New Black Basta ransomware springs into action with a dozen breaches

bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/

Lawrence Abrams

By
Lawrence Abrams

- April 27, 2022
- 05:46 PM
- 1

A new ransomware gang known as Black Basta has quickly catapulted into operation this month, breaching at least twelve companies in just a few weeks.

The first known Black Basta attacks occurred in the second week of April, as the operation quickly began attacking companies worldwide.

While ransom demands likely vary between victims, BleepingComputer is aware of one victim who received over a $2 million demand from the Black Basta gang to decrypt files and not leak data.

Not much else is known about the new ransomware gang as they have not begun marketing their operation or recruiting affiliates on hacking forums.

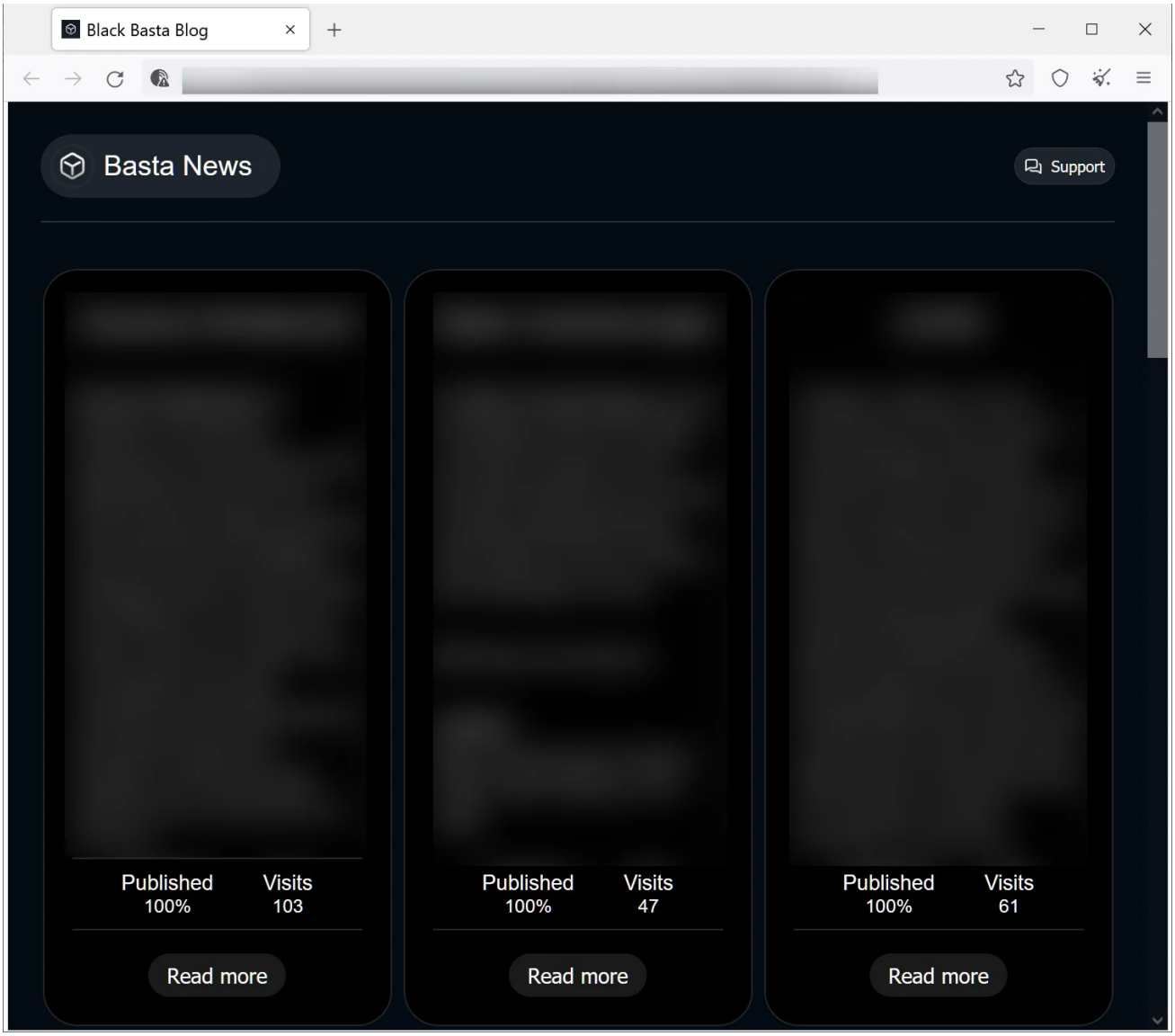
However, due to their ability to quickly amass new victims and the style of their negotiations, this is likely not a new operation but rather a rebrand of a previous top-tier ransomware gang that brought along their affiliates.

Steals data before encrypting

Like other enterprise-targeting ransomware operations, Black Basta will steal corporate data and documents before encrypting a company's devices.

This stolen data is then used in double-extortion attacks, where the threat actors demand a ransom to receive a decryptor and prevent the publishing of the victim's stolen data.

The data extortion part of these attacks is conducted on the 'Black Basta Blog' or 'Basta News' Tor site, which contains a list of all victims who have not paid a ransom. Black Basta will slowly leak data for each victim to try and pressure them into paying a ransom.



Black Basta data leak site

Source: BleepingComputer
The Black Basta data leak site currently contains data leak pages for ten companies they breached. However, BleepingComputer knows of other victims not currently listed on the data leak site.

Their most recent listed victim is Deutsche Windtechnik, who suffered a cyberattack on April 11th but had not disclosed it was a ransomware attack.

Yesterday, the data leak site also began leaking the data for the American Dental Association, which suffered an attack on April 22nd, but that page has since been removed. The removal of their page indicates that the company is negotiating with the threat actors.

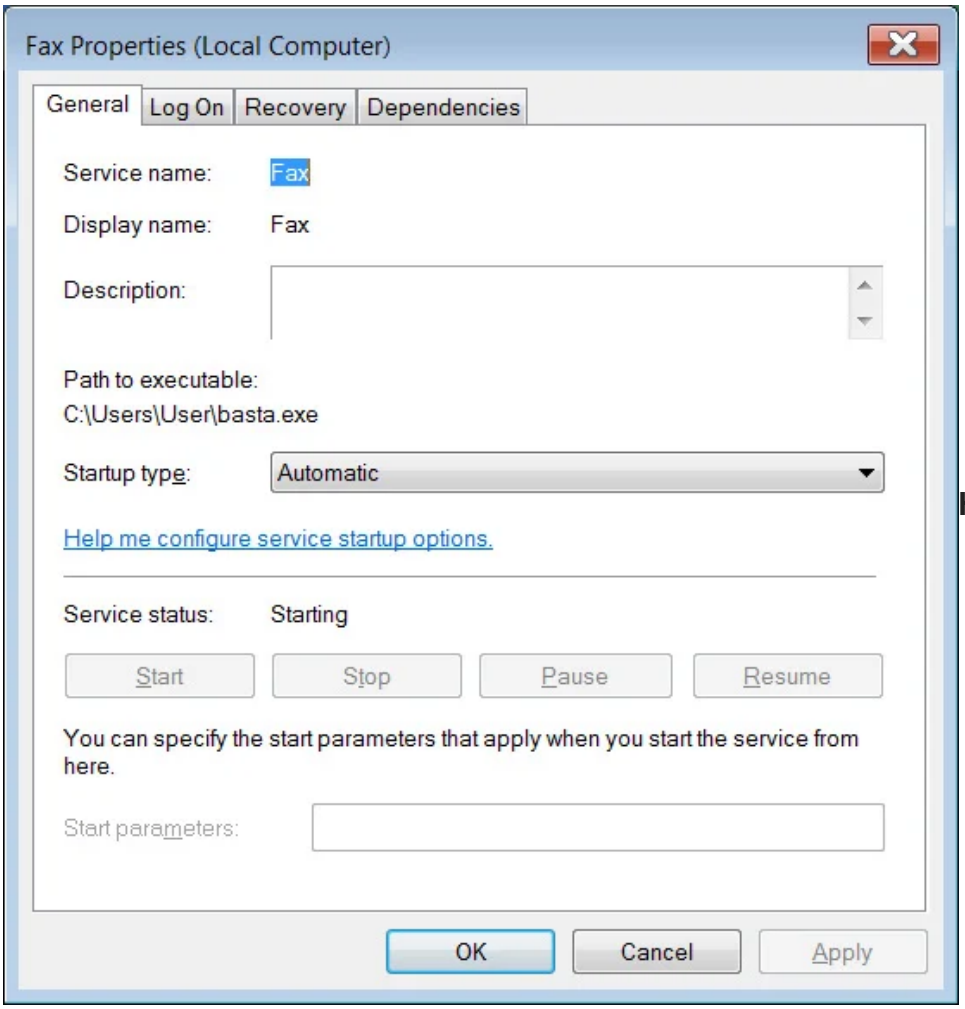
A deeper dive into Black Basta

BleepingComputer performed a brief analysis of the Black Basta ransomware from online samples.

When executed, the Black Basta encryptor needs to be run with administrative privileges, or it will not encrypt files. Once launched, the encryptor will delete Volume Shadow Copies using the following command:

```
C:\Windows\system32\cmd.exe /c C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet
```

It will then hijack an existing Windows service and uses it to launch the ransomware encryptor executable. In our tests, the Windows Service that was hijacked was the 'Fax' service, as shown below.



Hijacked Fax Windows service used to launch Black Basta

Source: BleepingComputer

The ransomware will also change the wallpaper to display a message stating, "Your network is encrypted by the Black Basta group. Instructions in the file readme.txt."

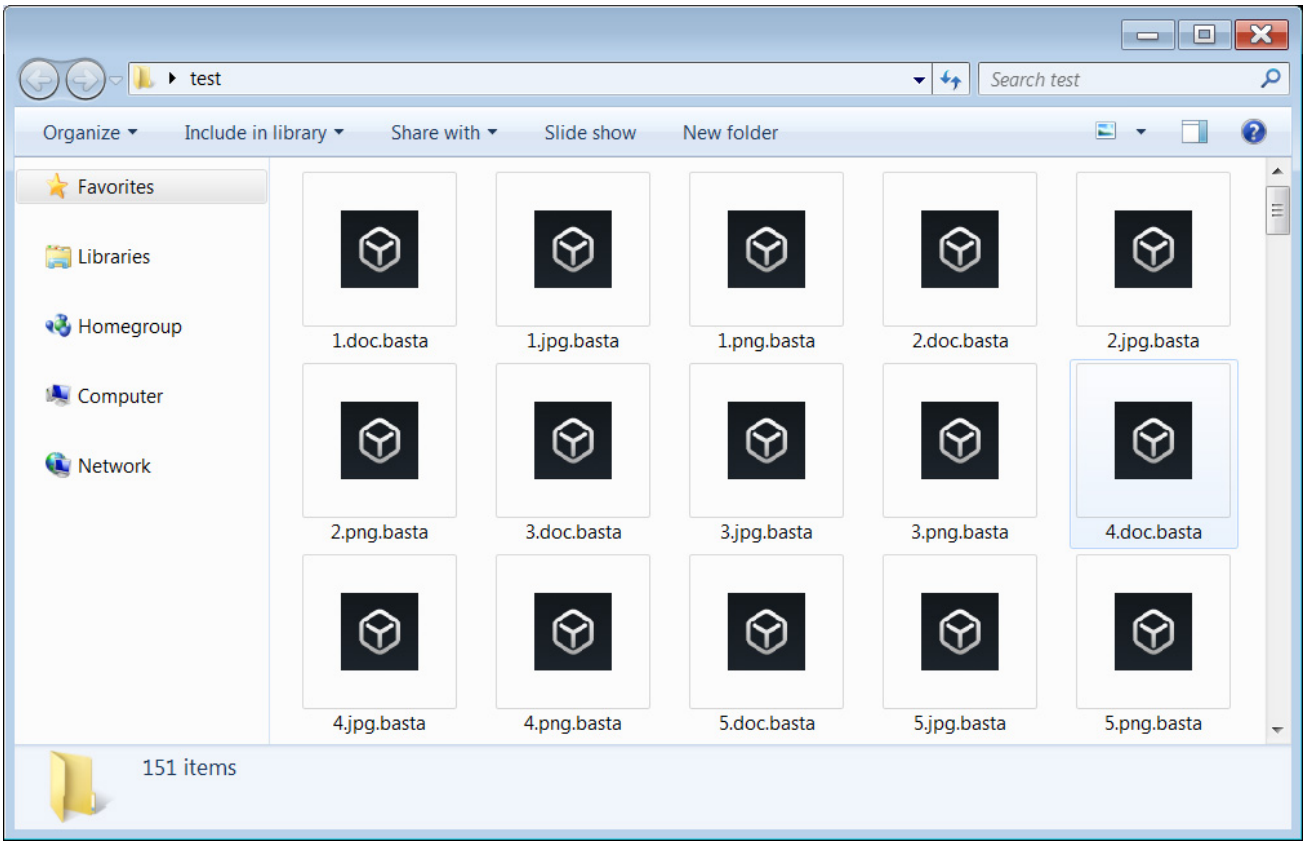
Wallpaper added by the Black Basta encryptor

Source: BleepingComputer

The ransomware will now reboot the computer into Safe Mode with Networking, where the hijacked Windows service will start and automatically begin to encrypt the files on the device.

Ransomware expert Michael Gillespie, who analyzed Black Basta's encryption process, told BleepingComputer that it utilizes the ChaCha20 algorithm to encrypt files. The ChaCha20 encryption key is then encrypted with a public RSA-4096 key included in the executable.

While encrypting files, the ransomware will append the **.basta** extension to the encrypted file's name. So, for example, test.jpg would be encrypted and renamed to test.jpg.basta.



Black Basta encrypted files

Source: BleepingComputer

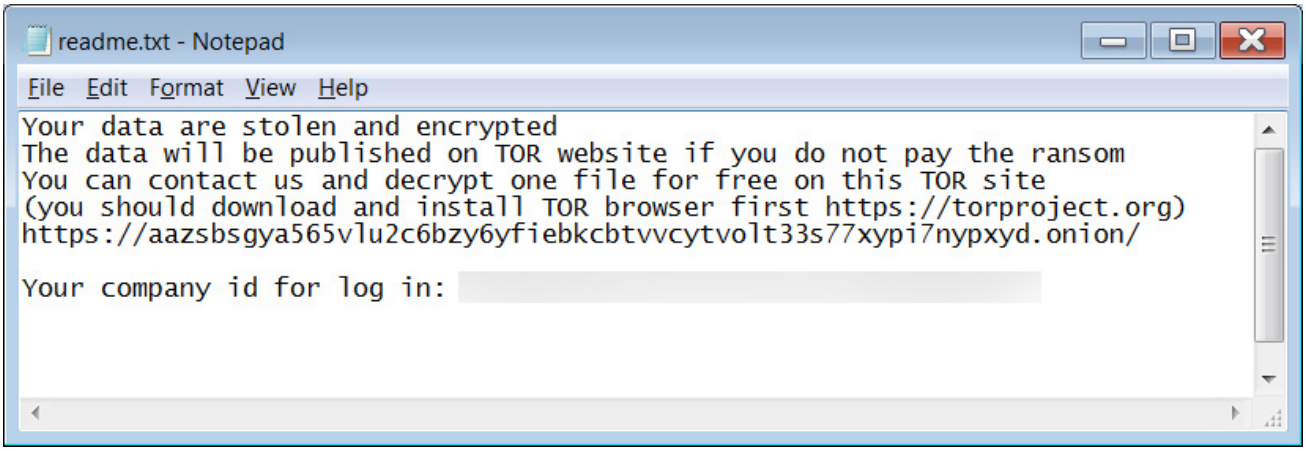
To display the custom icon associated with the .basta extension, the ransomware will create a custom extension in the Windows Registry and associate the icon with a randomly named ICO file in the %Temp% folder. This custom icon is very similar to one used by the icy.tools app.

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.basta]

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.basta\DefaultIcon]
@="C:\\Windows\\TEMP\\fkdjsadasd.ico"

In each folder on the encrypted device, the ransomware will create a **readme.txt** file that contains information about the attack and a link and unique ID required to log in to their negotiation chat session.

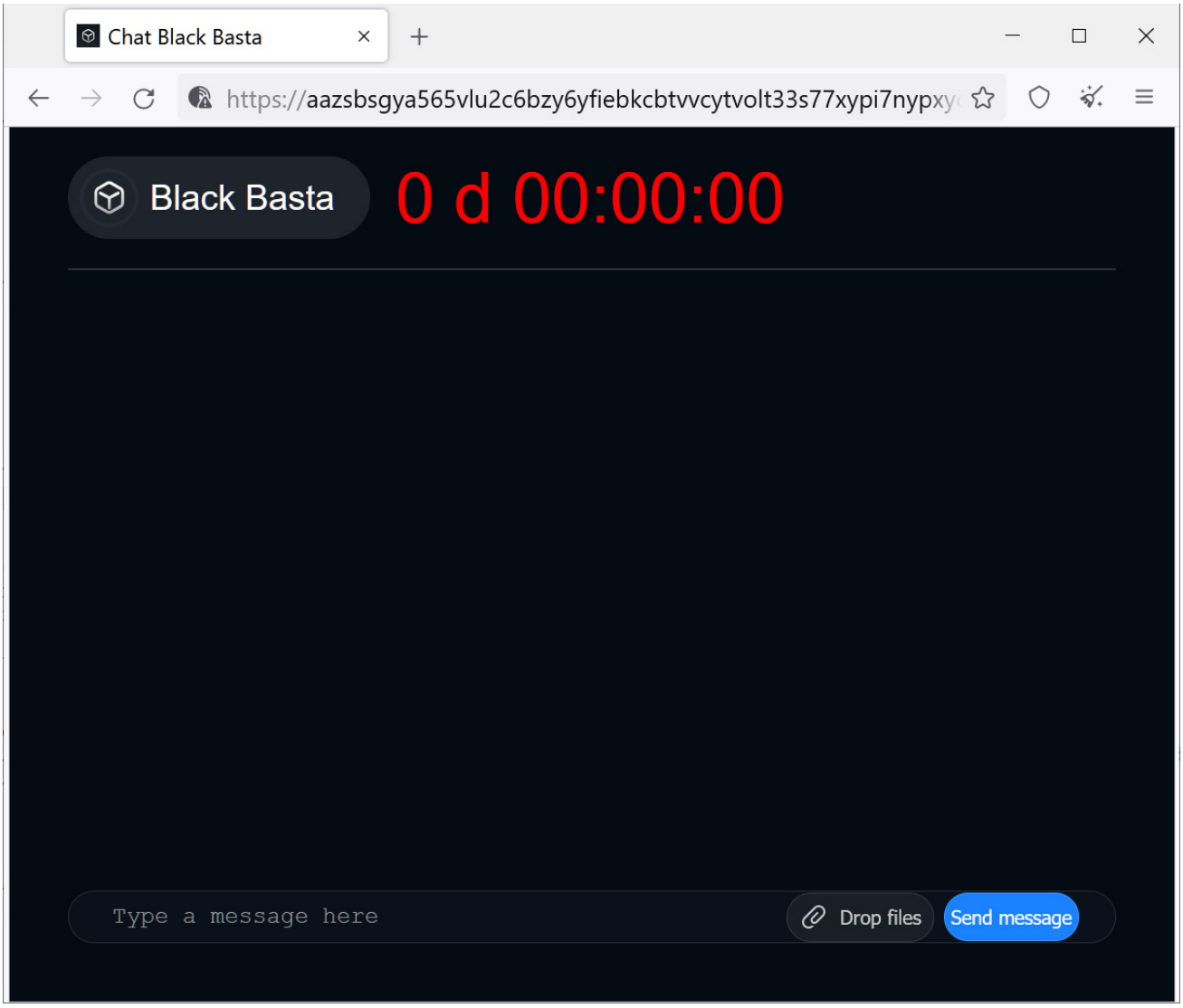


Black Basta Ransom Note

Source: BleepingComputer

The Tor negotiation site is titled 'Chat Black Basta' and only includes a login screen and a web chat that can be used to negotiation with the threat actors.

The threat actors use this screen to issue a welcome message that contains a ransom demand, a threat that data will be leaked if payment is not made in seven days, and the promise of a security report after a ransom is paid.



Black Basta Tor negotiation site

Source: BleepingComputer

Unfortunately, Gillespie says that the encryption algorithm is secure and that there is no way to recover files for free.

A likely rebrand

Based on how quickly Black Basta amassed victims and the style of their negotiations, this is very likely a rebrand of an experienced operation.

One theory discussed between security researcher MalwareHunterTeam and this author is that Black Basta is possibly an upcoming rebrand of the Conti ransomware operation.

Conti has been under heavy scrutiny over the past two months after a Ukrainian researcher leaked a treasure trove of private conversations and the ransomware's source code.

Due to this, it has been speculated that Conti would rebrand their operation to evade law enforcement and start over under a different name.

While the Black Basta encryptor is very different from Conti's, MalwareHunterTeam believes that there are numerous similarities in their negotiation style and website design.

Furthermore, Black Basta released the data for a brand new victim after a screenshot of the negotiation was leaked.

This "punishment" is the same that Conti introduced to stem the tide of negotiations being leaked on Twitter.

While these connections are tenuous, the Black Basta gang needs to be closely monitored as they have only just begun their operation.

Related Articles:

American Dental Association hit by new Black Basta ransomware

The Week in Ransomware - May 13th 2022 - A National Emergency

Costa Rica declares national emergency after Conti ransomware attacks

Conti, REvil, LockBit ransomware bugs exploited to block encryption

The Week in Ransomware - April 29th 2022 - New operations emerge

- Black Basta

- Cyberattack
- Ransomware
- Safe Mode

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

BigPete - 4 weeks ago

-
-

Seems to me like one particular group is really obsessed with the word "black"

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: