Ransomware

Examining the Black Basta Ransomware's Infection Routine

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 May 09, 2022 Read time: 6 min (1633 words)

Save to Folio

Subscribe

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

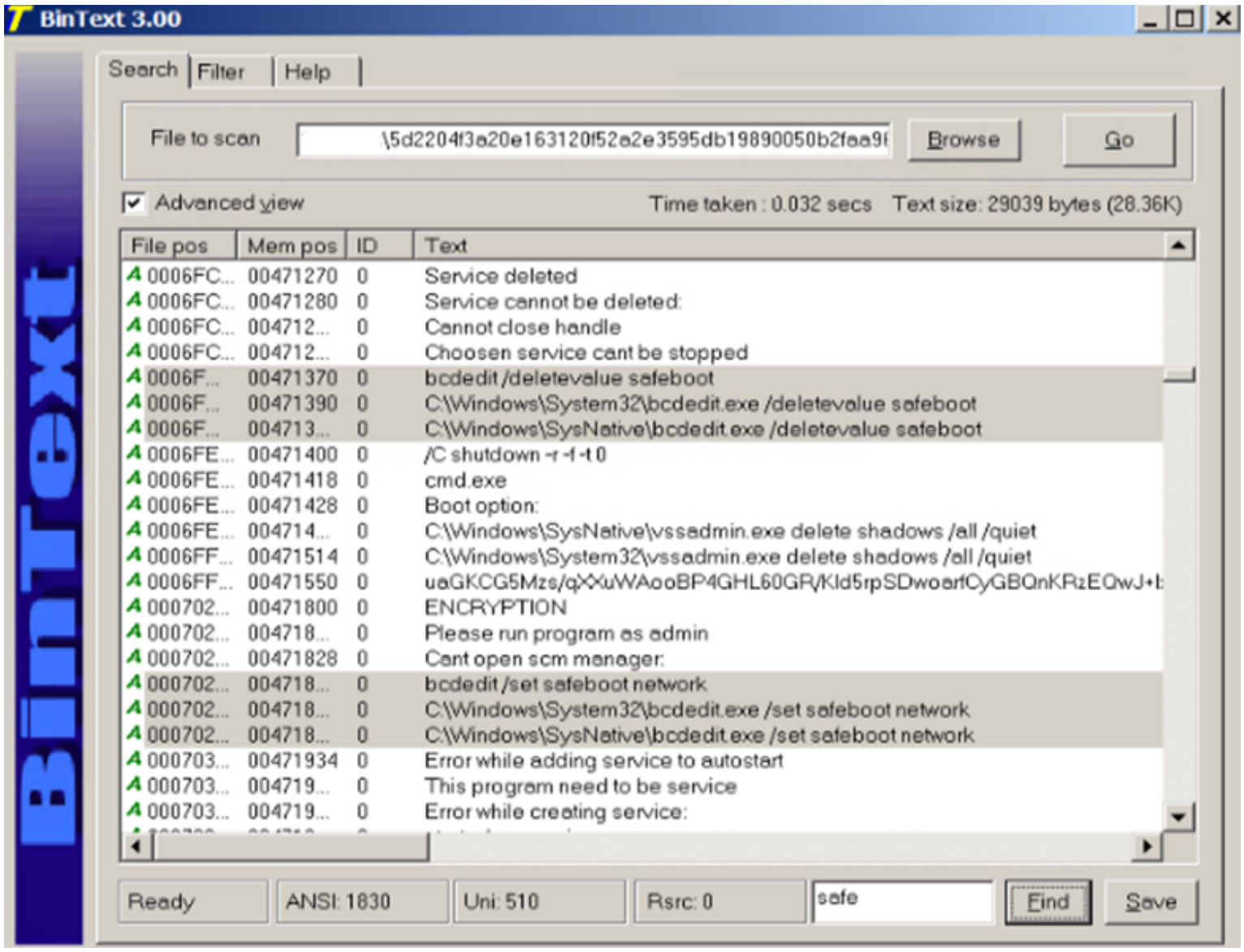


Figure 2. Commands such as "C:\Windows\SysNative\bcedit /set safeboot networkChanges" are embedded in the binary and can be viewed easily.

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

- %Temp%\fkdjsadasd.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;

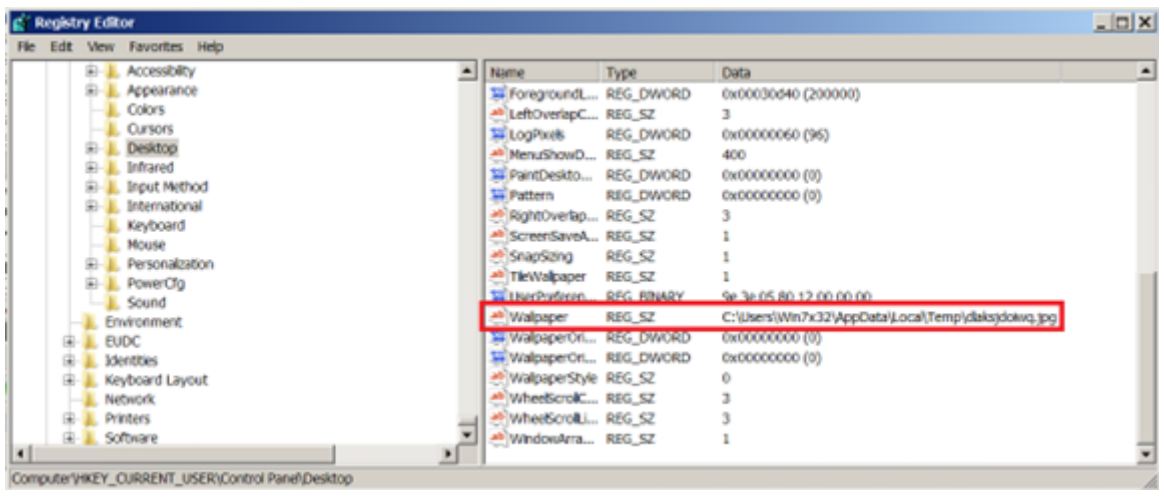


Figure 3. The registry entry created after Black Basta ransomware changes the wallpaper on the infected machine

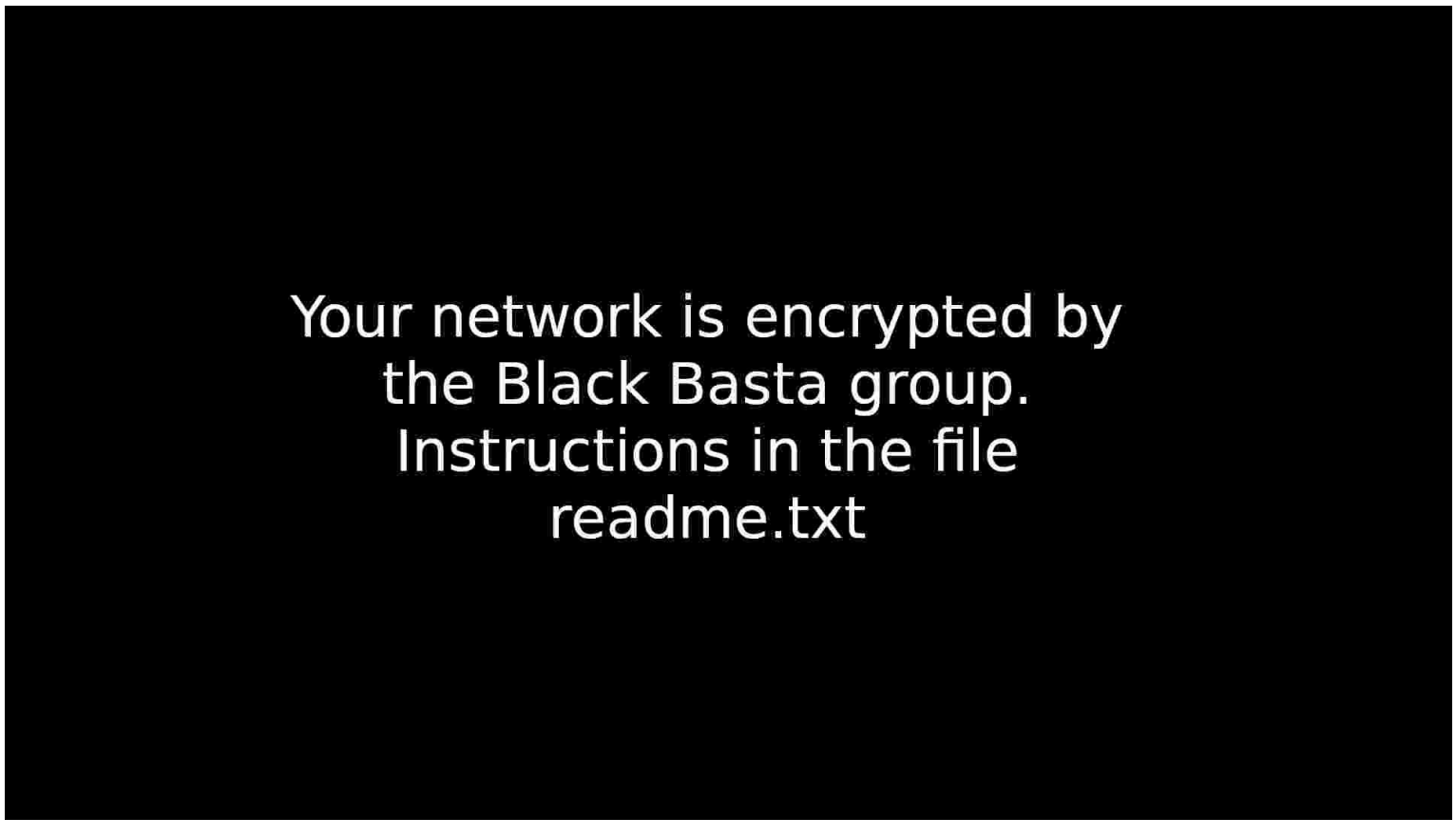


Figure 4. The desktop wallpaper created by the ransomware from the .jpg file dropped in the %temp% folder

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%\fkdjsadasd.ico

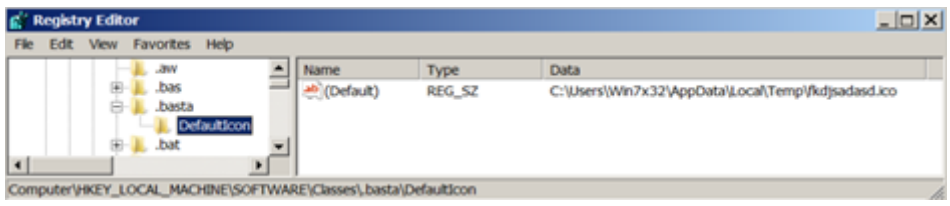


Figure 5. The registry keys added by the ransomware to change the icon of the files with the .basta extension

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.

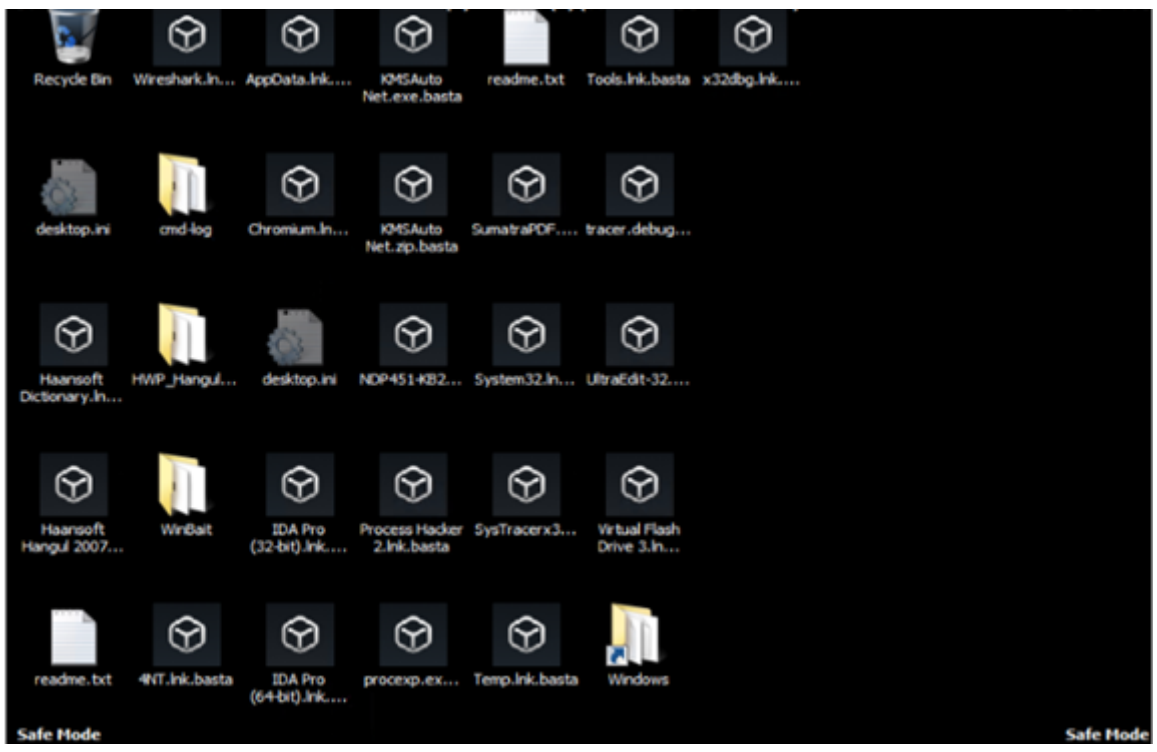


Figure 6. The infected files shown with the .basta extension

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.

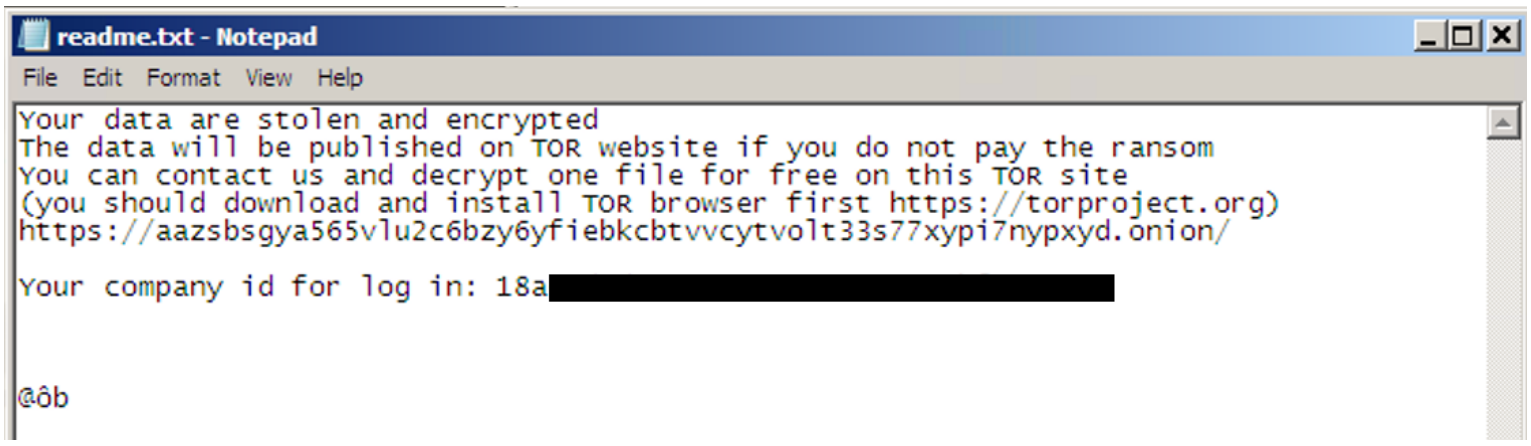


Figure 7. The ransom note dropped by Black Basta

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.

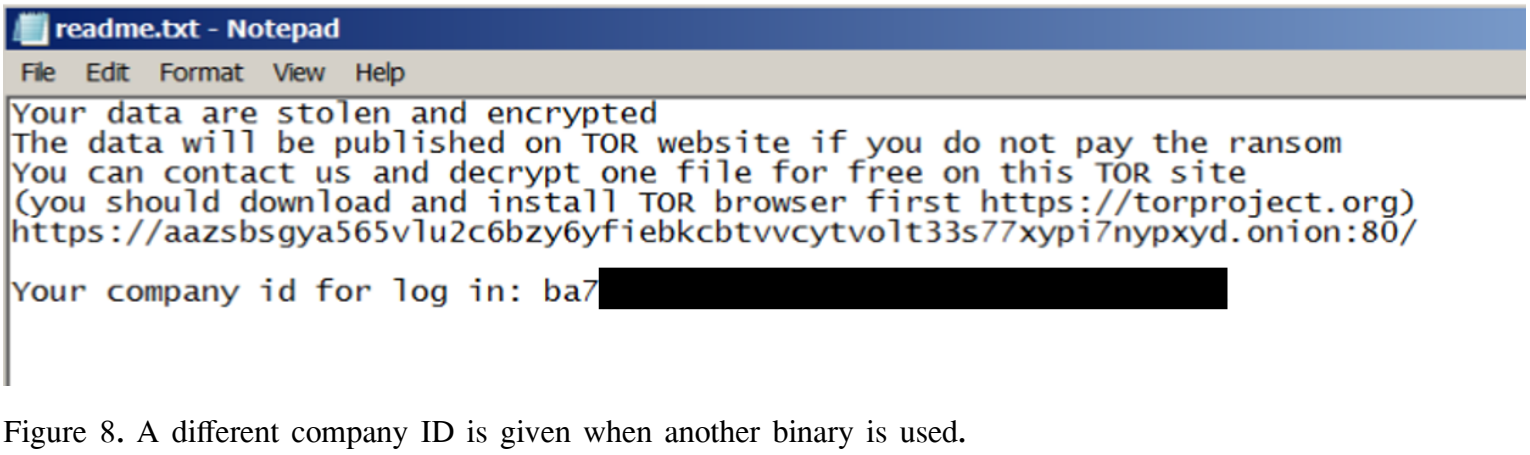


Figure 8. A different company ID is given when another binary is used.

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.

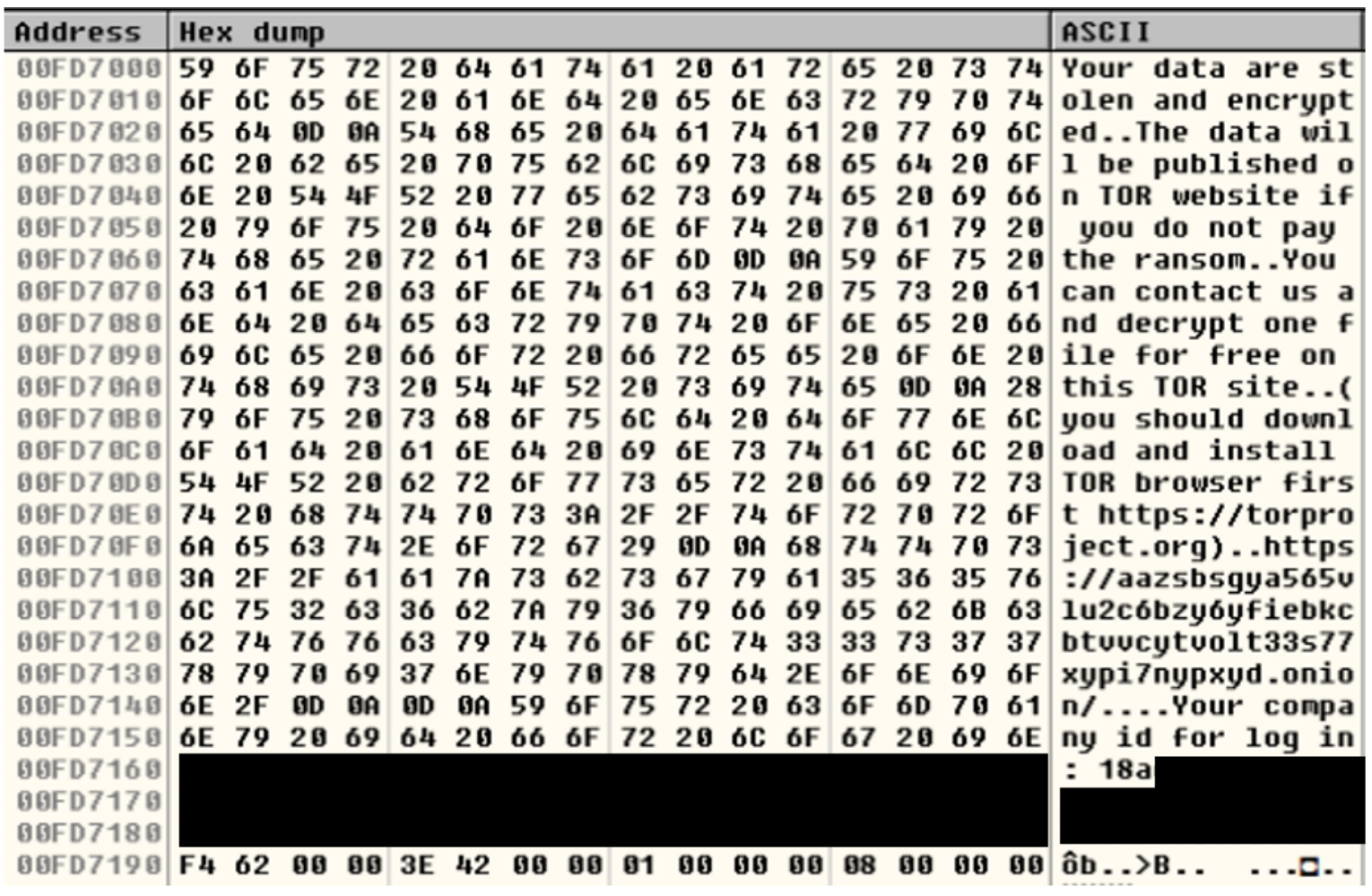
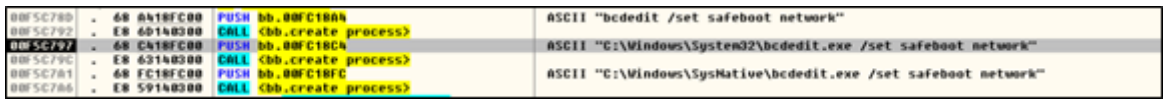


Figure 9. The company ID in the ransom note is hardcoded in the binary file.

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



```
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 D8      PUSH DWORD PTR SS:[EBP-28]      CommandLine
00FAB3E7  .  FF75 C0      PUSH DWORD PTR SS:[EBP-40]      ModuleFileName
00FAB3EA  .  FF15 D060FB0 CALL DWORD PTR DS:[<&KERNEL32.CreatePro  CreateProcessW
```

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 D8      PUSH DWORD PTR SS:[EBP-28]      CommandLine
00FAB3E7  .  FF75 C0      PUSH DWORD PTR SS:[EBP-40]      ModuleFileName
00FAB3EA  .  FF15 D060FB0 CALL DWORD PTR DS:[<&KERNEL32.CreatePro  CreateProcessW
```

```
0015F810  00FAB3F0  CALL to CreateProcessW from bb.00FAB3EA
0015F814  0028B5E8  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 bcdexit.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.

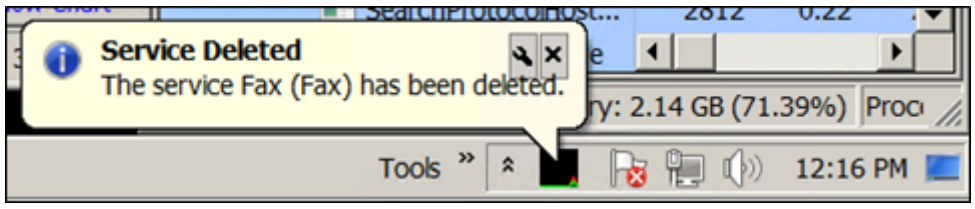


Figure 12. Pop-up notification when the Fax service is deleted

```
00F5CC4C  .  6A 00        PUSH 0                          pPassword = NULL
00F5CC4E  .  0FA355 24    CHOUMB EDX,DWORD PTR SS:[EBP+24]
00F5CC52  .  8D8D D8FDFFF LEA ECX,DWORD PTR SS:[EBP-228]
00F5CC58  .  83BD ECFDFFF CMP DWORD PTR SS:[EBP-214],0
00F5CC5F  .  8D45 0C      LEA EAX,DWORD PTR SS:[EBP+C]
00F5CC62  .  6A 00        PUSH 0                          ServiceStartName = NULL
00F5CC64  .  0FA38D D8FDF CHOUMB ECX,DWORD PTR SS:[EBP-228]
00F5CC6B  .  837D 20 00   CMP DWORD PTR SS:[EBP+20],0
00F5CC6F  .  6A 00        PUSH 0                          pDependencies = NULL
00F5CC71  .  0FA345 0C    CHOUMB EAX,DWORD PTR SS:[EBP+C]
00F5CC75  .  6A 00        PUSH 0                          pTagId = NULL
00F5CC77  .  6A 00        PUSH 0                          LoadOrderGroup = NULL
00F5CC79  .  52           PUSH EDX                        BinaryPathName
00F5CC7A  .  6A 01        PUSH 1                          ErrorControl = SERVICE_ERROR_NORMAL
00F5CC7C  .  6A 02        PUSH 2                          StartType = SERVICE_AUTO_START
00F5CC7E  .  6A 10        PUSH 10                         ServiceType = SERVICE_WIN32_OWN_PROCESS
00F5CC80  .  68 FF01F00   PUSH F01FF                      DesiredAccess = SERVICE_ALL_ACCESS
00F5CC85  .  51           PUSH ECX                        DisplayName
00F5CC86  .  50           PUSH EAX                        ServiceName
00F5CC87  .  FFB5 90FDFFF PUSH DWORD PTR SS:[EBP-270]     hManager
00F5CC8D  .  FF15 2460FB0 CALL DWORD PTR DS:[<&ADVAPI32.CreateServ  CreateServiceW
```

```
0015F6C0  00F5CC93  CALL to CreateServiceW from bb.00F5CC8D
0015F6C4  00291778  hManager = 00291778
0015F6C8  0015F984  ServiceName = "Fax"
0015F6CC  0015F750  DisplayName = "Fax"
0015F6D0  000F01FF  DesiredAccess = SERVICE_ALL_ACCESS
0015F6D4  00000010  ServiceType = SERVICE_WIN32_OWN_PROCESS
0015F6D8  00000002  StartType = SERVICE_AUTO_START
0015F6DC  00000001  ErrorControl = SERVICE_ERROR_NORMAL
0015F6E0  00293538  BinaryPathName = "        \bb.exe"
0015F6E4  00000000  LoadOrderGroup = NULL
0015F6E8  00000000  pTagId = NULL
0015F6EC  00000000  pDependencies = NULL
0015F6F0  00000000  ServiceStartName = NULL
0015F6F4  00000000  Password = NULL
```

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

```
00F5CF24  .  6A 00        PUSH 0                          pDisposition = NULL
00F5CF26  .  0FA345 0C    CHOUMB EAX,DWORD PTR SS:[EBP+C]
00F5CF2A  .  52           PUSH EDX                        pHandle
00F5CF2B  .  6A 00        PUSH 0                          pSecurity = NULL
00F5CF2D  .  68 03010000  PUSH 103                        Access = KEY_QUERY_VALUE|KEY_SET_VALUE|100
00F5CF32  .  6A 00        PUSH 0                          Options = REG_OPTION_NON_VOLATILE
00F5CF34  .  6A 00        PUSH 0                          Class = NULL
00F5CF36  .  6A 00        PUSH 0                          Reserved = 0
00F5CF38  .  50           PUSH EAX                        Subkey
00F5CF39  .  51           PUSH ECX                        hKey
00F5CF3A  .  FF15 3C60FB0 CALL DWORD PTR DS:[<&ADVAPI32.RegCreatel  RegCreateKeyExW
```

```
0015F868  00F5CF40  CALL to RegCreateKeyExW from bb.00F5CF3A
0015F86C  000000B0  hKey = B0
0015F870  0015F99C  Subkey = "Fax"
0015F874  00000000  Reserved = 0
0015F878  00000000  Class = NULL
0015F87C  00000000  Options = REG_OPTION_NON_VOLATILE
0015F880  00000103  Access = KEY_QUERY_VALUE|KEY_SET_VALUE|100
0015F884  00000000  pSecurity = NULL
0015F888  0015F89C  pHandle = 0015F89C
0015F88C  00000000  pDisposition = NULL
```

Figure 14. Functions used when creating a registry key

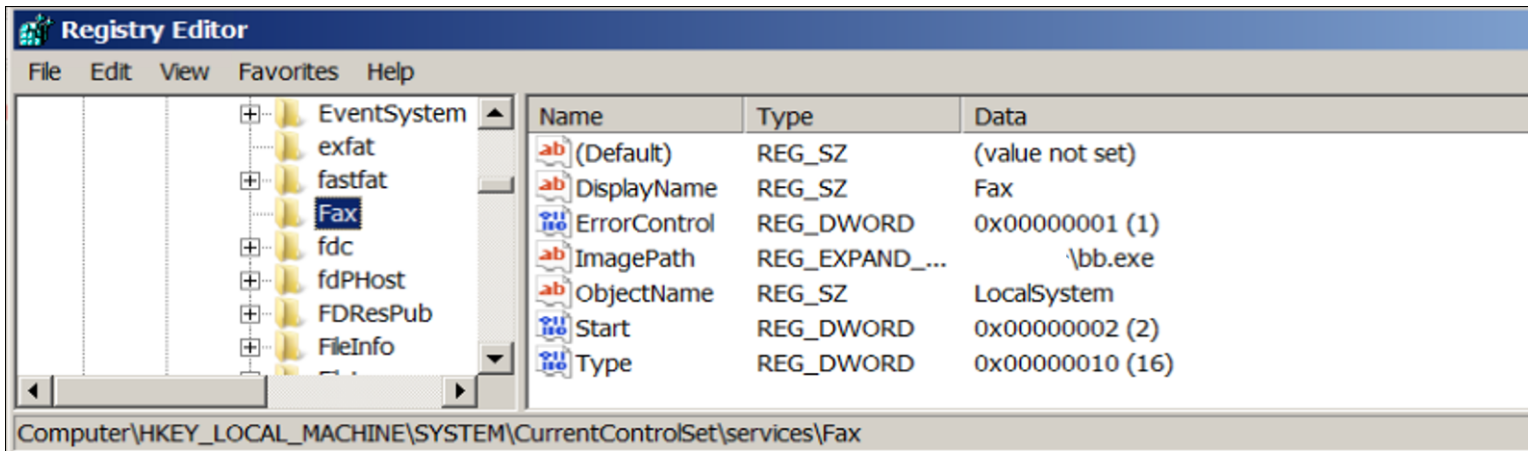


Figure 15. New registry key created for the new "Fax" service that replaces the deleted service

It then uses ShellExecuteA to shut down and restart the victim's machine.

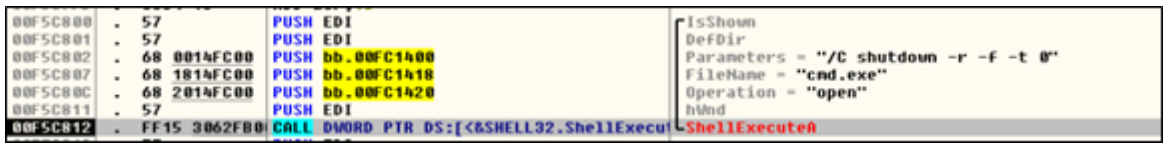


Figure 16. Function ShellExecuteA used to shut down and restart the victim's machine

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.

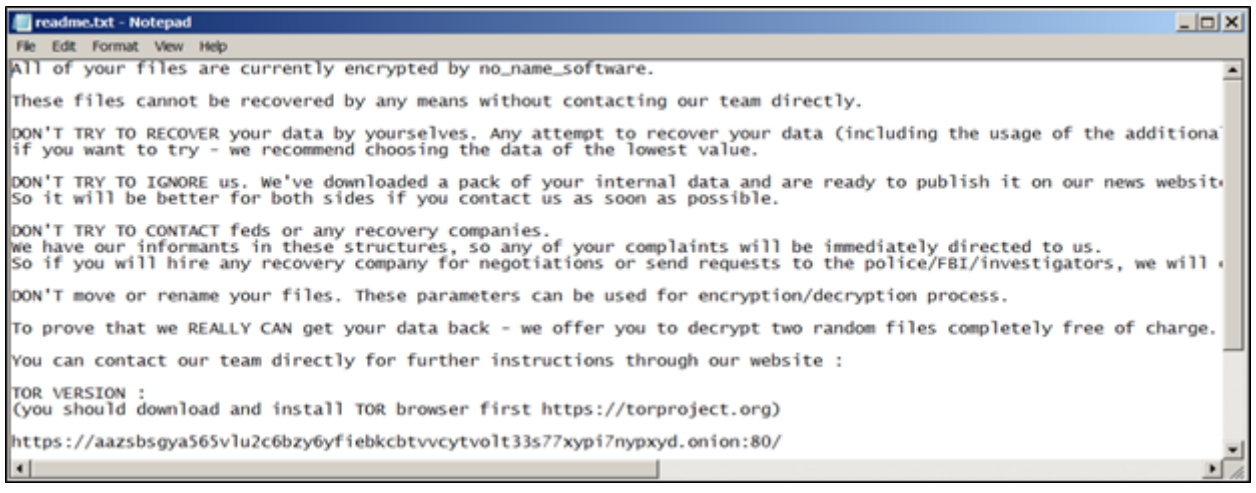


Figure 17. Ransom note used in an earlier sample

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.

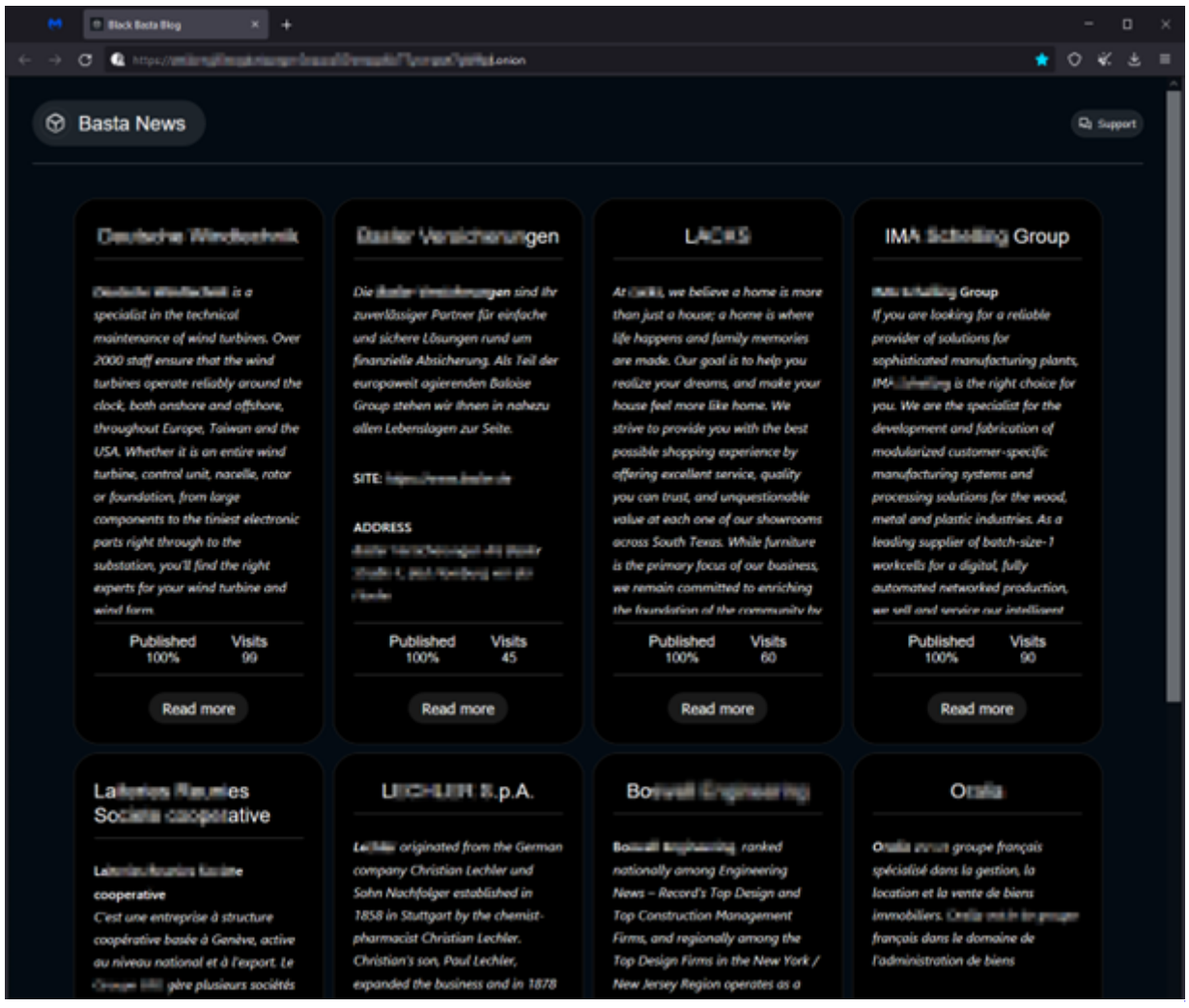


Figure 18. Black Basta's leak site, retrieved from https://twitter.com/MarceloRivero/status/1519398885193654273

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

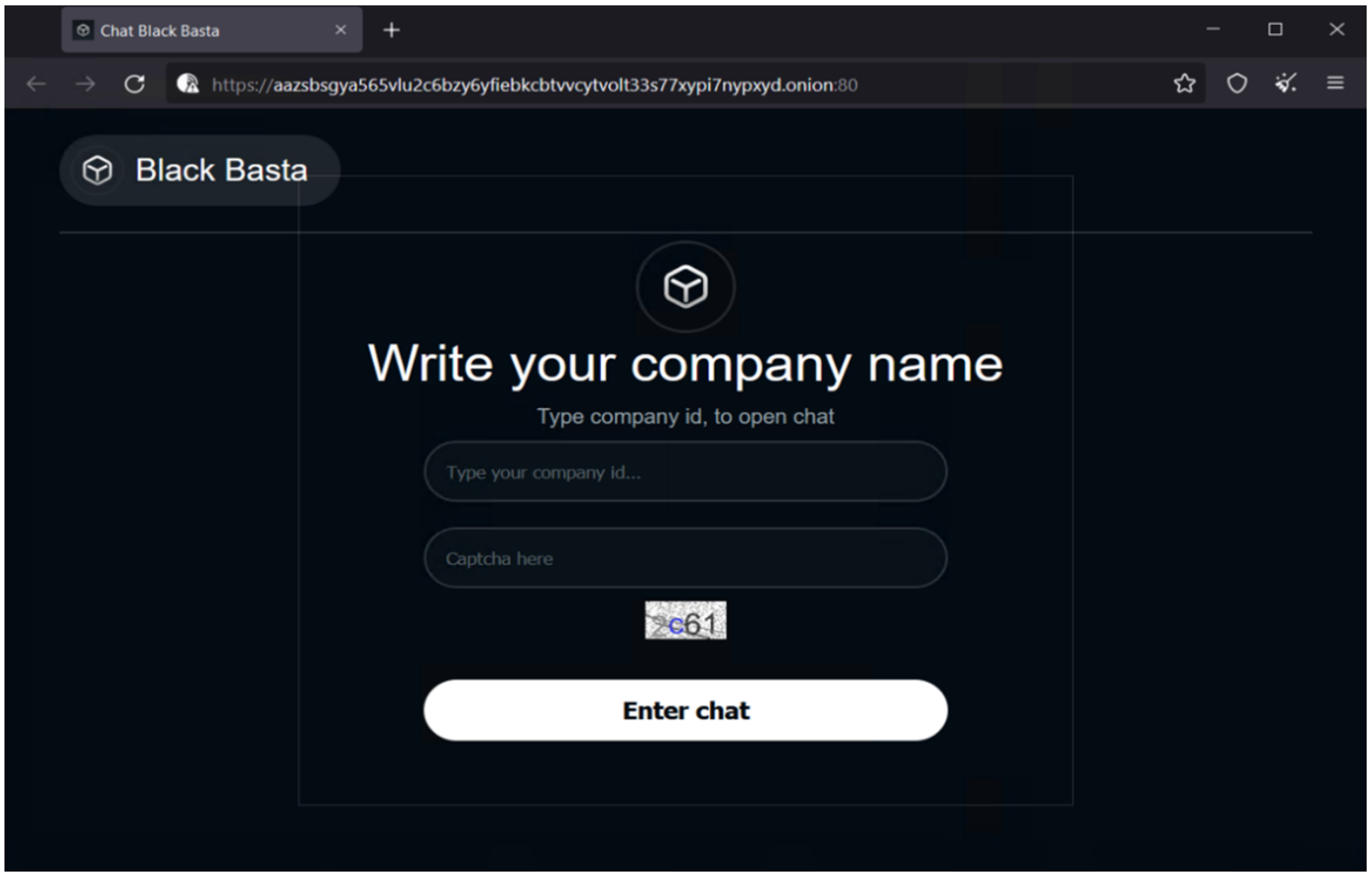


Figure 20. The Black Basta payment site

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
5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa	Ransom.Win32.BASTACRYPT.THDBGBB
7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a	Ransom.Win32.BASTACRYPT.YXCD2
ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e	Ransom.Win32.BASTACRYPT.THDBIBB
17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90	Ransom.Win32.BASTACRYPT.YXCD2
a54fef5fe2af58f5bd75c3af44f1fba22b721f34406c5963b19c5376ab278cd1	Ransom.Win32.BASTACRYPT.THDBGBB
1d040540c3c2ed8f73e04c578e7fb96d0b47d858bbb67e9b39ec2f4674b04250	Ransom.Win32.BASTACRYPT.YXCD2
2967e1d97d32605fc5ace49a10828800fbbefcc1e010f6004a9c88ef3ecdad88	Ransom.Win32.BASTACRYPT.YXCD2.note
f088e6944b2632bb7c93fa3c7ba1707914c05c00f9491e033f78a709d65d7cff	Ransom.Win32.BASTACRYPT.YXCD2.note

Tags Articles, News, Reports | Ransomware | Research

Authors

- Ieriz Nicolle Gonzalez

  Threat Analyst

- Ivan Nicole Chavez

  Threat Analyst

- Katherine Casona

  Threat Analyst

- Nathaniel Morales

  Threat Analyst

Related Articles

- NetDooka Framework Distributed via PrivateLoader Malware as Part of Pay-Per-Install Service
- AvosLocker Ransomware Variant Abuses Driver File to Disable Anti-Virus, Scans for Log4shell
- New APT Group Earth Berberoka Targets Gambling Websites With Old and New Malware

See all articles