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

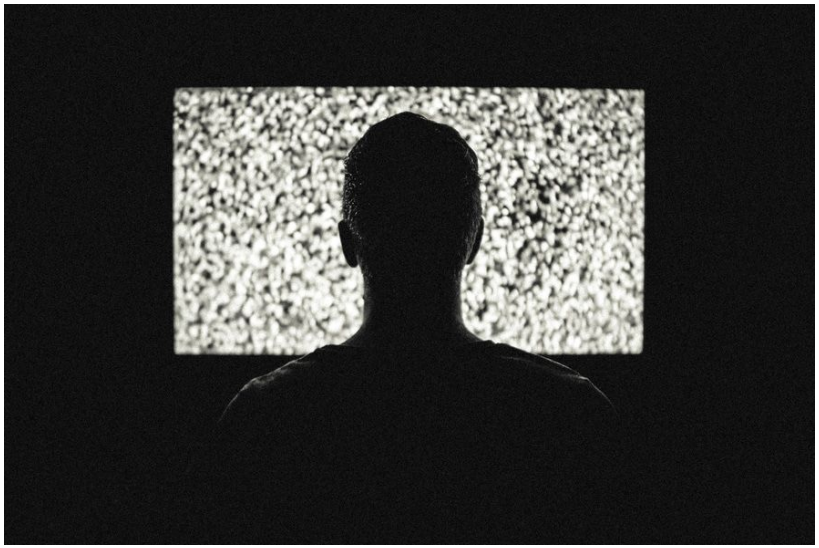
Covert Channels & Where to Find Them

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

Transport: Change the Channel

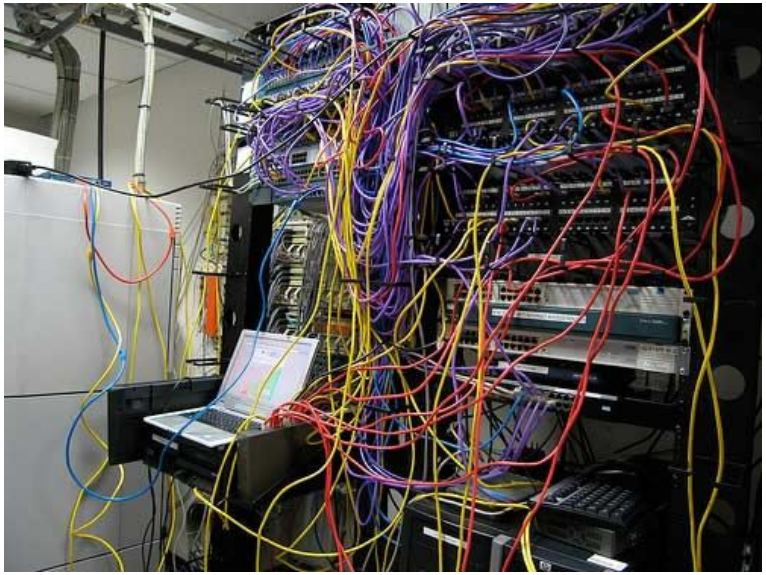
- Network Protocols
- 3rd Party Drops
- To the Airwaves



Network Protocols: Data on the Wire

- The Obvious
  - HTTP
  - SSH
  - Netcat
  - DNS?

- The Discreet
  - Using normal protocols in abnormal ways

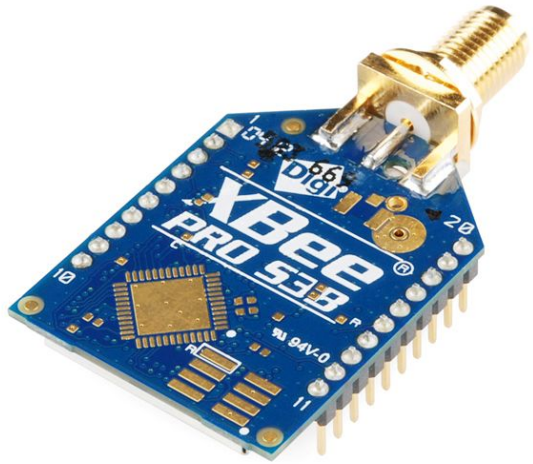


3rd Party Drops: Hide Yo Data

- The Obvious
  - Dropbox
  - OneDrive
  - Google Drive
  - Pastebin
- The Discreet
  - Flickr
  - Imgur
  - Twitter
  - Facebook

To the Airwaves: Breaking Layer One

- The Obvious
  - Wifi Adapter on a Raspberry Pi
- The Discreet
  - Xbee 900mhz Long Range Mesh Network
  - Over Ham Radio (APRS) w/ Repeaters
  - Lasers, just, lasers



Blue Team Says What?

Defenses & Detection

- Block endpoints by URI/IP
- Block egress at the firewall by port/proto
- Detect anomalies in payload size and frequency
- Block USB devices by class or device-id (USB serial)

Offensive Maneuvers

- Blacklists don’t work
- Disrupts normal business
- Context is critical, but difficult to automate
- USB Device IDs? Good luck with that.

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

```
willasaywhat:~/workspace (master) $ python -m squirrel
usage: python -m squirrel [-h] [-c CHANNEL] [-r RECV] [-f
FILENAME]
                          [-s SETTINGS] [-v]

Squirrel: Exfiltration for Nuts

optional arguments:
  -h, --help            show this help message and exit
  -c CHANNEL, --channel CHANNEL
                        selects the channel to use
  -r RECV, --recv RECV  tells squirrel to retrieve nuts
  -f FILENAME, --filename FILENAME
                        selects the file to exfiltrate
  -s SETTINGS, --settings SETTINGS
                        sets the settings dictionary for the
channel. ex: -s
                        '{"client_id": "value", "client_secret":
"value"}'
  -v, --verbosity       increase output velocity
None
```

Module Overview

Squirrels steal nuts, get it?

```
from abc import ABCMeta, abstractmethod,
abstractproperty


class Channel(object):
    __metaclass__ = ABCMeta

    _name = "Sample Channel Name"
    _description = "Sample Channel Description"
    _settings = {}
    _chunkSize = 0  # Size in bytes of the max chunk per send/recv

    def name(self):
        return self._name

    def description(self):
        return self._description

    def chunk_size(self):
        return self._chunkSize

    def __init__(self):
        pass

    @abstractmethod
    def send(self, chunks):
        pass

    @abstractmethod
    def recv(self):
        pass

    def get_settings(self): return self._settings

    def set_settings(self, value): self._settings = value

    _settings = abstractproperty(get_settings, set_settings)
```

https://github.com/willasaywhat/squirrel

Closing Remarks

Future Work

- Additional Squirrel Modules:
  - Facebook Attachments, Flickr, FTP, SFTP, Telnet, Netcat, etc.
- Executable payload generation with PyInstaller
  - Msfvenom style payloads
- Metasploit Post Module
- Longer range hardware, more nodes, less physical space using Teensy.
- Integrate Cloakify DLP avoidance ciphers
- Customizable timing of send/recv

Shoutouts

– – –

FamiLAB

VERACODE

LOCKHEED MARTIN

BSIDES ORLANDO

Thank you, okay? Cool. <3