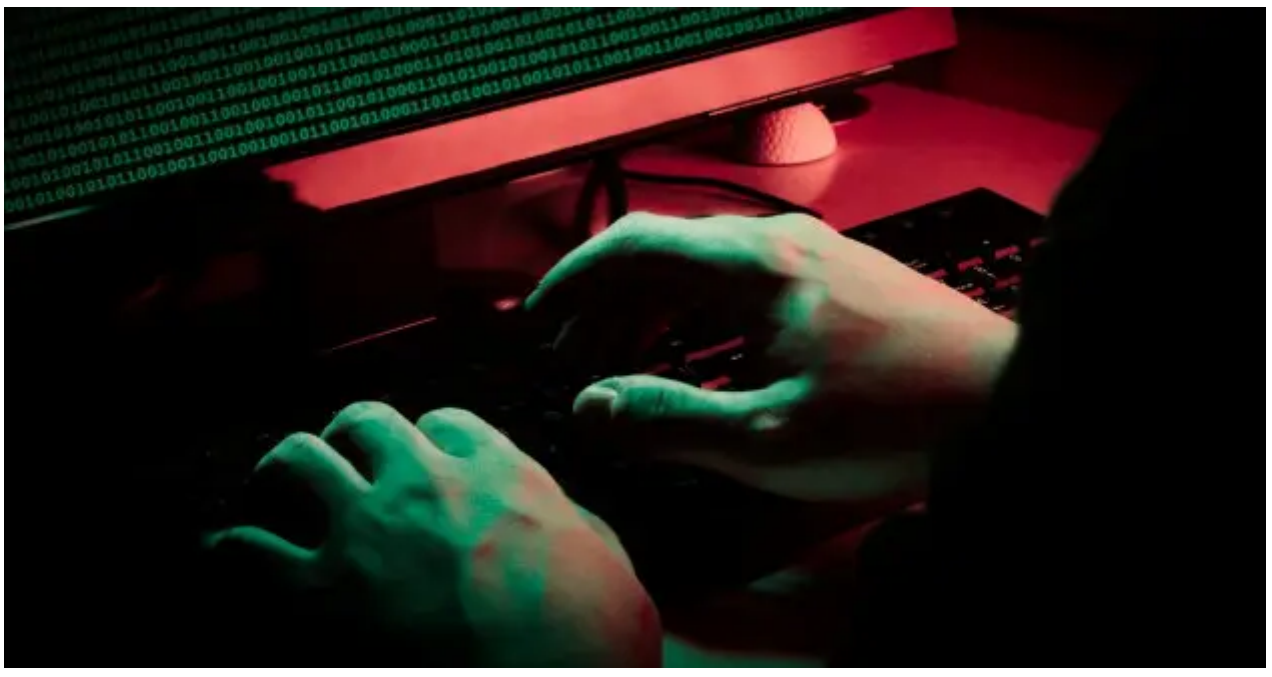

Intelligence & Analytics May 26, 2022 By Kevin Henson

7 min read

This post was written with contributions from Chris Caridi and Kat Weinberger.

IBM Security X-Force has been tracking the activity of Black Basta, a new ransomware group that first appeared in April 2022. To date, this group has claimed attribution of 29 different victims across multiple industries using a double extortion strategy where the attackers not only execute ransomware but also steal data and threaten to release it publicly if the ransom demands are not met. The data disclosure element of these attacks takes place on a data leak site available on the Tor network. As a mechanism to apply pressure to coerce the victim to pay the ransom, the operators of Black Basta will gradually release stolen data on the leak site.

The Black Basta group is still in the early stages of their organization and X-Force has not observed any attempts to advertise the malware or hire affiliates on underground forums. Due to operational similarities and the absence of affiliation attempts, it has been reported that Black Basta may potentially be a rebranded version of the Conti gang, a well-known ransomware group that already has affiliates. However, the Conti group announced on May 12 that they had no affiliations with the Black Basta ransomware group. X-Force's assessment of the possible relationship between these groups is ongoing.

The Black Basta ransomware variant acts at such a high speed that it rarely causes symptoms that would tip off defenders to the compromise before the ransomware has been deployed.

This blog post will detail X-Force's insights into the Black Basta ransomware, technical analysis of the sample, and indicators of compromise (IoC) to help organizations protect themselves from this malware.

X-Force Assessment

Black Basta's sudden appearance and subsequent high volume of successful compromises highlights the speed with which ostensibly "new" ransomware groups are able to become central figures in the threat landscape. While this group has yet to be linked by X-Force to existing or past ransomware operations, the impact that this group has had in such a short amount of time points to a practiced and effective set of tactics, techniques, and procedures (TTPs) that pose a significant threat to enterprise networks. Based on current intelligence, it does not appear that Black Basta targets specific industries or verticals. However, entities that collect large amounts of data that is attractive for extortion operations such as personally identifiable information (PII), financial information, or other sensitive data, are likely to stand out as lucrative targets for attackers.

We encourage security practitioners to review the IBM X-Force Definitive Guide to Ransomware and the mitigations highlighted below, action available IOCs, and ensure that detections are in place to alert on observed malicious behaviors.

Additional Risk Mitigations:

- Establish and maintain backup routines, including offline backups. Ensure you have backup redundancy stored separately from network zones attackers could access with read-only access. The availability of effective backups is a significant differentiator for organizations and can support recovery from a ransomware attack.
- Implement a strategy to prevent unauthorized data theft, especially as it applies to uploading large amounts of data to legitimate cloud storage platforms that attackers can abuse.
- Employ user behavior analytics to identify potential security incidents. When triggered, assume a breach has taken place. Audit, monitor and quickly act on suspected abuse related to privileged accounts and groups.

- Employ multifactor authentication on all remote access points into an enterprise network —— with particular care given to secure or disable remote desktop protocol (RDP) access. Multiple ransomware attacks have been known to exploit weak RDP access to gain initial entry into a network.

Download the Definitive Guide to Ransomware

Ransomware Analysis Details

Behavioral Analysis

Behavioral analysis describes the malware behavior observed on a system during execution. Behavioral analysis typically includes actions performed on the system such as files dropped, persistence, details surrounding process execution and any C2 communications. It should be noted that behavioral analysis may not capture all notable malware behavior as certain functions may only be performed by the malware under specific conditions.

Loader

Upon execution, the loader base64 decodes a Black Basta payload using the CryptStringToBinaryA() API function. The decoded payload is then RC4 decrypted using the key "1xJr13puJChWqiMeOnFDDSOmoSmws5n". Black Basta is then injected into a process instance of the loader and executed in memory. The injected Black Basta sample has a SHA256 hash: ef1382770f820e4b2e65981bb7b3a62d5f93e3b87763f83012ef7f7cb1bc9469 and compile time: Thursday, 28.04.2022 15:15:43 UTC.

Black Basta

Upon execution, Black Basta conducts the following activity:

- Deletes volume shadow copies using the commands:

```
C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet C:\Windows\System32\vssadmin.exe delete shadows /all /quiet
```

- Changes the desktop background to the following image using the file %Temp%\dlaksjdoiwq.jpg.
- Modifies the following registry key to set the desktop background.

```
HKCU\Control Panel\Desktop\Wallpaper = %Temp%\dlaksjdoiwq.jpg
```

- Drops the ICON file %Temp%\fkdjsadasd.ico to the system. This file is used as the default icon for encrypted files. To set the default icon, the ransomware creates the following registry key.

```
HKEY_CLASSES_ROOT\.basta\DefaultIcon = %Temp%\fkdjsadasd.ico
```

- Drops the ransom note readme.txt in directories where it encrypts files. The company id and ransom note is hardcoded in the sample. Example id: 18a6cdad-316c-4922-953e-c64bf4959a74.

```
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) hxxps[:]//aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd[.]onion/

Your company id for log in: <varying id per sample in GUID format>
```

- Appends the file extension .basta to encrypted files.
- Depending on the variant, Black Basta conducts the following activity:
  - Hijacks the existing Fax service to maintain persistence.
  - Disables windows recovery and repair with the command:

```
C:\Windows\SysNative\bcdedit.exe /deletevalue safeboot C:\Windows\System32\bcdedit.exe /deletevalue safeboot
```

- Reboots the system into safe mode using bcdedit and the shutdown command.

```
C:\Windows\SysNative\bcdedit.exe /set safeboot network C:\Windows\System32\bcdedit.exe /set safeboot
network cmd.exe /C shutdown –r –f –t 0
```

- The following files and folders are skipped during encryption:

```
$Recycle.Bin Windows boot readme.txt dlaksjdoiwq.jpg NTUSER.DAT fkdjsadasd.ico OUT.txt
```

Static Analysis

Static analysis is a deeper dive into the technical analysis of the malware. Static analysis typically includes further details about the functionality, obfuscation or packing in the sample, encryption used by the malware, configuration information or other notable technical detail.

Loader

The injection process for the loader is as follows:

1. The loader creates a suspended process instance of itself with CreateProcessA().
2. Then it calls GetThreadContext() to get the thread context of the suspended process.
3. Next, it calls ReadProcessMemory() to obtain the suspended process' image base from the Process Environment Block retrieved via the thread context.
4. The loader proceeds to allocate memory in the suspended process using VirtualAllocEx() and writes the payload to the buffer using WriteProcessMemory().
5. Finally, it sets the entry point of the injected payload using SetThreadContext() and executes the injected payload using ResumeThread().

Notably, samples similar to loader were found in VirusTotal with the following project paths. The payloads of these samples have not yet been determined.

```
c4fa34414fb1c199e13d7cd7def0e8f401c9649657a39224bc32310c9fd9d725, C:
\BHProject\Treasurer\SharpDepositorCrypter\PELoaderNative\PELoaderNative\Release\PELoaderNative.pdb
f132ffc8648d38833244e612c58224285e85e863a35c872490690217c082e59c, C:
\BHProject\Treasurer\SharpDepositorCrypter\PELoaderNative\PELoaderNative\Release\PELoaderNative.pdb
```

The following samples were compiled under a similar project path but are coded differently.

```
19c2710e498d55f2e3a3d4126064e960058e32c99dc35944b3fc09aa0eec4754, C:
\BHProject\Treasurer\SharpDepositorCrypter\PELoader\PELoader\Release\PELoader.pdb
c5fcd0643823082941bc827613baf0fa574ffd9cb03a8b265d62d657367b2ea2, C:
\BHProject\Treasurer\SharpDepositorCrypter\PELoader\PELoader\Release\PELoader.pdb
daa049b15bb5c1d0aef06276f9940d2fea76242f1a01ebfe299a63b7c74f7ea0, C:
\BHProject\Treasurer\SharpDepositorCrypter\PELoader\PELoader\Release\PELoader.pdb
```

Black Basta

Encryption

To start encrypting files, Black Basta calls the FindFirstVolumeW() and FindNextVolumeW() functions to enumerate volumes on the victim system. For each volume, the ransomware calls GetVolumePathNamesForVolumeNameW() to obtain a list of drive letters and mounted folder paths for the specified volume. Analysis indicates that Black Basta uses ChaCha20 encryption during the encryption process. Notably, it is observed that some files are not fully encrypted, possibly in an effort to hasten the encryption process. Black Basta encrypts some files in 64-byte blocks every 128 bytes as shown in the example encrypted notepad.exe file below.

Compile Times

The samples' compile times range from February 2022 to Apr 2022. The earlier samples in February contain a ransom note indicating the malware name is "no_name_software".

Sample	Compile Time
17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90	Thursday, 17.02.2022 00:46:11 UTC

5b6c3d277711d9f847be59b16fd08390fc07d3b27c7c6804e2170f456e9f1173	Thursday, 17.02.2022 00:46:11 UTC
7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a	Saturday, 16.04.2022 06:29:58 UTC
ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e	Saturday, 16.04.2022 06:29:58 UTC
b3661c6fecf46e6a7b96b3debc7efa65633bfde2f156392ff6506736457361be	Friday, 22.04.2022 14:41:00 UTC
5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa	Friday, 22.04.2022 20:31:36 UTC

Sample Ransom Note from versions compiled in February:

```
All of your files are currently encrypted by no_name_software. These files cannot be recovered by any means
without contacting our team directly. DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover
your data (including the usage of the additional recovery software) can damage your files. However, if you
want to try - we recommend choosing the data of the lowest value. DON'T TRY TO IGNORE us. We've downloaded
a pack of your internal data and are ready to publish it on our news website if you do not respond. So it
will be better for both sides if you contact us as soon as possible. DON'T TRY TO CONTACT feds or any
recovery companies. We have our informants in these structures, so any of your complaints will be
immediately directed to us. So if you will hire any recovery company for negotiations or send requests to
the police/FBI/investigators, we will consider this as a hostile intent and initiate the publication of
whole compromised data immediately. DON'T move or rename your files. These parameters can be used for
encryption/decryption process. To prove that we REALLY CAN get your data back - we offer you to decrypt two
random files completely free of charge. You can contact our team directly for further instructions through
our website : TOR VERSION : (you should download and install TOR browser first https://torproject.org)
https://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion:80/ Your company id for log in:
c98fa42b-3233-45df-bd7c-42529c44cb70 Your company key: 3 of any of your dc through comma. Example: "DC1,
DC2, DC3". You can type less if you have no enough YOU SHOULD BE AWARE! We will speak only with an
authorized person. It can be the CEO, top management, etc. In case you are not such a person - DON'T
CONTACT US! Your decisions and action can result in serious harm to your company! Inform your supervisors
and stay calm!
```

String Analysis

String analysis reveals misspelled strings “ERRRRRRRROr” and “ERRROR“.

The ransomware contains references to the following Windows services:

```
tokenbroker cdpsvc wcmsvc wsearch dnscache iphlpsvc appinfo coremessagingregistrar lsm vboxservice
brokerinfrastructure camsvc keyiso eventsystem dcomlaunch power samss lanmanserver comsysapp vaultsvc
wuauserv netsvcs remoteregistry sessionenv termservice netlogon
```

X-Force

If you have questions or want a deeper discussion on how IBM X-Force can help you with incident response, threat intelligence, or offensive security services schedule a follow up meeting here:

IBM X-Force Scheduler

If you are experiencing cybersecurity issues or an incident, contact X-Force to help.

US hotline 1-888-241-9812 | Global hotline (+001) 312-212-8034

IBM X-Force Research | ransomware attacks | Corporate Network Security | Network Security | Ransomware | X-Force Kevin Henson Malware Reverse Engineer, IBM

Kevin joined IBM Security’s X-Force IRIS team as a Malware Reverse Engineer in November 2018 after 21 years of experience in supporting various commercial,...