Covert Command & Control (C2) Channel

Luke Bradford ‘16
Faculty Advisor: Peter A. Yoon

What is a C2 Channel?

- Cyber attack asset that allows attackers to remotely and covertly send commands to enemy computers
- Provides command line interaction with enemy computers
- Often use websites such as social media to hide activity among normal network traffic

Motivation

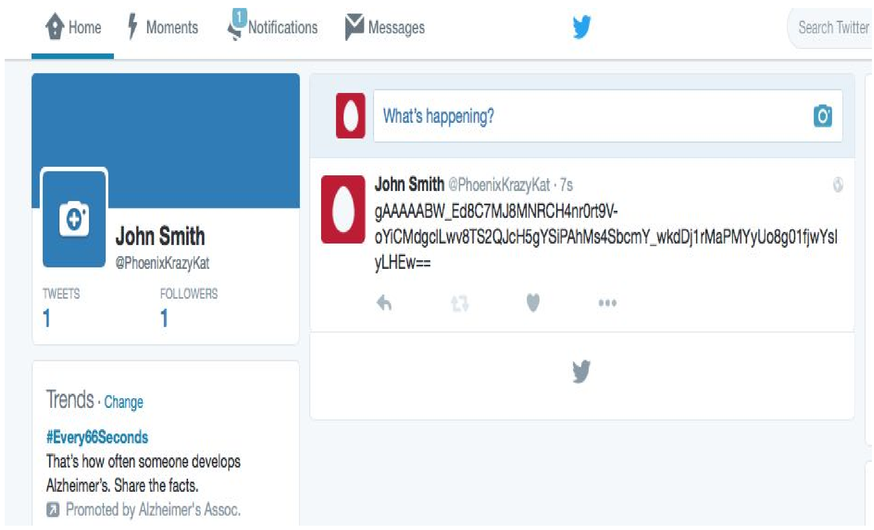
- Society depends upon computers
- Control of cyberspace will decide future engagements
- Need cyber assets to win cyber war

How does it work?

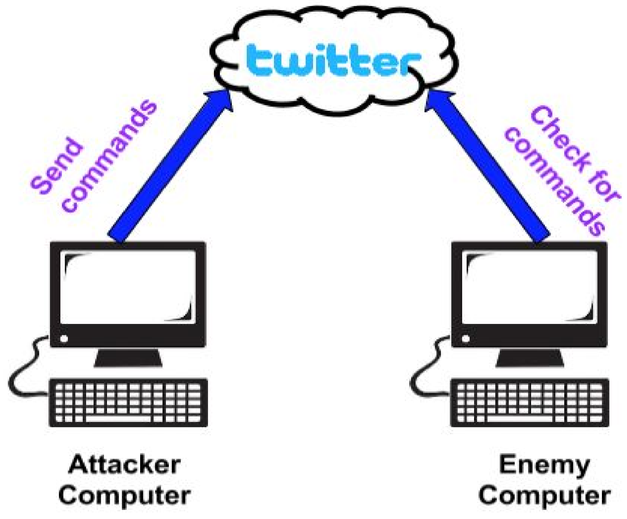
Attacker runs channel on their computer and enters a command

```
twitter_attack$ cat secretStuff.txt
```

Command is encrypted and posted as a tweet on a Twitter page



Enemy computer checks Twitter for tweet, decrypts it, executes command, information then displayed on attacker’s screen




```
twitter_attack$ cat secretStuff.txt
169 API calls remaining
bankPassword: a$$34klhg
masterKey: password123*
twitter_attack$
```

Technologies Used

- Python programming language
- Twitter Application Programming Interface (API)
- Advanced Encryption Standard (AES)

Conclusions

- Secure and reliable access to enemy computer
- Simple to use
- Easy to install on enemy computer via an email phishing scam
- Expandable:
  - Tweets could be links to another website containing exploit scripts
  - Foundation for a Twitter botnet

Check out the code on GitHub!

https://github.com/lmbradford115/seniorProjectTwitterC2