

# Ransomware Roundup - Black Basta

By **James Slaughter** and **Shunichi Imano** | June 23, 2023

On a bi-weekly basis, FortiGuard Labs gathers data on ransomware variants of interest that have been gaining traction within our datasets and the OSINT community. The Ransomware Roundup report aims to provide readers with brief insights into the evolving ransomware landscape and the Fortinet solutions that protect against those variants.

**FORTINET**®



**Impacted parties:** Microsoft Windows and ESXi Users

**Impact:** Encrypts files on the compromised machine and demands ransom for file decryption

**Severity level:** High

## Black Basta Ransomware Overview

Over the past few months, Black Basta ransomware has made headlines for allegedly compromising high-profile European and North American organizations across a variety of industries, such as outsourcing, technology, and manufacturing.

The history of Black Basta ransomware dates back to at least April 2022, with a professional organizations company in the United States being one of its first victims. Since then, Black Basta has slowly expanded their operations, with the group allegedly

compromising and stealing data from a US government contractor and a US aerospace and defense company in late 2022.

This ransomware is considered a successor to the now-defunct Conti ransomware because some former Conti members are believed to be in the Black Basta group. Some also believe there is a potential connection between Black Basta and the Fin7 threat actor due to the groups' similar Tactics, Techniques, and Procedures (TTPs).

Black Basta operates a Ransomware-as-a-Service (RaaS) model, in which the developers offer a service such as ransomware, an infrastructure for payment processing and ransom negotiation, and technical support to its affiliates. Once an affiliate gets a victim to pay a ransom, the Black Basta operator receives a portion. Affiliates are responsible for selecting their targets, moving laterally across a victims' network (often by using tools supplied by ransomware operators, leveraging dual-use tools, and employing living-off-the-land tactics), stealing data, and deploying the ransomware. Tools reportedly used by Black Basta threat affiliates include PsExec, Windows Management Instrumentation (WMI), PowerShell, Netcat, BITSAdmin, BCDEdit, SystemBC, Mimikatz, ColbaltStrike, Brute Ratel C4, remote access tools, and RClone.

Before deploying the ransomware to compromised networks, Black Basta attackers install and configure the open-source file-transfer utility "RClone" to steal the data that they collected. The stolen data is then used for their double-extortion scheme, where the files are leaked to the public if a victim fails to meet the ransom demands.

The Black Basta ransomware was initially only supported on Windows platforms. However, the Black Basta developer released a new variant targeting ESXi systems in 2022. The group also updated and released Black Basta ransomware 2.0, which reportedly incorporates a new encryption algorithm.

Note that FortiGuard Labs previously released a Threat Signal for Black Basta ransomware on May 2<sup>nd</sup>, 2022:

- **New Ransomware "Black Basta" in the Wild**

## Infection Vector

Black Basta has been seen to use techniques from spearphishing to purchasing access through Initial Access Brokers (IABs) to gain initial access. Access has also been obtained using malware from other groups, such as QakBot (QBot). The exploitation of

the PrintNightmare (CVE-2021-34527) and Follina (CVE-2022-30190) vulnerabilities have also been reported.

More details on CVE-2021-34527 and CVE-2022-30190 are available as Outbreak Alerts previously released by FortiGuard Labs:

- **Microsoft PrintNightmare Vulnerability**
- **Microsoft MSDT Follina Vulnerability**

## Ransomware Execution

FortiGuard Labs is aware that the ransomware component of Black Basta has been compiled as a Windows executable, more recently as a Windows DLL, and additionally as a Linux executable

## Windows Executable and DLL

The functionality between the two versions is identical, as is the final step in the attack chain.



Figure 1 . Launching the Black Basta DLL.

Black Basta has been observed using the XChaCha20 stream cipher (<https://en.wikipedia.org/wiki/ChaCha20-Poly1305>) to encrypt its files. This is built into the software using the Crypto++ C++ library (<https://www.cryptopp.com/>).

Function name	Address	Function	Instruction
CryptoPP::MessageQueue::MaxRetrievable(void)	.text:100218B4	sub_10021AE0	call CryptoPP::RoundupSize
CryptoPP::MessageQueue::TransferTo2(CryptoPP::MessageQueue &,CryptoPP::MessageQueue &)	.text:10021FAE	sub_10021F40	call CryptoPP::RoundupSize
CryptoPP::CRT(CryptoPP::Integer const &,CryptoPP::Integer const &)	.text:10022060	sub_10021F40	call CryptoPP::RoundupSize
CryptoPP::DiscreteLogWorkFactor(uint)	.text:10023451	?Inverse@ModularArithmetic...	call CryptoPP::Decrement
CryptoPP::IsPrime(CryptoPP::Integer const &)	.text:10024432	?MultiplicativeInverse@Mont...	call CryptoPP::Compare
CryptoPP::PrimeSieve::SieveSingle(std::vector<bool> &)	.text:100245D6	sub_10024580	call CryptoPP::Compare
CryptoPP::TrialDivision(CryptoPP::Integer const &,CryptoPP::Integer const &)	.text:1002460D	sub_10024580	call CryptoPP::Compare
CryptoPP::VerifyPrime(CryptoPP::RandomNumberGenerator &)	.text:100246A9	sub_10024580	call CryptoPP::Compare
CryptoPP::DetectX86Features(void)	.text:100246E5	sub_10024580	call CryptoPP::Compare
CryptoPP::SHA1_HashMultipleBlocks_SHANI(uint &)	.text:10024727	sub_10024580	call CryptoPP::Decrement
CryptoPP::SHA256_HashMultipleBlocks_SHANI(uint &)	.text:10024A1A	?PositiveCompare@Integer@...	call CryptoPP::Compare
CryptoPP::PolynomialMod2::PolynomialMod2(void)	.text:10024AFE	sub_10024A30	call CryptoPP::RoundupSize
CryptoPP::HexDecoder::IsolatedInitialize(CryptoPP::Integer const &)	.text:10024B24	sub_10024A30	call CryptoPP::RoundupSize
CryptoPP::ChaCha_OperateKeystream_SSE2(uint &)	.text:10024EF6	sub_10024E20	call CryptoPP::Decrement
CryptoPP::...anonymous_namespace_...AESNI_E...	.text:10024F1A	sub_10024E20	call CryptoPP::Compare
CryptoPP::Rijndael_Dec_AdvancedProcessBlocks...	.text:10024FC9	sub_10024E20	call CryptoPP::Decrement
CryptoPP::Rijndael_UncheckedSetKeyRev_AESNI...	.text:10025049	?Power2@Integer@CryptoPP...	call CryptoPP::RoundupSize
CryptoPP::CPU_ProbeSSE2(void)	.text:10025491	sub_10025410	call CryptoPP::TwosComplement
CryptoPP::dynamic_atexit destructor for 'AAD_CHA...	.text:10025594	sub_10025550	call CryptoPP::Compare
CryptoPP::dynamic_atexit destructor for 'AAD_CHA...	.text:100255D0	sub_10025550	call CryptoPP::Compare
CryptoPP::dynamic_atexit destructor for 'AAD_CHA...	.text:1002F01E	CryptoPP::TwosComplement	call CryptoPP::Decrement
CryptoPP::dynamic_atexit destructor for 'AAD_CHA...	.text:10030404	?HashMultipleBlocks@SHA1...	call CryptoPP::...anonymous_namespace_...SHA1_HashBlock_CXX

Figure 2. A partial list of Crypto++ library function calls.

Files are encrypted quickly using multi-threading, with the file extension for encrypted files being unique for each ransomware build.

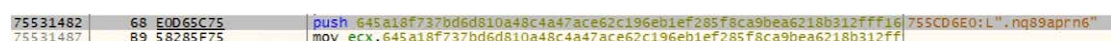


Figure 3. File extension hardcoded in this Black Basta file.

Name	Date modified	Type	Size
6.2.2022-02-15_PH5646564_xls.exe.400000.0.unpack.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	96 KB
7z2107-x64.exe.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	1,498 KB
2022-02-15_PH5646564_xls.exe.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	715 KB
7784d5a3e3e6c22ed74b1f7639be044d86ab3feb4922d545daa716c7ef709fca.msi.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	125 KB
220616-pcckrahde2_pw_infected.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	1,089 KB
b37761715d5a2405a3fa75abccaf6bb15b7298673aad91a158725be3c518a87.exe.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	141 KB
ChromeSetup.exe.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	1,311 KB
Comae-Toolkit-Light-3.0.20180129.1.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	1,164 KB
instructions_read_me.txt	30/05/2023 22:11	Text Document	2 KB
Firefox Installer.exe.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	327 KB
JavaSetup8u311.exe.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	2,055 KB
main.dll.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	681 KB
New folder.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	291 KB
odbg110.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	1,303 KB
smoke.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	463 KB
PO#23754-1.ISO.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	1,729 KB
staticlogs.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	1,349 KB
Uniza.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	277 KB
untitled folder.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	91 KB
odbg201.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	6,803 KB
vmp.exe.zip.nq89aprn6	30/05/2023 22:11	NQ89APRN6 File	4,402 KB
snapshot_2022-05-18_12-39.zip.nq89aprn6	30/05/2023 22:12	NQ89APRN6 File	33,090 KB

Figure 4. Files encrypted by Black Basta and its ransom note.

Name	Date modified	Type	Size
▼ Later this year (30)			
Wireshark-win64-3.6.0.exe.vokou2s5g	31/05/2023 20:48	VOKOU2S5G File	75,461 KB
JetBrains.dotPeek.2021.3.3.web.exe.voko...	31/05/2023 20:48	VOKOU2S5G File	36,830 KB
snapshot_2022-05-18_12-39.zip.vokou2s5g	31/05/2023 20:48	VOKOU2S5G File	33,090 KB
odbg201.zip.vokou2s5g	31/05/2023 20:47	VOKOU2S5G File	6,803 KB
vmp.exe.zip.vokou2s5g	31/05/2023 20:47	VOKOU2S5G File	4,402 KB
JavaSetup8u311.exe.vokou2s5g	31/05/2023 20:47	VOKOU2S5G File	2,055 KB
odbg110.zip.vokou2s5g	31/05/2023 20:47	VOKOU2S5G File	1,303 KB
PO#23754-1.ISO.vokou2s5g	31/05/2023 20:47	VOKOU2S5G File	1,729 KB
staticlogs.zip.vokou2s5g	31/05/2023 20:47	VOKOU2S5G File	1,349 KB
7z2107-x64.exe.vokou2s5g	31/05/2023 20:47	VOKOU2S5G File	1,498 KB
220616-pcckrahde2_pw_infected.zip.vok...	31/05/2023 20:47	VOKOU2S5G File	1,089 KB
ChromeSetup.exe.vokou2s5g	31/05/2023 20:47	VOKOU2S5G File	1,311 KB
Comae-Toolkit-Light-3.0.20180129.1.zip.v...	31/05/2023 20:47	VOKOU2S5G File	1,164 KB
Firefox Installer.exe.vokou2s5g	31/05/2023 20:47	VOKOU2S5G File	327 KB
main.dll.zip.vokou2s5g	31/05/2023 20:47	VOKOU2S5G File	681 KB
New folder.zip.vokou2s5g	31/05/2023 20:47	VOKOU2S5G File	291 KB
smoke.zip.vokou2s5g	31/05/2023 20:47	VOKOU2S5G File	463 KB
Uniza.zip.vokou2s5g	31/05/2023 20:47	VOKOU2S5G File	277 KB
untitled folder.zip.vokou2s5g	31/05/2023 20:47	VOKOU2S5G File	91 KB
6.2.2022-02-15_PH5646564_xls.exe.40000...	31/05/2023 20:47	VOKOU2S5G File	96 KB
2022-02-15_PH5646564_xls.exe.zip.vokou...	31/05/2023 20:47	VOKOU2S5G File	715 KB

Figure 5. Variation in file extensions for encrypted files.

The ransom note is assembled and dropped into each directory that includes files that have been encrypted. Note in Figure 6 that the Login ID (the ID used by the threat actor to identify the victim when they make contact) is hardcoded into the ransomware, which suggests some customization for a particular victim.



```

aAttentionYourN db 'ATTENTION!',0Dh,0Ah ; DATA XREF: sub_1000C200+1B7+o
db 'Your network has been breached and all data was encrypted. Please'
db ' contact us at:',0Dh,0Ah
db 'https://[REDACTED]wdtyctgvdyd.'
db 'onion/ ',0Dh,0Ah
db 0Dh,0Ah
db 0Dh,0Ah
db 'Login ID: 66a531a8-86fe-42cf-8a02-0d7e139cfbe2',0Dh,0Ah
db 0Dh,0Ah
db 0Dh,0Ah
db '!!* To access .onion websites download and install Tor Browser at'
db ': ',0Dh,0Ah
db 0Dh,0Ah
db ' https://www.torproject.org/ (Tor Browser is not related to us)'
db 0Dh,0Ah
db 0Dh,0Ah
db '!!* To restore all your PCs and get your network working again, f'
db 'ollow these instructions:',0Dh,0Ah
db 0Dh,0Ah
db '- Any attempts to modify, decrypt or rename the files will lead t'
db 'o its fatal corruption. It doesn',27h,'t matter, who are trying t'
db 'o do this, either it will be your IT guys or a recovery agency.',0Dh
db 0Ah
db 0Dh,0Ah
db 'Please follow these simple rules to avoid data corruption:',0Dh,0Ah
db 0Dh,0Ah
db '- Do not modify, rename or delete files. Any attempts to modify, '
db 'decrypt or rename the files will lead to its fatal corruption. ',0Dh
db 0Ah
db 0Dh,0Ah
db '- Do not hire a recovery company. They can',27h,'t decrypt withou'
db 't the key. ',0Dh,0Ah
db 'They also don',27h,'t care about your business. They believe that'
db ' they are ',0Dh,0Ah
db 'good negotiators, but it is not. They usually fail. So speak for '
db 'yourself.',0Dh,0Ah
db 0Dh,0Ah
db 0Dh,0Ah
db 0Dh,0Ah
db 'Waiting you in a chat.',0Dh,0Ah,0

```

Figure 6. Building the ransom note. Note that the “Login ID” is hardcoded here.

The ransom note labeled “Instructions\_read\_me.txt” is automatically opened in Notepad so the victim can easily see it.

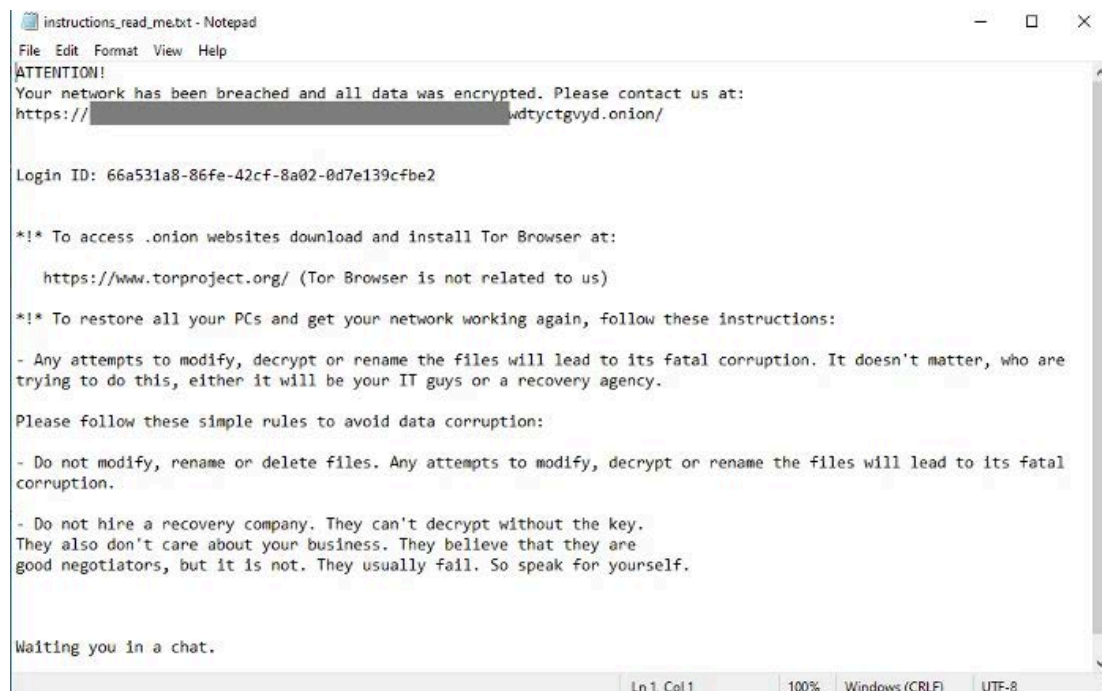


Figure 7. Black Basta ransom note as seen in Notepad.

The note demands that the victim use Tor to contact the ransomware gang = at a specified “.onion” site. Instructions for downloading and installing the Tor browser are

provided. It also suggests that the victim not contact a recovery company or outside ransom negotiators.

## Linux Executable

Black Basta has also developed a Linux executable primarily designed to target VMWare ESXi deployments rather than more general individual Linux systems. This can be easily shown by running the ransomware on a non-ESXi deployment. When executed, the malware will be unable to locate the “/vmfs/volumes/” directory and be unable to run. This directory (VMFS is the “Virtual Machine File System,” and “volumes” is where VM disk images reside, which would be the main target of the ransomware). If that folder is then put in place, it will execute (although nothing will occur on a non-ESXi host).

```
linux-mint211@linuxmint211:~/Downloads/staticlogs/d7f765d0fb6801ea18677381b121727076135de5a494d40c4f773a94f1493b45$ ./d7f765d0fb6801ea18677381b121727076135de5a494d40c4f773a94f1493b45
The soft limit is 65535
The hard limit is 65535
No such file or directory
```

Figure 8. Testing without “/vmfs/volumes/” present.

```
linux-mint211@linuxmint211:~/Downloads/staticlogs/d7f765d0fb6801ea18677381b121727076135de5a494d40c4f773a94f1493b45$ sudo mkdir /vmfs/
linux-mint211@linuxmint211:~/Downloads/staticlogs/d7f765d0fb6801ea18677381b121727076135de5a494d40c4f773a94f1493b45$ sudo mkdir /vmfs/volumes
linux-mint211@linuxmint211:~/Downloads/staticlogs/d7f765d0fb6801ea18677381b121727076135de5a494d40c4f773a94f1493b45$ cd /home/linux-mint211/Downloads/
linux-mint211@linuxmint211:~/Downloads$ sudo cp *.* /vmfs/volumes
linux-mint211@linuxmint211:~/Downloads$ cd ~/Downloads/staticlogs/d7f765d0fb6801ea18677381b121727076135de5a494d40c4f773a94f1493b45
linux-mint211@linuxmint211:~/Downloads/staticlogs/d7f765d0fb6801ea18677381b121727076135de5a494d40c4f773a94f1493b45$ ./d7f765d0fb6801ea18677381b121727076135de5a494d40c4f773a94f1493b45
The soft limit is 65535
The hard limit is 65535
```

Figure 9. Testing with “/vmfs/volumes/” present.

The Linux version of Black Basta has several command line flags that suggest it is designed to be executed by an individual who has remote access to a victim ESXi server.

```
a:00000000004E2473 aBomb db '-bomb',0 ; DATA XREF: ProcessCommonArguments(void)+3:0
a:00000000004E2479 aKillServices db '-killservices',0 ; DATA XREF: ProcessCommonArguments(void)+57:0
a:00000000004E2487 aForceprivate db '-forceprivate',0 ; DATA XREF: ProcessCommonArguments(void)+9C:0
a:00000000004E2495 aForcepath db '-forcepath',0 ; DATA XREF: ProcessCommonArguments(void)+D5:0
a:00000000004E24A0 ; const char aForcedPaths[]
a:00000000004E24A0 aForcedPathS db 'Forced path: %s',0Ah,0 ; DATA XREF: ProcessCommonArguments(void)+1D7:0
a:00000000004E24A0 ; DATA XREF: ProcessCommonArguments(void)+22A:0
a:00000000004E24B1 aNomutex db '-nomutex',0 ; DATA XREF: ProcessCommonArguments(void)+26F:0
a:00000000004E24BA aDisablewhitel db '-disablewhitelist',0 ; DATA XREF: ProcessCommonArguments(void)+2B4:0
a:00000000004E24CC aFile db '-file',0 ; DATA XREF: ProcessCommonArguments(void)+291:0
a:00000000004E24D2 aThreads db '-threads',0 ; DATA XREF: ProcessCommonArguments(void)+331:0
a:00000000004E24DB asc_4E24DB db '...',0 ; DATA XREF: RecursiveSearchFiles(void)+27C:0 ...
a:00000000004E24DE ; RecursiveSearchFiles(void)+73:0 ; DATA XREF: VisibleEntry(void)+73:0
a:00000000004E24DE aVmfsVolumes db '/vmfs/volumes/',0 ; DATA XREF: GLOBAL_sub_I_argList+1E2:0
a:00000000004E24ED aInstructionsRe db 'instructions_read_me.txt',0 ; GLOBAL_sub_I_ZN8Filters7SFStateC2EPNS_10S
a:00000000004E24ED ; DATA XREF: VisibleEntry(void)+29E:0
a:00000000004E2506 aC_0 db 'c:',0 ; DATA XREF: main:loc_4040D5:0
a:00000000004E250A aKillesxi db '-killesxi',0 ; DATA XREF: main:loc_4040D5:0
a:00000000004E2514 ; const char aUlimitN2000[]
a:00000000004E2514 aUlimitN2000 db 'ulimit -n 2000',0 ; DATA XREF: main+21A:0
```

Figure 10. Command line arguments.

Again, executing in a non-ESXi environment fails. However, it allows for the tracing of the event in assembly.

```
linux-mint211@linuxmint211:~/Downloads/staticlogs/d7f765d0fb6801ea18677381b121727076135de5a494d40c4f773a94f1493b45$ ./d7f765d0fb6801ea18677381b121727076135de5a494d40c4f773a94f1493b45 -killesxi
cat: /tmp/list.txt: No such file or directory
sh: 1: vim-cmd: not found
timeout: invalid option -- 't'
Try 'timeout --help' for more information.
sh: 1: esxcli: not found
```

Figure 11. Executing the “-killesxi” command line flag.

The “-killesxi” command triggers a fairly involved Bash sequence, as shown in Figure 12 below.

```
a:00000000004E2690 command      db 'timeout -t 10 sh -c "export whitelist=$(cat /tmp/list.txt); expor
a:00000000004E2690                ; DATA XREF: main+EA:0
a:00000000004E2690                db 't machines=$(vim-cmd vmsvc/getallvms | sed ',27h,'1d',27h,' | awk'
a:00000000004E2690                db ' ',27h,'{print $1":"$2}',27h,''; for i in $machines; do export to'
a:00000000004E2690                db 'tal_passed=0; for whitelist_item in $whitelist; do if [[ $( echo '
a:00000000004E2690                db '\$i\' | grep -i $( echo \"${whitelist_item}$\" ) ) ]]; then tot'
a:00000000004E2690                db 'al_passed=$((total_passed+1)); else echo \"\$i not Ends with $whit'
a:00000000004E2690                db 'elist_item\"; fi; done; if [ $total_passed == 0 ]; then export ma'
a:00000000004E2690                db 'chine_to_kill=$(echo $i| cut -d',27h,'-',27h,' -f 1); echo \"kill'
a:00000000004E2690                db 'ing machine at id $machine_to_kill\"; vim-cmd vmsvc/power.off $ma'
a:00000000004E2690                db 'chine_to_kill; else echo \"not killing whitelist machine $i\"; fi'
a:00000000004E2690                db ' '; done\";0
a:00000000004E28FF                align 20h
```

Figure 12. The Bash sequence for the “-killesxi” command line flag.

As ESXi installations are the primary focus of the Black Basta Linux variant, it is only interested in four related file types for encryption: “.vmsd”, “.vmx”, “.vmxf”, and “.vmdk”.

```
data:00000000004E255A aVmsd      db '.vmsd',0 ; DATA XREF: GLOBAL_sub_I_argList+235:0
data:00000000004E2560 aVmx      db '.vmx',0 ; DATA XREF: GLOBAL_sub_I_argList+248:0
data:00000000004E2565 aVmx     db '.vmxf',0 ; DATA XREF: GLOBAL_sub_I_argList+25E:0
data:00000000004E256B aVmdk     db '.vmdk',0 ; DATA XREF: GLOBAL_sub_I_argList+271:0
```

Figure 13. File types of interest.

As with the Windows version, the Linux version of Black Basta hardcodes the file extension for encrypted files into the code for deployment, and it changes from file to file.

```
a:00000000004E2A6A |a1hex4q5td db '.1hex4q5td',0
```

Figure 14. File extension hardcoded in the Linux version of Black Basta.

Whether using the “-forcepath” command line flag to encrypt a single, non-standard directory with files of interest or the default location of “/vmfs/volumes/”, this version will encrypt files as efficiently as the Windows version.

1.vmdk.1hex4q5td	1.6 MB	unknown	Sat 03 Jun 2023 17:37:52 BST
2.vmdk.1hex4q5td	69.5 MB	unknown	Sat 03 Jun 2023 17:37:55 BST
1998-h.vmdk.1hex4q5td	856.9 kB	HTML document	Sat 03 Jun 2023 17:37:52 BST
2641-h.vmdk.1hex4q5td	452.5 kB	XHTML page	Sat 03 Jun 2023 17:37:52 BST
2701-0.vmdk.1hex4q5td	1.3 MB	unknown	Sat 03 Jun 2023 17:37:52 BST
4300-0.vmdk.1hex4q5td	1.6 MB	unknown	Sat 03 Jun 2023 17:37:53 BST
4300-h.vmdk.1hex4q5td	1.7 MB	XHTML page	Sat 03 Jun 2023 17:37:52 BST
10840.vmsd.1hex4q5td	26.0 MB	unknown	Sat 03 Jun 2023 17:37:54 BST
10840-001.vmsd.1hex4q5td	11.8 MB	unknown	Sat 03 Jun 2023 17:37:53 BST
10840-002.vmsd.1hex4q5td	14.1 MB	unknown	Sat 03 Jun 2023 17:37:53 BST
a5ed581ad5cd1a2f29473cb56116c...	11.0 MB	program	Sat 03 Jun 2023 17:37:53 BST
A17_FlightPlan.vmsd.1hex4q5td	20.7 MB	unknown	Sat 03 Jun 2023 17:37:54 BST
go1.20.3.linux-amd64.vmsd.1hex4q...	100.1 MB	unknown	Sat 03 Jun 2023 17:37:55 BST
instructions_read_me.txt	1.1 kB	plain text document	Sat 03 Jun 2023 17:37:52 BST
pg1513.vmsd.1hex4q5td	169.6 kB	unknown	Sat 03 Jun 2023 17:37:53 BST
pg1998.vmsd.1hex4q5td	683.4 kB	unknown	Sat 03 Jun 2023 17:37:54 BST
pg2641.vmsd.1hex4q5td	415.9 kB	unknown	Sat 03 Jun 2023 17:37:52 BST

Figure 15. Encrypted files on a Linux host.

The ransom note for the Linux version of Black Basta is identical to the Windows version. Again, the victim must contact the gang at a specified “onion” site.



```
instructions_read_me.txt ×
ATTENTION!
Your network has been breached and all data was encrypted. Please contact us at:
https://[redacted]wdtyctgvdyd.onion/

Login ID: bfa34627-47c8-4484-85f5-80ce2c61ccbd

** To access .onion websites download and install Tor Browser at:
https://www.torproject.org/ (Tor Browser is not related to us)

** To restore all your PCs and get your network working again, follow these instructions:

- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't
matter, who are trying to do this, either it will be your IT guys or a recovery agency.

Please follow these simple rules to avoid data corruption:

- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to
its fatal corruption.

- Do not hire a recovery company. They can't decrypt without the key.
They also don't care about your business. They believe that they are
good negotiators, but it is not. They usually fail. So speak for yourself.

Waiting you in a chat.
```

Figure 16. Black Basta Linux ransom note.

## Black Basta Tor Sites

As the ransom notes above show, the Black Basta threat actors want their victims to contact them at a specific Tor address. Once there, the site requires the visitor to enter their “Login ID” from the ransom note to identify the organization they’re from, along with the completion of a captcha to prevent automated connections.

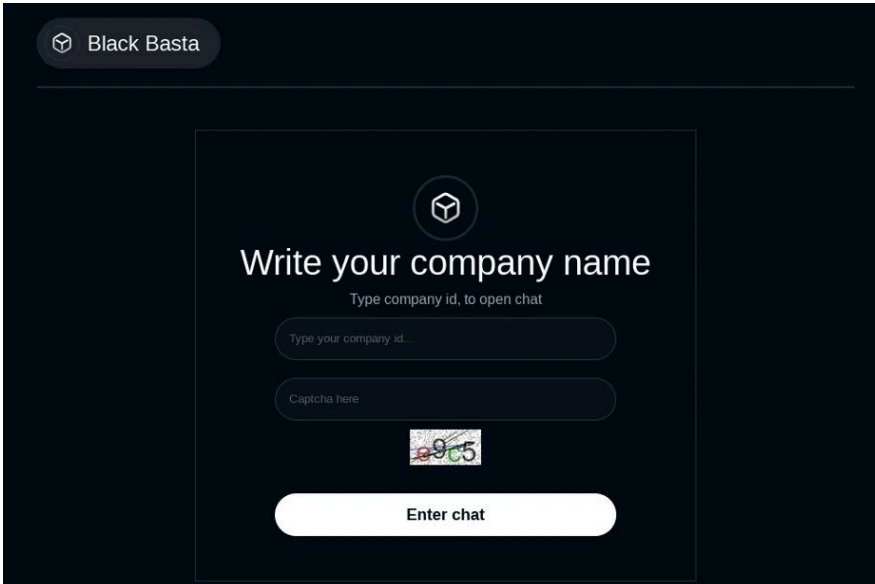
The image shows a dark-themed web interface for a Tor site. At the top left, there is a logo consisting of a cube inside a circle, followed by the text "Black Basta". Below this, there is a large white-bordered box containing the following elements: a cube icon in a circle at the top center; the text "Write your company name" in a large, bold font; the text "Type company id, to open chat" in a smaller font; a text input field with the placeholder "Type your company id..."; a text input field with the placeholder "Captcha here"; a small, pixelated captcha image showing the numbers "965"; and a large, rounded white button at the bottom with the text "Enter chat".

Figure 17. Black Basta Tor “chat” site.

In addition to the communication site, Black Basta operates a “name and shame” Tor site titled “Basta News”.



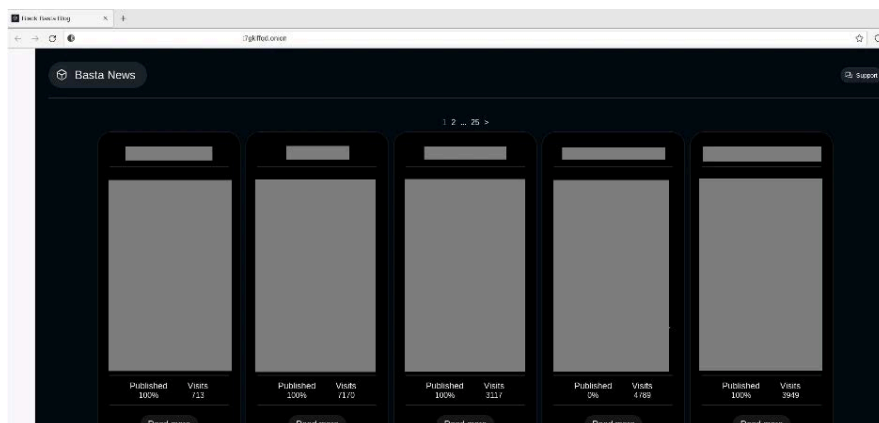


Figure 18. Black Basta “Basta News” site.

This site provides the group’s “proof” that it has compromised a given organization, publication status, and visitor count.

## Victimology

During our investigation, Black Basta’s data leak site listed more than 200 victims in North America and Europe. More than 60% of the alleged victims are U.S. organizations. Distant second place belongs to Germany at 15%, followed by Canada at close to 6%.

We divided the victim list into four groups: older victims to newer victims. While the oldest victim group spreads across 12 countries, the second and third group victims include only eight countries. The latest victim group has only six countries (U.S., Germany, Canada, Italy, UK, Slovenia), which may indicate that Black Basta affiliates have narrowed the target list.

As for its targeted industries, more than 25% of the victims listed on the leak site are in manufacturing, construction, service, and retail. However, 50% of the victims are in those four industries. Other affected sectors include legal, warehouse, finance, and IT.

Based on what’s in the data leak site, over 80% of the victims suffered from some or all of their stolen data being leaked to the public.

## Fortinet Protections

Fortinet customers are already protected from this malware variant through AntiVirus, and FortiEDR services, as follows:

FortiGuard Labs detects known Black Basta ransomware variants with the following AV signatures:

- W32/BlackBasta.A!tr.ransom
- W32/BlackBasta.D!tr.ransom
- W32/BlackBasta.F!tr.ransom
- W32/BlackBasta.FA18!tr.ransom
- W32/BlackBasta.PA!tr.ransom
- W32/BlackBasta.SA!tr.ransom
- W32/BlackBasta.4E32!tr.ransom
- W32/Filecoder\_BlackBasta.A!tr.ransom
- W32/Filecoder\_BlackBasta.B!tr
- W32/Filecoder\_BlackBasta.B!tr.ransom
- W32/Filecoder\_BlackBasta.C!tr
- W32/Filecoder\_BlackBasta.C!tr.ransom
- W32/Filecoder\_BlackBasta.D!tr.ransom
- W32/Filecoder\_BlackBasta.E!tr.ransom
- W32/Filecoder\_BlackBasta.F!tr
- W32/Filecoder\_BlackBasta.F!tr.ransom
- W32/Filecoder\_BlackBasta\_AGen.A!tr
- W32/Filecoder\_BlackBasta\_AGen.A!tr.ransom
- W32/Ransom.YXDADZ!tr.ransom
- W32/Ransom\_Win64\_BASTACRYPT.LKVCAGU!tr.ransom
- W32/Ransom\_Win64\_BASTACRYPT.YXDCXZ
- W64/BlackBasta.A!tr.ransom
- W64/BlackBasta.F!tr.ransom
- W64/Filecoder\_BlackBasta.A!tr.ransom
- ELF/BASTAD.GVYD!tr.ransom
- ELF/BlackBasta.6018!tr.ransom
- ELF/BlackBasta.D3E1!tr.ransom
- Linux/Filecoder\_BlackBasta.A!tr
- W32/Filecoder.4556!tr.ransom
- W32/Filecoder.506B!tr.ransom
- W32/Filecoder.OKW!tr
- W32/Filecoder.OMT!tr.ransom
- W32/GenKryptik.GBPY!tr.ransom
- W32/GenKryptik.GBRK!tr.ransom
- W32/GenKryptik.GCPP!tr.ransom
- W32/GenKryptik.GDSS!tr.ransom
- W32/GenKryptik.GFPG!tr.ransom
- W32/GenKryptik.GJNV!tr
- W32/Kryptik.ATLI!tr.ransom
- W32/Kryptik.CTJIRHO!tr.ransom

- W32/Kryptik.FKXJ!tr
- W32/Kryptik.FYBKLIK!tr
- W32/Kryptik.HOZJ!tr
- W32/Kryptik.HPRO!tr
- W32/Kryptik.HRKT!tr.ransom
- W32/Kryptik.HSAH!tr
- W32/Kryptik.HSSE!t
- W32/Kryptik.HSSE!tr
- W32/Kryptik.HSSE!tr.ransom
- W32/Kryptik.HTEE!tr
- W32/Kryptik.HTIE!tr
- W32/Kryptik.HTMN!tr
- W64/GenKryptik.GEJW!tr
- W32/ESQF.R002C0DC423!tr
- W64/REntS.1!tr.ransom
- W32/Generik.MJIYVEE!tr
- W32/Generik.NPGU!tr.ransom
- W32/PossibleThreat
- W32/PossibleThreat!tr.ransom
- Malicious\_Behavior.SB
- PossibleThreat
- W32/Malicious\_Behavior.SBX
- W32/Malicious\_Behavior.VEX

The FortiGuard AntiVirus service is supported by FortiGate, FortiMail, FortiClient, and FortiEDR. Fortinet EPP customers running current AntiVirus updates are also protected.

The following IPS signatures are in place for CVE-2021-34527 and CVE-2022-30190 respectively:

- MS.Windows.Print.Spooler.AddPrinterDriver.Privilege.Escalation
- MS.MSDT.URL.Protocol.Remote.Code.Execution

FortiEDR detects and blocks the execution of Black Basta ransomware before it can execute.

FortiEDR detects and blocks Black Basta ransomware from deleting volume shadow copies using the vssadmin utility with a security event triggered by the 'Suspicious Application' rule within the Ransomware Prevention security policy.



FortiEDR detects and blocks Black Basta ransomware from encrypting files within the "file Encryptor - Suspicious File Modification" rule in the Ransomware Prevention security policy.

FortiEDR detects and blocks Black Basta ransomware from changing the desktop background a 'Modify OS Setting' event triggered by the 'Unconfirmed Executable' rule in the Ransomware Prevention security policy.

**Note:** If you believe this or any other cybersecurity threat has impacted your organization, please contact our **Global FortiGuard Incident Response Team**.

IOCs

File-based IOCs:

SHA2	Malware
0180364e7dd8b5440920f1a85330bc5ec7e80756cb633014846378b9a5c9debd	
03309c90e6c60a2e3cd44374efa3003ae10cd9e05ba6a39c77aa5289b32cb969	

0595876dcfb02cbe4d85d3f9cb374b24473e5b338df781e18bd059ea48d60119
0825ae48606f05086efb7d2d03db4331a03e21017bdf1470cdc597c51381e6f5
08376a7b9bad22cc76ed74bcf1ff3c36fd26549c747e251980439074c0a22b65
09bc7247b50a166996b667b9a6e696cfbafa203ffcbec46ad0cca27deacd5c25
0bce6dc27d2cbdc231b563427c3489ddc69a0a88012abccd49b32c931dd93a81
0d6c3de5aebbbe85939d7588150edf7b7bdc712fceb6a83d79e65b6f79bfc2ef
10cd56acdf1bc7e91610f18583c4f88dc2f64a3caaf4faa8a3bccf3938599245
1354254499b2e3353708747d36c334074f40c1f726ea7590384f2192c972f8c3
1391c20a26f248f7c602f20096bf1886cfe7e4d151602a1258a9bbe7c02c1c80
1552079359d5e51fb862c3be8cc0daca5ae39b43255b87a9c185414944f8c43
15560b1e35a3a8612a7ba91d00dea6b8dd6e4f3f857399c22c0c75377c9b31a2
158e40a0009e6602303952694df6f3a49f40705c7ceb8b85854c0f1733aa2963
15abbff9fbce7f5782c1654775938dcd2ce0a8ebd683a008547f8a4e421888c4
17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90
1a8a283732f920d34233eac14ab03d681f3837b2e759df4ff1dd383249074e46
1bb7e645d4ff753157bbdd78829276356cb6660a767ab7158fc7dec3fe8b0e2f
1c711ca465dace4d2a8d0542e75410c417375c4ee484294fcd959e99651fccb8
1dd04aab97d6b65ac93ae3e8cfb4d3175d99f5b0395418abeb771d2db364cd3c
1ed076158c8f50354c4dba63648e66c013c2d3673d76ac56582204686aae6087

Black Basta  
ransomware



203d2807df6ef531efbec7bfd109986de3e23df64c01ea4e337cbe5ba675248b
21033cd24a9d775d7daa7bbc5c5b007553f205ac0febb6bae3fa35c700676bda
22aba8e0bdbbc9d50f6070ec50405c8ef31e5e22ad18fa9cc94d137fee0dd0536
2327018dab0e3beaed2123bcb5392405ab1e502dfa72a5a32c2c164346bb9bc6
240450721e47d4cabcd15d074f0a3a7b3e0b9f1a791006046e211ec302c28b0
245af5ac27f701bf320971c69f9317b37faaac228731a77fb06ad9944c9b6772
2558d0817586306d0ddf7beadd371785cd0a0b7ed860ac62760dbbc92866008a
2e2ec16d0b77bddbc2e88a0a914e7466a3c9dee38dc73a66dddd005e92bb3d6e
2edcf98e7031dad7d90df525db2951b83b2a82de57dfe853c98eae db609e49c4
2f8796499a7df61817126eb00c8aedff7b709f7f652503b2b9bd1c6a2f7f61e4
31e2288f0dd395423c22d2d20c9562211e97a2ab06d2403cf020203abe835993
3276df5b3b112c052d56919ad33de8404ec1a37d47d2c28d9deb f8323df22e16
350ba7fca67721c74385faff083914ecdd66ef107a765dfb7ac08b38d5c9c0bd
41b3d0d4419eac75017e76fe3bd76ec6a968cb68af4cf6335a27a196c47bac25
434a4f21549a1ae3dd623bfbc084d43c330821a279b2f4a4abdc7c a6e5584bfb
43e43276e250fc8a971fc3f0308827f98df09c52c08a09577b0cf636e9dc65ed
43f475bfa1f2c4fc35f08e6a96ca9698bd6f86357564d8243655e0f43aeff1a
47df319462909cbbcc0f2c1ab1fc4eec5363cae8344f9e4033542f221da97677
49ec36f03629f5993e496cfec6c5274c5f1db49bde704ef77ffe05f edd60e82b

Black Basta  
ransomware

4b83aaecddfcb8cf5caeff3cb30fee955ecfc3eea97d19dccf86f24c77c41fc4
4fa2e370c3e78afb50cdeac32b9b4f3e5262312b04b461d05ff73678f5526530
50d2d4c05bf810c1b57dd93f41430ddcd93838cc5367ed2c81de4563f59860c9
51eb749d6cbd08baf9d43c2f83abd9d4d86eb5206f62ba43b768251a98ce9d3e
5211ad84270862e68026ce8e6c15c1f8499551e19d2967c349b46d3f8cfcdcaa
5c6c40ddb666fe8b3a85fef39b6594337ebc6607b5eb9a4f16a62efc4402a0cb
5caa3f9665561b5b02f944cc33fb12faaec87d6ccb69af6a12d0f82cd0a5981d
5dcbec6d3370a2af103500325279d0c4f53df4c5a0c85b20a467797e61cb75ae
5ed057e99aed8356ccdf698f38fd3fe9ceabe517e1bd3245479fdd3cbb966fa9
60e9e8e25b64eabb59dc8667c286d91a8f4c6b6f9ea9aa12b55e7a2cb78d15f8
6264cae0ef62128667a295aef7154f4feb22dbfe53fc09fd01d122e01d43995e
645a18f737bd6d810a48c4a47ace62c196eb1ef285f8ca9bea6218b312fff16e
64921e6be1c8f44fddc6075621357496561924acecce48b73a243d5534c8d36e
653da5127b0ecbc5c373ce510c0d5191f61f2df912c9b6f4989aa3775933bc33
6b7d80a4e6b7b6d2a74f135313473415ecbbd7382688d0b536a7df6a7ccb2bab
6c0690782c3bfd790eddf460cba5b89769d740e78db90b56a54964ebffc9fb17
6cd7c9fa8314f2d7fb6819df38cffa1cccbd6f41b54c81bc6a667693351b3058
6cd92db9ebc8a8a879d86002971b93562928eca738a2fe14228479cb6cc1fe33
6cf61f55d7c40c703289b5692f7563c01d7bad54a2f5baf378a0e866622368e6

6def732c9ae7a4ce0dfd9d711033eed64fb5f481b56768c374289572c2743a0f
6ecd381ce0d3ad1ab83147712aa34772351e4d2dc43e1b66e3a999340e2b7f17
70161408185668a27da9d35ce4127003bda1acb6e31d9b01b576e64c17ec07cf
723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224
75f247f236a1f650c607e27d13b1c769340263f6b8caac946b0f1dacc5180b78
764b1117262d33f0a69b4f4c72fad607b7c71c262f60b9b2b35a21e7f4967786
7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a
7ab838960858870eaf2701a737411c6a65e00077136d938f4ef736b3c949833d
811e64d302089f4cb3cf7922c4310a1a00ef0a71c44ff402c1bf35c49c481f9e
81515e1c72fadae2c4bb15883e0c1d8979b49fd52d8c65ca03e05a75ca6683c9
83fc7095a91dc016bdbd965ae09182ea1d1a5b287cbfa4b0f3a58754336c8c33
856b5dc509c17f5be68186b6a8ab272fc0dd12000c978548d8488ee997b015e5
882019d1024778e13841db975d5e60aaae1482fcf86ba669e819a68ce980d7d3
8ded024d7fb62074d19cb9a364ca34646df42c971b9208227abc8bcb454d49f5
9770b4425a2c68ac8a861f3d5b484fad3c7bd7ea7a763248ad841821e19a01bc
97a997a2a3b270a4db3b56fec30319bc0f41f069a5089c47f08e4c554bf3ac32
99f82c9a80fc6556f28e50e2889d59325e8169dc3742bf34121dc85207c6d965
9b57d94b33cd712bf409e0128f26a75d2d9746ef65012ce6cd72caf47650d2a6
a083060d38984e7c6f36dcd2c57ec1aa3f50f9c201c8538257c8cbf2b3217e96

Black Basta  
ransomware

a252719d1712ec5aa37a8ce6e84474584c7d8d8221fa5aa033f32f5f5cf6d484
aa9f5321e9c5bede88d8f50342e9420f9ace7711950c9fae8536a0d5586ef86d
ab24df3877345cfab2c946d8a714f1ef17fe18c6744034b44ec0c83a3b613195
ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e
af75686852f329855981dd5953ff8ce40e713e6ef720ac26816091f40fede1a8
affcb453760dbc48b39f8d4defbcc4fc65d00df6fae395ee27f031c1833abada
b18b40f513bae376905e259d325c12f9d700ee95f0d908a4d977a80c0420d52e
b4749c9a449bc87703dda9db60e4562f0bd02c055c49c14704ed2d1e2eb0f4f6
b95487d9ee09dba89976b9b61b3eeb82f72972f270ca149ac0e2e1ea35640d5f
c4c8be0c939e4c24e11bad90549e3951b7969e78056d819425ca53e87af8d8ed
c5320ee1e5753c5cec7611e4c61aaf23778b5924aefac3a546318de7319581bc
c532d28f9700abba1a4803c3a9d886c8c4fb26f84cf2399c533d68cfdcec4fa7
cb0848a6f24a6a37bbceffa8dedade918f3a0717ceeff63bbb997b608823214f
cce74c82a718be7484abf7c51011793f2717cfb2068c92aa35416a93cbd13cfa
cf7fa7f54b06b09b750b8c50e4f8893e25ceaccfa9be8225f3279dc4e4ce0f4d
d0f05cd6957e1e93d1ca4154762b4d4bcaeb16c0bf878b59a1500c4974ef4502
d1949c75e7cb8e57f52e714728817ce323f6980c8c09e161c9e54a1e72777c13
d408fe3421f520710e8a6ac6f0b9a1759b03ab3f44134e451d72af3bb79a3ad0
d5770cd6451de0c45426fae230e41f3551af1c9dda690d2be44f69be3721d929



dc90ba17158501e8f6589d3805789f9ac51cefaafec63d6e00e10c7e0355faab	
dd32c037ed9b72acb6eda4f5193c7f1adc1e7e8d2aefcdd4b16de2f48420e1d3	
df5b004be71717362e6b1ad22072f9ee4113b95b5d78c496a90857977a9fb415	
e05791112b72f7430b74138bac4d4efcd2fbd1909714f8366a43eab77b26b13e	
e28188e516db1bda9015c30de59a2e91996b67c2e2b44989a6b0f562577fd757	
e686a6e3b9598c588202794f7670c2356e7bc80ecb69113eb3062ae4b57e7396	
e9fef053b8c77c7db13d528b97d2b974dfd86775a8cc9c53b8efd07db8842c	
eb758d64b49aec914b175165f232aeb8928a841566c083114e97844841afd82c	
ef2a754a8e713fd6deaa642e2220af372fd310a755a02126938ff233b16a4a83	
f0addbafed09fa1d3a5edfe56356475f1af5d711403c800617bcde9b22585d24	
f4f471241714fbf24a103f8a7fce00fecdf795dbf6edbc6420e34834cb93eb53	
f79188b716aeb2eaa34bce17f066aca3bbdf676b7977fe36b8277fd651dea251	
fbe5690e3a17947a9e208a1730d08e2496f27e1c62cac146fb567c63d781a1b6	
fe87fa7714266548fa5da52455f1788f588417ee800c86768d163abd279d0279	
fff35c2da67eef6f1a10c585b427ac32e7f06f4e4460542207abcd62264e435f	

## FortiGuard Labs Guidance

Due to the ease of disruption, damage to daily operations, potential impact to an organization's reputation, and the unwanted destruction or release of personally identifiable information (PII), etc., it is vital to keep all AV and IPS signatures up to date.

Since the majority of ransomware is delivered via phishing, organizations should consider leveraging Fortinet solutions designed to train users to understand and detect

phishing threats:

- The **FortiPhish Phishing Simulation Service** uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.
- Our FREE **NSE training: NSE 1 – Information Security Awareness** includes a module on internet threats designed to help end users learn how to identify and protect themselves from various types of phishing attacks and can be easily added to internal training programs.

Organizations will need to make foundational changes to the frequency, location, and security of their data backups to effectively deal with the evolving and rapidly expanding risk of ransomware. When coupled with digital supply chain compromise and a workforce telecommuting into the network, there is a real risk that attacks can come from anywhere. Cloud-based security solutions, such as **SASE**, to protect off-network devices; advanced endpoint security, such as **EDR** (endpoint detection and response) solutions that can disrupt malware mid-attack; and **Zero Trust Access** and network segmentation strategies that restrict access to applications and resources based on policy and context, should all be investigated to minimize risk and to reduce the impact of a successful ransomware attack.

As part of the industry's leading fully integrated **Security Fabric**, delivering native synergy and automation across your security ecosystem, Fortinet also provides an extensive portfolio of technology and human-based as-a-service offerings. These services are powered by our global FortiGuard team of seasoned cybersecurity experts.

## Best Practices include Not Paying a Ransom

Organizations such as CISA, NCSC, the **FBI**, and HHS caution ransomware victims against paying a ransom partly because the payment does not guarantee that files will be recovered. According to a **U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) advisory**, ransom payments may also embolden adversaries to target additional organizations, encourage other criminal actors to distribute ransomware, and/or fund illicit activities that could potentially be illegal. For organizations and individuals affected by ransomware, the FBI has a Ransomware Complaint **page** where victims can submit samples of ransomware activity via their Internet Crimes Complaint Center (IC3).

## How Fortinet Can Help

FortiGuard Labs' **Emergency Incident Response Service** provides rapid and effective response when an incident is detected. And our **Incident Readiness Subscription Service** provides tools and guidance to help you better prepare for a cyber incident through readiness assessments, IR playbook development, and IR playbook testing (tabletop exercises).

*Learn more about Fortinet's **FortiGuard Labs** threat research and intelligence organization and the FortiGuard AI-powered security **services portfolio**.*

---

## Related Posts



### **FORTIGUARD LABS THREAT RESEARCH**

Ransomware Roundup - Gwisin, Kriptor, Cuba, and More



### **FORTIGUARD LABS THREAT RESEARCH**

Ransomware Roundup - New FBI, Wise Guys, and "Psychedelic"

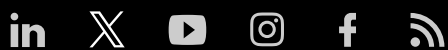


## **FORTIGUARD LABS THREAT RESEARCH**

Ransomware Roundup – Monti, BlackHunt, and Putin

---

**FORTINET®**



News & Articles

News Releases

News Articles

Security Research

Threat Research

FortiGuard Labs

Threat Map

Ransomware Prevention

Connect With Us

Fortinet Community

Partner Portal

Investor Relations

Product Certifications

Company

About Us

Exec Mgmt

Careers



[Training](#)

[Events](#)

[Industry Awards](#)

[Social Responsibility](#)

[CyberGlossary](#)

[Sitemap](#)

[Blog Sitemap](#)

[Contact Us](#)

[\(866\) 868-3678](#)

Copyright © 2025 Fortinet, Inc. All Rights Reserved | [Terms of Services](#) | [Privacy Policy](#) | [Cookie Settings](#)

Also of Interest:

[Progress against vulnerabilities](#)

[Network Security Vulnerabilities](#)

[Ten Best Practices for Outsmarting Ransomware](#)

[SamSam and WannaCry: Part of a Larger Security...](#)