Sectalks CTF 0x05

Two files:

IDF_mainframe_client_x64_ARM_i386_SPARC _...systemZ_Z80_PowerPC_RISCISBEST

and

IDF_mainframe_client_x64_ARM_i386_SPARC _...systemZ_Z80_Windows_RISCISBEST.exe

Sectalks CTF 0x05

- strings(1)

  …

```
Error loading Python DLL: %s (error code %d)

Error detected starting Python VM.
```

Sectalks CTF 0x05

- Google for Python bundlers
  - A few multiplatform candidates

- PyInstaller
  - Open source, so we can see how it bundles stuff up

Sectalks CTF 0x05

- PyInstaller
  - Actually ships with archive tool to extract/view

```
pos, length, uncompressed, iscompressed, type, name
[(0, 1529172, 1529172, 0, 'z', 'out00-PYZ.pyz'),
(1529172, 169, 234, 1, 'm', 'struct'),
(1529341, 1138, 2578, 1, 'm', 'pyi_os_path'),
(1530479, 4779, 12596, 1, 'm', 'pyi_archive'),
…
(1545191, 4545, 8984, 1, 's', 'balls'),
```

Sectalks CTF 0x05

```
#!/usr/bin/env python
# WICKED IMPORTS
from collections import OrderedDict
import random
...
# SWEET BASE64
data = 'ZnJvbSBjb2xsZWN0aW9ucyBpbXB...
# EXEC THE MOTHERFUCKER
exec(base64.decodestring(data))
```

Sectalks CTF 0x05

- Main Application!
  - RMS fanfic!
  - Stackoverflow
  - Unused “callhome” to lolipop.msm.ru (??)
  - Main routine
    - Menus – can skip
    - File submission

Sectalks CTF 0x05

- Submit IDF_...exe as both files:
  - Error: SHA1 does match

- Submit two different files:
  - Error: MD5s do not match

Sectalks CTF 0x05

- Need to find an MD5 collision!
  - … Google

- Submit two tiny different files that have the same MD5
  - Error: Files do not have expected prefix.. you are so close right now...

Sectalks CTF 0x05

- Marc Stevens’ HashClash
  - http://www.win.tue.nl/hashclash/
- Allows file prefix specification

- Generate and submit the files...

SUCCESS!