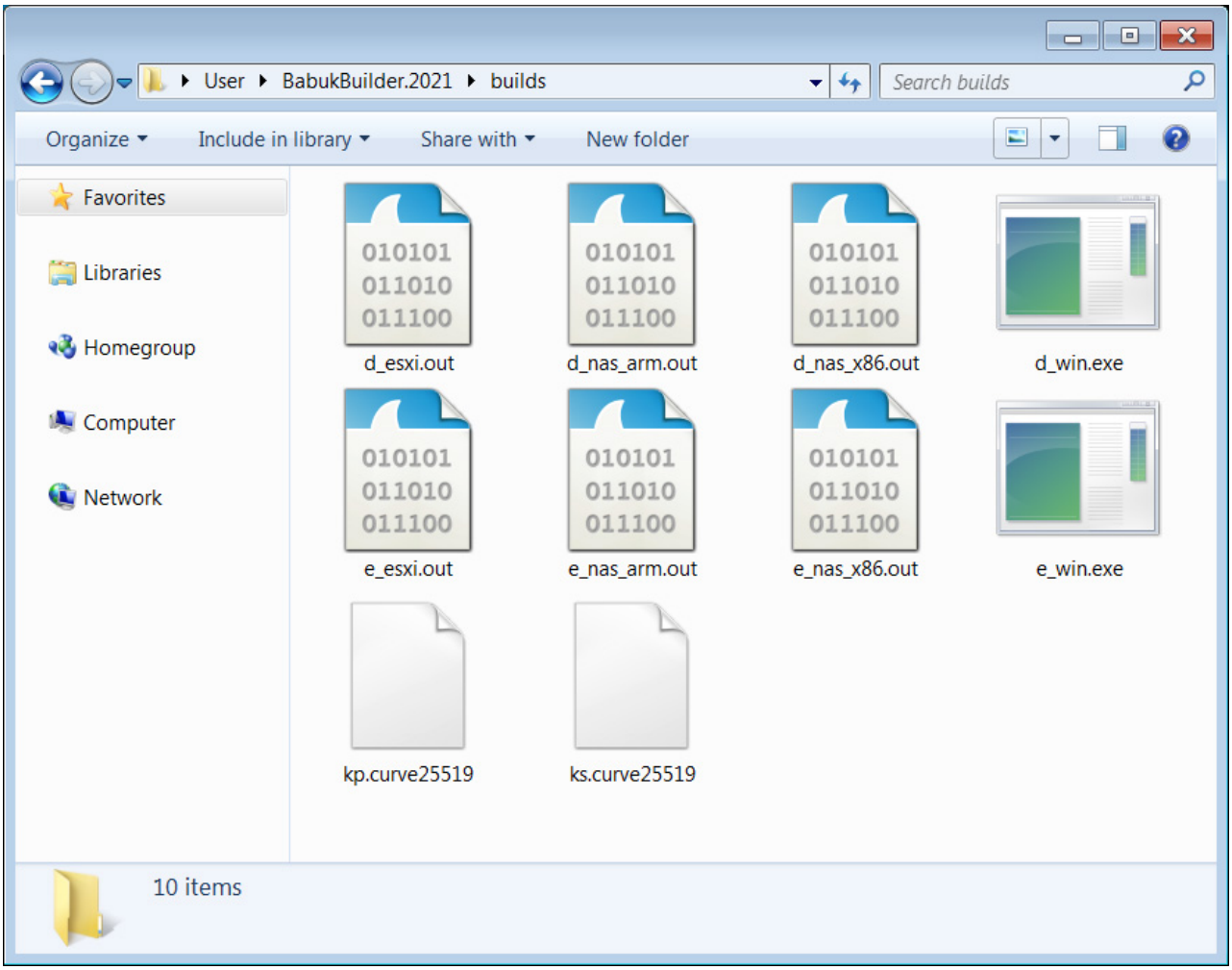
After performing an attack on Washinton DC's Metropolitan Police Department (MPD) and feeling the pressure from law enforcement, the ransomware gang shut down in April and switched to a non-encrypting data extortion model under the name PayLoad Bin.

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.



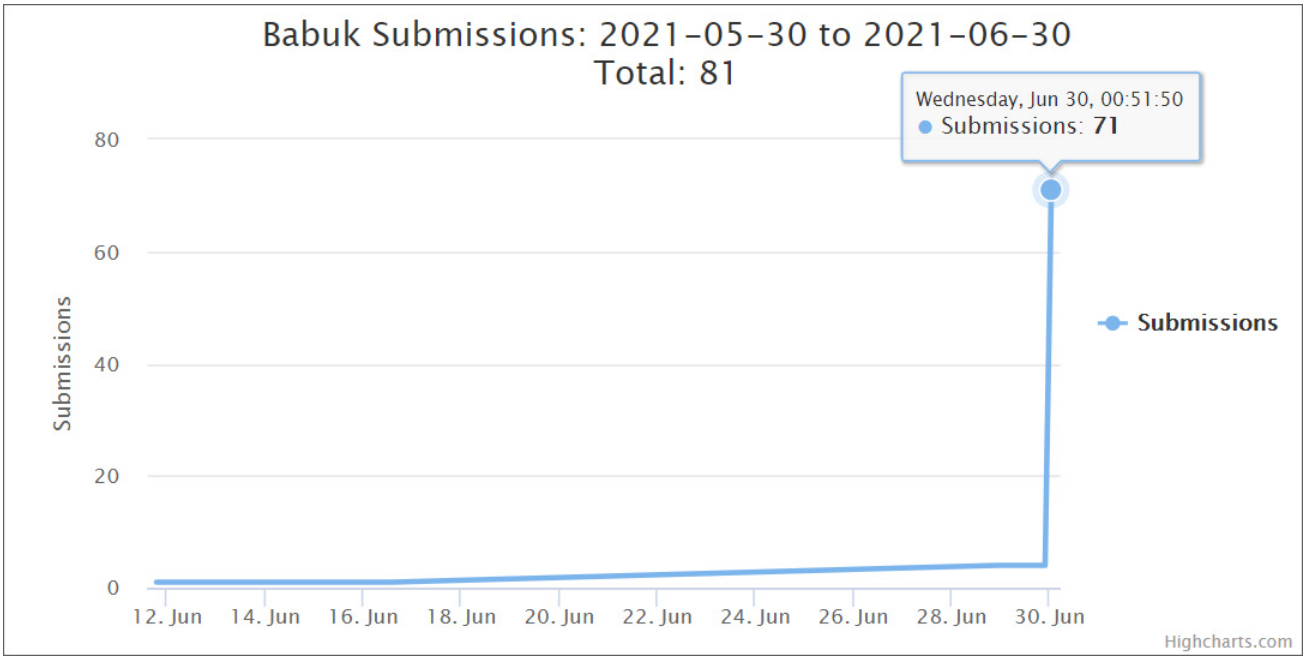
Using the builder to create a customized Babuk ransomware
Source: BleepingComputer.com

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.

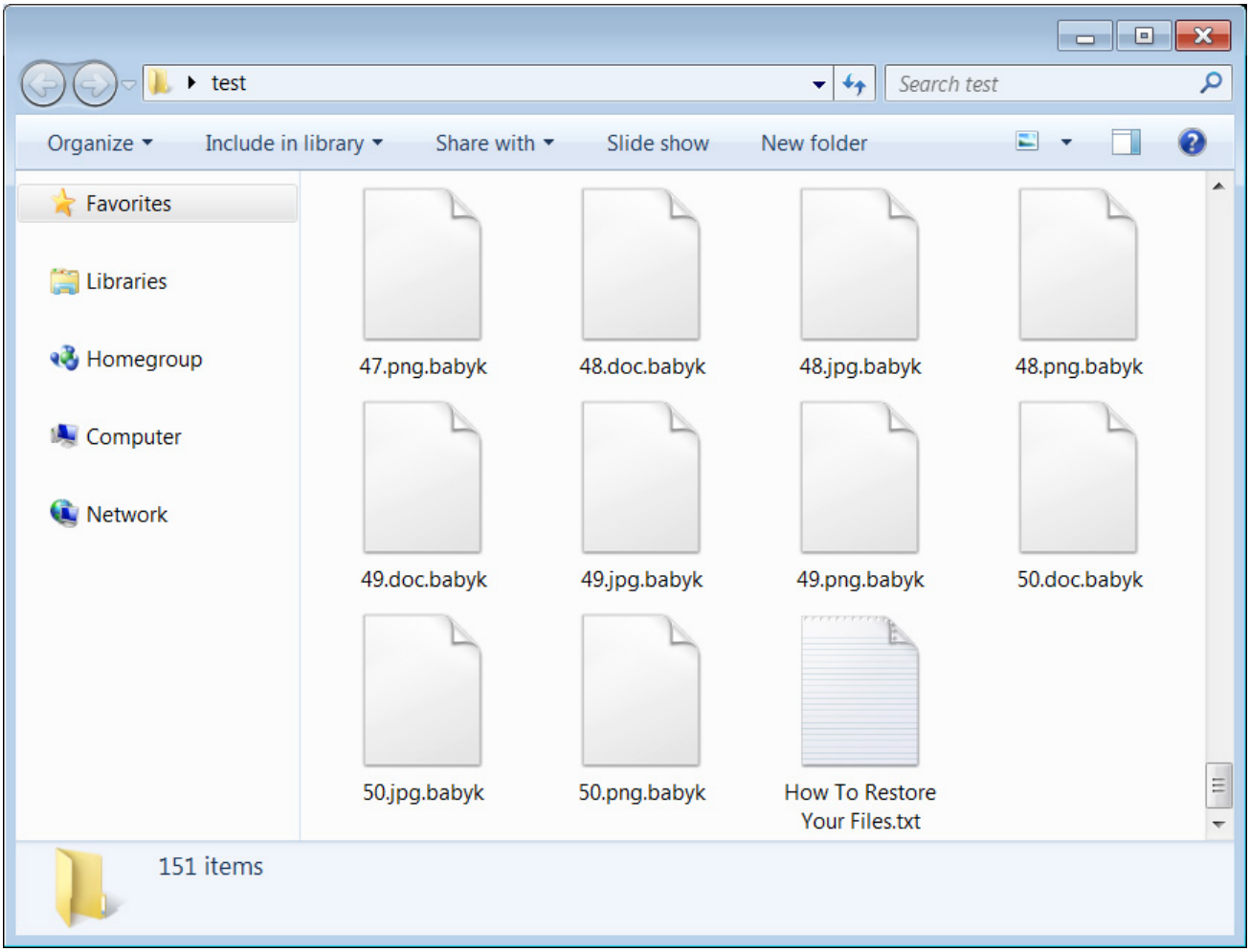
Starting on Tuesday, a victim reported on Reddit that they were hit by ransomware calling itself 'Babuk Locker.'

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

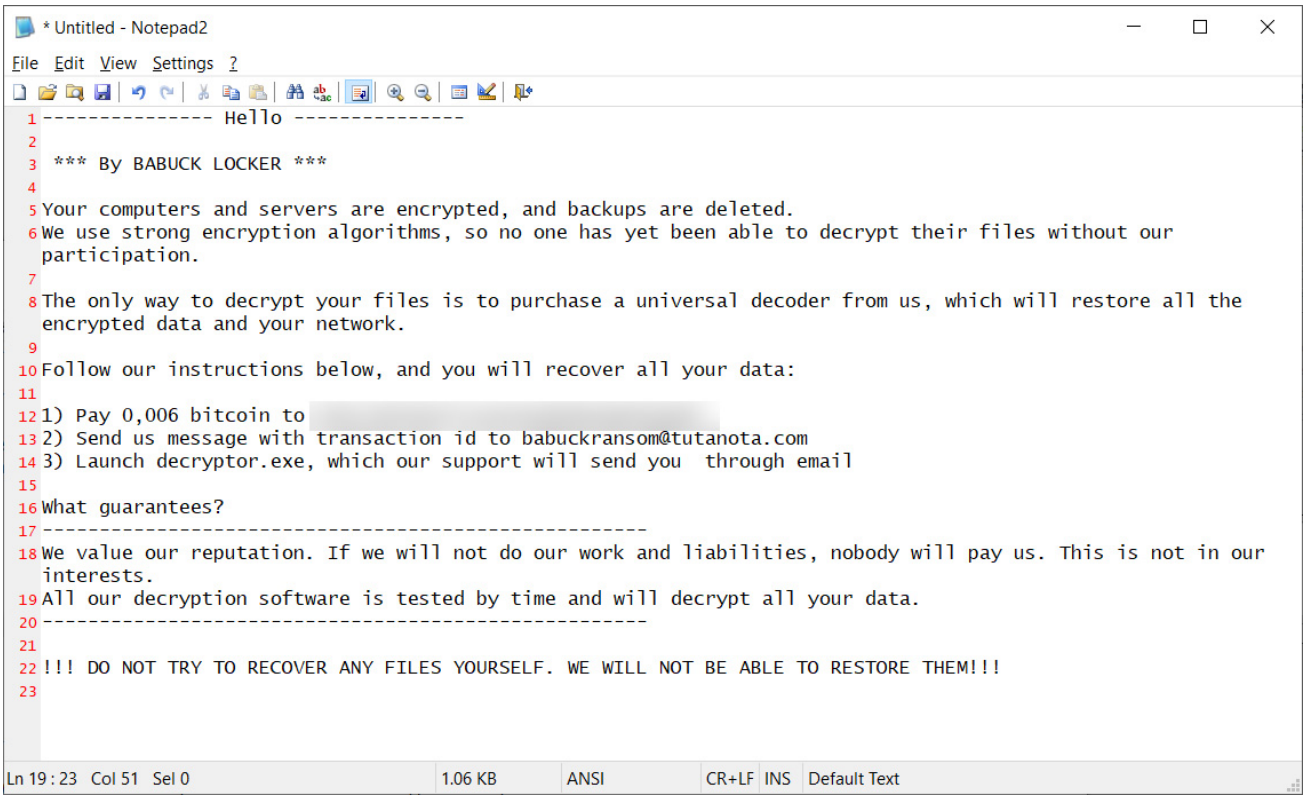
Like the original operation, this ransomware attack adds the **.babyk** extension to encrypted file names and drops a ransom note named **How To Restore Your Files.txt**.



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.



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 babukransom@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.

Related Articles:

Costa Rica declares national emergency after Conti ransomware attacks

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

Wind turbine firm Nordex hit by Conti ransomware attack

Hackers use Conti's leaked ransomware to attack Russian companies

- Babuk Locker
- Cyberattack
- Ransomware
- Ransomware Builder

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

- 
  vitorggrr - 10 months ago
  -
  -
  Hi, I'm Brazilian and I speak Portuguese but I'm translating the message so that it's easier to understand my computer was recently infected by Babuck Locker ransomware, and I am currently looking for a solution as all my files are inaccessible, I was infected on June 27, 2021. I believe the virus has infected my PC through crack for an antivirus. now every folder on my device has a note saying "How To Restore Your Files", I don't know what to do. if you need sample files i am willing to help fight this virus. Thank you very much in advance

- 

  buddy215 - 10 months ago

  -
  -

  You can ask for help in the Ransomware Help & Tech Support Forum here at Bleeping Computer.
  I deleted your email address to protect you.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: