Black Basta Ransomware

Published: 2022-05-06 · Archived: 2026-04-05 23:09:06 UTC

New ransomware variant targeting high-value organizations

A new ransomware group has emerged and has been highly active since April 2022, targeting multiple high-value organizations. Among other notable attacks, the Black Basta gang is also responsible for a data leak targeting a popular Dental Association. The gang extracted around 2.8 GB of data in this attack.

The ransomware appends extension .basta at the end of encrypted files. Cyble Research Labs identified a total of 18 global victims of the Black Basta ransomware, with the largest number of victims based in the US. The following image shows the victims based on country.

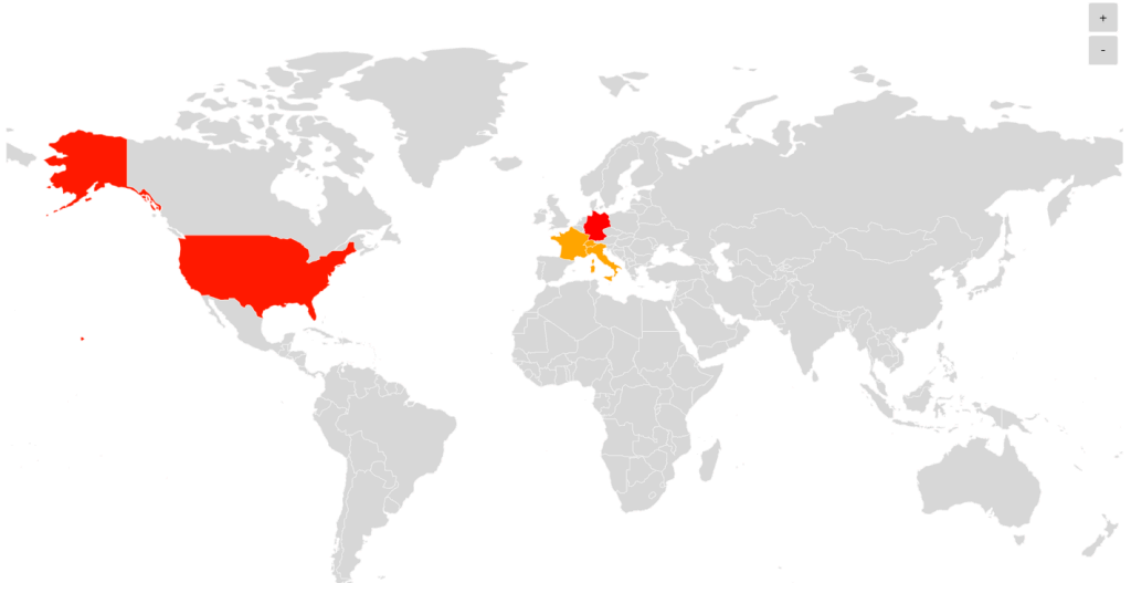

Figure 1 – Regions Targeted by the Black Basta Ransomware

We have prepared a breakdown of the industries targeted by the Black Basta ransomware in the figure below. As we can see, the ransomware gang primarily targets the construction and manufacturing industries.

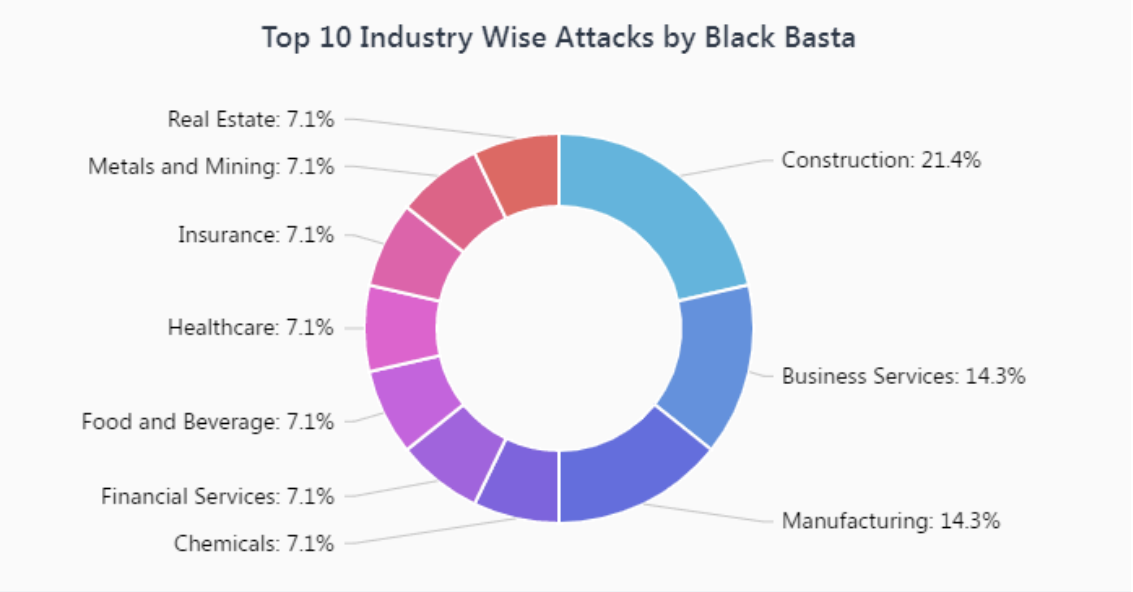

Figure 2 – Industries Targeted by the Black Basta Ransomware

The ransomware is a console-based executable and can only be executed with administrator privileges. The static file information of the Black Basta ransomware is shown below.

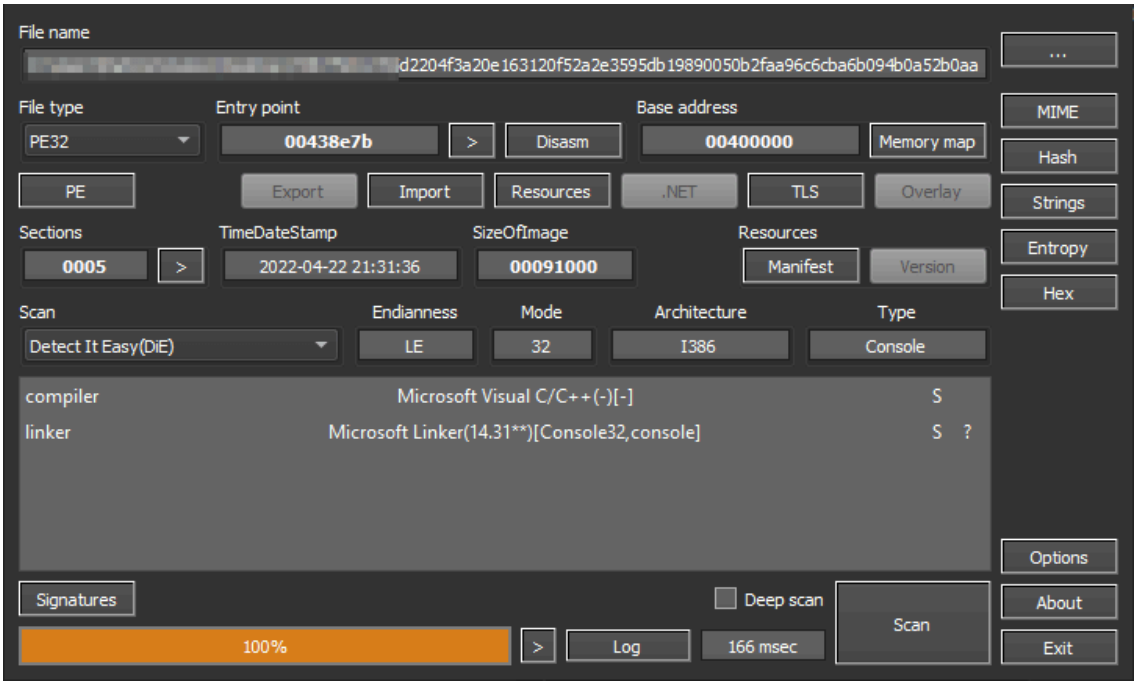

Figure 3 – Static File Information of Ransomware Executable

After execution, the ransomware deletes shadow copies from the infected system using *vssadmin.exe*. This action removes the Windows backup so that after encryption victim cannot revert the system to its previous state. The figure below shows the command in the ransomware binary.

```
v30 = &v20;
*(_DWORD *)pIdentifierAuthority.Value = 0;
*(_WORD *)&pIdentifierAuthority.Value[4] = 256;
AllocateAndInitializeSid(&pIdentifierAuthority, 1u, 0, 0, 0, 0, 0, 0, 0, 0, &pSid);
dword_489278 = GetCurrentProcessId();
FreeConsole();
sub_43DC04("C:\\Windows\\SysNative\\vssadmin.exe delete shadows /all /quiet");
sub_43DC04("C:\\Windows\\System32\\vssadmin.exe delete shadows /all /quiet");
v27 = 4;
strcpy((char *)lpMem, "AQAB");
v31 = 0;
v0 = sub_421320(v23, lpMem, 0);
LOBYTE(v31) = 1;
if ( (__int128 *)v0 != &xmmword_48721C )
```

Figure 4 – Ransomware Deleting Shadow Files

Then ransomware drops two image files into the temp folder of the infected system, as shown in the figure below.

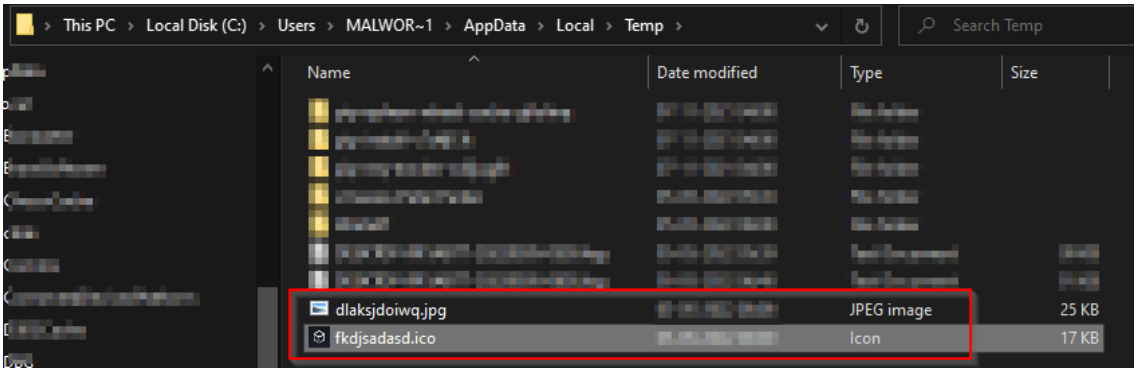

Figure 5 – Ransomware Dropping Two Files

The ransomware then changes the desktop background wallpaper using the API *systemparametersinfoW()*. The file ‘dlaksjdoiwq.jpg’ is used as the desktop background wallpaper by the ransomware.

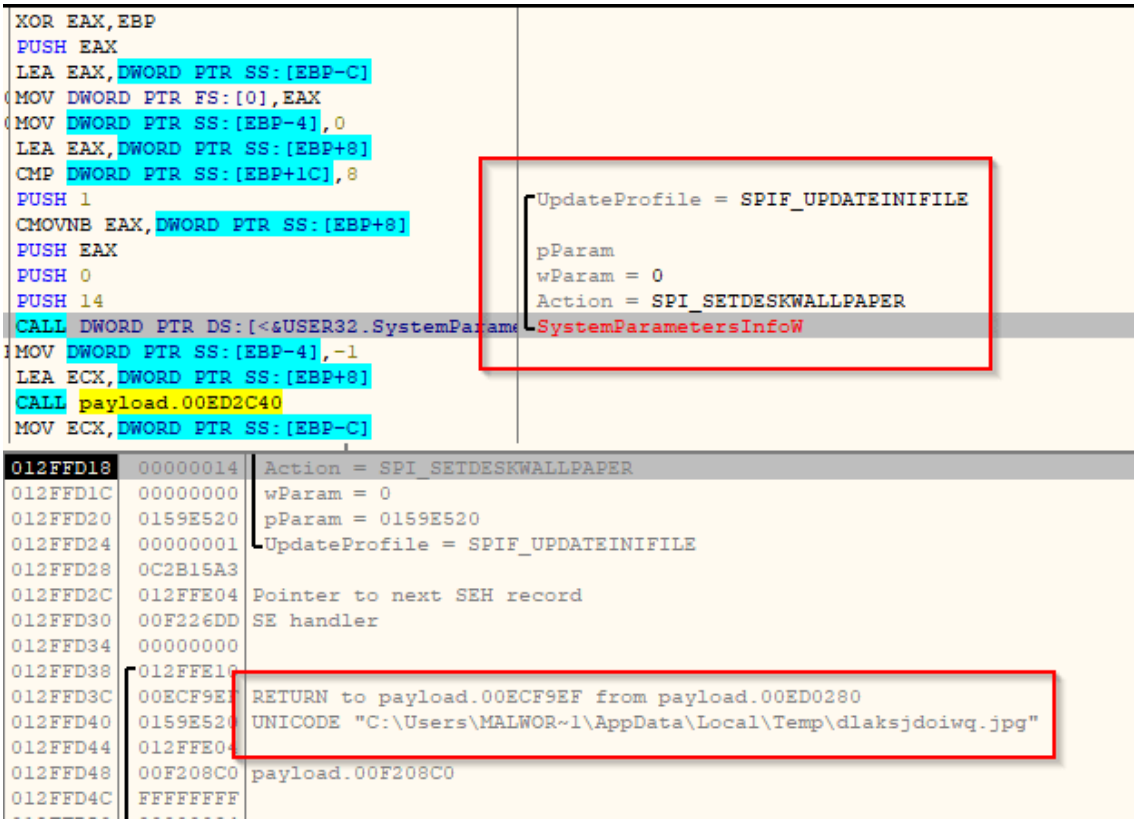

Figure 6 – Ransomware Changing Desktop Wallpaper

The second file, '*fkdjsadasd.ico,*' is used as a file icon for encrypted files with a .basta extension. Black Basta Ransomware achieves this by creating a registry key, as shown below.

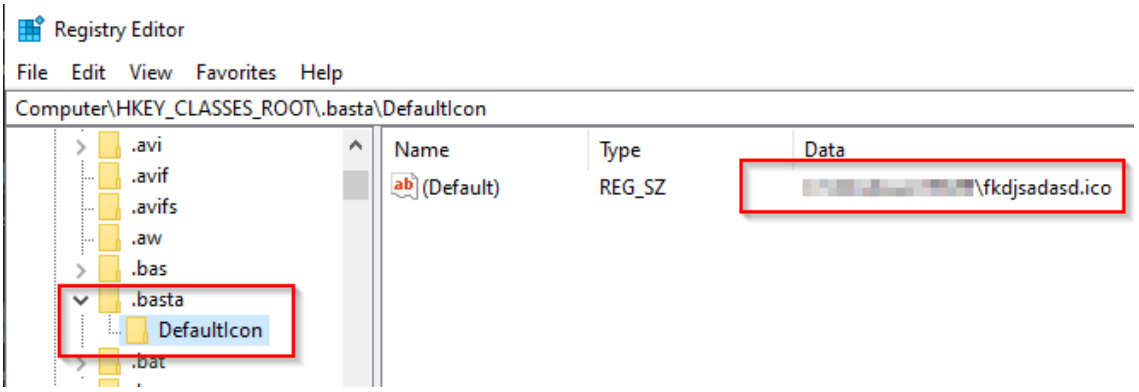

Figure 7 – Registry Entry for File Icon of Encrypted Files

After creating the registry entry, the ransomware hijacks the FAX service. It initially checks whether the service name FAX is present in the system. If present, it deletes the original and creates a new malicious service named 'FAX.' The figure below shows the code snippets for the service hijack.

Figure 8 – Ransomware Changing FAX Service

The screenshot below compares the malicious and genuine Windows FAX services.

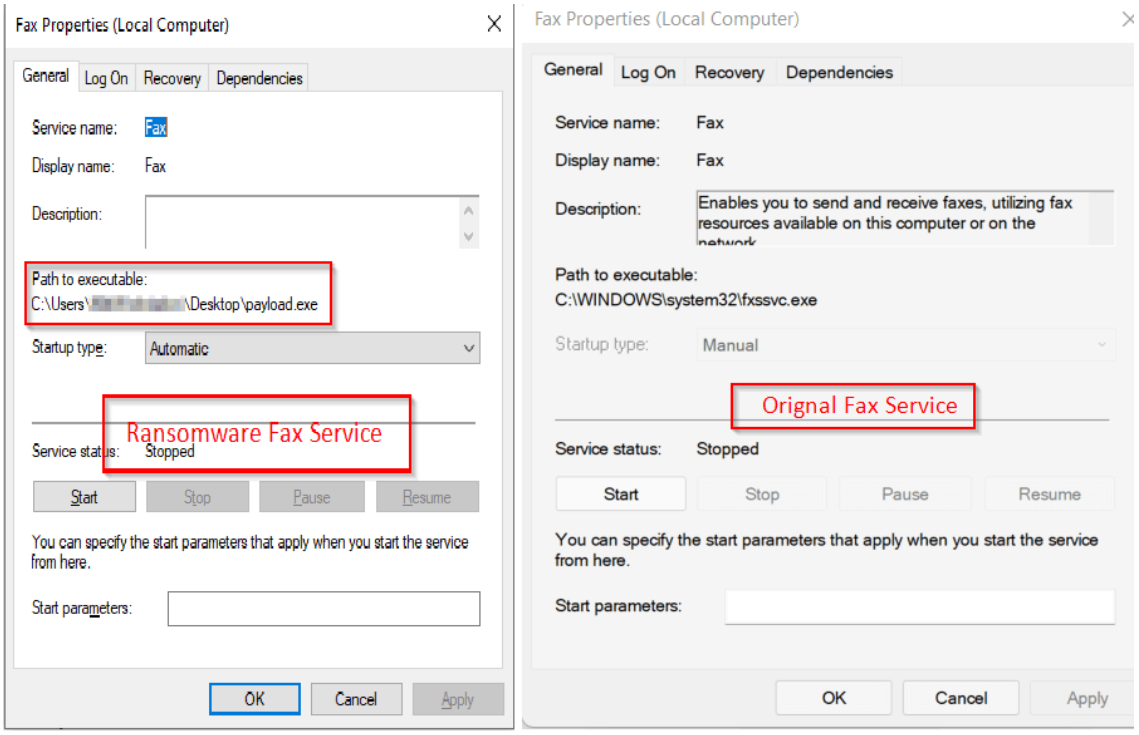

Figure 9 – Malicious vs. Genuine Fax Service Properties

The ransomware then checks the boot options using *GetSystemMetrics()* API and then adds *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Fax* entry in the registry to start the FAX service in safe mode. After completing all the customizations, the ransomware sets up the operating system to boot in safe mode using *bcedit.exe*, as shown in the figure below.

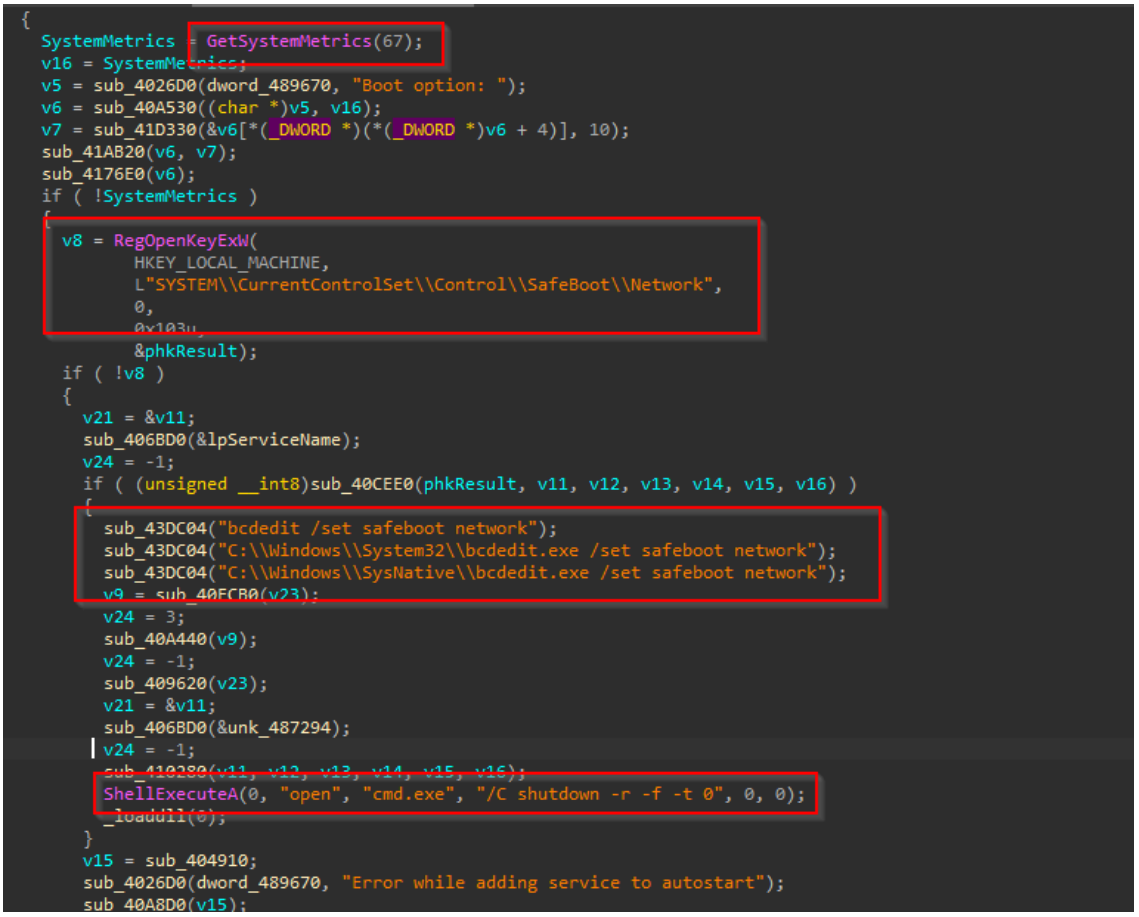

Figure 10 – Safe Boot Operation Performed by the Ransomware

After performing system changes, the ransomware reboots the system using the *ShellExecuteA()* API, as shown in Figure 9.

After rebooting, the FAX service launches and then initiates encryption and other ransomware processes.

The ransomware finds system volumes for file encryption using *FindFirstVolumeW()* and *FindNextVolumeW()* APIs and drops a readme.txt in any directories that it encounters. The figure below shows the APIs.

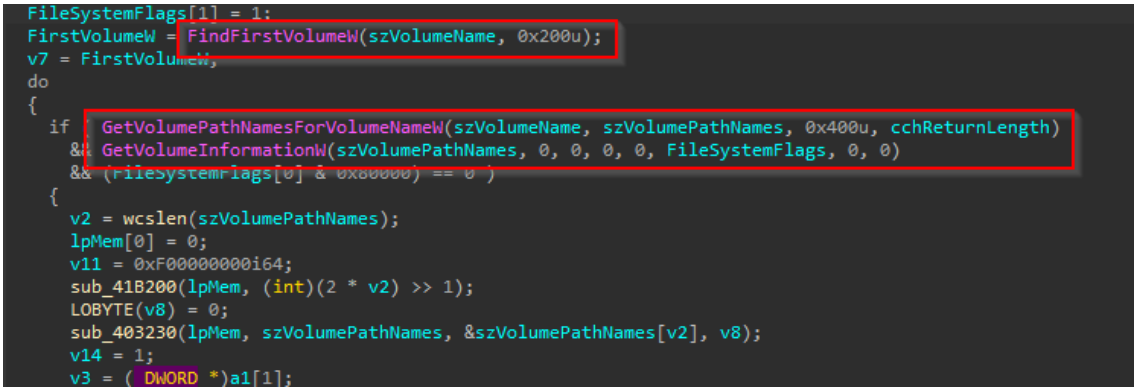

Figure 11 – Ransomware Finding Volume Information

The ransomware excludes the following list of files and folders from the encryption:

- Recycle.Bin

- Windows
- Local Settings
- Application Data
- OUT.txt
- boot
- readme.txt
- dlaksjdoiwq.jpg
- NTUSER.DAT
- fkdjsadasd.ico

Finally, the ransomware finds the files in the victims' machine using the *FindFirstFileW*() and *FindNextFileW()* APIs and encrypts them. The ransomware uses a multithreading approach for faster file encryption.

The figure below shows the infected system in safe mode and the encrypted files.

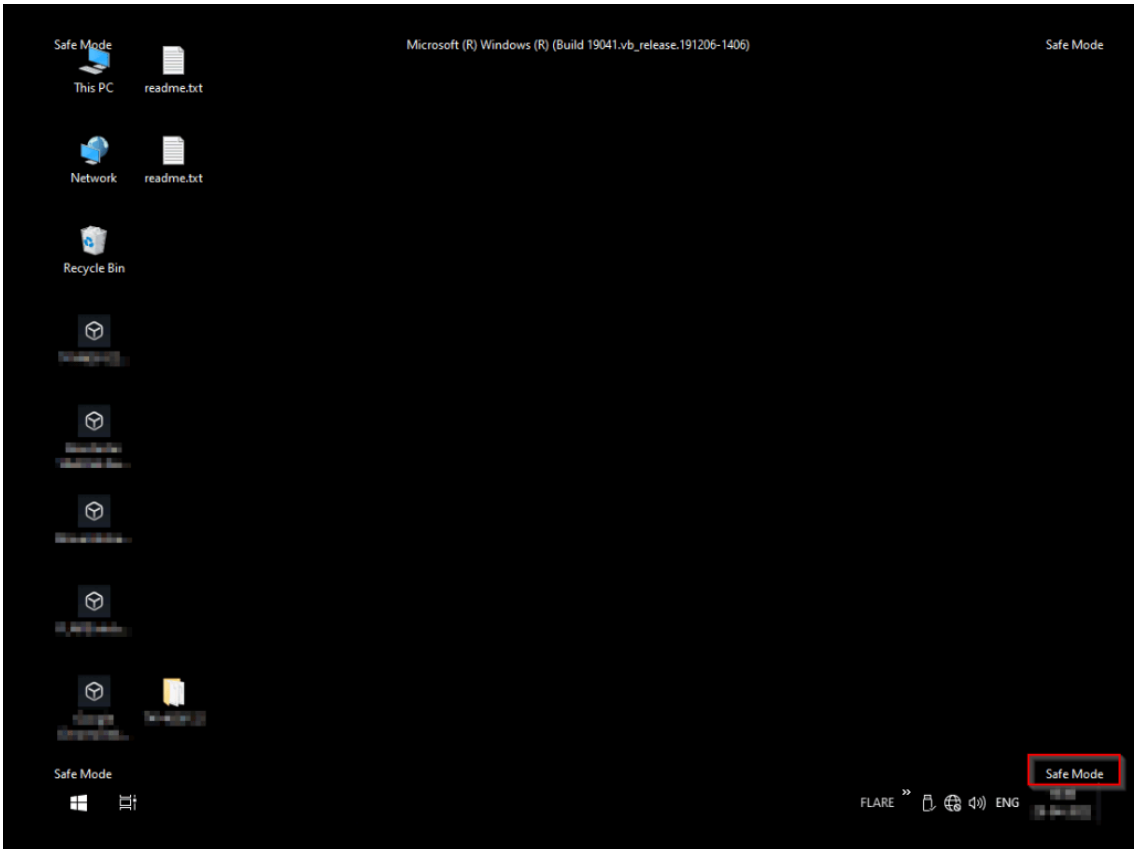

Figure 12 – Infected System Started with Safe Mode

The following image shows the screenshot of the ransom note dropped by the ransomware.

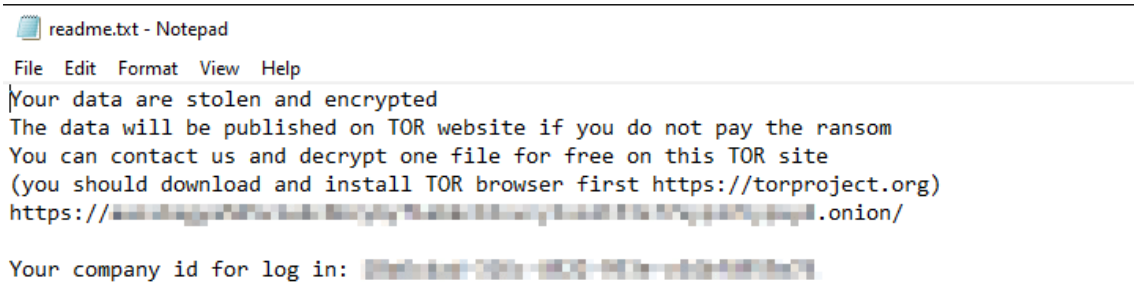

Figure 13 – Ransom note Dropped by the Black Basta Ransomware

After completing these operations, the ransomware reboots in normal mode, as shown in the figure below.

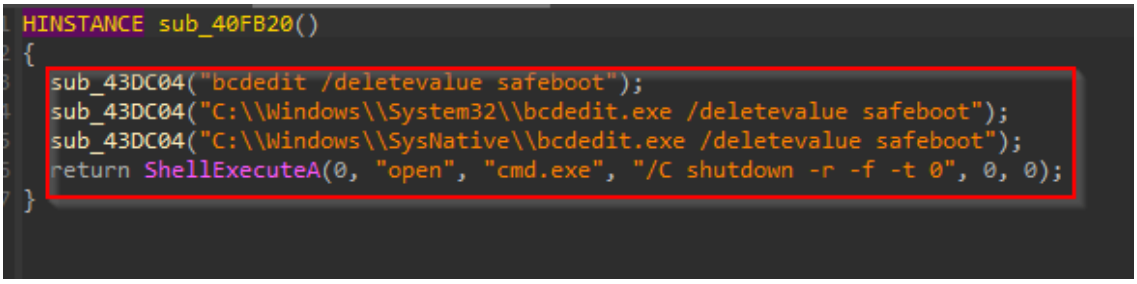

Figure 14 – Ransomware Restarting in Normal Mode

Possible Re-brand of Conti Ransomware:

The Threat Actors behind the ransomware share similarities with the Conti ransomware gang. Researchers attribute the Black Basta ransomware to the TA behind Conti Ransomware based on the victim data leak site. The below image shows the leak site of the Conti ransomware gang.

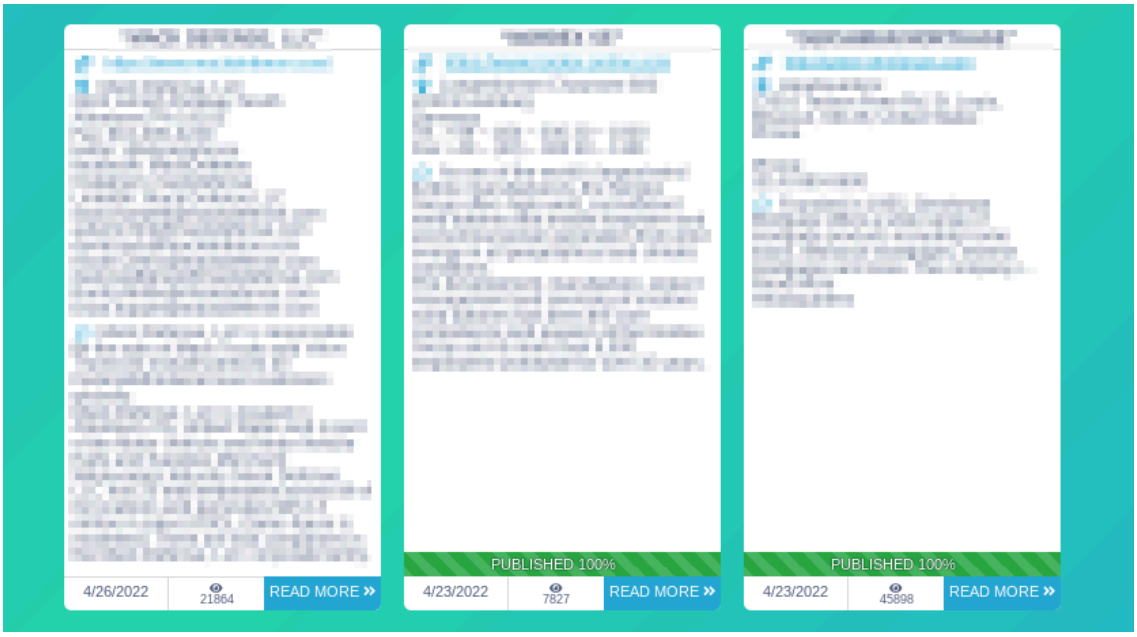

Figure 15 – Conti Data Leak Blog Post

Black Basta ransomware data leak site.

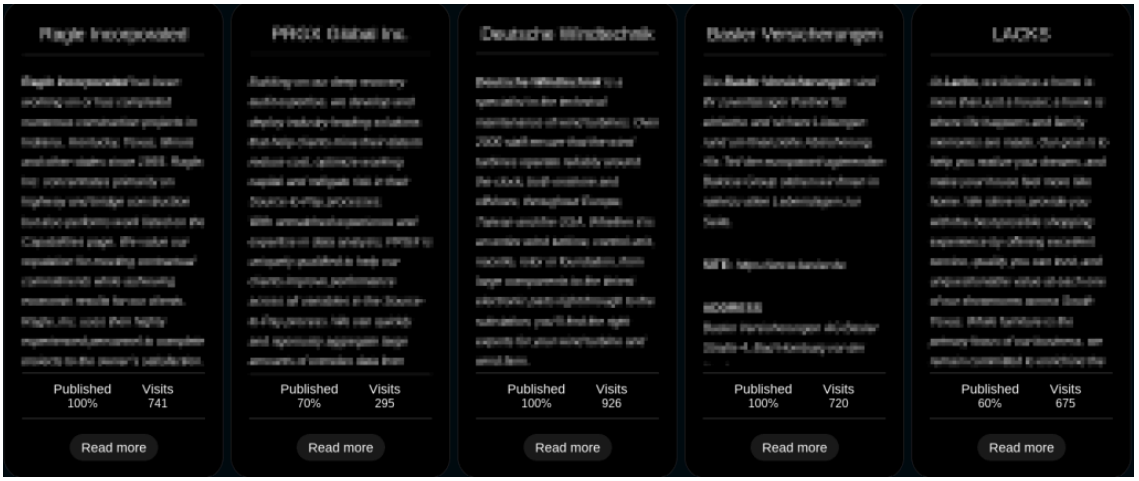

Figure 16 – Black Basta Data Leak Blog Post

Additionally, Conti and Black Basta ransomware have the same victim recovery portals as well, as shown below.

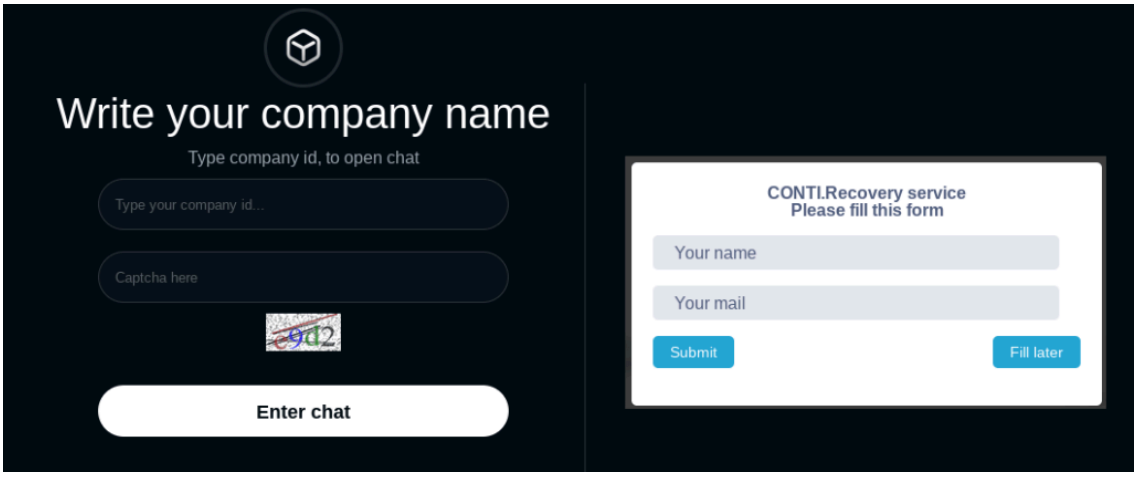

Figure 17 – Recovery Pages for Black Basta and Conti Ransomware Gangs

Conclusion:

With law enforcement agencies worldwide actively targeting ransomware gangs, ransomware gang operators are also evolving their TTPs to target new organizations. The Black Basta ransomware has multiple similarities with the Conti ransomware group, indicating a possible connection between the Threat Actors.

Organizations and individuals should thus continue to follow industry best cybersecurity practices to secure themselves and their firms.

Our Recommendations:

- Use strong passwords and enforce multi-factor authentication wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices.
- Use a reputed antivirus and internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without first verifying their authenticity.

- Educate employees in terms of protecting themselves from threats like phishing's/untrusted URLs.
- Block URLs that could spread the malware, e.g., Torrent/Warez.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.
- Enable Data Loss Prevention (DLP) Solutions on the employees' systems.

MITRE ATT&CK® Techniques

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

Indicators of Compromise (IoCs):

Indicators	Indicator type	Description
3f400f30415941348af21d515a2fc6a3 bd0bf9c987288ca434221d7d81c54a47e913600a 5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa	**Md5 SHA-1 SHA-256**	**eyqvn14ce.dll (Ransomware executable)**

Source: https://web.archive.org/web/20220506143054/https://blog.cyble.com/2022/05/06/black-basta-ransomware/