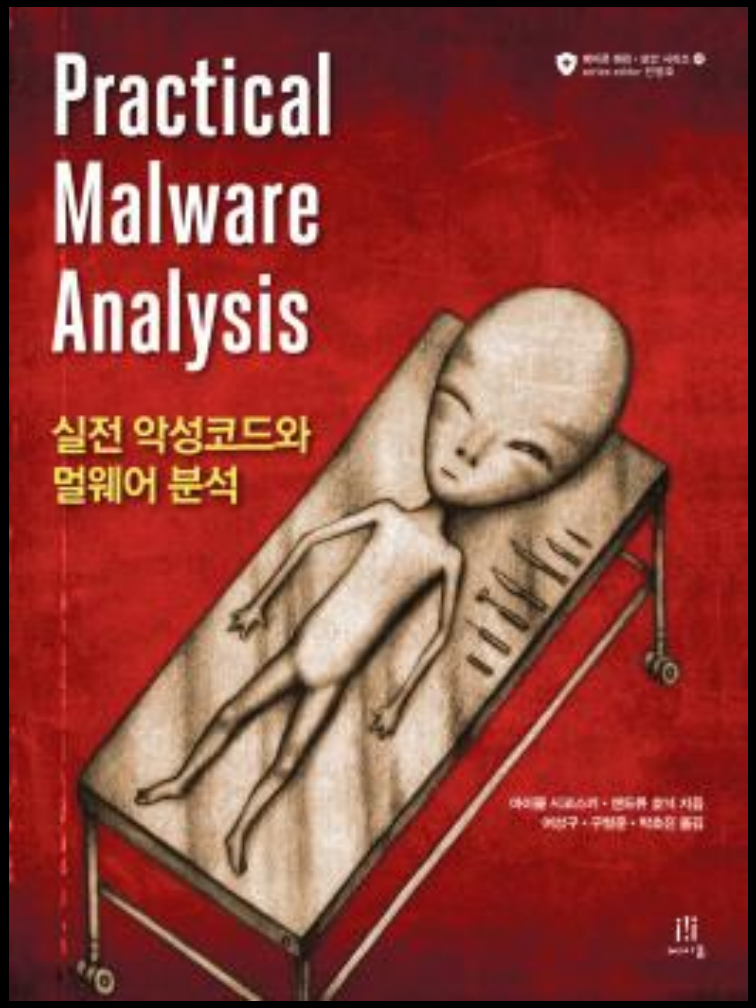
Dynamic Malware Analysis Workshop

Counterfeiting the Pipes with FakeNet

PRESENTED BY: Michael Sikorski & Andrew Honig

OCTOBER 17, 2014

No Starch Press



Outline

- Malware on the Network
- Faking the Network
- FakeNet
  - Features
  - Setup
  - Configuration
  - Implementation
  - Fame
  - New Features
- Conclusion

Background

Hiding in Plain Sight

- Attacker Goal: avoid being detected
  - Lose access to the victim machine
  - Risk of being detected in the future
- To blend in attackers often use many tactics
  - Mimic existing protocols
  - Use existing infrastructure
  - Using client-initiated beaconing
  - Dynamically changing destination address
- Still see many custom binary protocols

Mimicking Existing Protocols

- Attackers like popular protocols, such as HTTP, HTTPS, DNS etc…
  - This gives them a chance to blend in given the volume of legitimate traffic
  - IRC used to be a popular protocol
- HTTP or HTTPS are very popular
  - Commands and other communication can be passed through GET or POST requests
  - Most organizations see a very large volume of both protocols

Using Existing Infrastructure

- Attackers like to use existing, legitimate resources
  - Servers used for malware only stick out
  - Reduces the changes of being caught
  - Legitimate use helps mask malicious use
  - Investigation of the IP address reveals a legitimate address

Client-initiated Beaconing

- NATs and Proxies
  - All outbound connections appear to come from the same IP address
  - This can make it difficult for an attacker to know which machine is communicating
    - System survey in beacon
    - Understanding how the profile is passed on the network gives the defenders an opportunity for detection (Reversing)

Why Fake the Network?

- Trick the malware
- Malware often requires
  - IP address
  - Downloads a webpage or image
- More running = more indicators
  - Code Coverage

Existing Tools

Tools for Malware on the Network

- When writing Chapter 3
  - Nothing easy to use
  - Seemed to be a huge gap in the field
  - Surveyed all the tools

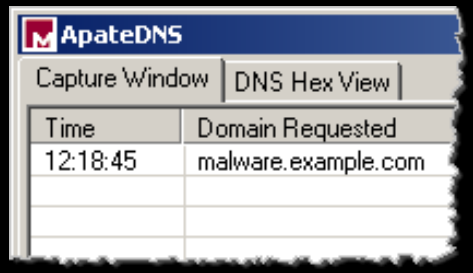
FakeDNS

- Included with iDefense Malcode Analysis Pack
  - Installed on the local machine
  - Responds to DNS requests from the malware
  - Displays the hex and ASCII results of all requests / responses
  - Unreliable
- To use
  - Install FakeDNS
  - Set the local DNS server to `127.0.0.1` (takes effort)
  - Start FakeDNS

FakeDNS Example

Other options for faking DNS

- ApateDNS
  - Mandiant GUI tool



- fakeDNS.py
  - Linux tool
  - With REMnux

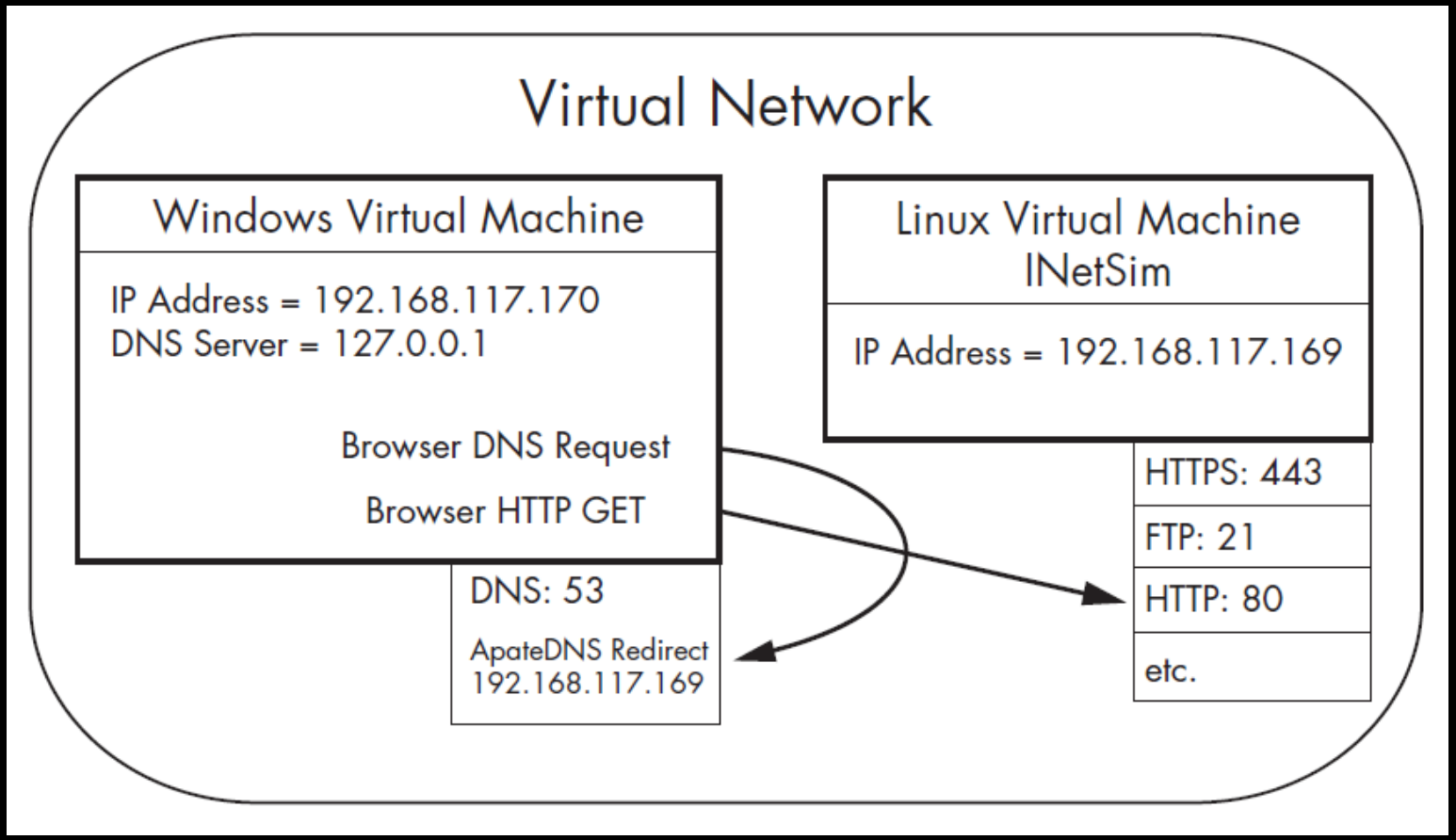
NetCat

- Redirect traffic by manipulating DNS
- Set NC in listen mode to accept the connection
- Usage:
  - `nc -l -p 80`
- Raw and difficult to customize

INetSim

- Free, Linux-based VM
- Emulates common services
- HTTP, HTTPS, FTP, IRC, DNS and so on
- Serves up what it can
- Fully configurable
- Some assembly required
- Available at:
  - http://www.inetsim.org/

INetSim


Virtual Network
Windows Virtual Machine
IP Address = 192.168.117.170
DNS Server = 127.0.0.1
Browser DNS Request
Browser HTTP GET
DNS: 53
ApateDNS Redirect
192.168.117.169
Linux Virtual Machine
INetSim
IP Address = 192.168.117.169
HTTPS: 443
FTP: 21
HTTP: 80
etc.

FakeNet

FakeNet

- Simple to run
- Easy to configure
- Covers the most popular protocols
- Runs on Windows
- Allows you to completely trick the malware networking operations
  - Most popular malware protocols
- Layered Service Provider (LSP)
- Supports pcap based capturing
- Extensions
- Easy Fake Web Servers

FakeNet Usage

- Available at: fakenet.info
- Bleeding Edge distributed in this workshop

```
[DNS Query Received.]
  Domain name: www.evilmalware.com
[DNS Response sent.]


[Received new connection on port: 80.]
[New request on port 80.]
  GET /iexplore.exe HTTP/1.1
  Accept: */*
  Accept-Encoding: gzip, deflate
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2
.0.50727; .NET CLR 1.1.4322; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648)
  Host: www.evilmalware.com
  Connection: Keep-Alive

[Sent http response to client.]
```

File download example

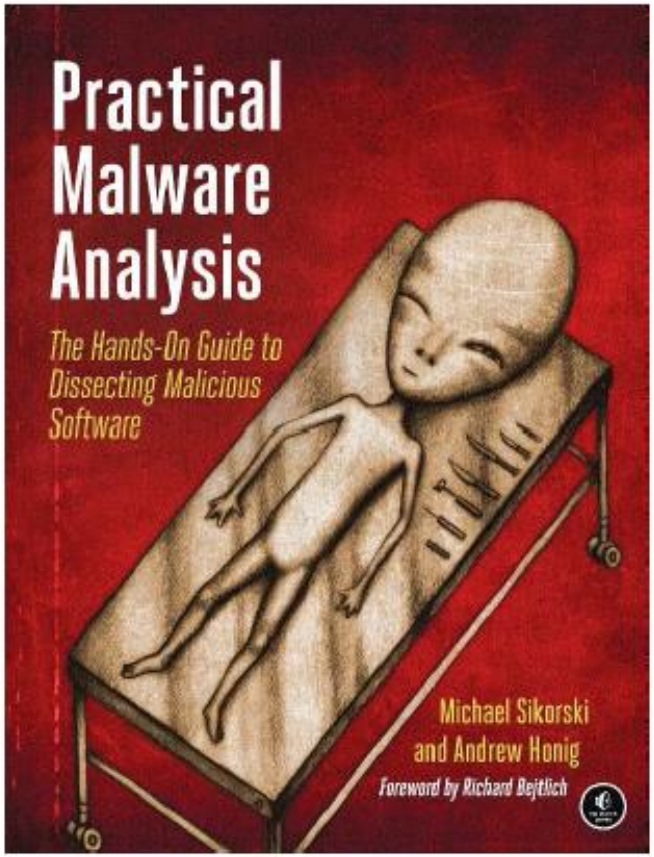
il.com/malicious.pdf - Microsoft Internet Explorer

Atteindre Favoris ?

Rechercher Favoris

/www.evil.com/malicious.pdf

OK Liens »

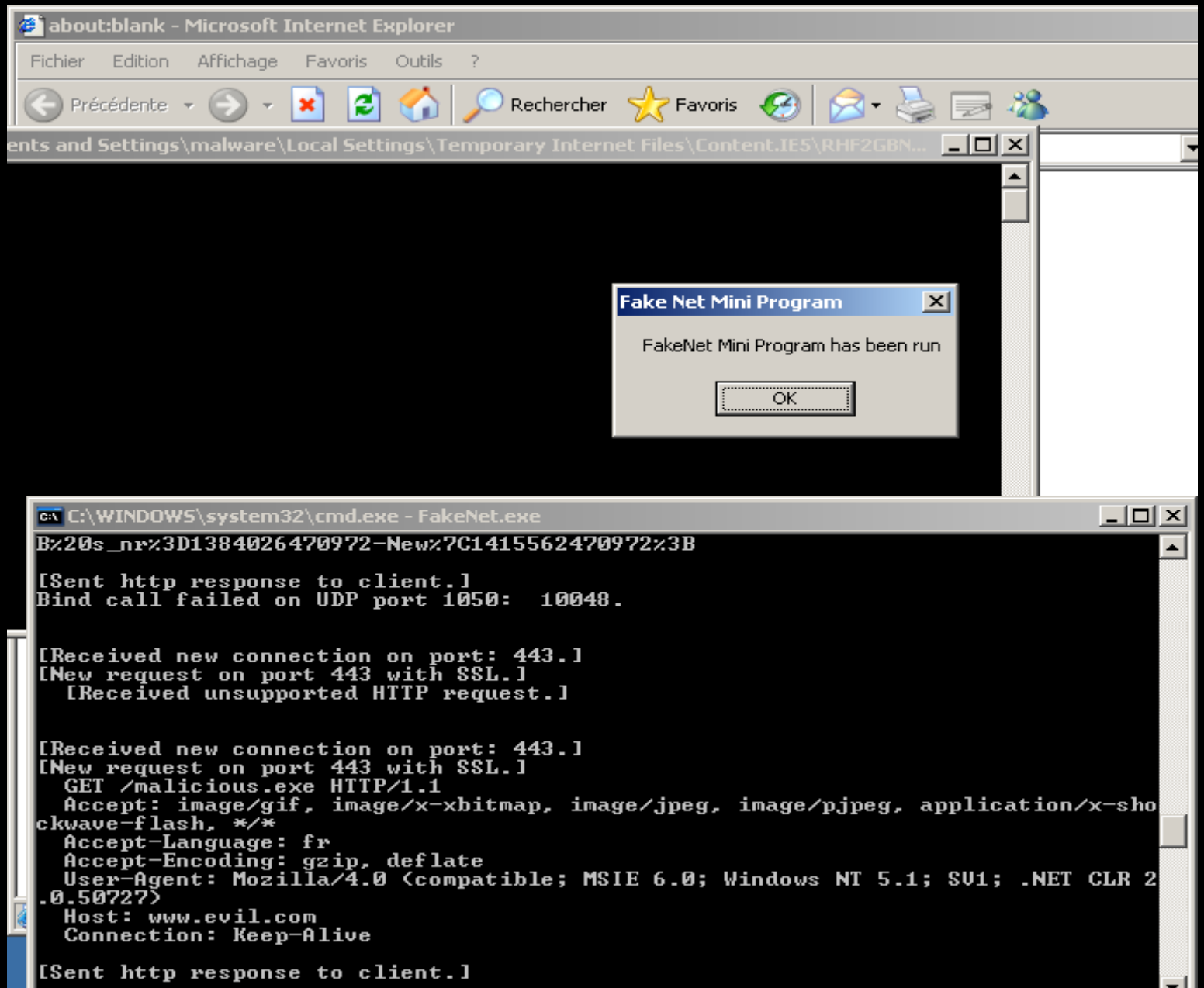


C:\WINDOWS\system32\cmd.exe - FakeNet.exe

```
[DNS Query Received.]
  Domain name: www.evil.com
[DNS Response sent.]


[Received new connection on port: 80.]
[New request on port 80.]
  GET /malicious.pdf HTTP/1.1
  Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, applicati
ckwave-flash, */*
  Accept-Language: fr
  Accept-Encoding: gzip, deflate
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .N
.0.50727)
  Host: www.evil.com
  Connection: Keep-Alive

[Sent http response to client.]
Bind call failed on UDP port 1042:  10048.

[DNS Query Received.]
  Domain name: acroipm2.adobe.com
[DNS Response sent.]
```

Zone inconnue

Downloaders



Implementation

LSPs & Listeners

- Layered Service Providers (LSP)
  - Malware uses LSP
    - Injection
    - Manipulate packets
  - Security product uses LSP
    - Quality of service (QOS)
    - URL filtering software
  - Why can’t we use it?
- Listeners
  - Other tools
  - Servers

LSP

- WSPdll.dll
  - Loaded into all Winsock processes
  - Configured by FakeNet in the Winsock system configuration database
    - WSCInstallProvider
      - SOFTWARE\\WinSock2\\FakeNet Layered Provider
      - GUID = 5a21f160-df30-11cf-8927-00aa00539f1c
      - Install in the chain
  - Gets the DLL loaded for hooking
    - WSPSocket, WSPCloseSocket
    - WSPAccept, WSPAcceptEx, WSPConnect, WSPRecv, WSPRecvFrom, WSPSend, and WSPSendTo

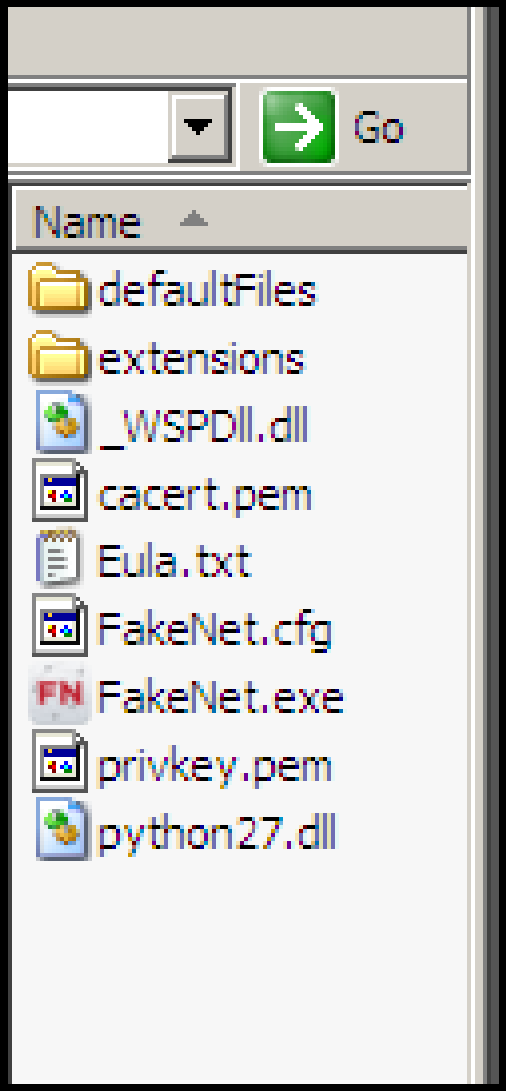
Listeners

- Listening on the ports you configure
  - Happens with or without the LSP
- TCP and UDP Listeners
  - HTTP
  - ICMP
  - Dummy
  - DNS
  - Special Listeners
    - HTTPS
    - Python

Setup

Files

- defaultFiles directory
- extensions directory
- FakeNet.cfg
- FakeNet.exe
- *.pem
- _WSPDll.dll



Running

- Double-click FakeNet.exe
- Recommended
  - Get an IP address
  - Reboot if you install a new version
    - FakeNet warns you

Configuration

PacketDumpOptions

- FakeNet reconstructs a packet capture that can be opened in Wireshark
- This is not a standard packet capture.
- Windows does not have a local network adapter for capturing packets
  - Wireshark can’t listen on localhost
- Useful when dealing with binary data that is not well displayed by FakeNet text output
  - Developing Network Decoders when you don’t have full pcap of all features
- `PacketDumpOptions DumpPackets:XXX Fileprefix:XXXX`

InvasiveOptions

- Supports
  - DummyService
  - Direct to IP
  - ConnectionBreak - NEW
- `InvasiveOptions EnableDummyService:XXX RedirectAllTraffic:XXX ConnectionBreak:XXX MaxListeners:##`

DNSOptions

- Options for DNS success
  - ModifyLocalDNS
  - StopDNSClientService - NEW
  - `DNSOptions ModifyLocalDNS:XXX StopDNSClientService:XXX`

OutputOptions

- `OutputOptions DumpHTTPPosts:Yes DumpOutput:Yes Fileprefix:output ProcessLogging:No POSTresponse:No`

Listeners

- Listener lines must start with a listener type from the following options:
  - DNSListener
    - `DNSListener Port:53 DNSResponse:127.0.0.1 NXDomains:0`
  - HTTPListener
    - `HTTPListener Port:80 UseSSL:No Webroot:None`
  - RawListener
    - `RawListener Port:1337 UseSSL:No`
  - ICMPListener
  - PythonListener
    - SMTP Listener option

Custom Python Listeners

- Required functions
  - FN_Init
  - FN_NewConnection
    - Must call recvData and sendData (imported from FakeNet) as necessary to send and receive data:
      - sendData takes two parameters
        - Context of the connection
        - String to send
        - Returns the number of bytes successfully sent.
      - recvData also takes two parameters
        - Context of the connection
        - Size to use for the internal buffer
- Useful for developing network decoders

Fame

Malware looks for us!

- Pushdo Botnet
  - https://www.bluecoat.com/security-blog/2013-09-11/look-evasion-techniques-pushdo-botnet
- Spams us if FakeNet is running!

TCP	40	28682 > smtp [SYN] Seq=0 Win=1024 Len=0
TCP	40	smtp > 28682 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
TCP	40	28682 > smtp [ACK] Seq=1 Ack=1 Win=1024 Len=0
SMTP	93	S: 220 PracticalMalwareAnalysis.COM STMP Service Ready

DNS	86	Standard query response 0xe21a A 127.0.0.1
DNS	58	Standard query 0x0169 A janpalduv.kz
DNS	86	Standard query response 0x0169 A 127.0.0.1
DNS	59	Standard query 0xcd1e A geojoglunu.kz
DNS	88	Standard query response 0xcd1e A 127.0.0.1
DNS	61	Standard query 0x943e A repadzeovuzf.kz
DNS	92	Standard query response 0x943e A 127.0.0.1
DNS	58	Standard query 0xcfd1 A zoswecboh.kz
DNS	86	Standard query response 0xcfd1 A 127.0.0.1
DNS	58	Standard query 0x760a A palralnos.kz
DNS	86	Standard query response 0x760a A 127.0.0.1
DNS	60	Standard query 0x9d85 A seojuvomojo.kz
DNS	90	Standard query response 0x9d85 A 127.0.0.1
DNS	58	Standard query 0x23d7 A nimziluff.kz
DNS	86	Standard query response 0x23d7 A 127.0.0.1
DNS	61	Standard query 0x9f46 A farurheoxuff.kz

Pushdo Botnet

- Changes when “FakeNet.exe” isn’t running:

DNS	89	Standard query response 0x6a4c A 184.107.236.2
DNS	97	Standard query response 0x50c4 A 64.99.80.30
DNS	79	Standard query 0x629b A www.acicinvestor.ca
DNS	109	Standard query response 0x629b CNAME acicinvestor.ca A 207.150.203.191
DNS	71	Standard query 0x0fc1 A biurimex.pl
DNS	87	Standard query response 0x0fc1 A 89.161.181.123
DNS	158	Standard query response 0x7413
DNS	95	Standard query 0x6e8f A x-cellcommunications.de.localdomain
DNS	78	Standard query 0xedd9 A orion-networks.net
DNS	84	Standard query 0x0c3a A bapasitaramsevatrust.org
DNS	100	Standard query response 0x0c3a A 68.67.76.41
DNS	80	Standard query 0xa17e A sortedorganizing.com
DNS	96	Standard query response 0xa17e A 69.195.124.64
DNS	86	Standard query response 0x9b33 A 218.150.78.243
DNS	78	Standard query 0x79e2 A hartmultimedia.com

New Features

Process Logging

- Logs the following:
  - Process name, PID, IP, Port to be displayed in the output to the user

```
[iexplore.exe (936) is connecting to 154.34.222.22:80]
```

  - Allows you to pin point the process is responsible for the network traffic
  - OutputOption
    - ProcessLogging:”Yes” or “No”
- Logs
  - SendTo
  - Connect
  - Socket
  - Close Socket
- Demo

Debug Breakpoint

- Enables the user to cause an exception upon a connection
- Can trace the source of the malicious connection
- Pauses upon WSAConnect in LSP
- Set up a JIT debugger (i.e. OllyDbg)!!!!!
- Trace the call stack in the debugger
- Quickly locate the code that performed the connection
  - “The Source”
  - Find injected shellcode
- InvasiveOption
  - ConnectionBreak: Yes” or “No“
- Demo

Stop DNS Service

- Stops the DNScache service
  - “DNS Client”
    - “Resolves and caches Domain Name System (DNS) names for this computer.”
- DNS requests more easily caught by FakeNet
- LSP won't see the request to port 53
  - Even if you restart the service!
- Stopping the service forces the browser to make the request themselves
  - Lazy IE and Mozilla can do their own requests
- InvasiveOption
  - StopDNSClientService:”Yes” or “No”
- Demo

POST Response

- Enables a response to an HTTP POST request
- Malware performs POST requests
  - Looks for data to be returned to it
- Option allows the user to specify if/when they want the POST to get data back
- OutputOption
  - POSTresponse: ”Yes” or “No"

No IP

- Detects when there is no IP address
- Suggests to the user that they restart FakeNet
- Get an IP!!!
  - FakeNet doesn't work as well without an IP
  - Malware Analysis doesn’t work as well without an IP

Additional (not useful) Changes

- Sexy new icon
- Bug fixes
  - Many user issues fixed
- fakenet.info
- Additional default files
  - bmp
  - ico

What’s next?

- WFP support
  - LSP deprecated since Windows Server 2012
  - Windows Filtering Platform is the new way to perform this same technique
  - Needed for Windows 8

Thanks

- People
  - Sébastien Damaye – http://www.aldeid.com/wiki/FakeNet
  - Willi Ballenthin
  - Richard Wartell
- Code
  - Bleeding Edge

Hands-on Section After Lunch

- Using FakeNet features
- Follow the lab steps
- Solve the challenge and win beer!

Questions

?

fakenet.info

@mikesiko
michael.sikorski@mandiant.com
sikorski@cs.columbia.edu

andyhonig@gmail.com