

An In-Depth Look at Black Basta Ransomware

 avertium.com/resources/threat-reports/in-depth-look-at-black-basta-ransomware



Executive Summary

In April 2022, a new ransomware group named Black Basta began targeting several high-value organizations. The ransomware gang has a total of 18 global victims, with the largest number of victims based in the U.S. Black Basta is known for stealing corporate data and documents before encrypting devices. They're also known for their double extortion attacks, which shame victims into paying the demanded ransom or risk having data leaked on a leak site.

Last week, Avertium published a [Threat Intelligence Report](#) discussing the state of ransomware in 2022. Ransomware trends are on the rise and one of those trends is victim shaming – a trend that Black Basta has made use of heavily. As we get ready to dive deeper into the tactics and techniques of Black Basta ransomware, let's remember that even though ransomware is here to stay, there are ways to protect your cyber environment and keep your organization safe from ransomware threat actors like Black Basta.

Black Basta Ransomware

Active since April 2022, Black Basta is both ransomware and a ransomware gang. The gang has been observed targeting organizations in the U.S with a hyper focus on the construction and manufacturing industries. They've also been observed targeting the real estate,

business services, food and beverage, chemicals, insurance, healthcare, and metals and mining industries.

Two of the most recent and well known Black Basta attacks include their attack on the American Dental Association (ADA), as well as their attack on Deutsche Windtechnik.

The ADA is a dentist and oral hygiene advocacy association. The organization had 2.8 GB of data stolen, with 30% of that data leaked on Black Basta's leak site. The attack disrupted some of the organization's email, phone, and chat systems. The ADA had to take their systems offline and worked with third party cyber security specialists to determine the severity of the attack.

The German wind farm operator, Deutsche Windtechnik was attacked in April 2022 and had to shut off their remote data monitoring connections to their wind turbines for about two days as they recovered. Despite the company not confirming if they were hit with a ransomware attack, researchers were able to confirm that they were due to finding the company's name on the leak site of Black Basta.

The attack on Deutsche Windtechnik is just one of several cyber attacks on German energy providers this year. In March 2022, Nordex was forced to shut down their IT systems across several locations due to a cyber attack. Viasat also suffered from a cyber attack this year, causing 5,800 Enercon wind turbines in Germany to malfunction. It has not been confirmed if the ADA or if Deutsche Windtechnik paid a ransom to Black Basta.

techniques and tactics

A deep dive analysis into Black Basta ransomware reveals that the cyber criminals' ransomware appends the extension ".basta" at the end of encrypted files. According to Cyble Research Labs, Black Basta is a console-based executable ransomware that can only be executed with administrator privileges. After the ransomware executes, it deletes shadow copies by using **vssadmin.exe**, removing the Windows backup so their victims can't revert the system to its previous state after encryption.

After removing the backups, Black Basta drops two image files into the temp folder of the infected system. Next, the ransomware changes the desktop wallpaper using the API **systemparametersinfoW()** and uses a file called **dlaksjdoiwq.jpg** as the desktop background wallpaper. Once Black Basta creates the registry entry, it hijacks the FAX service, checking to see if the service name FAX is present in the system. Once it verifies that it's present, Black Basta deletes the original, creating a new malicious service named FAX.

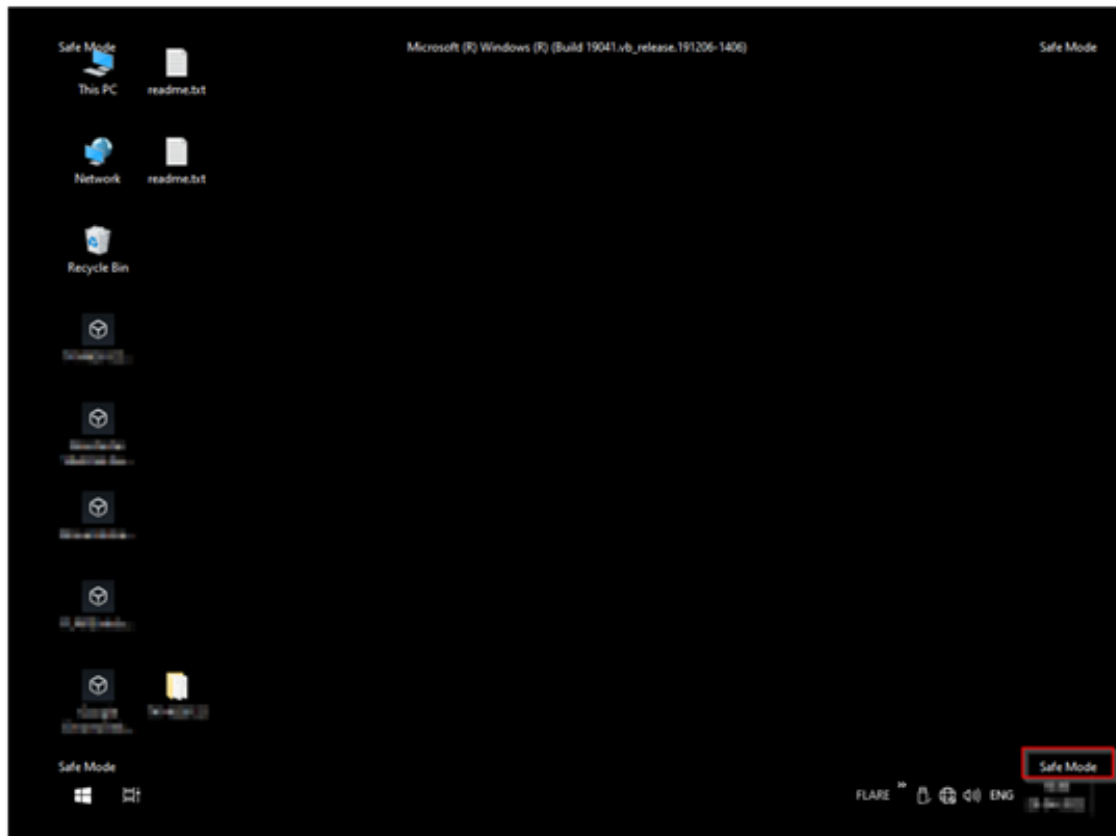
Next, the boot options are checked using **GetSystemMetrics()** API, while **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Fax** is added in the registry to start the FAX service in safe mode. After the ransomware reboots the

system using the **ShellExecuteA()** API, FAX service launches and begins encryption. According to *Cyble Research Labs*, the following list of files and folders are excluded from encryption:

- Bin
- Windows
- Local Settings
- Application Data
- txt
- boot
- txt
- jpg
- DAT
- ico

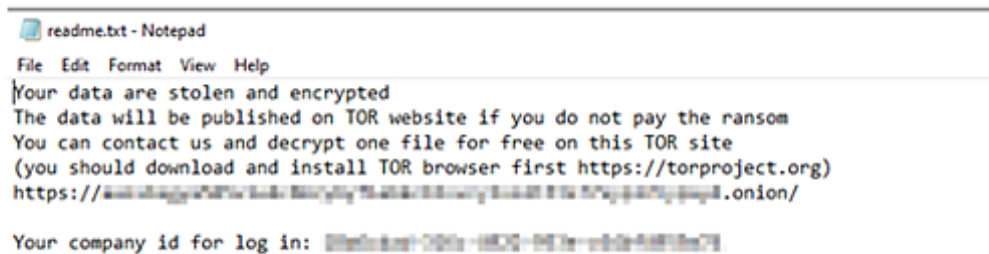
Using **FindFirstFileW()** and **FindNextFileW()** APIs to find files, Black Basta finds the files in their victim's machines and encrypts them – using a multithreading approach for faster encryption.

Image 1: Infection System in Safe Mode



Source: *Cyble Research Labs*

Image 2: Ransom Note by Black Basta



```
readme.txt - Notepad
File Edit Format View Help
Your data are stolen and encrypted
The data will be published on TOR website if you do not pay the ransom
You can contact us and decrypt one file for free on this TOR site
(you should download and install TOR browser first https://torproject.org)
https://[redacted].onion/
Your company id for log in: [redacted]
```

Source: *Cyble Research Lab*

Researchers believe that Black Basta hasn't started recruiting affiliates in underground forums, but their previous advertisements they posted before their attacks suggest they use stolen credentials (purchased on the dark net) to get into organization's systems.

connections to conti

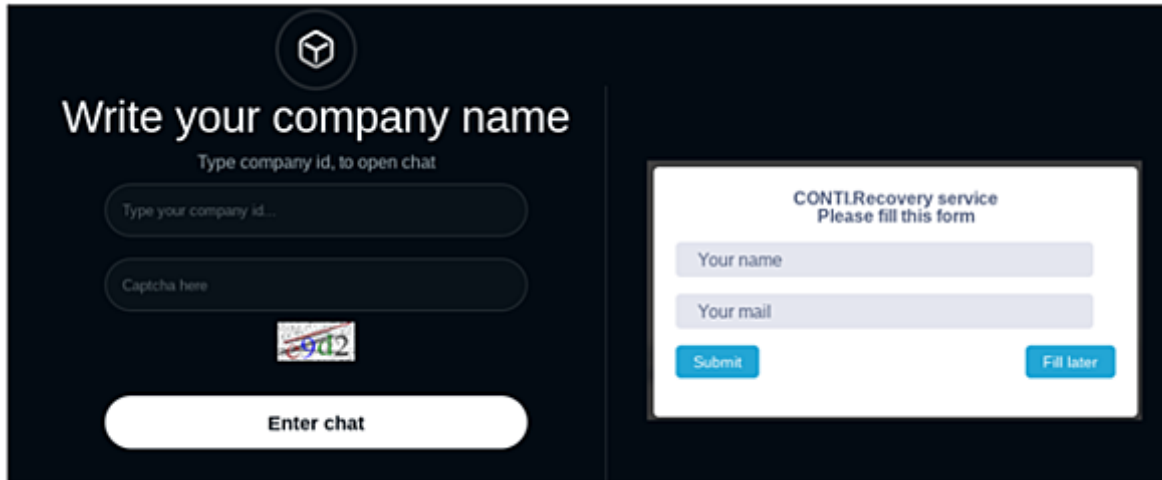
The threat actors behind Black Basta were suspected to be a rebrand of the ransomware gang, Conti. In a previous [Threat Intelligence Report](#) we explained that Conti is a Russian-speaking RaaS organization, who uses RaaS to deploy disruptive ransomware attacks that target critical infrastructure, like hospitals and government organizations. Conti generally focuses on attacking companies with more than \$100 million in annual revenue. They specialize in double extortion operations of simultaneous data encryption and data exfiltration for financial gain. If the ransom is not paid, Conti will blackmail their victims by threatening to publish stolen files.

In May 2021, the FBI notified the public stating that Conti tried to breach over a dozen healthcare and first responder organizations. By September 2021, the gang successfully stole the data of several healthcare organizations. In March 2022, we published another [Threat Intelligence Report](#) featuring the gang. This time, we discussed Conti's leaked internal chats, published on Twitter by a Ukrainian security researcher in February 2022. The leak contained several years' worth of internal chat logs linked to Conti and can be read [here](#).

Because of the leaked chats and Conti's leaked source code, there was speculation that Conti's successful ransomware operation was soon to be dismantled, but researchers found that not to be the case. In fact, it appears as if Conti has simply started to rebrand and strategize despite the leaked chats.

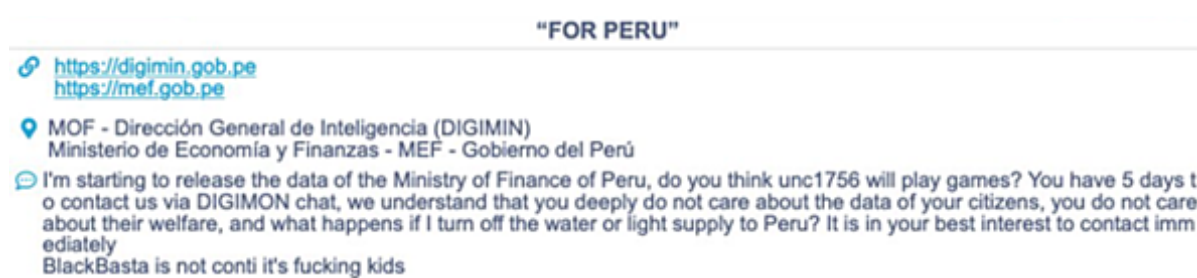
When Black Basta hit the scene in April 2022, researchers stated that the ransomware gang shared similarities with Conti. For example, Black Basta's data leak site was very similar to Conti's data leak site. The gangs also shared the same victim recovery portals. However, Conti denied that they rebranded as Black Basta and called the group "kids".

Image 3: Black Bata and Conti's Recovery Portals



Source: Cyble Research Lab

Image 4: Conti's Message



Source: Twitter.com/BrettCallow

Despite this declaration, researchers still held the belief that Conti rebranded as Black Basta. When Black Basta was discovered and the similarities between the two groups were pointed out, there was speculation that Black Basta could have been a faction of Conti that went rogue, and Conti was not telling the truth. When Conti's chats were leaked, we not only learned how the ransomware gang operated, but we also learned how some Conti employees truly felt about attacking certain critical industries, such as healthcare.

In October of 2020, Conti's members had plans to attack 400 hospitals in the U.S and in Britain. The attacks were launched during the height of the COVID-19 pandemic, when hospitals needed their computers the most. Additionally, Conti ultimately had access to over 400 healthcare facilities (not specifically hospitals). In May 2021, Conti attacked Ireland's Health Service Executive (HSE) that operates the country's public health system. It ended up disrupting the public health system and the recovery costs were expected to exceed \$600 million.

The attack on HSE led to questions from some Conti members because the members were under the assumption that the group didn't attack public resources like hospitals. Some of Conti's managers adhered to this policy, and in June 2021, a manager named "Reshaev" told another user named "Pin" that he wouldn't attack a target he infiltrated because of this policy. "Pin" countered "Reshaev" and said that the network belonged to a sports clinic. "Reshaev" replied that they don't touch the healthcare sector at all, therefore they would be avoiding the clinic.

However, the ban wasn't upheld across the entire Conti organization because in October 2021, "Reshaev" asked someone named "Stern" (the most senior Conti manager) if he approved of a ransomware attack against a hospital by an affiliate called "Dollar". However, there was no reply, so the question was asked again.

Reshaev: "Did you give the green light to the hospital lock to Dollar?"

Stern: "I usually don't approve locks," replied Stern. "Dollar" was later sent an encrypted note.

"Dollar" responded with a series of numbers and sums apparently calculating a 20 percent share of something. In the case above, you can see how it's possible for a former Conti employee to branch off and start their own ransomware gang due to differing opinions. However, Cyberint Research, dug a little deeper and found that a ransomware sample from February 2022, generated a ransomware note from a group named "no_name_software". The group took responsibility for Black Basta ransomware, and the Onion page disclosed in the ransom note was the same Onion page Black Basta currently operates.

CONTI REBRANDING INTO SMALLER GROUPS

Conti may not be associated with Black Basta, but that doesn't mean they aren't trying to rebrand at all. According to our partners, AdvIntel, Conti is currently rebranding as multiple ransomware groups and that the brand, not the organization, is shutting down. On May 19, 2022, Conti's official website went offline, as well as their negotiations service site. Conti's infrastructure (chat rooms, servers, proxy hosts, etc.) went through a massive reset.

The publicity function of Conti's blog is still active, but the operational function of "Conti News" (used to upload new data to force victims to pay) is defunct – including infrastructure related to data uploads, negotiations, and the hosting of stolen data. AdvIntel believes that Conti can no longer support and obtain extortion and that the shutdown was not spontaneous but calculated. May 19, 2022 is Conti's official date of death with their attack on Costa Rica being their final dance.

The attack on Costa Rica, which forced the country to declare a state of emergency, was Conti's way of keeping the illusion that they were still active and diverting everyone's attention, while working on their restructuring. During the diversion tactics, Conti's extension

groups such as [BlackByte](#) and [KaraKurt](#) were actively and silently attacking organizations. Additionally, infiltration specialists who were the backbone of Conti, were forming alliances with [BlackCat](#), [AvosLocker](#), [HIVE](#), and [HelloKitty/FiveHands](#).

There is no evidence that suggests that Conti's leaked chats have an impact on their recent activities, but perhaps the event that provoked the leak (Conti's support of Russia) in the first place may have played a part in their demise. By engaging in political discourse, Conti intervened in Russian state matters, and opened themselves up for scrutiny and attacks from hackers like Anonymous and [NB65](#).

g shorter. This happened with Microsoft Exchange Server Vulnerabilities (CVE-2021-26855 and CVE-2021-27065).

Stay Vigilant

As we stated in our previous Threat Intelligence Report featuring AvosLocker ransomware, ransomware trends are on the rise and ambitious threat actors like Black Basta are in it for the long haul. Black Basta's recent attacks prove that they are not only consistent but persistent. Conti even addressed them in their blog when there was speculation surrounding a connection to the gang. This acknowledgement could be an indicator of Black Basta's talent, as well as their gaining popularity. It's important for organizations to remain vigilant in implementing [cyber security best practices](#) and to keep a watchful eye on threat actors on the rise.

How Avertium is Protecting Our CUSTOMERS

Sometimes anti-malware solutions just aren't enough. Ransomware like Black Basta is a great risk to organizations, especially when they are persistent and attack critical industries like healthcare and manufacturing. However, despite Black Basta's success with attacking these industries, Avertium had advanced services that can help your organization remain safe and proactive:

- Avertium recommends utilizing our service for [DFIR](#) (Digital Forensics and Incident Response) to help you rapidly assess, contain, eradicate, and recover from a security incident like a malware attack.

- Implement XDR as a prevention method. Our XDR is a combination of monitoring software like LogRhythm, Microsoft Azure Sentinel, or AlienVault, combined with endpoint protection such as SentinelOne. XDR platforms enable cybersecurity through a technology focus by collecting, correlating, and analyzing event data from any source on the network. This includes endpoints, applications, network devices, and user interactions.
- MDR provides an in-depth investigation into potential threats on an organization's network. Avertium's risk-based approach to managed security delivers the right combination of technology, field-validated threat intelligence, and resource empowerment to reduce complexity, streamline operations, and enhance cybersecurity resilience. If you need a more advanced security solution, MDR is the next step. MDR is an outsourced security control solution that includes the elements of EDR, enhanced with a range of fundamental security processes.
- Avertium offers Zero Trust Architecture, like AppGate, to stop malware lateral movement.

Avertium's Recommendations

- Regularly back up data, air gap, and password-protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- DLP (Data Loss Prevention) solutions should be implemented on all employee systems.
- Block URLs that may spread malware
- Don't open untrusted links and email attachments without verifying their authenticity.
- Use strong passwords and multi-factor authentication.

- Use antivirus and internet security software on your devices.
- Monitor the beacon networks to block data exfiltration malware or TAs.
- Educate employees on threats like phishing.

MITRE Map

Execution	Defense Evasion	Discovery	Impact
T1059: Command and Scripting Interpreter	T1112: Modify Registry	T1082: System Information Discovery	T1490: Inhibit System Recovery
	T1027: Obfuscated Files or Information	T1083: File and Directory Discovery	T1489: Service Stop
	T1562.001: Impair Defenses: Disable or Modify Tools		T1486: Data Encrypted for Impact

Indicators of Compromise (IoCs)

- 3f400f30415941348af21d515a2fc6a3bd0bf9c987288ca434221d7d81c54a47e913600a
- 5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa

SUPPORTING DOCUMENTATION

[AdvIntel: Conti rebranding as several new ransomware groups \(techtarget.com\)](https://www.techtarget.com)

[New Black Basta Ransomware Possibly Linked to Conti Group | SecurityWeek.Com](https://www.securityweek.com)

[Hydra with Three Heads: BlackByte & The Future of Ransomware Subsidiary Groups \(advintel.io\)](https://www.advintel.io)

[German wind farm operator confirms cybersecurity incident - The Record by Recorded Future](#)

[American Dental Association hit by new Black Basta ransomware \(bleepingcomputer.com\)](#)

[DisCONTInued: The End of Conti's Brand Marks New Chapter For Cybercrime Landscape \(advintel.io\)](#)

[New Black Basta ransomware springs into action with a dozen breaches \(bleepingcomputer.com\)](#)

[Inside the Conti leaks rattling the cybercrime underground | README_](#)

[Understanding Cybersecurity Best Practices \(avertium.com\)](#)

[American Dental Association confirms cyberattack after ransomware group claims credit - The Record by Recorded Future](#)

<https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/>

[New Black Basta Ransomware Group - Cyberint](#)

[Cyble — Black Basta Ransomware](#)

[Examining the Black Basta Ransomware's Infection Routine \(trendmicro.com\)](#)

[Beware of new Black Basta ransomware! Here is what damage it can cause | Tech News \(hindustantimes.com\)](#)

[Inside Conti leaks: The Panama Papers of ransomware - The Record by Recorded Future](#)

APPENDIX II: Disclaimer

This document and its contents do not constitute, and are not a substitute for, legal advice. The outcome of a Security Risk Assessment should be utilized to ensure that diligent measures are taken to lower the risk of potential weaknesses be exploited to compromise data.

Although the Services and this report may provide data that Client can use in its compliance efforts, Client (not Avertium) is ultimately responsible for assessing and meeting Client's own compliance responsibilities. This report does not constitute a guarantee or assurance of Client's compliance with any law, regulation or standard.

COPYRIGHT: Copyright © Avertium, LLC and/or Avertium Tennessee, Inc. | All rights reserved.

Related Resource: [An In-Depth Look at Conti's Leaked Log Chats](#)