

# Examining the Black Basta Ransomware's Infection Routine

[trendmicro.com/en\\_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html](https://trendmicro.com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html)

May 9, 2022



## Ransomware

We analyze the Black Basta ransomware and examine the malicious actor's familiar infection tactics.

By: Ieriz Nicolle Gonzalez, Ivan Nicole Chavez, Katherine Casona, Nathaniel Morales, Don Ovid Ladores May 09, 2022

Read time: ( words)

Black Basta, a new [ransomware](#) gang, has swiftly risen to prominence in recent weeks after it caused massive breaches to organizations in a short span of time.

On April 20, 2022, a user named Black Basta posted on underground forums known as XSS.IS and EXPLOIT.IN to advertise that it intends to buy and monetize corporate network access credentials for a share of the profits. The advertisement also specified that it was looking for organizations based in the United States, Canada, United Kingdom, Australia, and New Zealand, which are all English-speaking countries. A [report](#) noted that malicious actors acquired stolen credentials from some darknet websites that peddle an enormous amount of exfiltrated data to the underground market.

On April 26, Twitter user PCrisk [tweeted](#) about the new Black Basta ransomware that appends the extension .basta and changes the desktop wallpaper.

This blog entry takes a closer look at the Black Basta ransomware and analyzes this newcomer's familiar infection techniques.

## The infection routine

Black Basta ransomware needs administrator rights to run. It otherwise displays a command prompt message as shown on Figure 1.

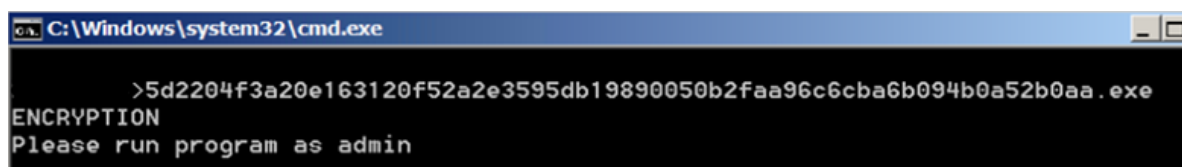


Figure 1. A

command prompt is displayed if Black Basta ransomware is not run with administrator rights.

After running the ransomware as administrator, it removes shadow copies, disables Windows recovery and repair, and boots the PC in safe mode.

- C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet
- C:\Windows\SysNative\bcdedit.exe /deletevalue safeboot
- C:\Windows\SysNative\bcdedit /set safeboot networkChanges

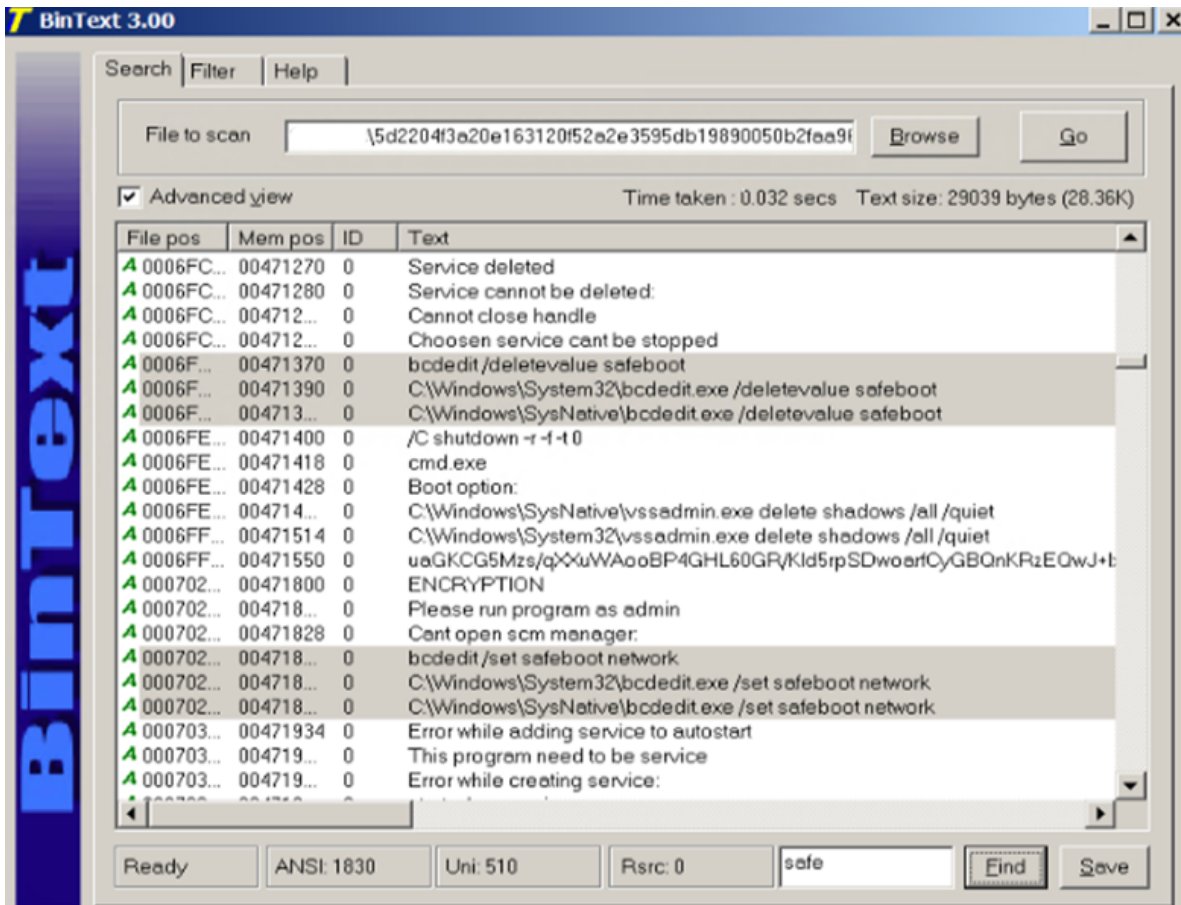


Figure 2.

Commands such as "C:\Windows\SysNative\bcdedit /set safeboot networkChanges" are embedded in the binary and can be viewed easily.

It also drops the following files, which will be used later when changing the desktop wallpaper and icons for encrypted files:

- %Temp%\fkdsadasd.ico
- %Temp%\dlaksjdoiwq.jpg

Before booting the infected device into safe mode, it changes the desktop wallpaper by dropping the .jpg file into the %temp% folder and creating the following registry entry:

Key: HKCU\Control Panel\Desktop; Value: Wallpaper; Data:%Temp%\dlaksjdoiwq.jpg;

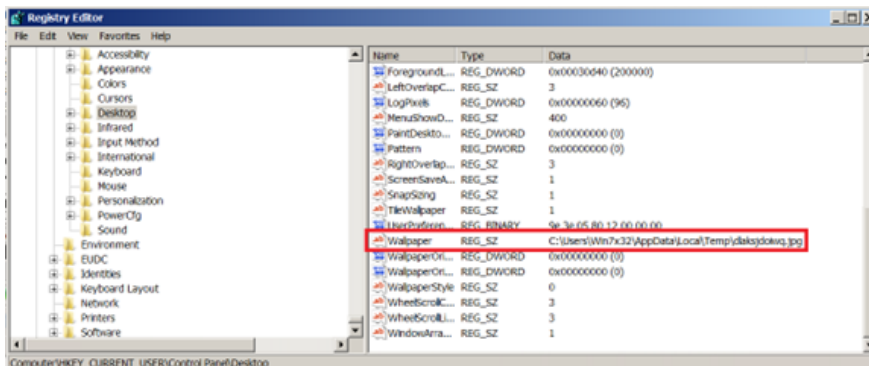


Figure 3. The registry entry created after

Black Basta ransomware changes the wallpaper on the infected machine

# Your network is encrypted by the Black Basta group. Instructions in the file readme.txt

Figure 4. The desktop wallpaper created by the ransomware from the .jpg file dropped in the %temp% folder  
After changing the desktop wallpaper, it then adds the following registry keys to change the icon of the encrypted files with the .basta extension:

- HKLM\SOFTWARE\Classes\.basta
- HKLM\SOFTWARE\Classes\.basta\DefaultIcon data: %TEMP%\fkdsadasd.ico

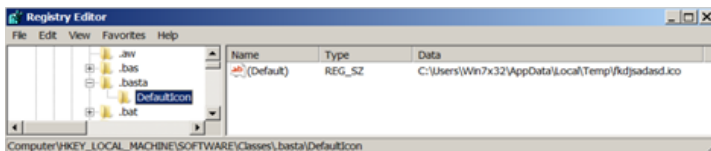


Figure 5. The registry keys added by the ransomware to

change the icon of the files with the .basta extension

The ransomware proceeds to encrypt files while the device is in safe mode, appending all encrypted files with the .basta extension. The ransom note is found in all the folders the ransomware has affected.

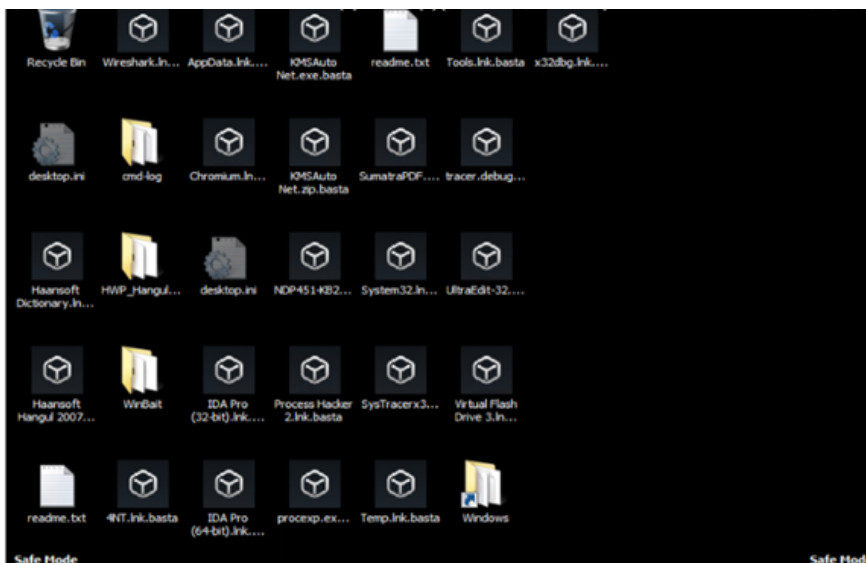


Figure 6. The infected files shown with the

.basta extension

The ransom note indicates the malicious actor's onion site and a company ID. Despite running the same ransomware (SHA256 hash: 5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa) on different virtual machines, the company ID the gang provides is the same across all devices.

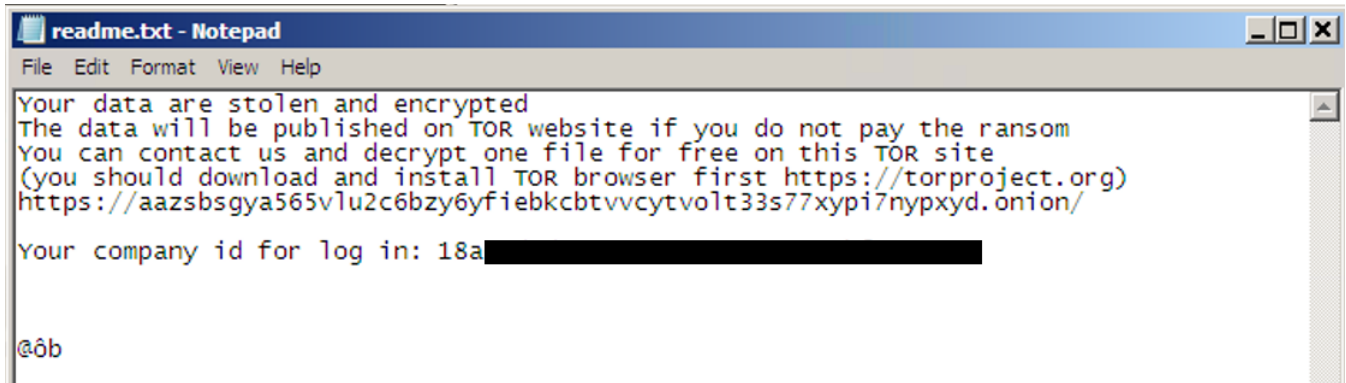


Figure 7. The ransom note dropped by Black Basta

Using another binary (SHA256 hash: 7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a), a different company ID is shown on the ransom note. The files are likewise appended with the .basta extension.

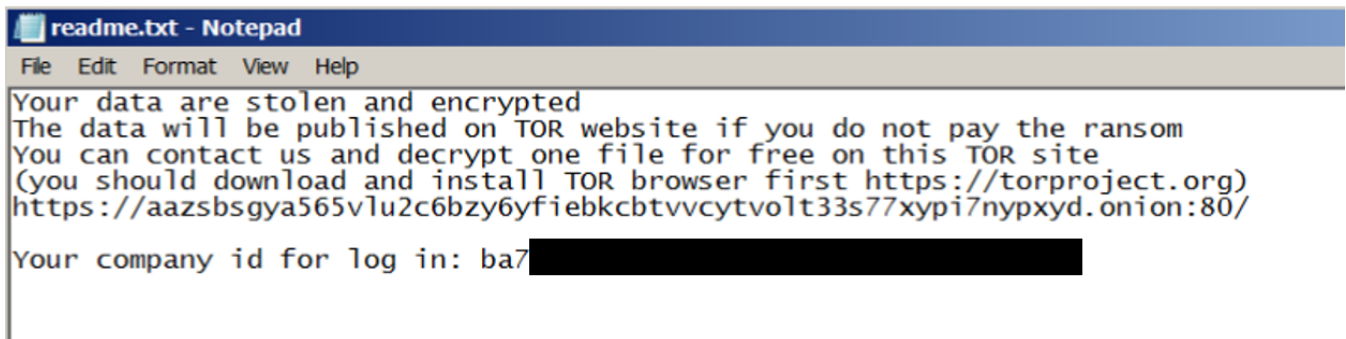


Figure 8. A different company ID is given when another binary is used.

Analyzing the infection routine

Black Basta's recent entry to the cybercrime world suggests that information about their operations is still limited. According to a [report](#), the gang has neither started marketing its operations nor has it begun recruitment of affiliates in underground forums. Based on advertisements they posted before the attacks, the malicious actor likely uses stolen credentials — purchased in darknet websites or underground forums — to get into an organization's system.

We probed further and found that the company ID written in the ransom note is hardcoded in the binary file.



Address	Hex dump	ASCII
00FD7000	59 6F 75 72 20 64 61 74 61 20 61 72 65 20 73 74	Your data are st
00FD7010	6F 6C 65 6E 20 61 6E 64 20 65 6E 63 72 79 70 74	olen and encrypt
00FD7020	65 64 0D 0A 54 68 65 20 64 61 74 61 20 77 69 6C	ed..The data wil
00FD7030	6C 20 62 65 20 70 75 62 6C 69 73 68 65 64 20 6F	l be published o
00FD7040	6E 20 54 4F 52 20 77 65 62 73 69 74 65 20 69 66	n TOR website if
00FD7050	20 79 6F 75 20 64 6F 20 6E 6F 74 20 70 61 79 20	you do not pay
00FD7060	74 68 65 20 72 61 6E 73 6F 6D 0D 0A 59 6F 75 20	the ransom..You
00FD7070	63 61 6E 20 63 6F 6E 74 61 63 74 20 75 73 20 61	can contact us a
00FD7080	6E 64 20 64 65 63 72 79 70 74 20 6F 6E 65 20 66	nd decrypt one f
00FD7090	69 6C 65 20 66 6F 72 20 66 72 65 65 20 6F 6E 20	ile for free on
00FD70A0	74 68 69 73 20 54 4F 52 20 73 69 74 65 0D 0A 28	this TOR site..(
00FD70B0	79 6F 75 20 73 68 6F 75 6C 64 20 64 6F 77 6E 6C	you should downl
00FD70C0	6F 61 64 20 61 6E 64 20 69 6E 73 74 61 6C 6C 20	oad and install
00FD70D0	54 4F 52 20 62 72 6F 77 73 65 72 20 66 69 72 73	TOR browser firs
00FD70E0	74 20 68 74 74 70 73 3A 2F 2F 74 6F 72 70 72 6F	t https://torpro
00FD70F0	6A 65 63 74 2E 6F 72 67 29 0D 0A 68 74 74 70 73	ject.org)..https
00FD7100	3A 2F 2F 61 61 7A 73 62 73 67 79 61 35 36 35 76	://aazsbsgya565v
00FD7110	6C 75 32 63 36 62 7A 79 36 79 66 69 65 62 6B 63	lu2c6bzy6yfiebk
00FD7120	62 74 76 76 63 79 74 76 6F 6C 74 33 33 73 37 37	btvucytvolt33s77
00FD7130	78 79 70 69 37 6E 79 70 78 79 64 2E 6F 6E 69 6F	xypi7nypxyd.onio
00FD7140	6E 2F 0D 0A 0D 0A 59 6F 75 72 20 63 6F 6D 70 61	n/....Your compa
00FD7150	6E 79 20 69 64 20 66 6F 72 20 6C 6F 67 20 69 6E	ny id for log in
00FD7160		: 18a
00FD7170		
00FD7180		
00FD7190	F4 62 00 00 3E 42 00 00 01 00 00 00 08 00 00 00	ôb...>B.. ...□..

Figure 9. The company ID in the ransom note is hardcoded in the binary file.

Black Basta attempts to delete shadow copies using vssadmin.exe and boots the device in safe mode using bcdedit.exe from different paths, specifically, %SysNative% and %System32%.

005C780	48 A10FC00	PUSH bb.00C180	ASCII "bcdedit /set safeboot network"
005C782	E8 4014000	CALL cb.create_process	
005C797	68 CA1FC00	PUSH bb.00C180	ASCII "C:\Windows\System32\bcdedit.exe /set safeboot network"
005C79C	E8 6314000	CALL cb.create_process	
005C7A1	48 F31FC00	PUSH bb.00C180	ASCII "C:\Windows\SysNative\bcdedit.exe /set safeboot network"
005C7A6	E8 5914000	CALL cb.create_process	
00FAB3CE	> FF75 2C	PUSH DWORD PTR SS:[EBP+2C]	pProcessInfo
00FAB3D1	. FF75 28	PUSH DWORD PTR SS:[EBP+28]	pStartupInfo
00FAB3D4	. 53	PUSH EBX	CurrentDir
00FAB3D5	. FF75 20	PUSH DWORD PTR SS:[EBP+20]	pEnvironment
00FAB3D8	. FF75 1C	PUSH DWORD PTR SS:[EBP+1C]	CreationFlags
00FAB3DB	. FF75 18	PUSH DWORD PTR SS:[EBP+18]	InheritHandles
00FAB3DE	. FF75 14	PUSH DWORD PTR SS:[EBP+14]	pThreadSecurity
00FAB3E1	. FF75 10	PUSH DWORD PTR SS:[EBP+10]	pProcessSecurity
00FAB3E4	. FF75 08	PUSH DWORD PTR SS:[EBP-28]	CommandLine
00FAB3E7	. FF75 C0	PUSH DWORD PTR SS:[EBP-A0]	ModuleFileName
00FAB3EA	. FF15 D060FB0	CALL DWORD PTR DS:[<KERNEL32.CreatePro	CreateProcessV

Figure 10. Black Basta's attempts to

delete shadow copies using vssadmin.exe

00FAB3CE	> FF75 2C	PUSH DWORD PTR SS:[EBP+2C]	pProcessInfo
00FAB3D1	. FF75 28	PUSH DWORD PTR SS:[EBP+28]	pStartupInfo
00FAB3D4	. 53	PUSH EBX	CurrentDir
00FAB3D5	. FF75 20	PUSH DWORD PTR SS:[EBP+20]	pEnvironment
00FAB3D8	. FF75 1C	PUSH DWORD PTR SS:[EBP+1C]	CreationFlags
00FAB3DB	. FF75 18	PUSH DWORD PTR SS:[EBP+18]	InheritHandles
00FAB3DE	. FF75 14	PUSH DWORD PTR SS:[EBP+14]	pThreadSecurity
00FAB3E1	. FF75 10	PUSH DWORD PTR SS:[EBP+10]	pProcessSecurity
00FAB3E4	. FF75 08	PUSH DWORD PTR SS:[EBP-28]	CommandLine
00FAB3E7	. FF75 C0	PUSH DWORD PTR SS:[EBP-A0]	ModuleFileName
00FAB3EA	. FF15 D060FB0	CALL DWORD PTR DS:[<KERNEL32.CreatePro	CreateProcessV
0015F810	00FAB3F0	CALL to CreateProcessV from bb.00FAB3EA	
0015F814	002805E8	ModuleFileName = "C:\Windows\system32\cmd.exe"	
0015F818	00294228	CommandLine = "C:\Windows\system32\cmd.exe /c bcdedit /set safeboot network"	
0015F81C	00000000	pProcessSecurity = NULL	
0015F820	00000000	pThreadSecurity = NULL	
0015F824	00000001	InheritHandles = TRUE	
0015F828	00000000	CreationFlags = 0	
0015F82C	00000000	pEnvironment = NULL	
0015F830	00000000	CurrentDir = NULL	
0015F834	0015F8D4	pStartupInfo = 0015F8D4	
0015F838	0015F918	pProcessInfo = 0015F918	

Figure 11. Black Basta boots the device in

safe mode using bcdedit.exe from different paths, specifically, %SysNative% and %System32%.

At this stage, the ransomware deletes the service named Fax, and creates a new one with the same name using the malware's path and adds it to the registry for persistence.

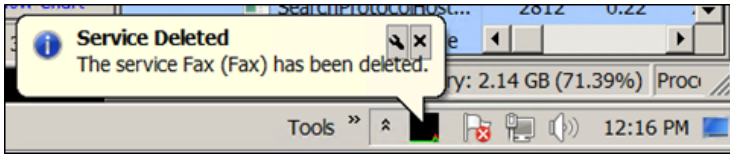


Figure 12. Pop-up notification when the Fax service is

deleted

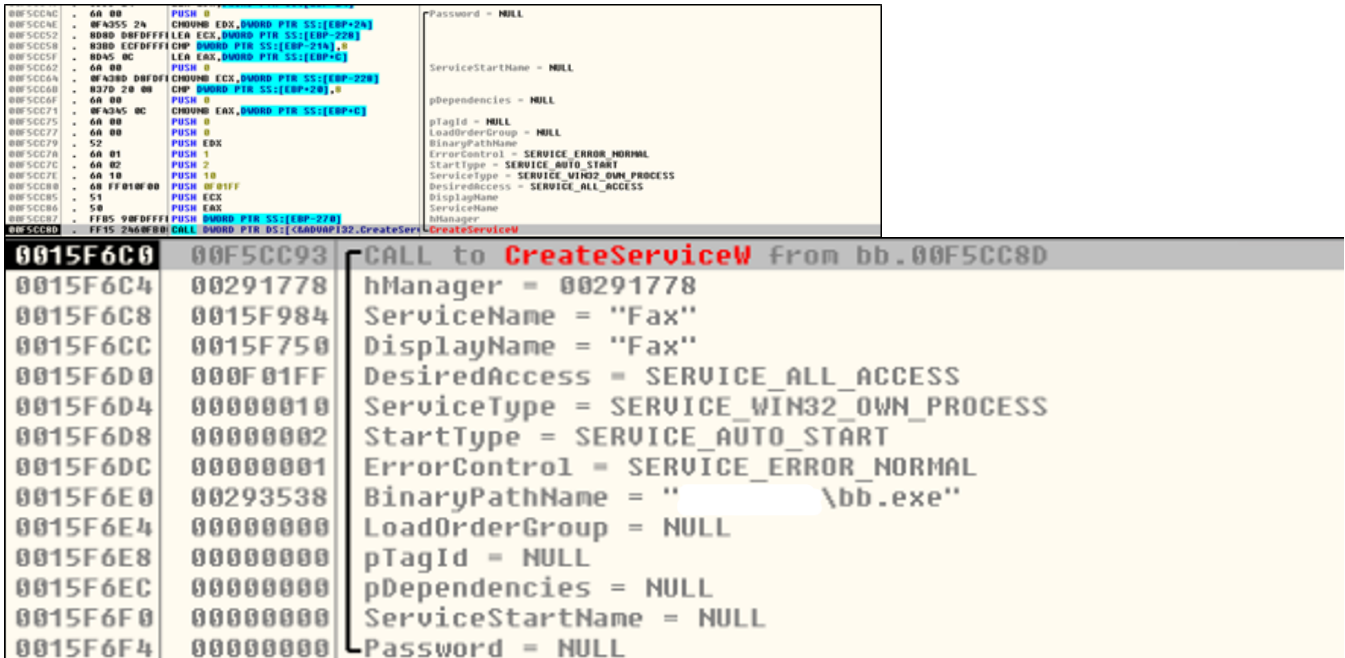


Figure 13. Functions used in creating a new service, also named “Fax,” that uses the file path of the malware as its binary path name

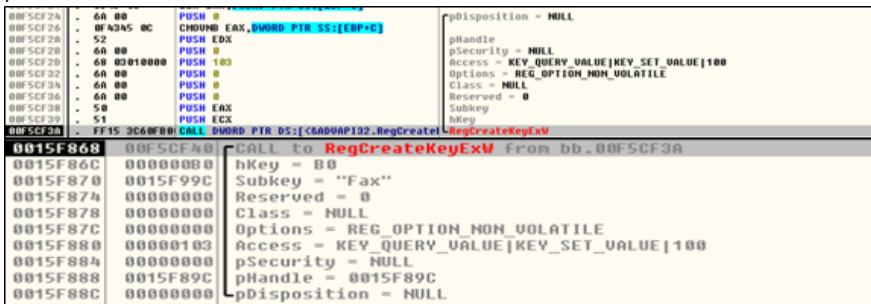


Figure 14. Functions used when creating

a registry key

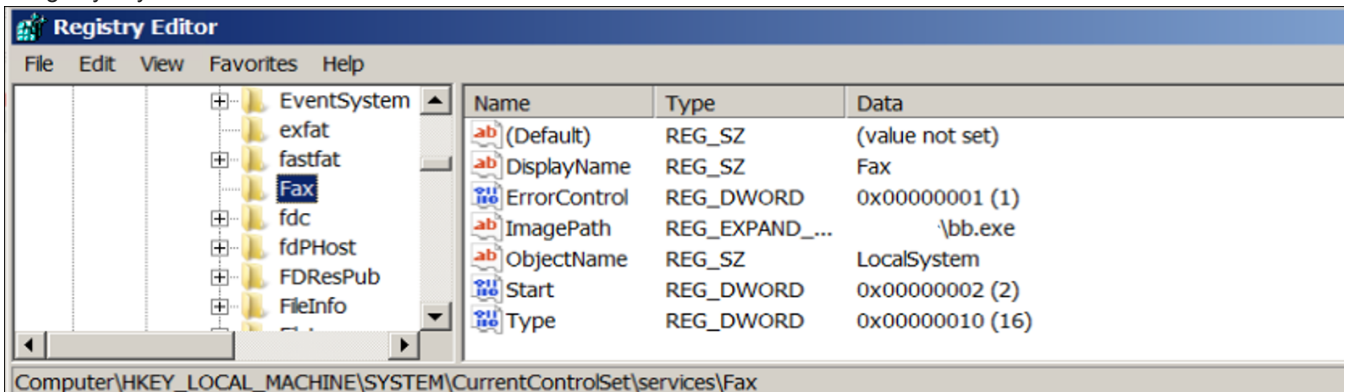


Figure 15. New registry key created for the new “Fax” service that replaces the deleted service It then uses ShellExecuteA to shut down and restart the victim’s machine.



Figure 16. Function ShellExecuteA used

to shut down and restart the victim’s machine

## Extortion phase

For a newcomer in the field, Black Basta is quite prolific for having compromised at least a dozen organizations in just a few weeks. The group's [first known attack](#) using the Black Basta ransomware occurred in the second week of April 2022. But an [earlier sample](#) was also spotted back in February 2022 with the ransomware name "no\_name\_software," which appends the extension "encrypted" to encrypted files. According to some [threat researchers](#), it appears that Black Basta has been in development since early February 2022.

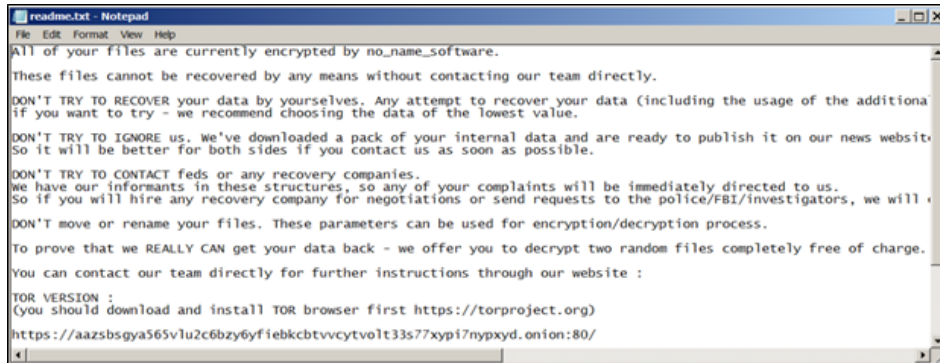


Figure 17. Ransom note used in an

earlier sample

Like other enterprise-focused ransomware operations, Black Basta employs a [double extortion](#) scheme that involves exfiltrating confidential data before encryption to threaten victims with public release of the stolen data.

The gang carries out the extortion phase of its attacks on its Tor site, Basta News, which contains a list of all the victims who have not paid the ransom.

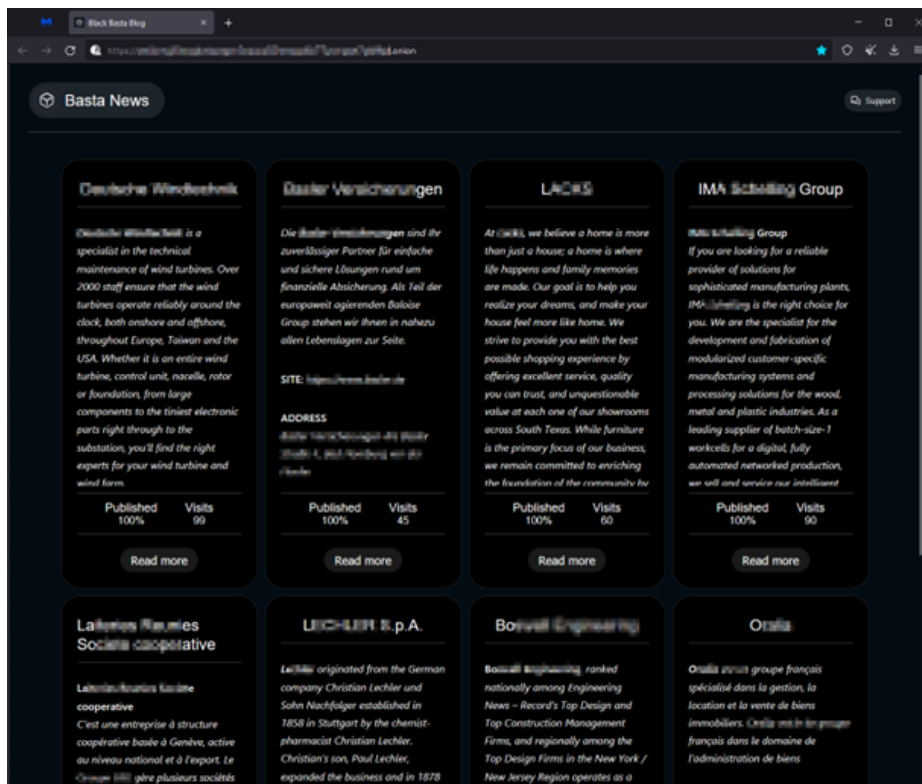


Figure 18. Black Basta's leak site,

retrieved from <https://twitter.com/MarceloRivero/status/1519398885193654273>

Possible relation to an APT

Security researchers exchanged speculations on Twitter that Black Basta is possibly a rebranding of the [Conti](#) ransomware operation. [MalwareHunterTeam](#) pointed out many similarities in its leak site, payment site, and negotiation style to those of Conti's. Twitter user [Arkbird](#) echoed the same observation. Lawrence Abrams of BleepingComputer also mentioned that the malicious actors behind Black Basta seem like they are exerting a lot of effort to avoid any resemblance to their previous identity.



We have also noticed some similarities between the Black Basta and Black Matter payment sites. Like Black Matter, Black Basta implements user verification on its Tor site. However, the leak site does not implement a session key.



Figure 19. The Black Matter payment site

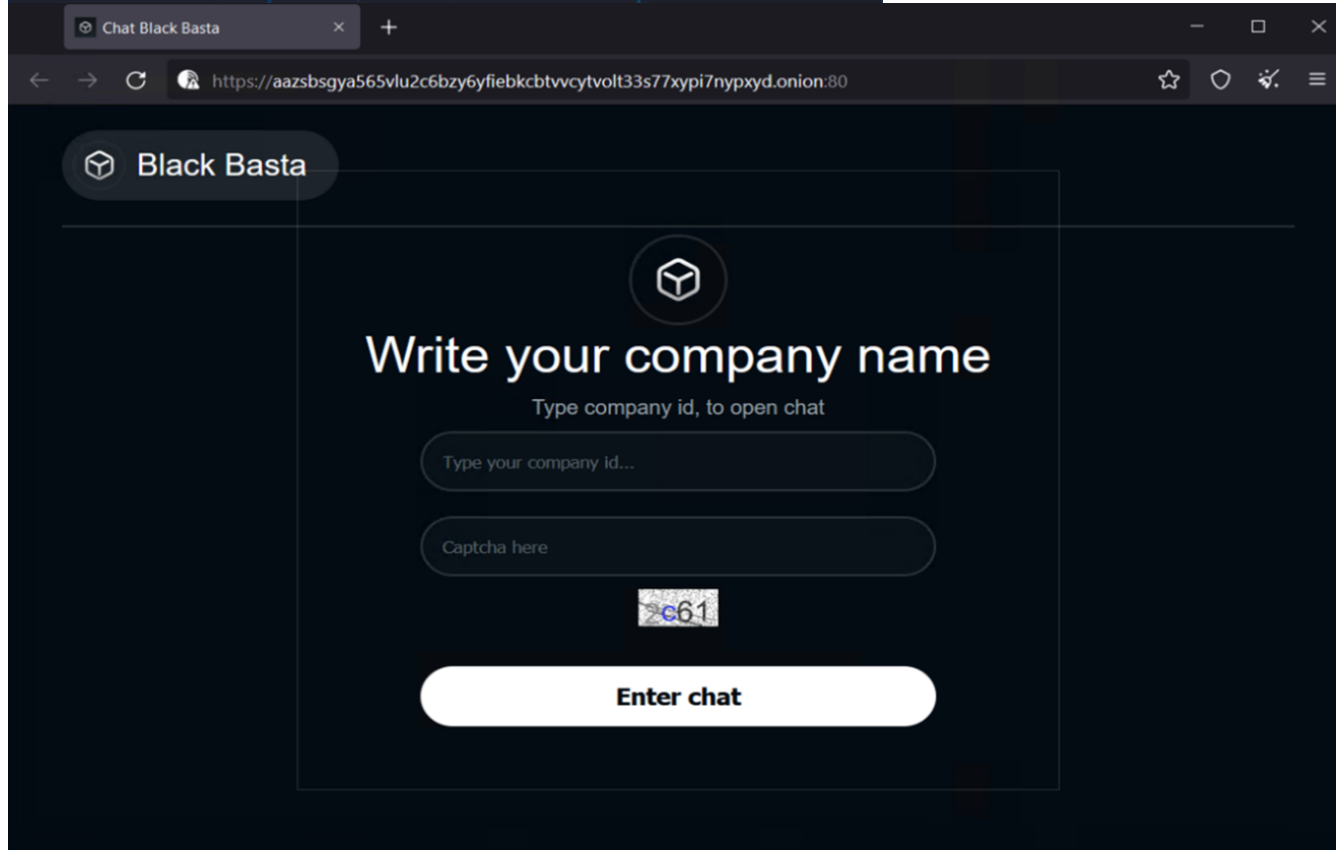


Figure 20. The Black Basta payment site  
New findings: QAKBOT possibly related to Black Basta

Based on our analysis of another set of samples monitored within a 72-hour timeframe, we discovered a possible correlation between QAKBOT and Black Basta ransomware. We observed the following:

- As with QAKBOT, the malware is downloaded and executed from a malicious Excel file. Similar to the typical routine of the QAKBOT binary, it then executes certain PowerShell commands as part of its staging phase.
- From information gathered in our telemetry, we found the presence of the Black Basta ransomware within the 72-hour period in which it encrypted files on victims' machine. Trend Micro detects this as Ransom.Win32.BASTACRYPT.YACEDT.
- Other researchers pointed out that QAKBOT deploys its version of the exploit PRINTNIGHTMARE (aka QUAKNIGHTMARE) during the same timeframe. We also observed the presence of the weaponized exploit. This, in turn, executes another binary with escalated privilege. Unfortunately, we were unable to find the presence of the file pointed by the hardcoded path. string to complete the attack chain. Trend Micro detects this as Trojan.Win64.QUAKNIGHTMARE.YACEJT.

Malicious actors also use certain tools as seen through our sensors, but we were unable to obtain the complete kit. We have so far gathered paths related to the tools themselves that include the following:

- AdwareCleaner (C:\AdwCleaner\*)



- Either PC-Cleaner or Pervasive PSQL/SQL (C:\pvs\\*)

The structure of the ransomware loader is also different from the external article. In this case, instead of dropping and executing the ransomware itself, the loader downloads to the device's memory then uses reflective loading to launch the ransomware.

The information we have collected so far indicates that the malicious actor behind Black Basta possibly used QAKBOT as a new means to deliver the ransomware.

## Insights

The malicious actors could be using a unique binary for each organization that they target. This can be seen from the ransom note that they drop, which is hardcoded in the malware itself. A ransomware typically creates a unique ID for each victim despite being infected by the same executable. Their choice of target organizations also suggests this to be the case. They buy corporate network access credentials in underground markets, which could mean that they do not distribute their malware sporadically. Instead, they use a certain kind of binary or variant for a specific organization.

## Recommendations

Threat researchers suggest that the recent attacks by Black Basta can be seen as early manifestations of Conti's rebranding efforts. True or not, organizations should keep a watchful eye against ransomware threats. An organization's thorough assessment of its security posture and its implementation of solid cybersecurity defenses give it a better fighting chance against such threats.

To protect systems against similar attacks, organizations can establish security frameworks that allocate resources systematically for establishing a strong defense strategy against ransomware. Here are some best practices that organizations can consider:

### Audit and inventory

- Take an inventory of assets and data
- Identify authorized and unauthorized devices and software
- Audit event and incident logs

### Configure and monitor

- Manage hardware and software configurations
- Grant admin privileges and access only when necessary to an employee's role
- Monitor network ports, protocols, and services
- Activate security configurations on network infrastructure devices such as firewalls and routers
- Establish a software allowlist that only executes legitimate applications

### Patch and update

- Conduct regular vulnerability assessments
- Perform patching or virtual patching for operating systems and applications
- Update software and applications to their latest versions

### Protect and recover

- Implement data protection, backup, and recovery measures
- Enable multifactor authentication (MFA)

### Secure and defend

- Employ sandbox analysis to block malicious emails
- Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network
- Detect early signs of an attack such as the presence of suspicious tools in the system
- Use advanced detection technologies such as those powered by AI and machine learning

### Train and test

- Regularly train and assess employees in security skills
- Conduct red-team exercises and penetration tests

A multilayered approach can help organizations guard possible entry points into their system (endpoint, email, web, and network). Security solutions can detect malicious components and suspicious behavior, which can help protect enterprises.

- [Trend Micro Vision One™](#) provides multilayered protection and behavior detection, which helps block questionable behavior and tools before the ransomware can do any damage.
- [Trend Micro Cloud One™ – Workload Security](#) protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.
- [Trend Micro™ Deep Discovery™ Email Inspector](#) employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.
- [Trend Micro Apex One™](#) offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

### Indicators of compromise (IOCs)

SHA256	Trend Micro Detection
5d2204f3a20e163120f52a2e3595db19890050b2faa96c6c6ba6b094b0a52b0aa	Ransom.Win32.BASTACRYPT.THDBGGB
7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a	Ransom.Win32.BASTACRYPT.YXCD2
ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e	Ransom.Win32.BASTACRYPT.THDBIBB
17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90	Ransom.Win32.BASTACRYPT.YXCD2
a54fef5fe2af58f5bd75c3af44f1fba22b721f34406c5963b19c5376ab278cd1	Ransom.Win32.BASTACRYPT.THDBGGB
1d040540c3c2ed8f73e04c578e7fb96d0b47d858bbb67e9b39ec2f4674b04250	Ransom.Win32.BASTACRYPT.YXCD2
2967e1d97d32605fc5ace49a10828800fbefcc1e010f6004a9c88ef3ecdad88	Ransom.Win32.BASTACRYPT.YXCD2.note
f088e6944b2632bb7c93fa3c7ba1707914c05c00f9491e033f78a709d65d7cff	Ransom.Win32.BASTACRYPT.YXCD2.note

### For QAKBOT-related samples:

SHA256	Trend Micro Detections
a48ac26aa9cdd3bc7f219a84f49201a58d545fceb0646ae1d676c7e43c6ac3e	TrojanSpy.Win32.QAKBOT.YACEDT
82c73538322c8b90c25a99a7afc2fafcd7e7e03fe920a3331ef0003300ac10b8	TrojanSpy.Win32.QAKBOT.YACEDT
82c73538322c8b90c25a99a7afc2fafcd7e7e03fe920a3331ef0003300ac10b8	TrojanSpy.Win32.QAKBOT.YACEDT
2083e4c80ade0ac39365365d55b243dbac2a1b5c3a700aad383c110db073f2d9	TrojanSpy.Win32.QAKBOT.YACEDT
2e890fd02c3e0d85d69c698853494c1bab381c38d5272baa2a3c2bc0387684c1	TrojanSpy.Win32.QAKBOT.YACEDT
2d906ed670b24ebc3f6c54e7be5a32096058388886737b1541d793ff5d134ccb	TrojanSpy.Win32.QAKBOT.YACEDT
72fde47d3895b134784b19d664897b36ea6b9b8e19a602a0aaff5183c4ec7d24	TrojanSpy.Win32.QAKBOT.YACEDT
ffa7f0e7a2bb0edf4b7785b99aa39c96d1fe891eb6f89a65d76a57ff04ef17ab	TrojanSpy.Win32.QAKBOT.YACEDT
1e7174f3d815c12562c5c1978af6abbf2d81df16a8724d2a1cf596065f3f15a2	TrojanSpy.Win32.QAKBOT.YACEDT
130af6a91aa9ecbf70456a0bee87f947bf4ddc2d2775459e3feac563007e1aed	Trojan.Win64.QUAKNIGHTMARE.YACEJT
81a6c44682b981172cd85ee4a150ac49f838a65c3a0ed822cb07a1c19dab4af5	Ransom.Win32.BASTACRYPT.YACEDT
94428d7620fff816cb3f65595978c6abb812589861c38052d30fa3c566e32256	Ransom.Win32.BASTACRYPT.YACEDT
c9df12fbfcae3ac0894c1234e376945bc8268acdc20de72c8dd16bf1fab6bb70	Ransom.Win32.BASTACRYPT.YACEJT
0d3af630c03350935a902d0cce4dc64c5cfff8012b2ffc2f4ce5040fdec524ed	Trojan.Win32.BLACKBASTA.YXCEJ

3fe73707c2042fefe56d0f277a3c91b5c943393cf42c2a4c683867d6866116fc	Trojan.Win32.BLACKBASTA.YXCEJ
3fe73707c2042fefe56d0f277a3c91b5c943393cf42c2a4c683867d6866116fc	Trojan.Win32.BLACKBASTA.YXCEJ
0e2b951ae07183c44416ff6fa8d7b8924348701efa75dd3cb14c708537471d27	Trojan.Win32.BLACKBASTA.YXCEJ
8882186bace198be59147bcabae6643d2a7a490ad08298a4428a8e64e24907ad	Trojan.Win32.BLACKBASTA.YXCEJ
df35b45ed34eaca32cda6089acbfe638d2d1a3593d74019b6717afed90dbd5f8	Trojan.Win32.BLACKBASTA.YXCEJ
b8aa8abac2933471e4e6d91cb23e4b2b5a577a3bb9e7b88f95a4ddc91e22b2cb	TrojanSpy.VBS.KEYLOAD.A
fb3340d734c50ce77a9f463121cd3b7f70203493aa9aff304a19a8de83a2d3c9	TrojanSpy.VBS.KEYLOAD.A
5ab605b1047e098638d36a5976b00379353d84bd7e330f5778ebb71719c36878	TrojanSpy.VBS.KEYLOAD.A
9707067b4f53caf43df5759fe40e9121f832e24da5fe5236256ad0e258277d88	TrojanSpy.VBS.KEYLOAD.A
9707067b4f53caf43df5759fe40e9121f832e24da5fe5236256ad0e258277d88	TrojanSpy.VBS.KEYLOAD.A
d7580fd8cc7243b7e16fd97b7c5dea2d54bcba08c298dc2d82613bdc2bd0b4bf	TrojanSpy.VBS.KEYLOAD.A
919d1e712f4b343856cb920e4d6f5d20a7ac18d7386673ded6968c945017f5fd	TrojanSpy.VBS.KEYLOAD.A
012826db8d41ff4d28e3f312c1e6256f0647bf34249a5a6de7ecac452d32d917	TrojanSpy.VBS.KEYLOAD.A
d36a9f3005c5c24649f80722e43535e57fd96729e827cdd2c080d17c6a53a893	TrojanSpy.VBS.KEYLOAD.A
580ce8b7f5a373d5d7fbfbfef5204d18b8f9407b0c2cbf3bcae808f4d642076a	Backdoor.Win32.COROXY.YACEKT