Esoteric Exfiltration

Willa Riggins

Who Am I?

Seriously, people. Does someone know? Cause I don’t.

- Senior Penetration Tester @ Veracode
- FamiLAB Member
- DC407 Point of Contact
- OWASP Orlando Marketing Coordinator
- BSides Orlando Social Media Lady
- @willasaywhat on Twitter

Exfiltration 101

What Is It?

“Data exfiltration is the unauthorized transfer of sensitive information from a target’s network to a location which a threat actor controls.”, Trend Micro

Why Should You Care?

- Data loss costs time, money, and your sanity.
- Ever found a credential dump on pastebin?
- Come on, are we still reading the slides?
- If you didn’t care you wouldn’t be here.

82%

Of those surveyed in 2012 from /r/netsec said that preventing exfiltration was important to the security of their information systems

Esoteric Exfiltration

- Mask traffic with normal usage patterns
  - Social media
  - Web traffic
  - Protocols used for day to day business
- Hide data in known “safe” payloads
  - Status updates
  - HTTP POST Payloads
- Stay quiet, within normal payload sizes
  - Throttle exfil chunks
  - Set payload sizes based on the channel used
  - Encode and/or encrypt chunks

Covert Channels & Where to Find Them

Transport: Change the Channel

- Network
- 3rd Party
- Airwaves

Network: Data on the Wire

- The Obvious
  - HTTP
  - SSH
  - Netcat

- The Discreet
  - Using normal protocols in abnormal ways

3rd Party: Hide Yo Data

- The Obvious
  - Dropbox
  - Pastebin

- The Discreet
  - Flickr
  - Twitter

Airwaves: Breaking Layer One

- The Obvious
  - Wifi Adapter on a Raspberry Pi
- The Discreet
  - Xbee 900mhz Long Range Mesh Network

Weaponizing Squirrels

Squirrel: Exfiltration for Nuts

- Python 2.7 based application
- Open Source; MIT License
- Extensible via simple module based plugins
- Upload and execute with CLI arguments

Module Overview

Squirrels steal nuts, get it?

<REDACTED>

Squirrel Demo

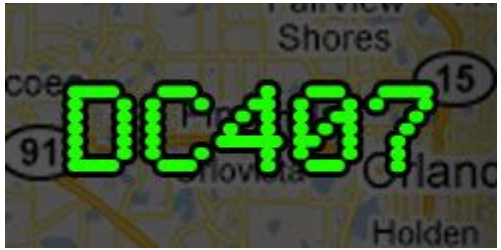
Closing Remarks

Future Work

- Additional Squirrel Modules:
  - <REDACTED>
- Metasploit Post Module
- Longer range, more nodes, less physical space using Teensy.

Shoutouts

FamiLAB



VERACODE

LOCKHEED MARTIN

BSIDES ORLANDO