

# Internet Security and Fraud

Current Online Trends

by Nick von Dadelszen

# Security-Assessment.com – Who We Are

- NZ's only pure-play security firm
- Largest team of security professionals in NZ
- Offices in Auckland, Wellington and Sydney
- 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](#)
- [Zone-H club](#)
- [Staff performance](#)
- [Meet our staff](#)
- [Link to us](#)
- [Contact us](#)
- [Commercials/Campaigns](#)
- [Zone-H e-Shop](#)
- [Disclaimer](#)
- [Black or White hat?](#)

## DIGITAL ATTACKS ARCHIVE

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

Attacker:  Domain:   
 Date:  :

### 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
2005/03/28	<a href="#">illegalteam.com</a>	H	<a href="#">forum.aucklandfiji.org.nz</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/28	<a href="#">illegalteam.com</a>		<a href="#">architecture.org.nz/bbs</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/28	<a href="#">Q8crackers</a>		<a href="#">...co.nz/Q8Crackers.html</a>	Win 2000	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/28	<a href="#">illegalteam.com</a>		<a href="#">unicycle.org.nz/bb</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/28	<a href="#">illegalteam.com</a>		<a href="#">getmoving.org.nz/bboard</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/27	<a href="#">dodo885</a>		<a href="#">.../bbguestbook/index.php</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/27	<a href="#">core-project</a>	H	<a href="#">learningmedia.co.nz</a>	MacOSX	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/26	<a href="#">illegalteam.com</a>		<a href="#">repraent.org.nz/forum</a>	Win 2000	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/26	<a href="#">illegalteam.com</a>		<a href="#">freezaoui.org.nz/forumphp</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/26	<a href="#">dodo885</a>	M	<a href="#">...ernet.co.nz/hacked.htm</a>	Win 2003	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/26	<a href="#">dodo885</a>	M	<a href="#">...aging.co.nz/hacked.htm</a>	Win 2003	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/26	<a href="#">dodo885</a>	M	<a href="#">liberty.net.nz/hacked.htm</a>	Win 2003	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/26	<a href="#">dodo885</a>	M	<a href="#">nzmapped.co.nz/hacked.htm</a>	Win 2003	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/26	<a href="#">dodo885</a>	M	<a href="#">...epics.co.nz/hacked.htm</a>	Win 2003	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/26	<a href="#">illegalteam.com</a>	M	<a href="#">abba.org.nz/forum</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/26	<a href="#">illegalteam.com</a>	M	<a href="#">...planning.org.nz/forum1</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/26	<a href="#">core-project</a>	H M	<a href="#">zydeco.co.nz</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/26	<a href="#">core-project</a>	H M	<a href="#">xboxhacking.co.nz</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/23	<a href="#">illegalteam.com</a>	M	<a href="#">ttbrc.co.nz/forum</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/23	<a href="#">illegalteam.com</a>	M	<a href="#">monkeyfish.co.nz/forum</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/23	<a href="#">illegalteam.com</a>	M	<a href="#">referee.co.nz/forums</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/23	<a href="#">illegalteam.com</a>	M	<a href="#">speedwaybikes.co.nz/forum</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/23	<a href="#">illegalteam.com</a>	M	<a href="#">c-search.co.nz/phpbb</a>	Linux	<a href="#">view</a>   <a href="#">mirror</a>
2005/03/23	<a href="#">illegalteam.com</a>	M	<a href="#">thevatican.co.nz/forums</a>	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

- 119 .nz sites mirrored in March
  - Those are only the ones zone-h.org hears about
- Of those sites:
  - 98 .co.nz, 12 are .org.nz, 7 .net.nz, and 1 is .govt.nz
- Of all hacks on Zone-H.org:
  - 60% Linux, 30% Windows, 10% Other
  - (General web server statistics show 70% Linux, 20% Windows, 10% Other)

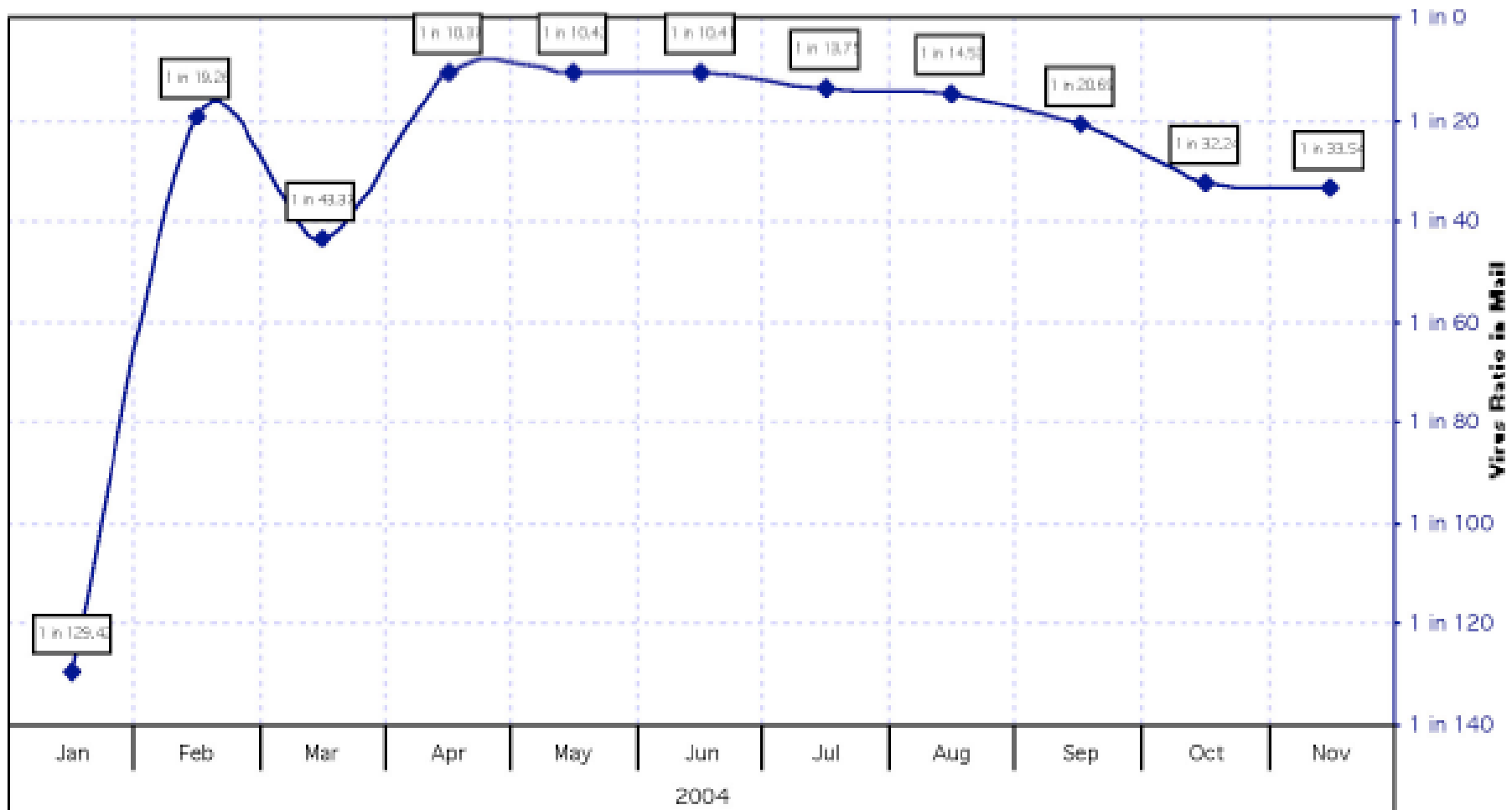


# Virus Statistics (from MessageLabs)

- 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

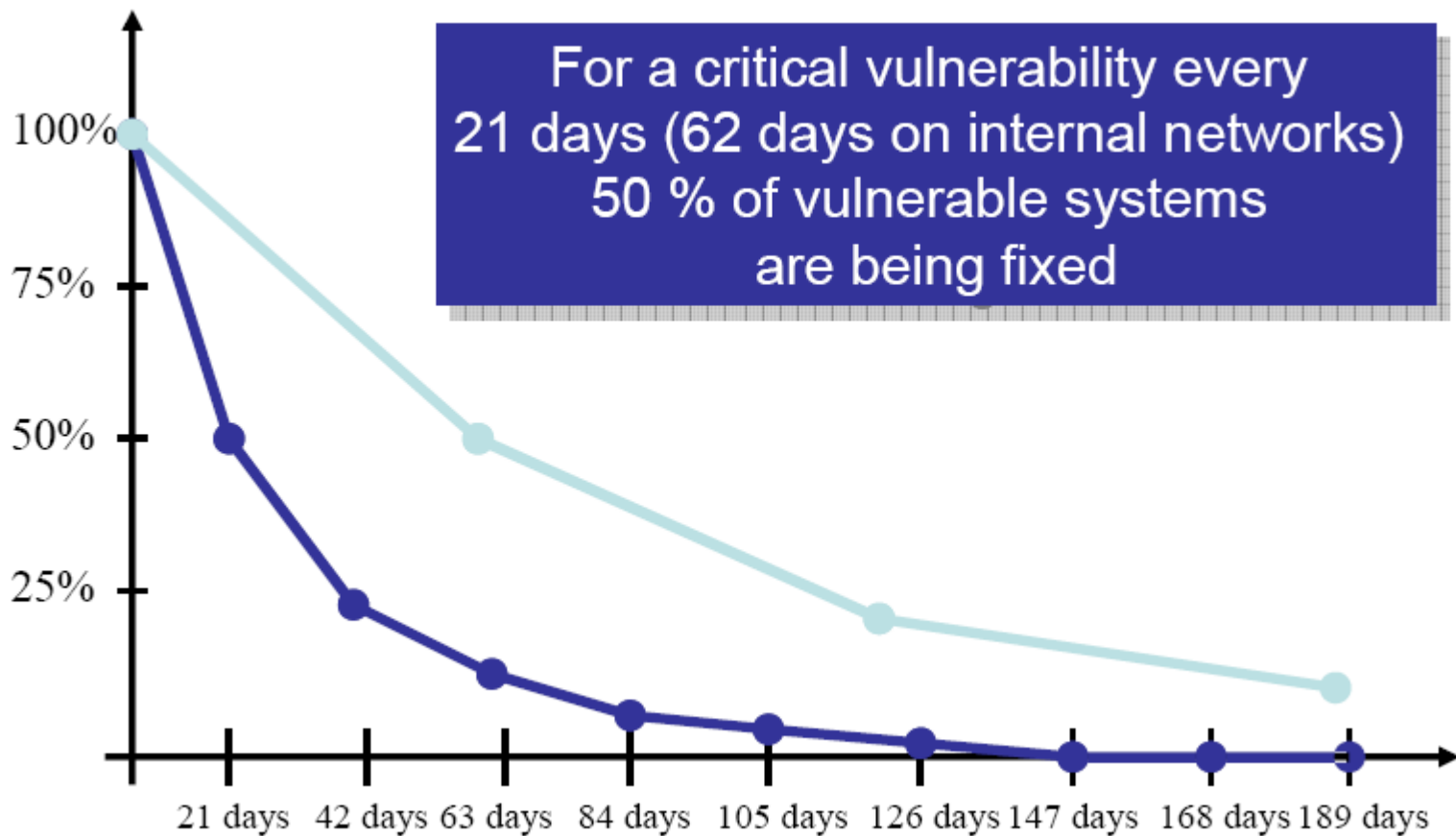


# Decreasing Time-to-exploit

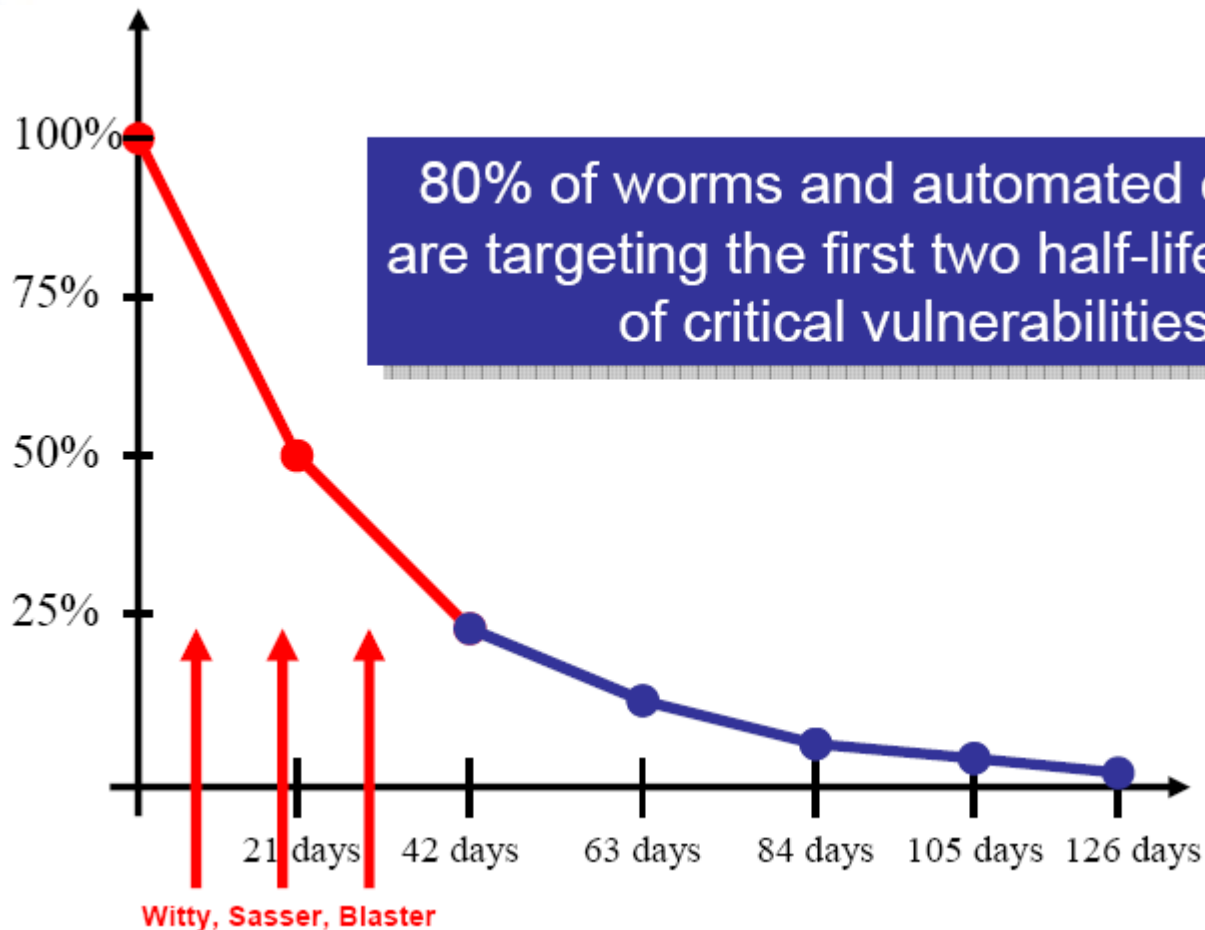
- People patching sooner
  - 2003 – every 30 days the number of vulnerable systems reduces by 50%
  - 2004 – every 21 days the number of vulnerable systems reduces by 50%
- But time-to-exploit is decreasing as well
  - 80% of worms and automated exploits are targeting the first two half-life periods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



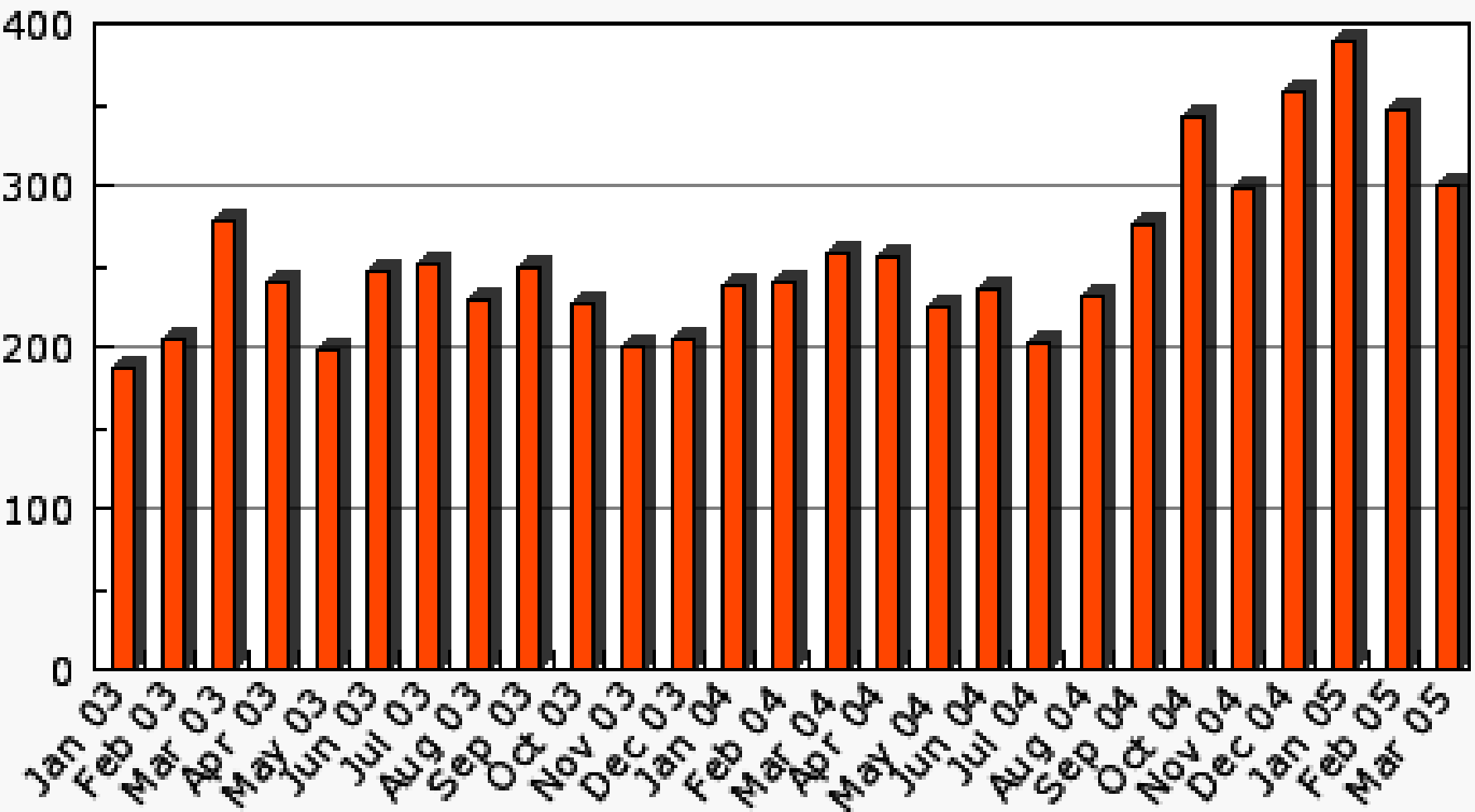
# Vulnerability Half-Life



# Vulnerability Exploitation



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



This graph was generated by Secunia.

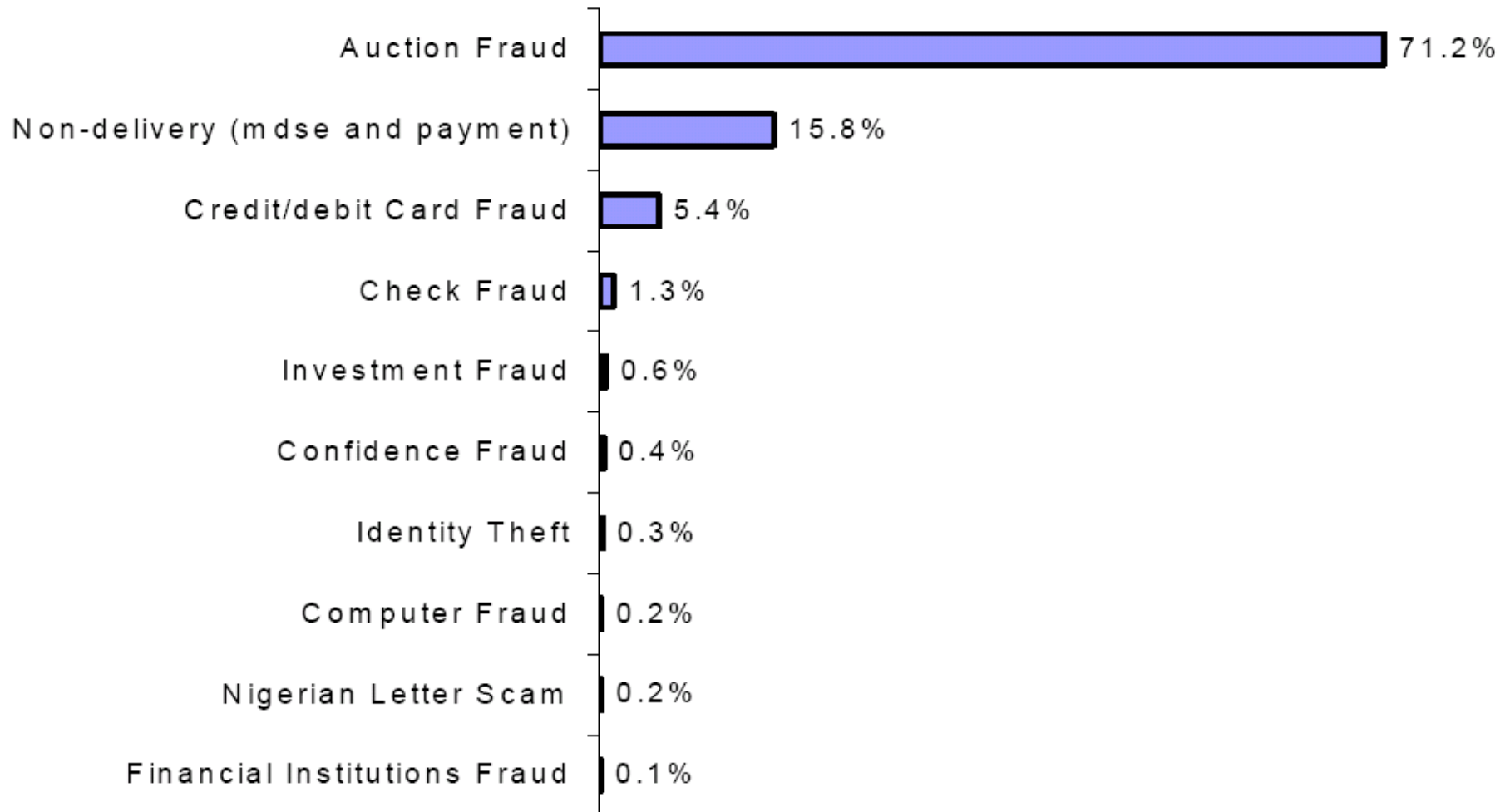
Based on Secunia Advisories freely available at <http://secunia.com/>

# New Security Trends

- Organised crime on the rise
- Hacking for profit
  - CyberExtortion
- Targeting users as well as sites:
  - Key loggers
  - Trojans
  - Phishing
  - Browser-based attacks / spam / spyware



**Chart 3**  
**Top 10 IC3 Complaint Categories**



Source: IC3 2004 Internet Fraud - Crime Report



# Identity Theft

- Stealing of a user's identity
- Fastest growing area of online fraud
- Several different mechanisms
  - Credit Card number capturing
  - Phishing / Social Engineering
  - Malicious code
    - Trojans
    - Man-in-the-middle attacks



# Identity Theft Online vs Offline

Offline	Percentage
Lost or stolen wallet, check book or credit card	28.8%
Known acquaintances with access to information	11.4%
Accessed as part of offline transactions	8.69%
Corrupt employee with access to information	8.7%
Stolen paper mail/fraudulent change of address	8.0%
Taken from garbage	2.0%
<b>Total</b>	<b>68.2%</b>
Online	
Computer spyware	5.2%
Accessed as part of an online transaction	2.51%
Computer virus/hacker	2.2%
Phishing	1.7%
<b>Total</b>	<b>11.6%</b>



# Credit Card Capturing

- Many sites still do not protect Credit Card numbers as well as they should
- Black market for stolen Credit Card numbers
- Gathered by breaking into sites or capturing traffic

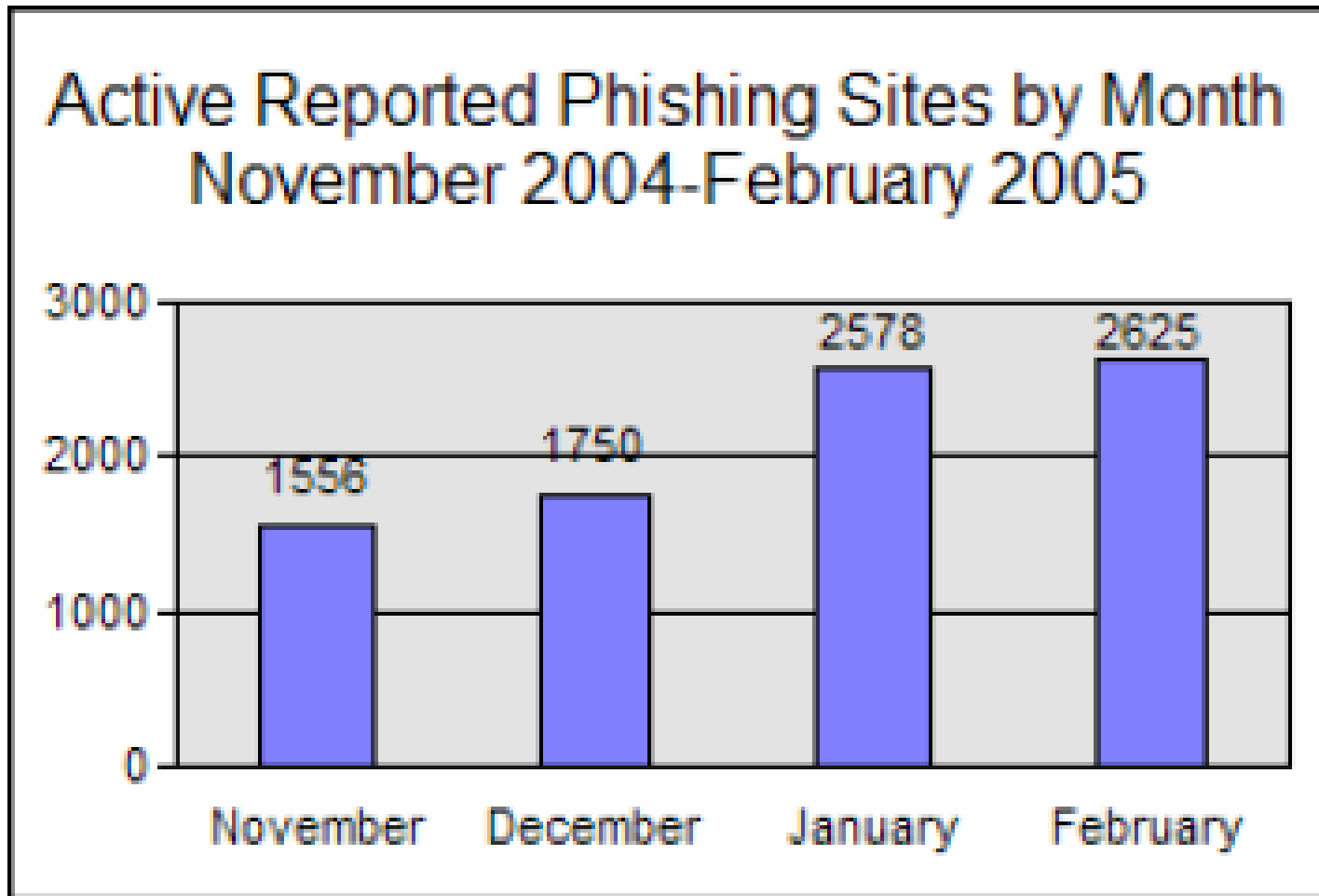


# Phishing

- Attacker send fake email to victim pretending to be trusted institution
- Victim responds to email (either directly or by clicking on a link)
- Victim provides attacker with information required to access services



# 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



# Malicious Code

- Keyloggers
- Trojans
- Fake sites
- Man-in-the-middle attacks (MarketScore)



# Internal Fraud

- Still major risk
- Statistics show majority of losses are the result of internal attacks
- Have seen recent examples of this in New Zealand
  - MSD
  - MinHealth



# How To Stop It

- Three types of controls
  - Preventative
  - Detective
  - Deterrent
- Effective strategy requires use of all three
  - Preventative – technical controls, 2-factor, limiting services, education
  - Detective – increased monitoring and reporting
  - Deterrent – New anti-hacking laws



# What is Two-Factor Authentication

- Many different types of two-factor
  - One-time passwords
    - Password-generating token (SecureID, Vasco)
    - SMS tokens
    - Scratch pads
  - Client-side Certificates
    - Smart cards
    - USB keys
  - Biometrics



# The Benefits of Two-Factor

- Requires more than just a username/password combination
- Protects against the majority of the attacks currently being performed today
- Provides an extra level of comfort for security-conscious users



# The Trouble With Two-Factor

- Designed for small user base
- Has a usability cost
- No clear market leader
- Potentially large implementation costs
- Will not stop all attacks
  - Man-in-the-middle
  - Intelligent Trojans



# The Weakness Of SSL

- Relies on trust
- Tells you that you have a secure session with A website, not THE website
- Certificates can be faked
- Root certificates can be installed – MarketScore
- Allows for Man-in-the-middle and IDN attacks



# MITM vs Two-Factor

<b>Customer</b>	-> Here is my username and password	<b>Man-in-the-middle</b>		<b>Website</b>
			-> Here is my username and password	
	<- What is your token password?		<- What is your token password?	
	-> Here is my token password			
			-> Here is my token password	
	<- Authenticated		<- Authenticated	
	-> Transfer \$10 to Bill			
			-> Transfer \$10 to Fred	
	<- Please re-authenticate		<- Please re-authenticate	
	-> Here is my token password			
			-> Here is my token password	
	<- Transaction accepted		<- Transaction accepted	

# Will Two-Factor Help?

- Does increase security
- Makes attacks harder
- Will require attacks to be more focused
- Must be a business decision
  - Amount of security required
  - Cost vs benefit



# Defence Against Client Attacks

- Authentication is the key
  - Client authentication
  - Server authentication
- Users must protect themselves
  - Don't use public terminals
  - Anti-virus
  - Firewall
  - Automatic updates
  - Anti-Spyware



# State of Security In New Zealand

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



# State of Security in New Zealand

- Security awareness increasing
- Lack of incident response planning
  - Leads to increased response time
- Lack of business continuity planning
  - Leads to increased downtime
- Anyone can be a target:
  - Aria Farms



# Some Recent NZ Stories

- Online bankers blocked for spyware (12/3/2005)
  - <http://www.stuff.co.nz/stuff/0,2106,3215585a10,00.html>
- TAB outage costs \$320,000 (17/2/2005)
  - <http://www.computerworld.co.nz/news.nsf/0/538ACA88CBEB7149CC256FB5002EC454?OpenDocument&pub=Computerworld>
- Paradise tracks hackers (3/2/2005)
  - <http://www.nzherald.co.nz/index.cfm?ObjectID=10009248>
- Hospital computer failure could be hackers (28/10/2004)
  - <http://www.nzherald.co.nz/index.cfm?ObjectID=3604834>
- Ministry man cracks computer to steal \$2m (30/9/2004)
  - <http://www.nzherald.co.nz/index.cfm?ObjectID=3596124>



# More Recent NZ Stories

- Hacker breaks into firms' phones (28/9/2004)
  - <http://www.nzherald.co.nz/index.cfm?ObjectID=3595229>
- Aria Farms hacked - spurious recall notices sent (9/9/2004)
  - <http://computerworld.co.nz/news.nsf/UNID/70D94B0F7C9700DBCC256F460014813D?opendocument>
- Bookies hit with online extortion (21/7/2004)
  - <http://australianit.news.com.au/articles/0,7204,10651299%5E15306%5E%5Enbv%5E,00.html>
- Online credit-card fraudster jailed (31/5/2004)
  - <http://www.nzherald.co.nz/index.cfm?ObjectID=3569745>
- Police called after National party website hacked (15/3/2004)
  - <http://www.nzherald.co.nz/index.cfm?ObjectID=3554851>



# Questions?