



# PROFILE

## Black Basta Ransomware

### ZEROFOX INTELLIGENCE

P-2022-08-16a

Classification: TLP Green

Criticality: Medium

Intelligence Requirements: Deep Dark Web & Criminal Underground

August 16, 2022



## Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 8:00 AM (EDT) on August 10, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

**First Seen: April 2022**

**Origin: Unknown; Russian-speaking**

**Motivation: Financial**

**Targeted Industries: Automotive, Construction, Cosmetics, Finance, Government, Healthcare, Insurance, Manufacturing, Pharmaceuticals, Professional Services, Real Estate, Retail, Telecommunications, Transportation, and Utilities**

## History

Black Basta is a highly-effective ransomware strain used by threat actors to infect and extort victims. Consistent with most ransomware collectives, Black Basta operators exfiltrate sensitive corporate data before encrypting devices and leverage double-extortion tactics, threatening to release the exfiltrated data if ransom demands are not met. The ransomware was identified in mid-April 2022 following the first reported incidents of compromise, though evidence indicates it was in development as early as February 2022.<sup>1</sup> The group also made its presence known on the Russian underground forum Exploit.in in late April; ZeroFox Intelligence observed a user with the name “Black Basta” posting an advertisement that offered to purchase and monetize access to corporate networks for a percentage of profits. According to the announcement, the actor was interested in organizations located in the United States, Canada, the United Kingdom, Australia, and New Zealand.

Since its emergence, researchers have linked Black Basta to Conti ransomware, with intelligence suggesting that the group is likely one of several Conti subdivisions forming part of a measured Conti rebranding.<sup>2</sup> Researchers tracking Black Basta’s activity have indicated that the group—which appeared a month before Conti announced its shutdown—has shown signs of overlap with Conti’s tactics, techniques,

---

<sup>1</sup>

[hXXps://twitter\[.\]com/Arkbird\\_SOLG/status/1519452352763281408?s=20&t=D9hGjGpXFgAVNxxok5S-lw](https://twitter.com/Arkbird_SOLG/status/1519452352763281408?s=20&t=D9hGjGpXFgAVNxxok5S-lw)

<sup>2</sup>

[hXXps://www.advintel\[.\]io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cyber-crime-landscape](https://www.advintel[.]io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cyber-crime-landscape)



and procedures (TTPs), citing similarities between the groups' data leak sites (DLS), payment sites, recovery portals, and negotiation methods.<sup>3</sup> Notably, Conti denied reports linking it to Black Basta in May 2022, though this is to be expected if the group is attempting to hide its affiliations to avoid potential backlash.<sup>4</sup>

ZeroFox Intelligence has identified no evidence directly linking Black Basta to Conti but assesses with moderate confidence that Black Basta likely includes former members of Conti or other previously shuttered groups. ZeroFox Intelligence notes the tendency for ransomware gangs and affiliates to rebrand or restructure to divert attention from authorities or to avoid sanctions. For instance, Darkside—responsible for the Colonial Pipeline attack in May 2021—is considered to have resurfaced as BlackMatter after ceasing its operations due to intense scrutiny from authorities.<sup>5</sup> Likewise, Conti is previously assessed to have succeeded Ryuk ransomware in 2020 and, due to the significant disruption inflicted by the ContiLeaks breach in February 2022, is highly likely to be reshaping the organization again in an attempt to avoid further exposure.

The rate at which Black Basta has accumulated victims and developed its capabilities also indicates the involvement of seasoned ransomware operatives. In the first two months of operating, Black Basta offered its own Ransomware-as-a-Service, partnered with QBot malware, and developed a Linux-based variant to target VMware ESXi virtual machines (VMs) on enterprise servers—putting it on par with groups such as BlackMatter, Hive, and Lockbit. As a result, Black Basta has quickly become one of the most prolific variants. Between April and August 2022, Black Basta accounted for the third-highest number of ransomware incidents among the most notable strains, targeting over 50 organizations globally across multiple industries. ZeroFox Intelligence notes that Black Basta has so far shown a propensity to target organizations within the manufacturing, retail, and construction industries.

---

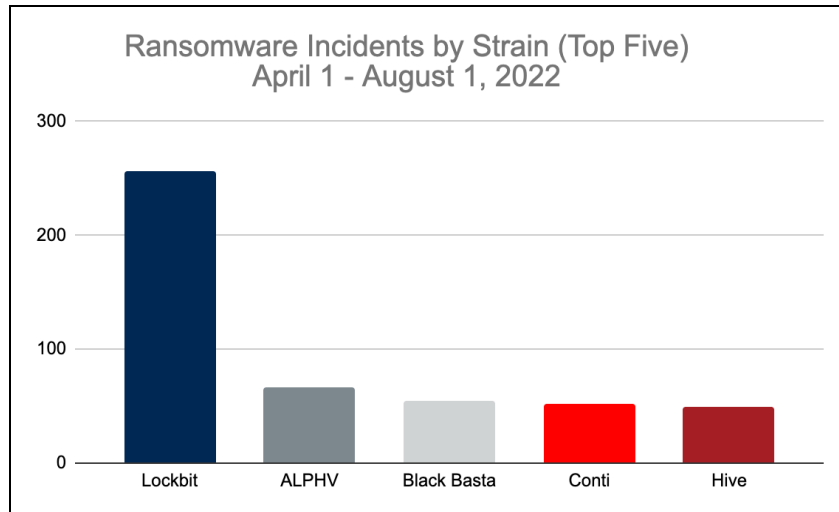
<sup>3</sup>

[hXXps://www.trendmicro\[.\]com/en\\_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html](https://www.trendmicro.com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html)

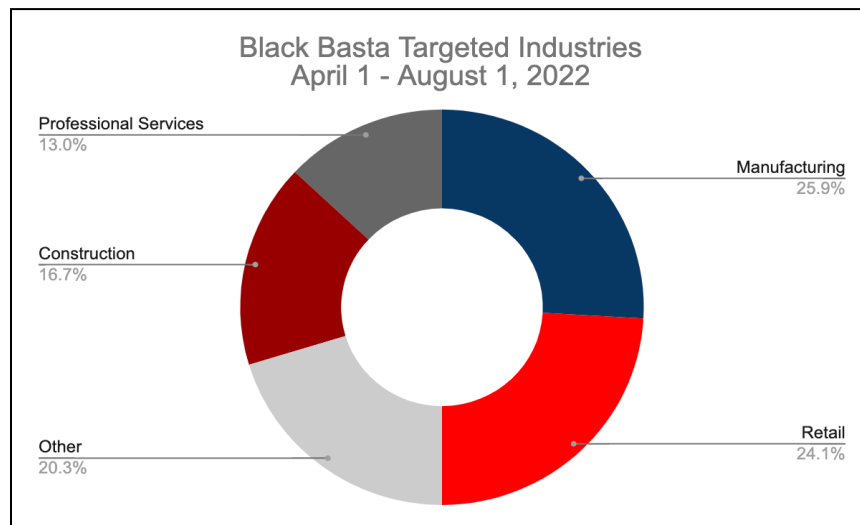
<sup>4</sup> [hXXps://twitter\[.\]com/BrettCallow/status/1524387838531301377/photo/1](https://twitter.com/BrettCallow/status/1524387838531301377/photo/1)

<sup>5</sup>

[hXXps://news.sophos\[.\]com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/](https://news.sophos.com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/)



Source: ZeroFox Intelligence



Source: ZeroFox Intelligence

## Tactics, Techniques, and Procedures

Black Basta operators leverage a variety of intrusion vectors to compromise victims' systems, including phishing, credential stuffing, and Remote Desktop Protocol (RDP) exploitation. The group makes use of initial access brokers selling access to already-compromised victims and has reportedly sought out insiders within organizations to compromise networks.<sup>6</sup> Operators have been observed exploiting the Microsoft PrintNightmare vulnerability after gaining initial access to perform privileged file operations. Black Basta's partnership with QBot also greatly improves

<sup>6</sup> [hXXps://cybernews\[.\]com/security/black-basta-a-new-ransomware-group-or-a-conti-faction/](https://cybernews.com/security/black-basta-a-new-ransomware-group-or-a-conti-faction/)



operators' ability to perform reconnaissance, collect data and credentials, maintain presence and move laterally within compromised systems, and deliver payloads. Notably, Black Basta cannot execute without administrator privileges, meaning operators will either compromise an account with appropriate access or move laterally to escalate privileges.

Upon execution, the ransomware begins removing shadow copies to prevent system recovery, disables Windows recovery and repair, and reboots the system in safe mode. It then proceeds to encrypt files while the device is in safe mode, appending all encrypted files with the .basta extension. Black Basta uses the ChaCha20 algorithm to encrypt files, which uses faster encryption speeds than other well-known algorithms like Advanced Encryption Standard.<sup>7</sup> This is run in tandem with multithreading to make encryption faster, improve ransomware throughput, and evade detection. The ChaCha20 encryption key is then itself encrypted with a public RSA-4096 key, which is included in the executable. Further hastening the encryption process, Black Basta will partially-encrypt files in 64-byte blocks of a file interspaced by 128-bytes; partial encryption is a tactic also leveraged by other ransomware groups, such as BlackMatter and LockBit.

Once encryption is complete, a ransom note called "readme.txt" is dropped into all affected files, along with changes to the desktop wallpaper. The ransom note contains a unique victim ID and a URL to the group's TOR browser site, "Chat Black Basta." This is intended to be used to conduct extortion negotiations with the victim.

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

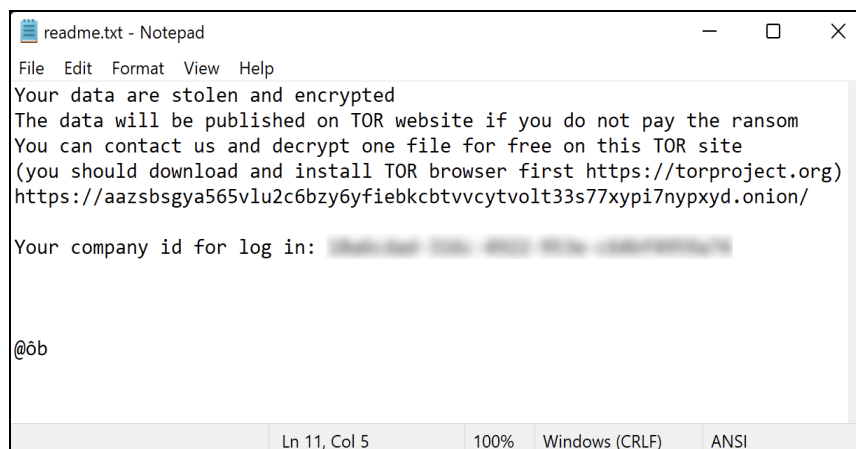
**Desktop wallpaper change upon encryption**

*Source: ZeroFox Intelligence*

---

<sup>7</sup>

[hXXps://nordpass\[.\]com/blog/xchacha20-encryption-vs-aes-256/#:-:text=The%20main%20difference%20between%20AES,XChaCha20%20is%20still%20fairly%20new.](https://nordpass[.]com/blog/xchacha20-encryption-vs-aes-256/#:-:text=The%20main%20difference%20between%20AES,XChaCha20%20is%20still%20fairly%20new.)



### Readme.txt ransom note

Source: [hXXps://twitter\[.\]com/pcrisk/status/1518535862614728705](https://twitter.com/pcrisk/status/1518535862614728705)

## The Knauf Group Attack

June 2022

- In June 2022, The Knauf Group (Knauf), a German-based multinational producer of construction materials, announced that it was the target of a cyberattack that forced its global IT systems to shut down.
- Black Basta later claimed responsibility for the attack via an announcement on its DLS, listing Knauf as a victim on July 16, 2022.
- The intrusion vector is unknown.
- Black Basta immediately released 20 percent of the exfiltrated data, a commonly used tactic by ransomware groups to pressure victims into negotiations.
- Email communications, employee and user credentials, ID scans, and production documents were included in the leaked files.
- It is not known if Knauf engaged with Black Basta, and the ransom demanded has not been disclosed.

## Recommendations

- Regularly back up critical data, including password-protected backup copies kept offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, or the cloud).
- Ensure proper network segmentation.
- Never download email attachments from unknown senders or click links from untrusted sources. Provide user training programs to fight against phishing or social engineering attacks used to obtain critical information that can lead to attacks.



- Enable multi-factor authentication wherever possible.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- Patch disclosed vulnerabilities with updated software versions as quickly as practical.
- Disable PowerShell wherever possible to limit the possibility of operators employing lateral movement modules.

## Indicators of Compromise

### Domain

- aazsbsgya565vlu2c6bzy6yfiebkcbtvvcyvtvolt33s77xypi7nypxyd[.]onion

### MD5

- a70f03beb3a8246595eab83935227914
- 3f400f30415941348af21d515a2fc6a3

### SHA-1

- bd0bf9c987288ca434221d7d81c54a47e913600a

### SHA-256

- eb07a24f63d7f56fb13e34dd60e45a4c8522c32892c8be7dca7d3f742fa86b0a
- f088e6944b2632bb7c93fa3c7ba1707914c05c00f9491e033f78a709d65d7cff
- ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e
- a54fef5fe2af58f5bd75c3af44flfba22b721f34406c5963b19c5376ab278cd1
- 7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770elf0b8a
- 5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa
- 2967e1d97d32605fc5ace49a10828800fbbefcc1e010f6004a9c88ef3ecdad88
- 1d040540c3c2ed8f73e04c578e7fb96d0b47d858bbb67e9b39ec2f4674b04250
- 17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cclld3c274095eb90



## Appendix: Traffic Light Protocol for Information Dissemination

### Red

#### WHEN SHOULD IT BE USED?

##### Sources may use TLP:

**RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

#### HOW MAY IT BE SHARED?

##### Recipients may NOT share TLP:

**RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

### Amber

##### Sources may use TLP:

**AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

##### Recipients may ONLY share TLP:

**AMBER** information with members of their own organization and only as widely as necessary to act on that information.

### Green

#### WHEN SHOULD IT BE USED?

##### Sources may use TLP:

**GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

#### HOW MAY IT BE SHARED?

##### Recipients may share TLP:

**GREEN** information with peers & partner organizations within their sector or community but not via publicly accessible channels.

### White

##### Sources may use TLP:

**WHITE** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

##### Recipients may share TLP:

**WHITE** information without restriction, subject to copy-right controls.