

# Late-Breaking Computer Attack Vectors



---

**PaulDotCom Enterprises, LLC**


September 2008  
Paul Asadoorian  
PaulDotCom Enterprises, LLC  
[paul@pauldotcom.com](mailto:paul@pauldotcom.com)

# Introduction

---

- (Paul Asadoorian \* Geek) = PaulDotCom
- PaulDotCom Security Weekly
- Penetration Testing, Security Consulting, Device Testing
- WRT54G Hacking book & SANS Course



  
PaulDotCom Security Weekly  
<http://www.pauldotcom.com>



# Outline

---

- Nmap - The new network swiss army knife
- Botnets Count
- Mobile Insecurity
- Wireless Router Driver Vulnerabilities
- FAIL Of The Month (FOTM)

*“...hacking is the action of outsmarting the others and as such it may take any form”*

- pdp, gnucitizen.org

# Nmap – Not Just A Portscanner

---

- Nmap is a:
  - portscanner
  - operating system fingerprinter
  - service identifier
  - visual network mapper
  - extensible framework
  - tracerouter
  - netcat implementation
  - network historian



# Newer Nmap Features

---

- ndiff - Takes two Nmap scans and shows you the differences

**Only  
available in  
the current  
svn versions!**

```
minime (00:1F:C6:7B:4E:A2):  
  Host is up, was unknown.  
  Add mac address 00:1F:C6:7B:4E:A2.  
  Add ipv4 address 192.168.69.6.  
  Add hostname minime.pauldotcom.com.  
  22/tcp is open.  
  999 tcp ports are closed.  
linky (00:12:1E:BE:D0:D2):  
  80/tcp is filtered, was open.  
  443/tcp is filtered, was open.  
johnnymo (192.168.69.67):  
  Host is up, was unknown.  
  Add ipv4 address 192.168.69.77.  
  Add hostname johnnymo.pauldotcom.com.  
  22/tcp is open.
```

# Extending Nmap

---

- Important to identify rogue access points on your network
- Wireless IDS can miss stuff (802.11n)
- Wired-Side detection is one way, and a method you should implement
- Nmap is now, in my opinion, the best free tool to do this, with a little help from Perl

# Nmap Command To Hunt Rogue APs

---

- Scan selected ports to save time
- Run all scripts and version checks
- Save files with time/date stamps
- Perform OS finger print
- Do it with “aggressive” timing

```
nmap -PN -pT:80,443,23,21,22,U:161,1900,5353,53 \  
-sUVS --script=all -oA osfinger%T%D \  
-O -T4 192.168.69.0/24
```

# Nmap : : Parser

---

- Easy to use Perl library for extending Nmap

```
rogueapdetect.pl v0.001 - ( paul@pauldotcom.com )
```

```
-----
```

```
Scan Information:
```

```
Number of services scanned: 7
```

```
Start Time: 1221793134
```

```
Scan Types: syn udp
```

```
Hosts scanned:
```

```
Address      : 192.168.69.95
```

```
OS match     : OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34)
```

```
Device Type: WAP
```

<http://pauldotcom.com/rogueapdetect.pl>

# Visualize Your Network

Scan Tools Profile Help

Target: 192.168.1.0/24 Profile: Operating System Detection Scan

Command: nmap -O -v 192.168.1.0/24

Hosts Services

OS	Host
	192.168.1.30
	192.168.1.226
	192.168.1.97
	192.168.1.51
	192.168.1.95
	192.168.1.92
	gogo.paul.com 192.168.
	192.168.1.204
	madmonk.paul.com 192.
	192.168.1.230
	192.168.1.14
	betty.paul.com 192.168.
	192.168.1.218
	192.168.1.2
	linky.paul.com 192.168.1
	192.168.1.50
	192.168.1.244
	192.168.1.210
	minime.paul.com 192.16

Nmap Output Ports / Hosts Topology Host Details Scans

Hosts Viewer Fisheye Controls

Action

Interpolation

Layout

View

- address
- hostname
- icon

Navigation 225.0

Zoom 156

Ring gap 30

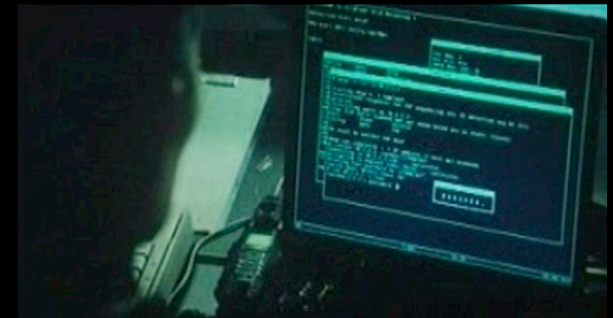
Lower ring gap 10

Fisheye on ring 1.05 with interest factor 2.00 and spread factor 0.50

# Nmap – Good Things Coming

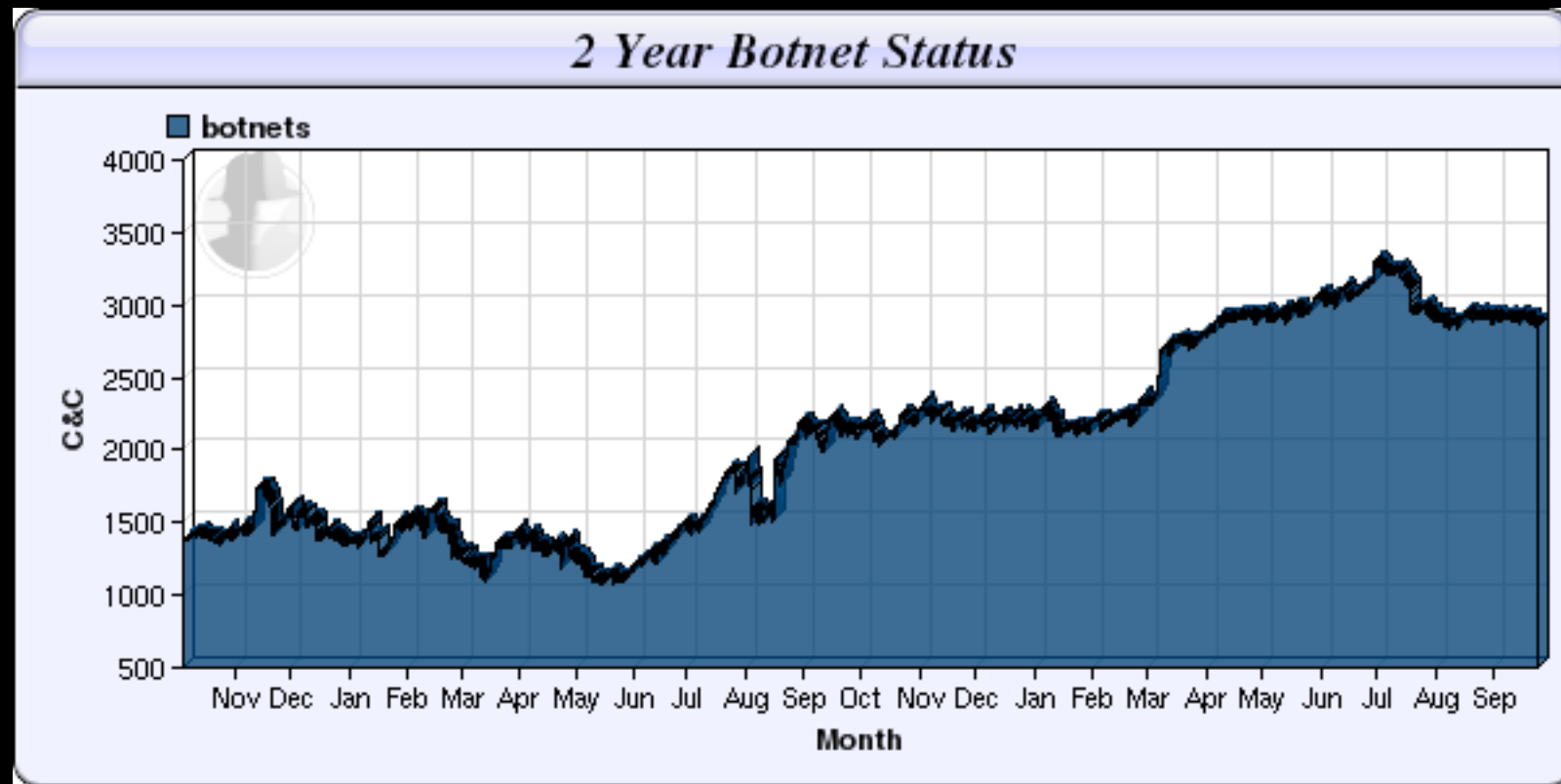
---

- ncat will come with Nmap and be the netcat we always wanted
  - SSL and IPv6 support
- NSE (Nmap Scripting Engine) will continue to improve and gain functionality
- Upgrade to the latest version, very important
- Many uses, should be a tool that you are familiar with



# Botnet Counts: For Good Measure

- A picture speaks a thousand botnets:



Reference: <http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.BotnetCharts>

# Botnet Counts: For Good Measure

---

- Automated SQL injection attacks appear to be part of the problem
- Code find SQL injection flaws automatically
- Searches database for text fields
- Adds script code to every text field
- Resulting code, usually <SCRIPT> tag is added to pages

# Botnet/SQL Injection Defense

---

- Check IIS web server logs for:

```
RA;DECLARE%20@S%20NVARCHAR(4000);SET  
%20@S=CAST(0x4400450043004C004100520045002000400054002000760  
0610072006300680061007200280032003500350029002C004000430020  
<snip>
```

- Use URLScan/Mod\_security
- Find and fix all SQL injection points
  - Grendel-Scan is great for this

# Mobile Insecurity

---

- S40 is an older operating system for ARM-based phones
- However, reportedly there are over 100 million phones “in the wild”
- A Java vulnerability plagues this platform
- This could mean bad things...



# Mobile InSecurity

---

- Vulnerabilities allow malicious Java programs to:
  - Make calls
  - Record conversations
  - Send text messages
  - Take pictures and/or video
  - Access data (address book typically)



# Mobile Security: Defenses

---

- Disable features you do not need, such as Java (not always possible)
- Use anti-virus software on your phone (F-Secure)
- Implement security features (screen locks, sim card locks)
- Two cans and a string?

# Wireless Router Driver Vulnerabilities

---

- Several wireless routers contained vulnerabilities in wireless drivers
- Simply need to be in range of the AP to exploit
- Netgear router has no patch yet
- Wireless drivers, yes the same ones from Maynor/Cache debacle, still pose threats
- They are in routers, phones, laptops, printers

# Defending Your Wireless Devices

---

- If you don't need wireless, disable it
- Keep your drivers up-to-date
- Use WPA encryption on all your wireless devices that support them
- Use IDS to detect post-compromise behavior
  - After the fact, but better than not having it
  - [emergingthreats.net](http://emergingthreats.net) has some good Snort rules

# FAIL Of The Month (FOTM)

- Never leave it unattended!
- Story 1 - Don't leave it near the door
- Story 2 - The lone laptop at Starbucks
- Same goes for cell phones, USB thumb drives, access tokens



**/\* End \*/**

---

- Web: <http://pauldotcom.com/>
- Wiki: <http://pauldotcom.com/wiki/> - Show notes for each episode
- Forum: <http://forum.pauldotcom.com>
- Email: [paul@pauldotcom.com](mailto:paul@pauldotcom.com)



PaulDotCom Enterprises, LLC

