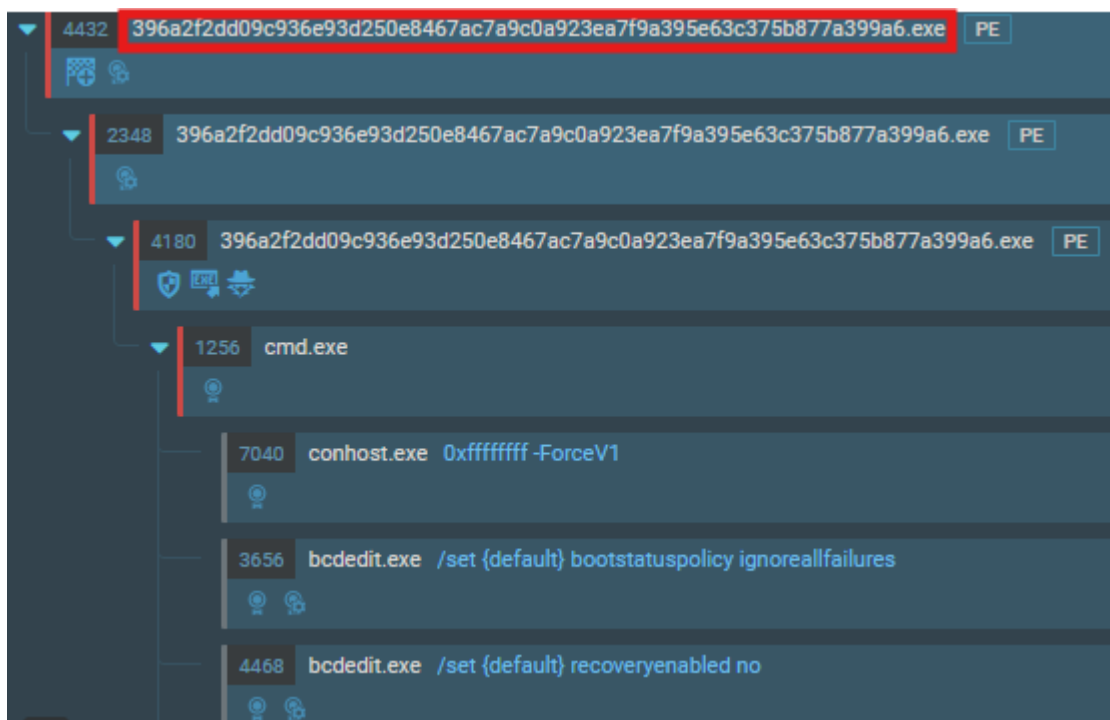


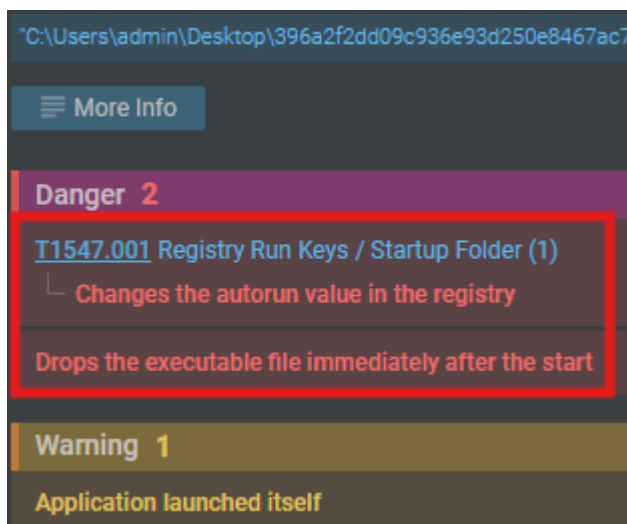
BONUS CONSEGNA U3 S9 L5


1. Eseguibile malevolo

Nel primo caso si tratta di un eseguibile malevolo che a sua volta si serve di diversi processi che va a richiamare per effettuare una serie di operazioni.



Come prima cosa va a modificare le chiavi di registro.



 **Danger / Installation**
Changes the autorun value in the registry
[T1547.001](#) Registry Run Keys / Startup Folder

Operation:	WRITE
Name:	396A2F2DD09C936E93D250E8467AC7A9C0A923EA7F9A395E63C375B877A399A6
Value:	C: \\Users\\admin\\AppData\\Local\\396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe
Key:	HKEY_LOCAL_MACHINE\\SOFTWARE\\MICROSOFT\\WINDOWS\\CURRENTVERSION\\RUN
TypeValue:	REG_SZ

Poi fa effettua una serie di operazioni accessorie, come la lettura del nome della macchina, le lingue supportate e la nazionalità.

Other 2

[T1012](#) Query Registry (2)

- Reads the computer name
- Checks supported languages

[T1082](#) System Information Discovery (2)

- Reads the computer name
- Checks supported languages

Other 3

[T1614](#) System Location Discovery (1)

- Process checks computer location settings

Il comportamento che viene descritto è quello di un ransomware. L'eseguibile si occupa inizialmente di creare una directory nel sistema.

Danger 4

[T1552.001](#) Credentials In Files (1)

- Actions looks like stealing of personal data


[T1518](#) Software Discovery (1)

- Actions looks like stealing of personal data

[T1486](#) Data Encrypted for Impact (2)

- Renames files like ransomware
- PHOBOS has been detected

Drops the executable file immediately after the start

 **Danger / Stealing**
Actions looks like stealing of personal data
[T1552.001](#) Credentials In Files
[T1518](#) Software Discovery

Operation:

CREATE

Device:

DISK_FILE_SYSTEM

Object:

DIRECTORY

Name:

C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnbdlolhkh\1.73.6_0_locales\az

Status:

0x00000000

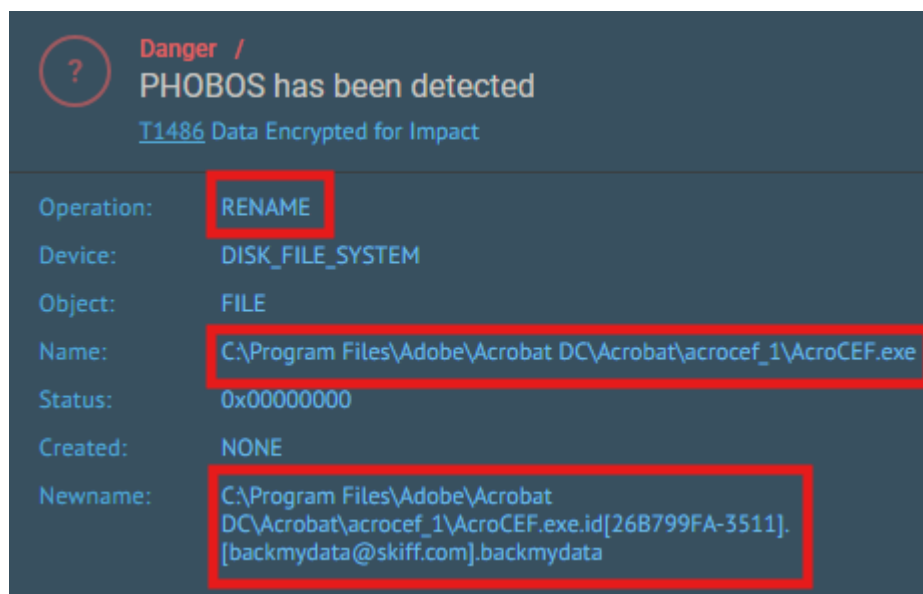
Created:

OPENED

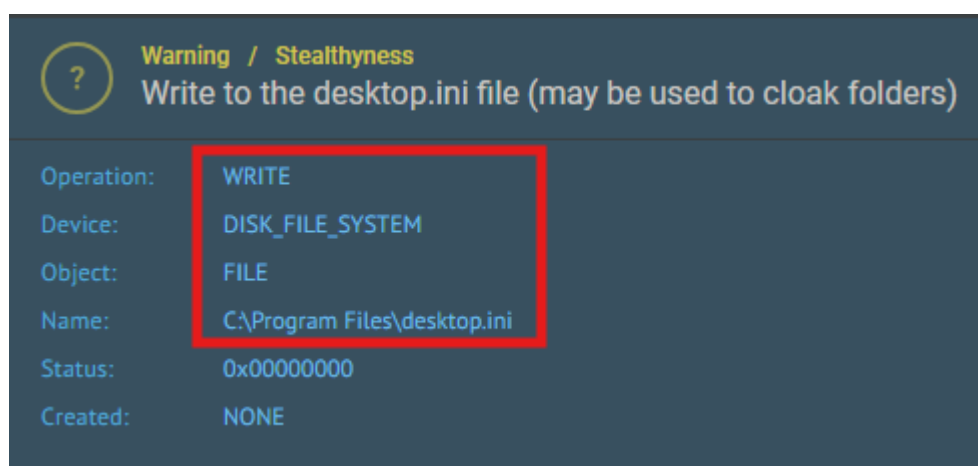
Access:

SYNCHRONIZE, FILE_READ_DATA

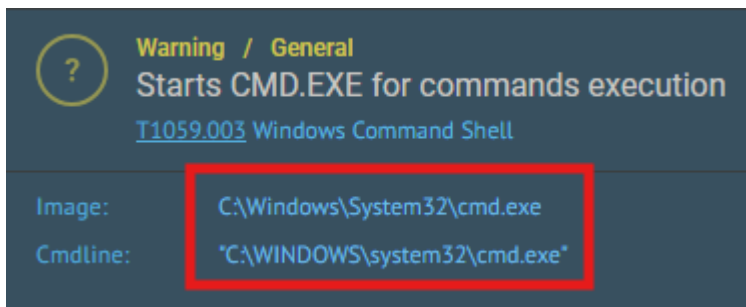
Successivamente si occupa di modificare il nome di un file nella directory **C:\Program Files\Adobe\Acrobat DC\Acrobat**. Il file che viene rinominato è **AcroCEF.exe**. L'estensione usata per il file è **backmydata**.



Crea un file **desktop.ini** nella directory **C:\Program Files**.

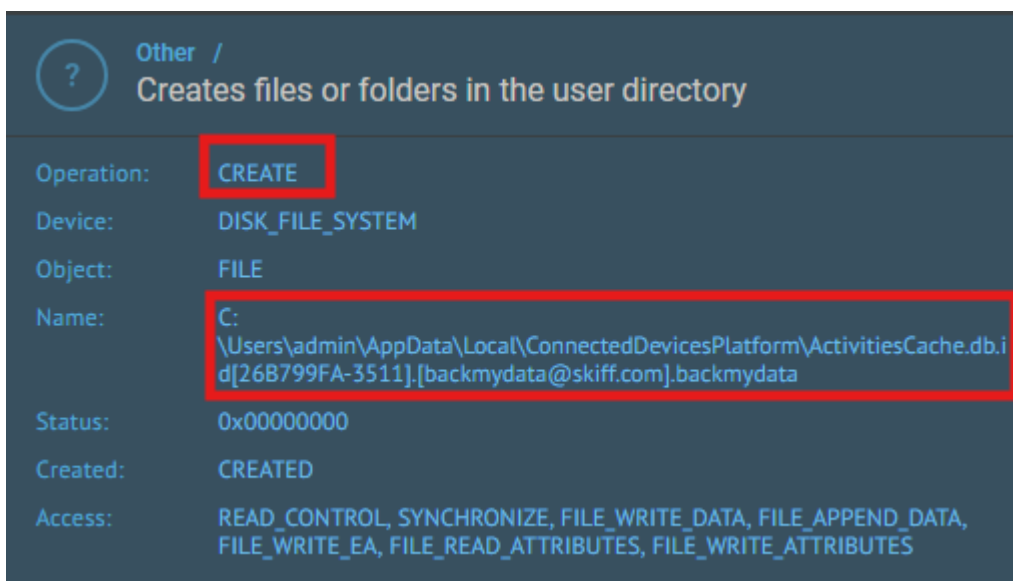


Esegue un terminale di windows.

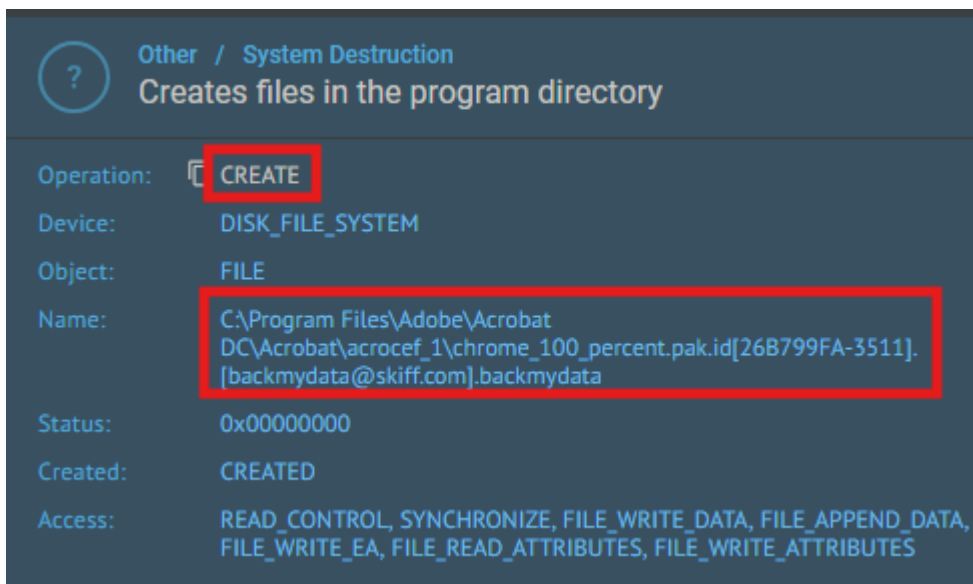


Crea un file nella directory

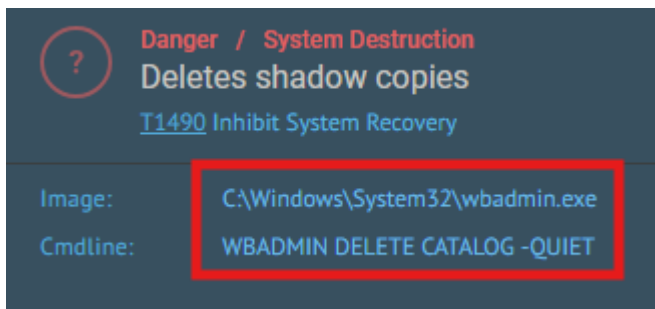
C:\Users\admin\AppData\Local\ConnectedDevicesPlatform con estensione **backmydata**.



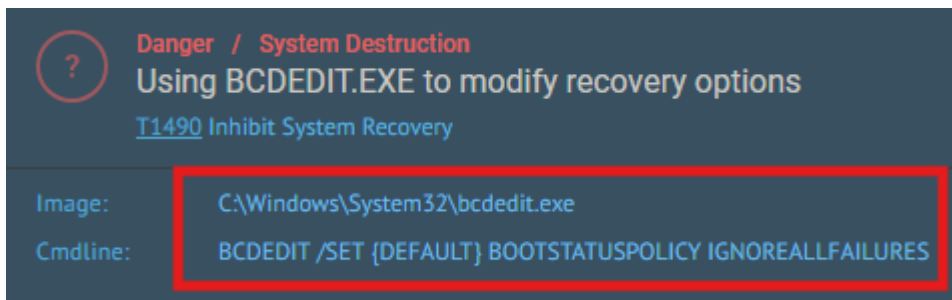
Crea un altro file sempre con la stessa estensione nella directory di Adobe Acrobat.



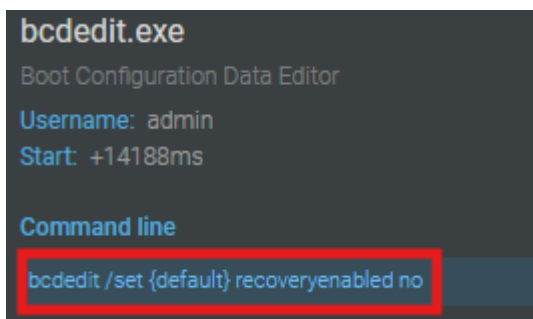
Tramite il comando **WBADMIN DELETE CATALOG -QUIET** elimina tutte le copie del catalogo di backup presenti nel sistema.



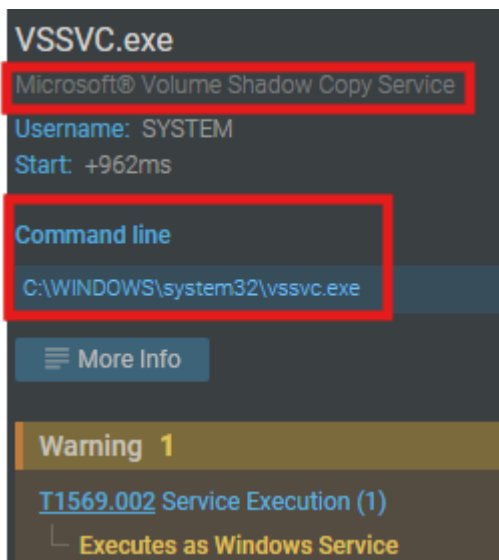
Sempre dal prompt dei comandi esegue il comando **BCEDIT /SET {DEFAULT} BOOTSTATUSPOLICY IGNOREALLFAILURES**. Il comando va a modificare le boot entry options di Windows, e in questo caso specifico il comando dice al sistema di ignorare qualsiasi errore di avvio o di spegnimento del sistema e di agire come se nulla fosse accaduto.



Tramite il comando **bcdedit /set {default} recoveryenabled no** il programma va a disabilitare il recovery di Windows all'avvio in caso si verificano degli errori di sistema.



Poi sempre dal prompt dei comandi va ad avviare il processo **vssvc.exe** che è un eseguibile di Windows che si occupa della gestione delle copie shadow. Si occupa di creare delle copie di backup o istantanee di file o volumi.



Esegue poi il programma slui.exe che si occupa dell'attivazione telefonica delle licenze Microsoft. La sigla "slui" sta per Windows **S**oftware **L**icensing **U**ser **I**nterface.

