

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
  - [Cloud Security](#)
  - [Identity & Access](#)
  - [Data Protection](#)
  - [Network Security](#)
  - [Application Security](#)
- ▼ [Security Strategy](#)
  - [Risk Management](#)
  - [Security Architecture](#)
  - [Disaster Recovery](#)
  - [Training & Certification](#)
  - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Cybercrime](#)



# Black Basta Ransomware Becomes Major Threat in Two Months

By [Kevin Townsend](#) on June 24, 2022

Share

Tweet

推荐 0



Security researchers have assessed the Black Basta ransomware threat level as **HIGH**, and the number of victims is still rising

[Black Basta ransomware](#) has become a major new threat in just a couple months. Evidence suggests it was still in development in February 2022, and only became operational in April 2022. Since then, the Black Basta group has claimed responsibility for 36 victims in English-speaking countries, and the number is growing.

On April 20, 2022, a user named BlackBasta announced on underground forums an intention to purchase [corporate network accesses](#) for a share of the profits. This helps explain its rapid rise. Researchers at Cybereason have reported that it became known in early June that the new Black Basta group has partnered with the [QBot](#) malware operation to spread their ransomware.

A QBot partnership is a well-worn path, with criminal groups including [MegaCortex](#), [ProLock](#), [DoppelPaymer](#), [Conti](#) and [Egregor](#) all having done the same. “QBot has many built-in capabilities that are very useful for attackers,” say Cybereason researchers in a [report](#). “Some of them used to perform reconnaissance, collect data and credentials, move laterally, and download and execute payloads.”

The suggestion is that Black Basta is copying the techniques of the major ransomware gangs. Its rapid rise has led to some speculation that this is not their first time on the dance floor - with some suggestions that the gang might be [related to Conti](#). There are several similarities between the two operations, including the appearance of the leak Tor site, the ransom note, the payment site and behavior of the support team. Conti has denied this, saying, “BlackBasta is not conti it’s... kids.”

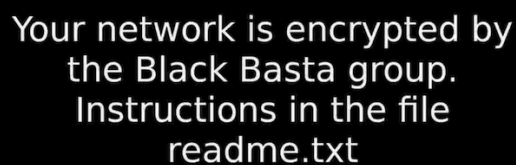
Nevertheless, “Black Basta is likely operated by former members of the defunct Conti and REvil gangs, the two most profitable ransomware gangs in 2021,” comments Lior Div, Cybereason CEO and co-founder.

Like most groups operating targeted attacks, Black Basta employs the double extortion strategy. It’s too early to know how successful it is at gaining ransom payments, but the group has been seen demanding millions of dollars as the ransom fee.

The alliance with QBot saves the group time and effort in its attacks. QBot’s capabilities can be used to perform reconnaissance, collect data and credentials, move laterally, and download and execute payloads. Once inside the network, Black Basta targets the Domain Controller, and moves laterally using *Psexec*. On compromised DCs, it creates a Group Policy Object (GPO) to disable Windows Defender while it also tries to take down any anti-virus products - a technique also used by QBot-Egregor attacks.

The final stage is to deploy the ransomware on targeted endpoints. It does this with an encoded PowerShell command that uses WMI to push the payload to the selected IP addresses. Once executed, the ransomware deletes the virtual shadow copies and other backup files before performing the encryption.

It changes the background image of the desktop to include the message, ‘your network is encrypted by the Black Basta group. Instructions in the file readme.txt’. This is the ransom note, and a copy is dropped into each folder. The ransom note is tailored for each different victim and includes a unique id for the victim to use in the negotiation chat.



Your network is encrypted by  
the Black Basta group.  
Instructions in the file  
readme.txt

In early June 2022, Black Basta added support for encrypting VMware ESXi virtual machines running on enterprise Linux servers. This meshes with ransomware gangs’ big game hunting for targeting enterprises. It also enables faster encryption of multiple servers with a single command. Other gangs doing similar include [LockBit](#), [Hive](#), and Cheerscrypt.

Not much is yet known for certain about Black Basta. The gang has not begun marketing its operation nor recruiting affiliates on hacking forums. If it does start hiring out its code, the threat

will increase rapidly. The Cybereason Nocturnus researchers have already assessed the threat level as **HIGH**, and the number of victims is still rising.

The initial BlackBasta forum post looking to buy corporate accesses was written in Russian, while the accesses sought are for companies in 'the USA, Canada, the UK, Australia, and New Zealand'. The implication, unstated by Cybereason, is that this is likely to be a group with Russian sympathies, or a Russian group trying to make sure it doesn't upset the Russian authorities.

**Related:** [New Black Basta Ransomware Possibly Linked to Conti Group](#)

**Related:** [Access Brokers and Ransomware-as-a-Service Gangs Tighten Relationships](#)

**Related:** [Ransomware, Malware-as-a-Service Dominate Threat Landscape](#)

**Related:** [Beating Ransomware With Advanced Backup and Data Defense Technologies](#)

**Related:** [Ransomware Often Hits Industrial Systems, With Significant Impact: Survey](#)

**Related:** [Doesn't Pay to Pay: Study Finds 80% Percent of Ransomware Victims Attacked Again](#)

Share

Tweet

推荐 0



Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.

Previous Columns by Kevin Townsend:

[Black Basta Ransomware Becomes Major Threat in Two Months](#)

[From Basecamp to Icefall: Secure by Design OT Makes Little Headway](#)

[Do Privacy and Data Protection Regulations Create as Many Problems as They Solve?](#)

[Researchers Discover Way to Attack SharePoint and OneDrive Files With Ransomware](#)

[Koverse Launches Zero Trust Data Platform](#)

[2022 ICS Cyber Security Conference | USA \[Hybrid: Oct. 24-27\]](#)

sponsored links

[2022 Singapore/APAC ICS Cyber Security Conference](#)

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

[2022 CISO Forum: September 13-14 - A Virtual Event](#)

Tags:

[NEWS & INDUSTRY](#)

[Cybercrime](#)

Search

**Get the Daily Briefing**

**BRIEFING**

Business Email Address

Subscribe