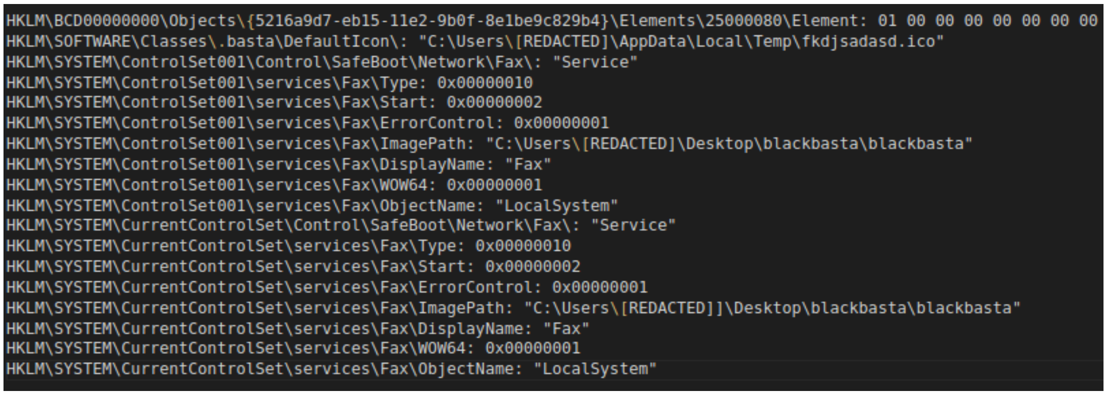
Introduction:

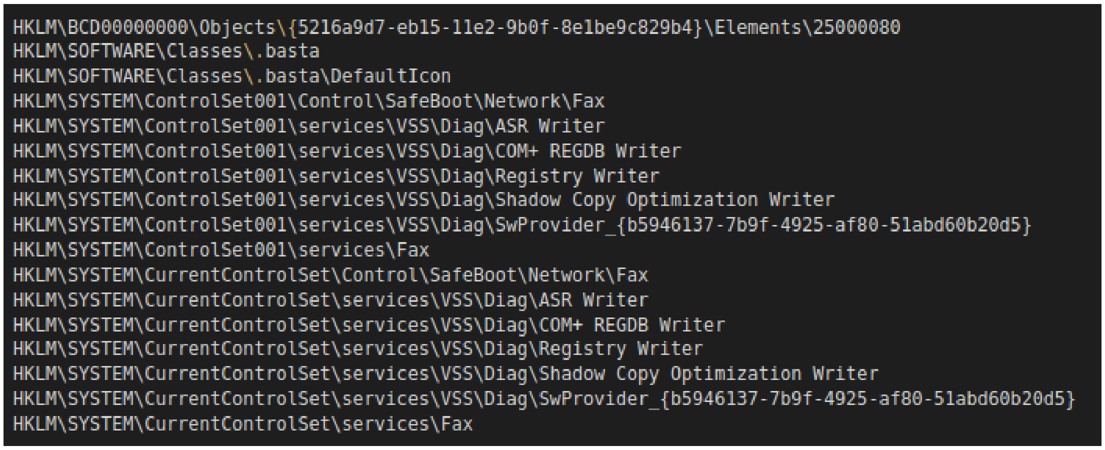
Black Basta ransomware hit American Dental Association on the weekend of the week of 4/17, 2022. The ransomware group responsible for this act also stole sensitive data from W2 forms, NDAs, and accounting spreadsheets. This report will go over Black Basta's capabilities and IOCs to prevent future attacks.

Installation:

Basta installs itself as a service using the registry, then hiding itself by labeling it as a fax machine service.



```
HKLM\BCD00000000\Objects\{5216a9d7-eb15-11e2-9b0f-8e1be9c829b4}\Elements\25000080\Element: 01 00 00 00 00 00 00 00
HKLM\SOFTWARE\Classes\.basta\DefaultIcon\: "C:\Users\[REDACTED]\AppData\Local\Temp\fkdjsadasd.ico"
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Network\Fax\: "Service"
HKLM\SYSTEM\ControlSet001\services\Fax\Type: 0x00000010
HKLM\SYSTEM\ControlSet001\services\Fax\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\services\Fax\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\services\Fax\ImagePath: "C:\Users\[REDACTED]\Desktop\blackbasta\blackbasta"
HKLM\SYSTEM\ControlSet001\services\Fax\DisplayName: "Fax"
HKLM\SYSTEM\ControlSet001\services\Fax\WOW64: 0x00000001
HKLM\SYSTEM\ControlSet001\services\Fax\ObjectName: "LocalSystem"
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Fax\: "Service"
HKLM\SYSTEM\CurrentControlSet\services\Fax\Type: 0x00000010
HKLM\SYSTEM\CurrentControlSet\services\Fax\Start: 0x00000002
HKLM\SYSTEM\CurrentControlSet\services\Fax\ErrorControl: 0x00000001
HKLM\SYSTEM\CurrentControlSet\services\Fax\ImagePath: "C:\Users\[REDACTED]]\Desktop\blackbasta\blackbasta"
HKLM\SYSTEM\CurrentControlSet\services\Fax\DisplayName: "Fax"
HKLM\SYSTEM\CurrentControlSet\services\Fax\WOW64: 0x00000001
HKLM\SYSTEM\CurrentControlSet\services\Fax\ObjectName: "LocalSystem"
```



```
HKLM\BCD00000000\Objects\{5216a9d7-eb15-11e2-9b0f-8e1be9c829b4}\Elements\25000080
HKLM\SOFTWARE\Classes\.basta
HKLM\SOFTWARE\Classes\.basta\DefaultIcon
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Network\Fax
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\ASR Writer
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\COM+ REGDB Writer
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\Registry Writer
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\Shadow Copy Optimization Writer
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
HKLM\SYSTEM\ControlSet001\services\Fax
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Fax
HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\ASR Writer
HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\COM+ REGDB Writer
HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\Registry Writer
HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\Shadow Copy Optimization Writer
HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
HKLM\SYSTEM\CurrentControlSet\services\Fax
```

Upon installation, Basta will restart the computer. The installation allows the newly created service to run on startup, where it then begins the process of encrypting files.

Commands Issued:

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

- C:\Windows\System32\bcdedit.exe /set safeboot network
- C:\Windows\System32\ vssadmin.exe /deletevalue safeboot
- C:\Windows\System32\ vssadmin.exe /deletevalue safeboot
- cmd.exe /C shutdown –r –f –t 0

Basta is executed with admin privileges based on the commands issued. Deleting shadow copies is a standard method used by ransomware to prevent backups. If offline backups are not implemented, this attack will leave the victim at the expense of the attacker.

Based on the analysis, there is no indication that this sample can elevate its privileges. Therefore, it can be concluded that the attacker already had higher-level privileges upon execution.

The recommended course of action is that offsite backups are created if an attacker does gain admin-level privileges on the victim machine.

IOCs

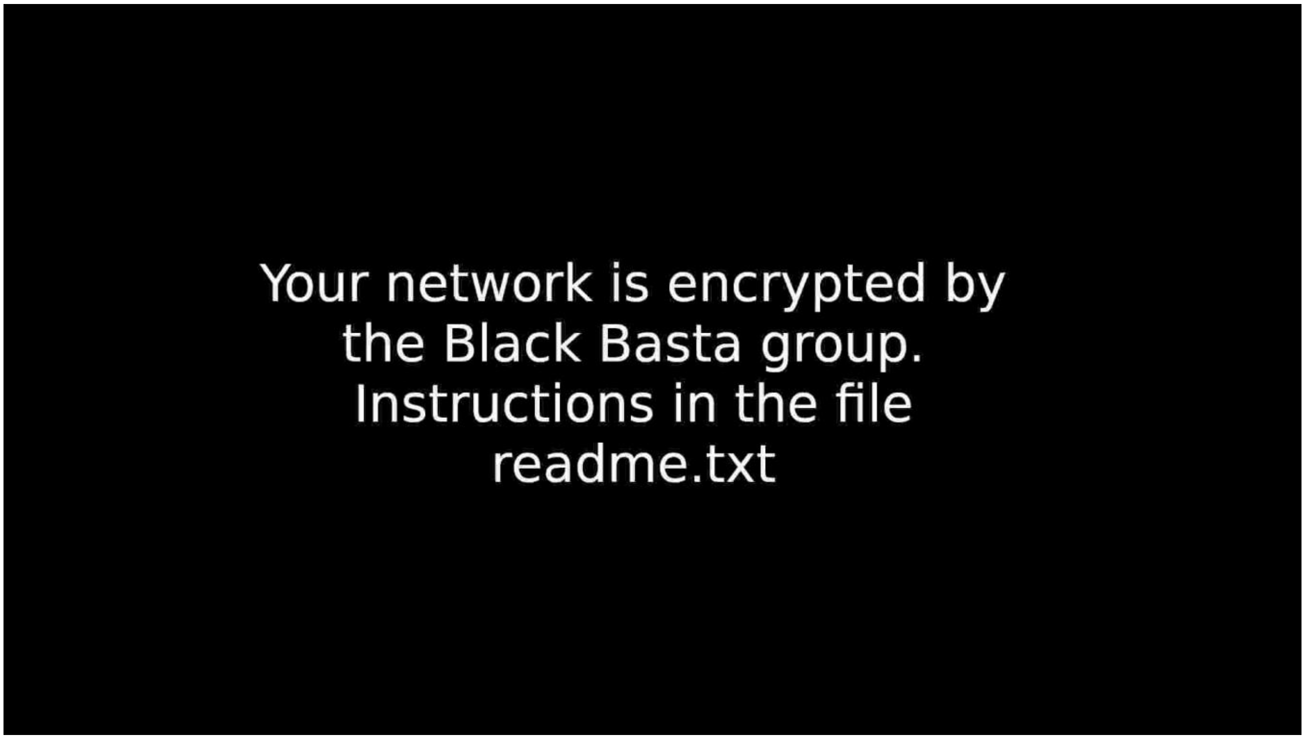
MD5: 3f400f30415941348af21d515a2fc6a3

SHA-1: bd0bf9c987288ca434221d7d81c54a47e913600a

SHA-256: 5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa

Ransomware File Extension: .basta

Ransomware Background Image



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

Further Reading:

https://www.pcrisk.com/removal-guides/23666-black-basta-ransomware

Conclusion:

For now, more analysis is needed to find more of its capabilities. From analysis, a command line argument "–forcepath" was found but it was not determined the intended behavior of this argument