EXPLORING C2: PART 3 "GETTING SOCIAL"

Rick Matthews
CSC 842
Cycle 9
Blue Team

Status

- Continued with same project from Cycles 3 and 6 but use social media as the server
  - *Hide in plain site*
    - Posts can be somewhat normal, appear innocent
    - Traffic wouldn't obviously appear out of the ordinary
  - *Nimble*
- Proof of Concept
- Still very basic but I'm enjoying learning and using various concepts and techniques

Technologies Considered

- Twitter
- Facebook
- Snapchat
- Flickr
  - *Embed commands in meta data*
- GitHub
- Blog

Twitter

- Considered
  - *Tweepy – Python Library*
    - Uses Twitter API
    - Must register application
    - Easy to use
    - Functionality
  - *Screen Scrape*
    - Lightweight – no registration
    - Fragile
- Chose to Screen Scrape
  - *Assumed most bad actors would choose this solution*
  - *Found a great script I used as a library*
  - *http://thepythondjango.com/virtual-environment-python-pocket-guide/*

Environment

- Python
- Ubuntu
- IA Lab
  - *Ubuntu VM*
- Twitter
  - *Server*

Functionality

- Client pulls list of tweets of a specific user
- Only looks at last Twitter post
- Parses information
- Executes command

Future Work

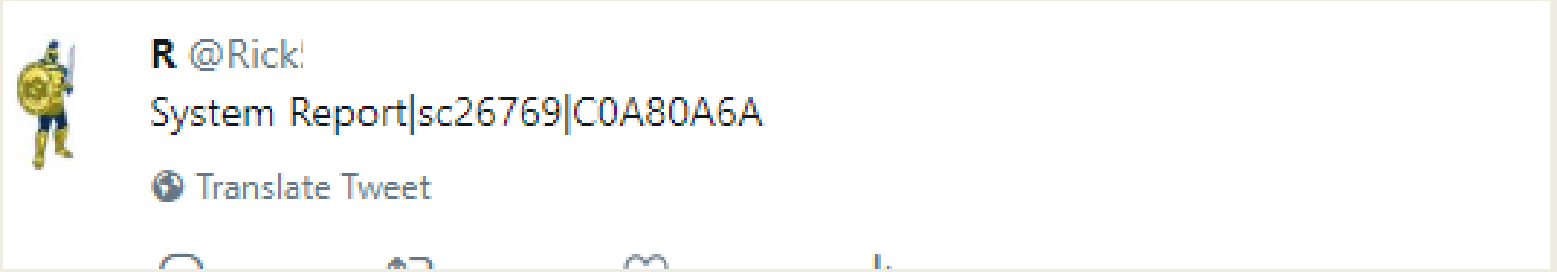
- Focus on infecting other machines
  - *Won't have a malicious payload*
  - *Probably won't post to GitHub*
- I may not pursue but ideas to enhance this script
  - *Incorporate multiple, different social media accounts*
    - Twitter
    - Flickr
    - GitHub
    - Blogger
  - *Incorporate a tracking system so client can execute multiple commands*

Tweet File and Command Format


```
{"tweets": ["System Report|sc26769|C0A80A6A","System Report|ac73456|C0A80A6A","System Report|ds7656|
C0A80A6A",]}
```

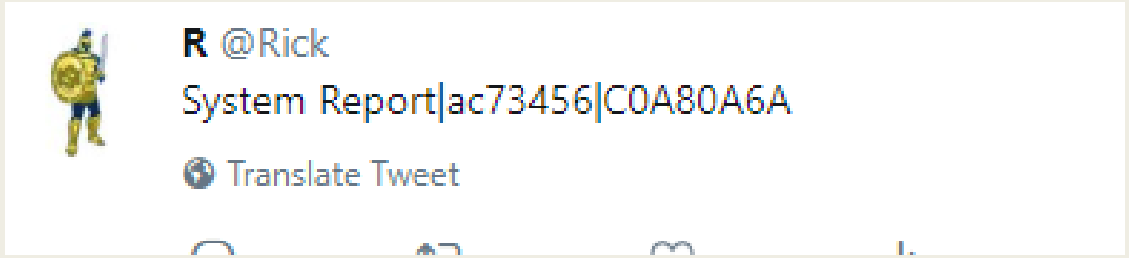

- Lists all tweets
- The program currently only pulls the most recent (first on the list)
- 3 parameters
  - *Filler: System Report is not used for anything. I'm hoping it makes it look more normal than an encrypted string. Perhaps a label system could be used to make the script more robust. Maybe a system to switch platform*
  - *Command: The letters and numbers are just a made up code.*
    - sc26769 = Scan System
    - ds7656 = DoS
    - ac73456 = Add Client
  - *IP Address of target*
    - Hexidecimal string
    - C0(192) A8(168) 0A(10) 6A(106)

Scan a System




```
dsu@UbuntuB:~/code$ sudo python twit_client.py
scan 192.168.10.106
Nmap Scan running: ETC: 0 DONE: 0%
Nmap Scan running: ETC: 0 DONE: 0%
Nmap Scan running: ETC: 1531497735 DONE: 23.35%
rc: 0 output: Nmap done at Fri Jul 13 11:02:08 2018; 1 IP address (1 host up) sc
anned in 5.44 seconds
```

Add Client to List




```
dsu@UbuntuB:~/code$ sudo python twit_client.py
add client 192.168.10.106
```

DoS via Ping


```
dsu@UbuntuB:~/code$ sudo python twit_client.py
ping 192.168.10.106
PING 192.168.10.106 (192.168.10.106) 56(84) bytes of data.
64 bytes from 192.168.10.106: icmp_seq=1 ttl=64 time=0.489 ms
64 bytes from 192.168.10.106: icmp_seq=2 ttl=64 time=0.477 ms
64 bytes from 192.168.10.106: icmp_seq=3 ttl=64 time=0.360 ms
64 bytes from 192.168.10.106: icmp_seq=4 ttl=64 time=0.552 ms
64 bytes from 192.168.10.106: icmp_seq=5 ttl=64 time=0.477 ms
64 bytes from 192.168.10.106: icmp_seq=6 ttl=64 time=0.543 ms
64 bytes from 192.168.10.106: icmp_seq=7 ttl=64 time=0.504 ms
64 bytes from 192.168.10.106: icmp_seq=8 ttl=64 time=0.480 ms
64 bytes from 192.168.10.106: icmp_seq=9 ttl=64 time=0.437 ms
64 bytes from 192.168.10.106: icmp_seq=10 ttl=64 time=0.449 ms

--- 192.168.10.106 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9210ms
rtt min/avg/max/mdev = 0.360/0.476/0.552/0.058 ms
```

REVIEW CODE