Minerva Labs Blog

News & Reports

New Black Basta Ransomware Hijacks Windows Fax Service

May 02, 2022 | Natalie Zargarov

The Black Basta ransomware was first observed in mid-April 2022, but had already caused substantial damage to over ten organizations. This new ransomware became more public after leaking data of the American Dental Association, from which the Black Basta gang was able to exfiltrate 2.9 GB of data.

Black Basta ransomware must be executed with Administrator privileges, otherwise this ransomware is harmless.

This means that the threat actor needs to remain undetected inside the organization's network for quite some time in order to gain privilege access or use stolen credentials (there are a number of darknet websites who offer a large amount of these for sale).

Black Basta begins by checking if any parameters were passed. The only parameter that this ransomware accepts is "-forcepath", which we assume that if passed, will encrypt files in the specific path only. However, in dynamic analysis selecting a specific path, no differences in encryption routine were observed. Next, the ransomware deletes shadow copies by executing "C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet" command.

Black basta drops two files: dlaksjdoiwq.jpg and fkdjsadasd.ico in the user Temp folder. dlaksjdoiwq.jpg is a desktop wallpaper, pointing to read a ransom note, that is set by the ransomware using the SystemParametersInfoW API call:

```
push    eax             ; pvParam
push    0               ; uiParam
push    SPI_SETDESKWALLPAPER ; uiAction
call    ds:SystemParametersInfoW
```

Figure 1 - Set Desktop Wallpaper

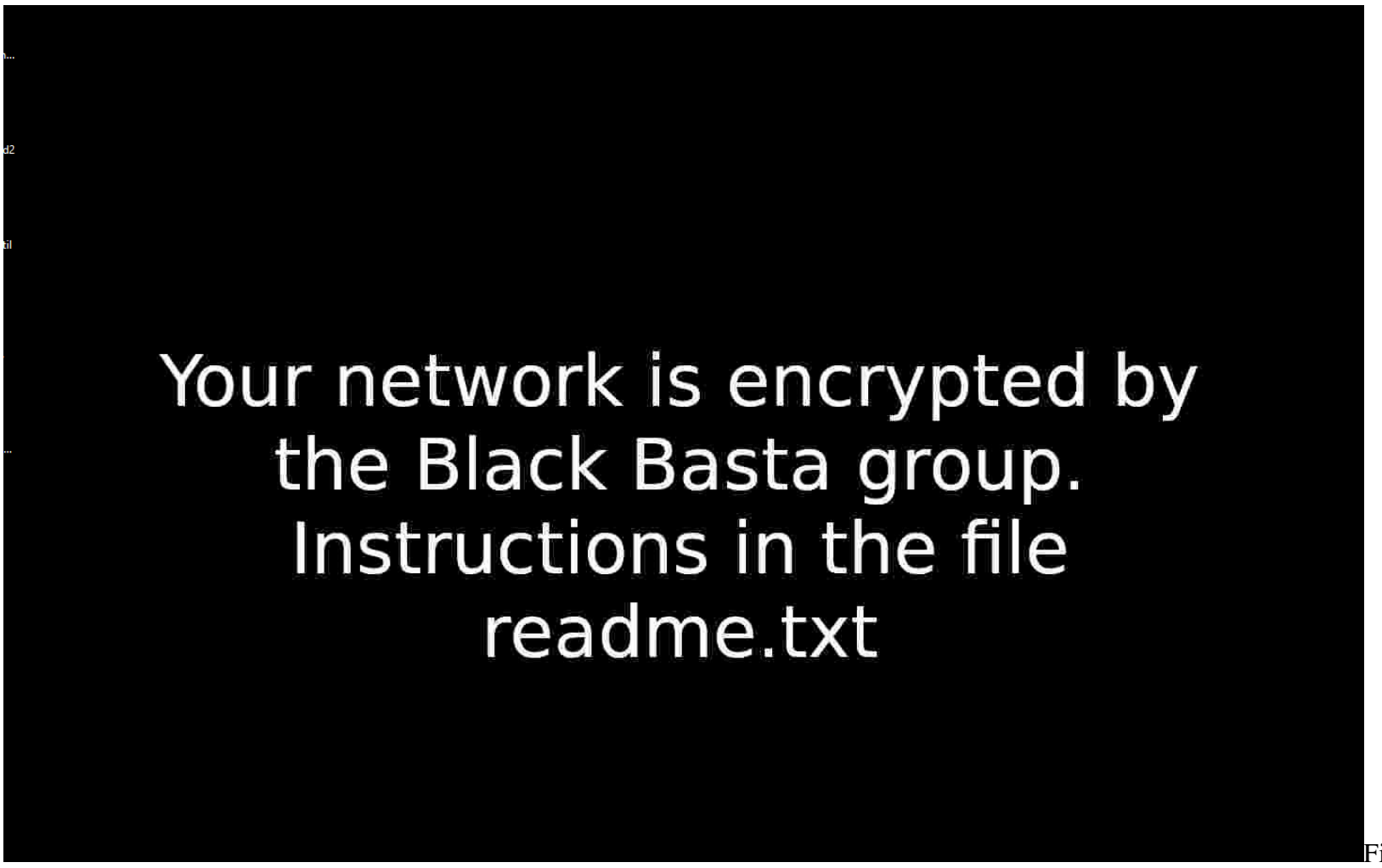

Figure 2 - New Wallpaper

Next, the ransomware assigns a second dropped file (fkdjsadasd.ico) as a custom icon to all files with ".basta" extension. The icon is assigned by creating and setting a new registry key "HKEY_CLASSES_ROOT\.basta\DefaultIcon"

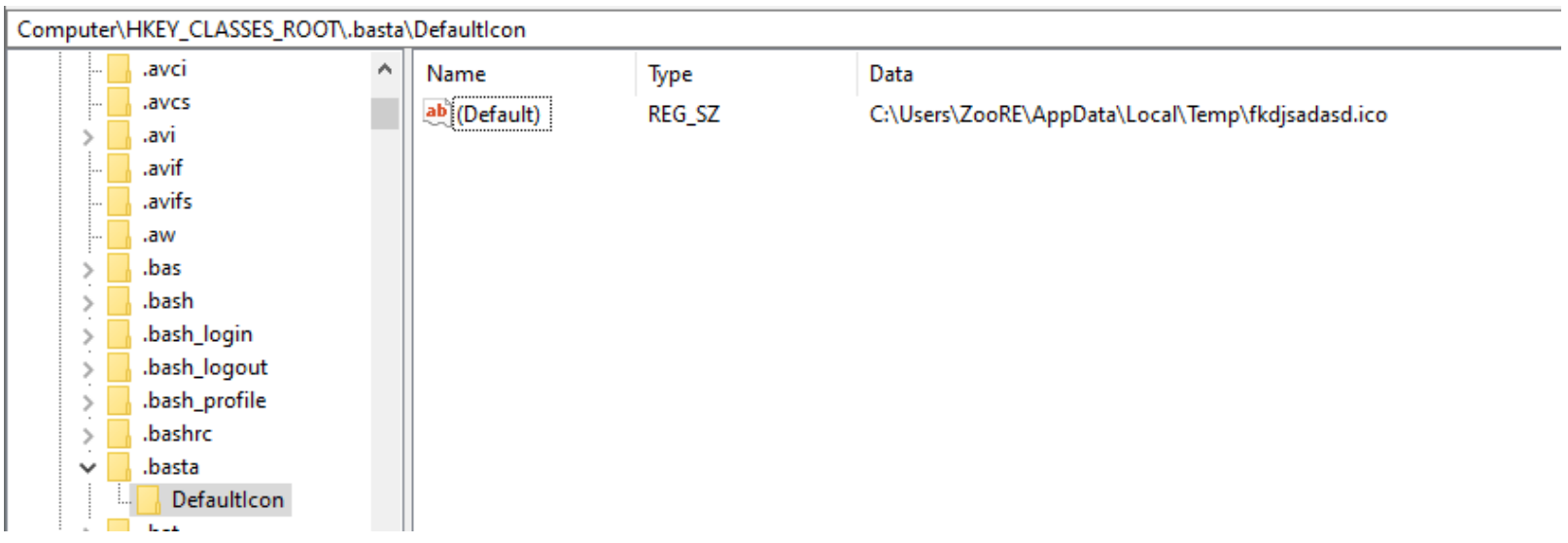

Figure 3 - Assigning custom icon

Now come the interesting part - the persistence mechanism of the Black Basta ransomware is implemented by "stealing" an existing service name, deleting the service, and then creating a new service with the same("stolen") name. In our sample, the legitimate service whose name was stolen is "FAX":

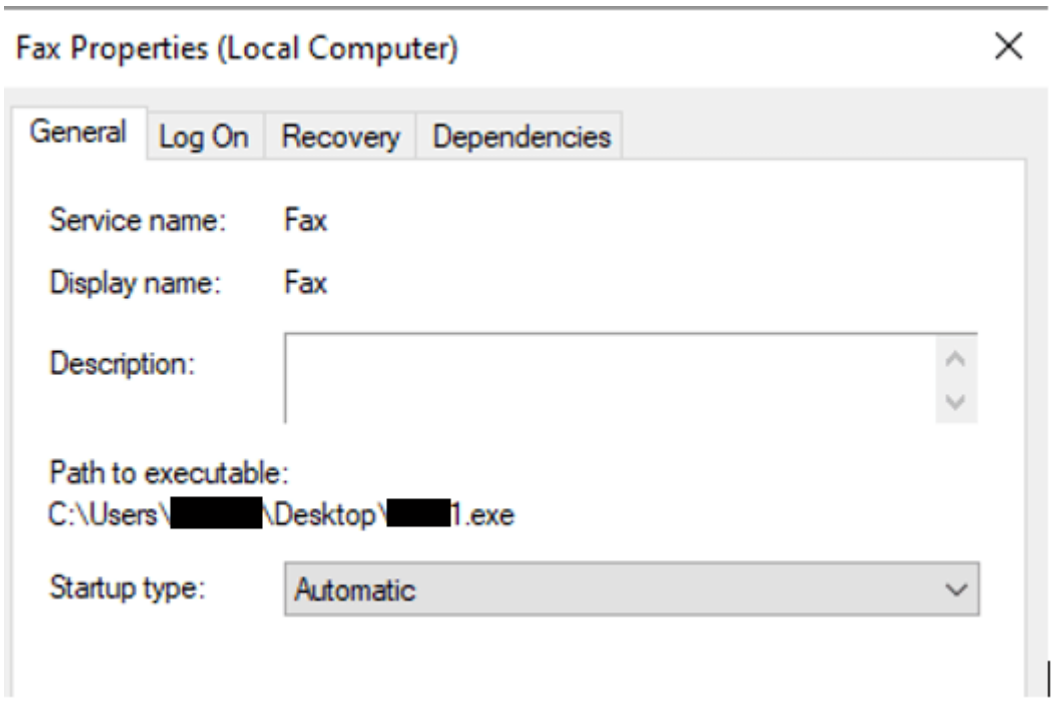

Figure 4 - "New" Service

Before the encryption routine begins, the ransomware checks the system boot configuration by using the GetSystemMetrics API call. It then adds "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Fax" to enable a FAX service to run in safe mode:

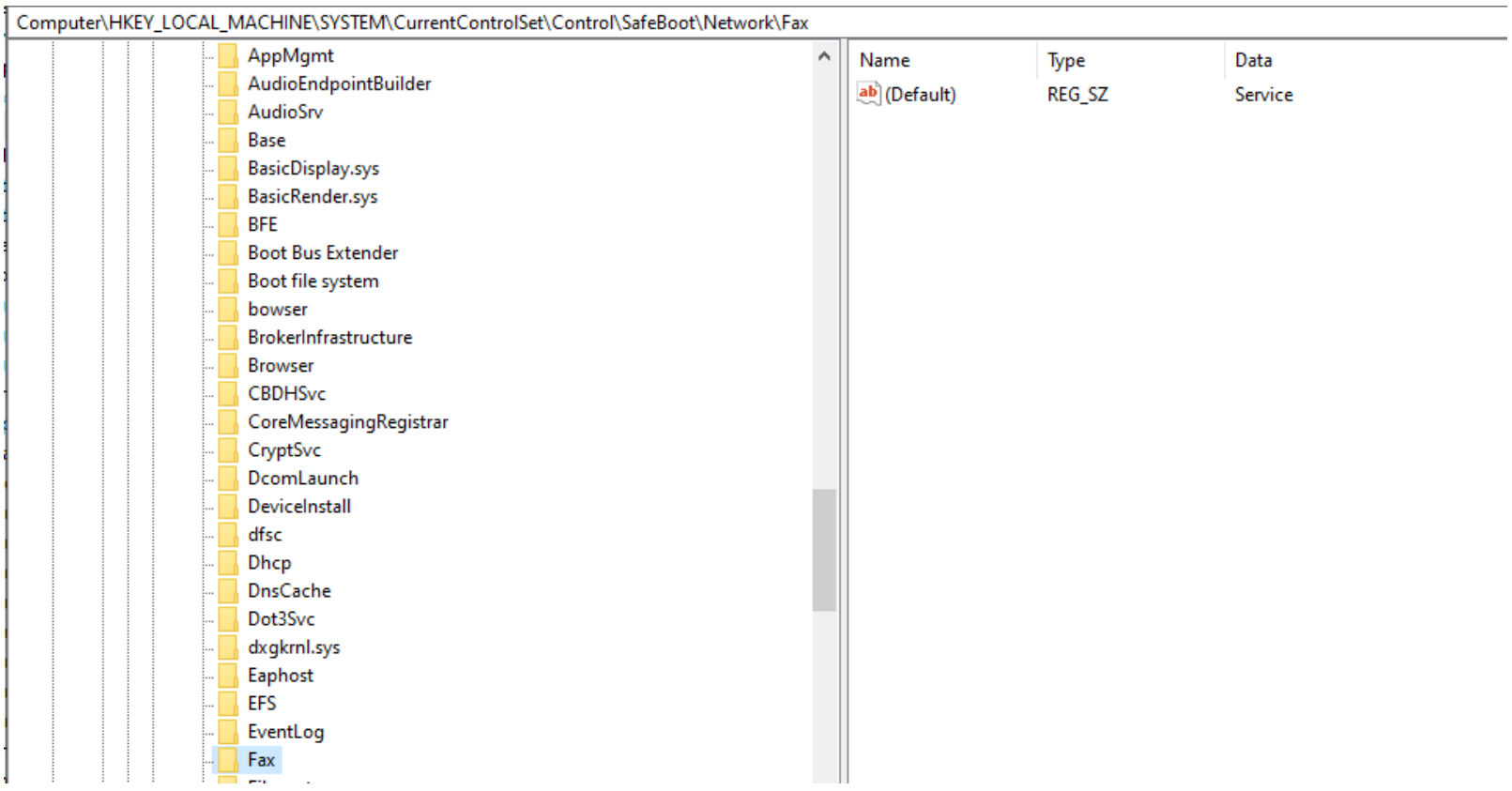

Figure 5 - Safe Boot Configuration

After all configurations are set, the ransomware reboots the pc in safe mode with networking by executing the " bcdedit /set safeboot network" command:

```
push    offset aBcdeditSetSafe ; "bcdedit /set safeboot network"
call    run_command_line
push    offset aCWindowsSystem ; "C:\\Windows\\System32\\bcdedit.exe /set"...
call    run_command_line
push    offset aCWindowsSysnat ; "C:\\Windows\\SysNative\\bcdedit.exe /se"...
call    run_command_line
```

Figure 6 - Reboot in safe mode

Due to the reboot mode change performed by the ransomware earlier, the PC will reboot in safe mode with the 'Fax' service running. This service will then execute the ransomware again, but this time for the purpose of encryption. As most ransomwares these days, Black Basta first enumerates volumes and puts a readme.txt file, a surprisingly short ransom note (maybe because the initial presentation is done in the desktop wallpaper) containing a data publication threat, TOR website address of the gang, and a company ID. This note is written to every folder as a part of the encryption routine.

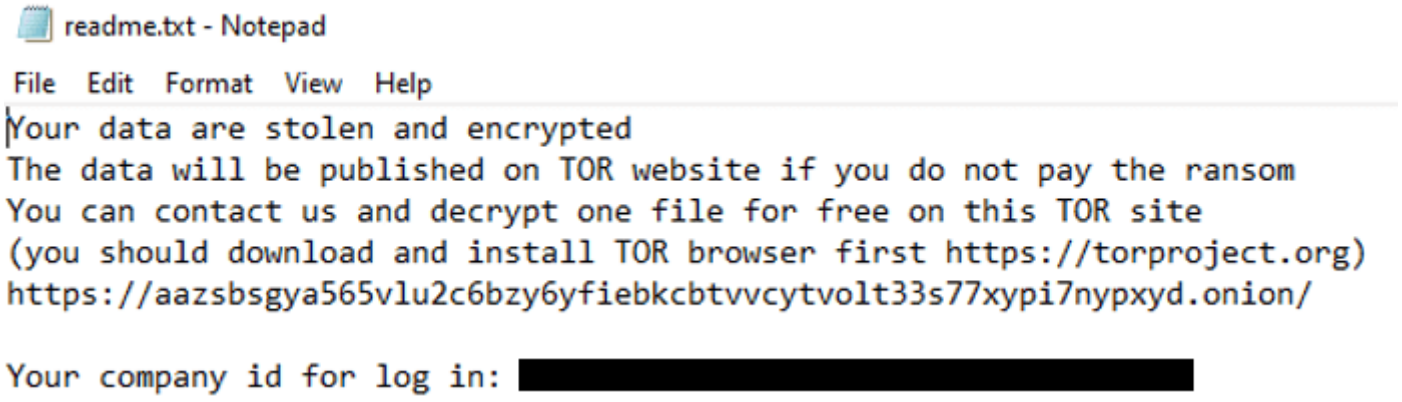

Figure 7 - Ransom Note

The encryption process runs in several threads simultaneously to speed up the encryption, despite high CPU usage:

Figure 8 - 92.83% CPU usage

When the encryption is finished, the ransomware reboots the pc in normal mode.

It would seems that every sample is created for a specific company, as a company id is hardcoded into the ransom note as well as a public key. Recent Victims of this ransomware include Deutsche Windtechnik and the American Dental Association.

This article focuses only on the final stages of the Black Basta ransomware, that occurs only after the attacker has achieved initial access and has managed to perform substantial lateral movement within the network. Minerva's Anti-Ransomware solution recognizes attempts to bypass security measures in order to remain undetected, and uses these very methods to prevent them from ever starting the attack.

Resources:

- https://www.bleepingcomputer.com/news/security/american-dental-association-hit-by-new-black-basta-ransomware/

IOC's:

- 5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa — The Black Basta ransomware
- A70F03BEB3A8246595EAB83935227914 - dlaksjdoiwq.jpg — desktop wallpaper
- eb07a24f63d7f56fb13e34dd60e45a4c8522c32892c8be7dca7d3f742fa86b0a - fkdjsadasd.ico - .basta custom icon

« Previous Post Next Post »