

# From The Trenches (Australia)

What We Are Seeing Within Security Today

by Peter Benson

# Security-Assessment.com – Who We Are

- Australasia's pure-play security firm
- Largest team of security professionals in NZ
- Offices in Sydney, Auckland, Wellington
- Specialisation in multiple security fields
  - Security assessment
  - Security management
  - Forensics / incident response
  - Research and development



# Continuing Security Trends

- Still seeing opportunity hacks “script-kiddie” style
  - Windows machine fresh installed will be hacked in approximately 20 minutes
- Virus levels continuing to increase
- Time-to-exploit once a vulnerability is known is continuing to go down
- The number of vulnerability advisories is increasing





**LANGUAGE**

**SEARCH**

- MAIN MENU**
- [Homepage](#)
  - [News from zone-h](#)
  - [News from the world](#)
  - [Advisories](#)
  - [Download area](#)
  - [Zone-H works](#)
  - [Digital attacks](#)
  - [Attacks archive](#)
  - [Attacks archive](#)
  - [Top Attackers](#)
  - [Attack notification](#)
  - [Internet spam/frauds](#)
  - [Stay tuned](#)
  - [Infosec pager](#)
  - [Mailing list subscription](#)
  - [Early Warning subscription](#)
  - [Zone-H Mirrors](#)
  - [Become a Zone-H Partner \*\*NEW!\*\*](#)
  - [Passive public area](#)
  - [Stats & Graphs](#)
  - [Active public area](#)
  - [Legal corner](#)
  - [Forum section](#)
  - [Join Zone-H IRC chat](#)
  - [Zone-H events](#)
  - [The World Meets](#)
  - [Interviews section](#)

**DIGITAL ATTACKS ARCHIVE**

[ [Disable filters](#) | [View Top Attackers](#) ]

Attacker:  Domain:

Date:  :    System:

**Legend:**

- H** - Homepage defacement
- M** - Mass defacement (click to view all defacements of this IP)
- R** - Redefacement (click to view all defacements of this site)
- ★** - Special defacement

Time	Attacker		Domain	OS	View
2005/05/01	effdee	H M	...kcommunications.com.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	coopers.com.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	concordia.sa.edu.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	concordia.sa.edu.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	collina.com.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	collina.com.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	charlesmeltonwines.com.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	charlesmeltonwines.com.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	ccwcoop.com.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	ccwcoop.com.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	...re.medialibrary.com.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	bendigoland.com.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	ashwoodstudio.com.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	arrowcrestgroup.com.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	aldridgetraffic.com.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/05/01	effdee	H M	laynebeachley.com.au	Linux	<a href="#">view</a>   <a href="#">mirror</a>

Q8crackers

w@sh3re

N-1 >;D

-={ Syst3m\_p4ss3d . DeadLine . DosMan . SarraG . N-1 }=-

-=[ Mess With The Best Die Like The ResT ]=-

Everything is Hackable

Copyright 2005 © Q8crackers

f0r h3lp Join

Efnet

# Zone-H.org Statistics

- 473 .au sites mirrored in the last month
  - Those are only the ones zone-h.org hears about
- Of those sites:
  - 334 .com.au, 22 .net.au, and 2 is .gov.au
- Of all hacks on Zone-H.org:
  - 60% Linux, 30% Windows, 10% Other
  - (General web server statistics show 70% Linux, 20% Windows, 10% Other)

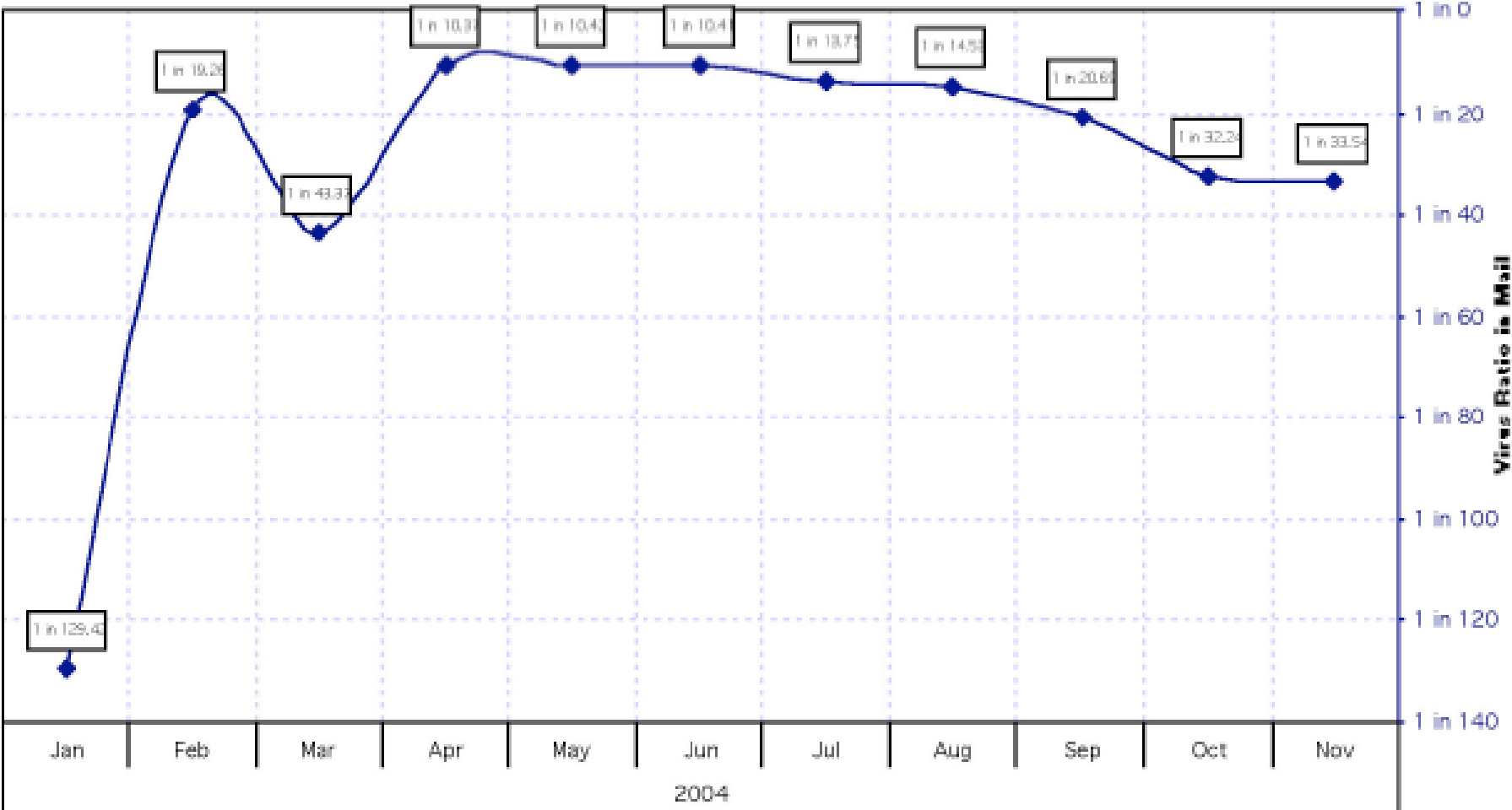


# Virus Statistics (from MessageLabs)

- Virus levels continuing to increase
- Virus ratio in email
  - 2002 – 0.5%
  - 2003 – 3%
  - 2004 – 6%
- 2004 saw several large viruses including:
  - MyDoom
  - Netsky/Bagle war



# 2004 virus Levels

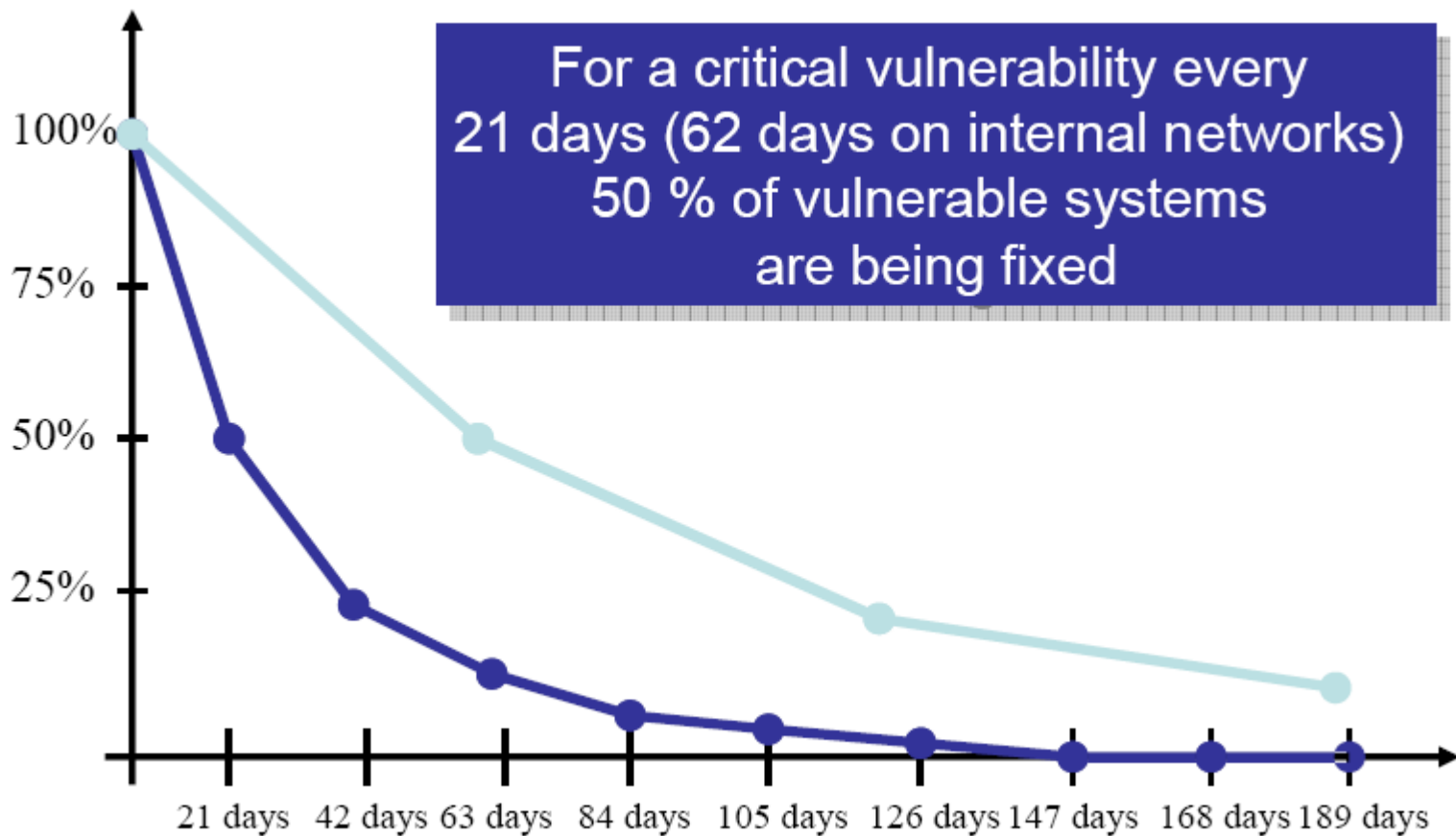


# Decreasing Time-to-exploit

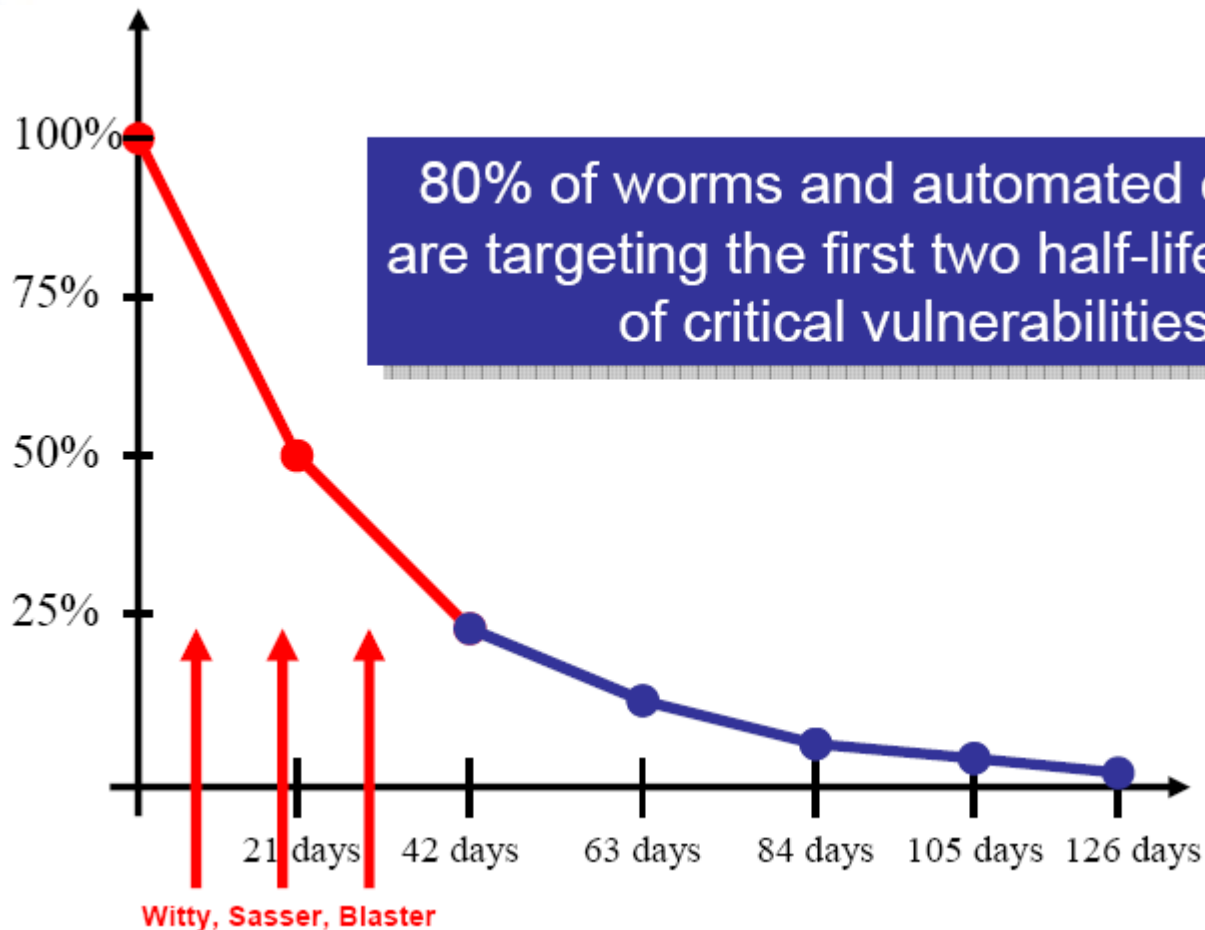
- People patching sooner
  - 2003 – every 30 days the number of vulnerable systems reduces by 50%
  - 2004 – every 21 days the number of vulnerable systems reduces by 50%
- But time-to-exploit is decreasing as well
  - 80% of worms and automated exploits are targeting the first two half-life periods of critical vulnerabilities



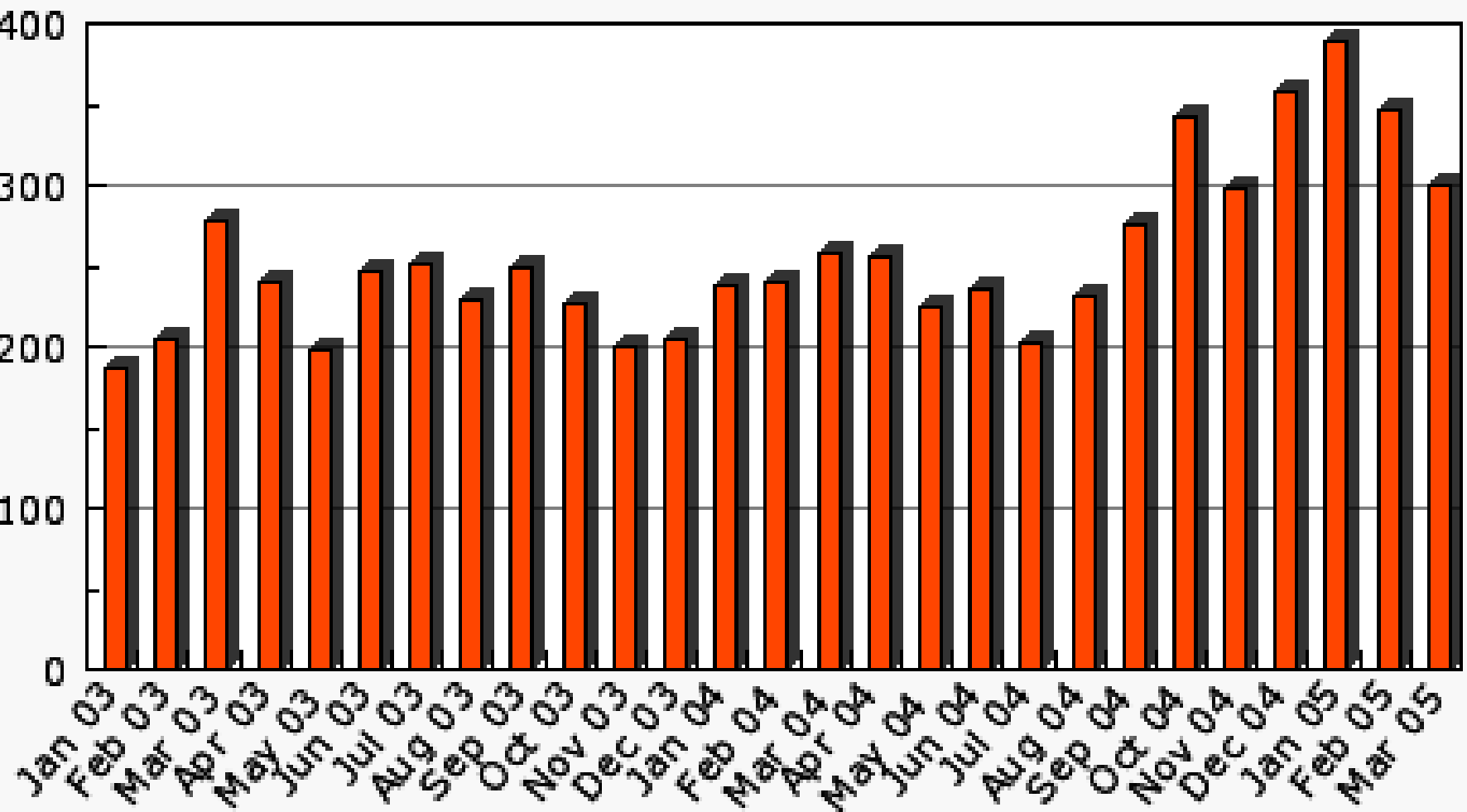
# Vulnerability Half-Life



# Vulnerability Exploitation



## Secunia Security Advisories All Advisories (2003 - 2005)



This graph was generated by Secunia.

Based on Secunia Advisories freely available at <http://secunia.com/>

# New Security Trends

- Organised crime on the rise
- Hacking for profit
  - CyberExtortion
- Infrastructure maturing
  - Application level attacks on the increase
- New Attack Methodologies
  - GHDB ([johnny.ihackstuff.com](http://johnny.ihackstuff.com))
  - Wikto (Google attack tool)



Quit

Mined directories

cl

/papers  
/de

Start Googling

Stop Googling



www.security-assessment.com

Site/Domain

spx,wsdl,xml,xls,sh,css,txt,doc,pdf,mdb,zip,html,htm

File Types

Google Keyword

[http://www.security-assessment.com/Papers/Buffer\\_Overflow\\_In\\_HyperTerminal.pdf](http://www.security-assessment.com/Papers/Buffer_Overflow_In_HyperTerminal.pdf)  
[http://www.security-assessment.com/Brochure\\_Security\\_Risk%20\\_and%20\\_Requirements\\_Analysis.pdf](http://www.security-assessment.com/Brochure_Security_Risk%20_and%20_Requirements_Analysis.pdf)  
<http://www.security-assessment.com/BrochureSA-ISO.pdf>  
<http://www.security-assessment.com/DE/sa-top.htm>  
<http://www.security-assessment.com/PhysicalSecurityReview.htm>  
<http://www.security-assessment.com/OurConsultants.htm>  
<http://www.security-assessment.com/Jobs.htm>  
<http://www.security-assessment.com/IncidentResponseCapabilityDevelopment.htm>  
<http://www.security-assessment.com/sa-left.htm>  
<http://www.security-assessment.com/SystemForensic&EmployeeInvestigations.htm>  
<http://www.security-assessment.com/ISO17799GapAnalysis&Accreditation.htm>  
<http://www.security-assessment.com/Disasters.htm>  
<http://www.security-assessment.com/Technical&ECommerceSecuritySolutionReview.htm>  
<http://www.security-assessment.com/Overview.htm>  
<http://www.security-assessment.com/sa-top.htm>  
<http://www.security-assessment.com/SecuritySelection&Recruitment.htm>  
<http://www.security-assessment.com/OurClients.htm>  
<http://www.security-assessment.com/PenetrationTesting.htm>  
<http://www.security-assessment.com/Papers.htm>  
<http://www.security-assessment.com/SecurityRisk&RequirementsAnalysis.htm>  
<http://www.security-assessment.com/SecurityArchitectureReview.htm>  
<http://www.security-assessment.com/OurServices.htm>  
<http://www.security-assessment.com/SecurityPolicy&ProcedureDevelopment.htm>  
<http://www.security-assessment.com/SecurityOrganisationReview.htm>  
<http://www.security-assessment.com/SecurityProject&ProgrammeManagement.htm>

# New Security Trends

- Targeting users as well as sites:
  - Key loggers
  - Trojans
  - Phishing
  - Browser-based attacks / spam / spyware



# Phishing Increases



# Phishing Trends

- Unique Phishing Attempts December 2003
  - 113
- Unique Phishing Attempts July 2004
  - 1974
- Unique Phishing Attempts February 2005
  - 13,141
- Now using different techniques, IM, pharming



# Organisations Targeted For Phishing

- Financial Institutions
- Auction Sites
- ISPs
- Online Retailers



# State of Security In Australia / NZ

- Patch process improving but...
- Majority of incidents investigated in the last year due to un-patched systems/mis-configurations
- Organisations still leaving security until late in the development cycle



# State of Security in Australia / NZ

- Web applications still slow to improve security
  - Infrastructure attacks due to single point of security failure
  - Increasing application level attacks
  - Exposure of IP / directorys
  - Cross Site Scripting
  - SQL Injection
  - Open source code / poor coding root causes



# State of Security in Australia / NZ

- Security awareness increasing
- Lack of incident response planning
  - Leads to increased response time
- Lack of business continuity planning
  - Leads to increased downtime
- Compliance requirements driving behaviours
  - Increased regulatory controls
  - ISO 17799, SOX, California Disclosure Law
- Anyone can be a target:
  - Aria Farms



# Some Recent Australasian Stories

- Online bankers blocked for spyware (Marketscore) (12/3/2005)
  - <http://www.stuff.co.nz/stuff/0,2106,3215585a10,00.html>
- Union boss applauds NSW anti-surveillance bill (4/5/2005)
  - <http://www.zdnet.com.au/news/security/0,2000061744,39190490,00.htm>
- Phone hackers tap into hospital (31/3/2005)
  - <http://finance.news.com.au/story/0,10166,12699755-31037,00.html>
- How to protect your computer (2005)
  - <http://australianit.news.com.au/articles/0,7204,12819346%5E15841%5E%5Enbv%5E,00.html>
- Antipodean hacker activity on the rise, now ranked 4th (2004)
  - <http://www.silicon.com/software/security/0,39024655,39119257,00.htm?nl=d20040318#>



# More Recent Australasian Stories

- Bookies hit with online extortion (21/7/2004)
  - <http://australianit.news.com.au/articles/0,7204,10651299%5E15306%5E%5Enbv%5E,00.html>
- Internet banking 'no longer safe' (9/3/2004)
  - [http://www.theadvertiser.news.com.au/common/story\\_page/0,5936,8912876%255E421,00.html](http://www.theadvertiser.news.com.au/common/story_page/0,5936,8912876%255E421,00.html)
- Network to research protection (2005)
  - <http://australianit.news.com.au/articles/0,7204,12366219%5E15306%5E%5Enbv%5E,00.html>
- Lapse at Melbourne IT Enabled Panix.com Hijacking
  - [http://news.netcraft.com/archives/2005/01/18/lapse\\_at\\_melbourne\\_it\\_enabled\\_panixcom\\_hijacking.html](http://news.netcraft.com/archives/2005/01/18/lapse_at_melbourne_it_enabled_panixcom_hijacking.html)
- NZ jails Aussie bank hacker (21/10/2004)
  - <http://australianit.news.com.au/articles/0,7204,11087415%5E15331%5E%5Enbv%5E15306%2D15318,00.html>



# Questions?