black hat®
ARSENAL

DECEMBER 2-5, 2019
EXCEL LONDON, UK

PyExfil

Stress Testing Detection (and your creativity)

What is PyExfil?

A little Python package for data exfiltration.
Started as a playground, turned PoC collection, to proper package.
Intended to help test DPI/DLP/other network instrumentation.
Let’s go to Version 1.0.0

What’s new in version 1.3

- More modules converted to new calling convention.
- 4 brand new modules.
- General fixups.
- Setting the groundwork for version 2.0

We still need GOlang coders!

Classes Overview - NO BEST! (½)

- Comm(unication)
  - Network based communication.
  - Usually short burst/size messages.
  - Mainly intended for C&C communication.
- Network
  - Network based communication.
  - Intended for larger volumes of communication.
  - In version 2.0 - separate between LAN vs. WAN communication.

Classes Overview - NO BEST! (2/2)

- Physical
  - Anything involving physical exfiltration.
  - Intended for air-gapped networks.
  - Usually requires SYSTEM/root level access.
- Stega(nography)
  - Designed to hold steganography exfiltration modules.
  - However, currently holds file-based exfiltration as well.
  - Should be fixed in version 2.0.

Modules Overview

- **Comm**
  - AllJoyn
  - ARP Broadcast
  - MDNS Query
  - NTP Request
  - DropBox LSP (Broadcast or Unicast)
  - DNS over TLS
  - ARP Broadcast
  - JetDirect
  - GQUIC - Google Quick UDP
  - UDP Source Port
  - Cert Exchange
- **Network**
  - DNS query
  - HTTP Cookie
  - ICMP (8)
  - NTP Body
  - BGP Open
  - HTTPS Replace Certificate
  - QUIC - No Certificate
  - Slack Exfiltration
  - POP3 Authentication
  - FTP MKDIR
  - Source IP-based Exfiltration
  - HTTP Response
- **Physical**
  - Audio - No listener.
  - QR Codes
  - WiFi - On Payload
- **Steganography**
  - Binary Offset
  - Video Transcript to Dictionary
  - PNG Transparency
  - ZIPCeption

What should i do with it?

1. Test your detection systems for C&C or Data Exfiltration.
2. Compare what vendors promise to what is being delivered.
3. Utilize during Red Teaming.
4. *Use your creativity to create more modules.

What’s there to expect in v2.0?

- More backwards compatibility of modules.
- Easier py2exe compilation.
- ~~Full Python3/Python2 support.~~
- Conversion of modules to Go.
- More modules.
- Split network class into LAN and WAN subclasses.
- Create frameworks for combining modules.

How can i help?

- TEST.
  - Give us your feedback. A module breaks, doesn’t work under certain conditions - let us know and open a ticket on GitHub or send us an email.
- Suggest
  - Got an idea for a module? Send it our way. Please add explanation as to the merits of the method you’re suggesting.
  - Got into a scenario where none of the modules work? Let us know and we can probably find a module that will or write up a new one.
- Write
  - Submit changes on GitHub.