What will be the Next Attack in Internet

By

Alan S H Lam

Outlines

- Current threads
- Attack Trends
- Recent virus and worm review
- Prediction: Next attack in Internet
- How we counteract
- Q & A

Facts and Threats (1)

- Over 171 million computers connected
- Grow at rapid pace
- Users with different knowledge and background
- Bandwidth and machine capability keep rising
- Computer system become more and more sophisticated and complicated. The complexity of the Internet, protocols, and applications introduce vulnerabilities

Facts and Threats (2)

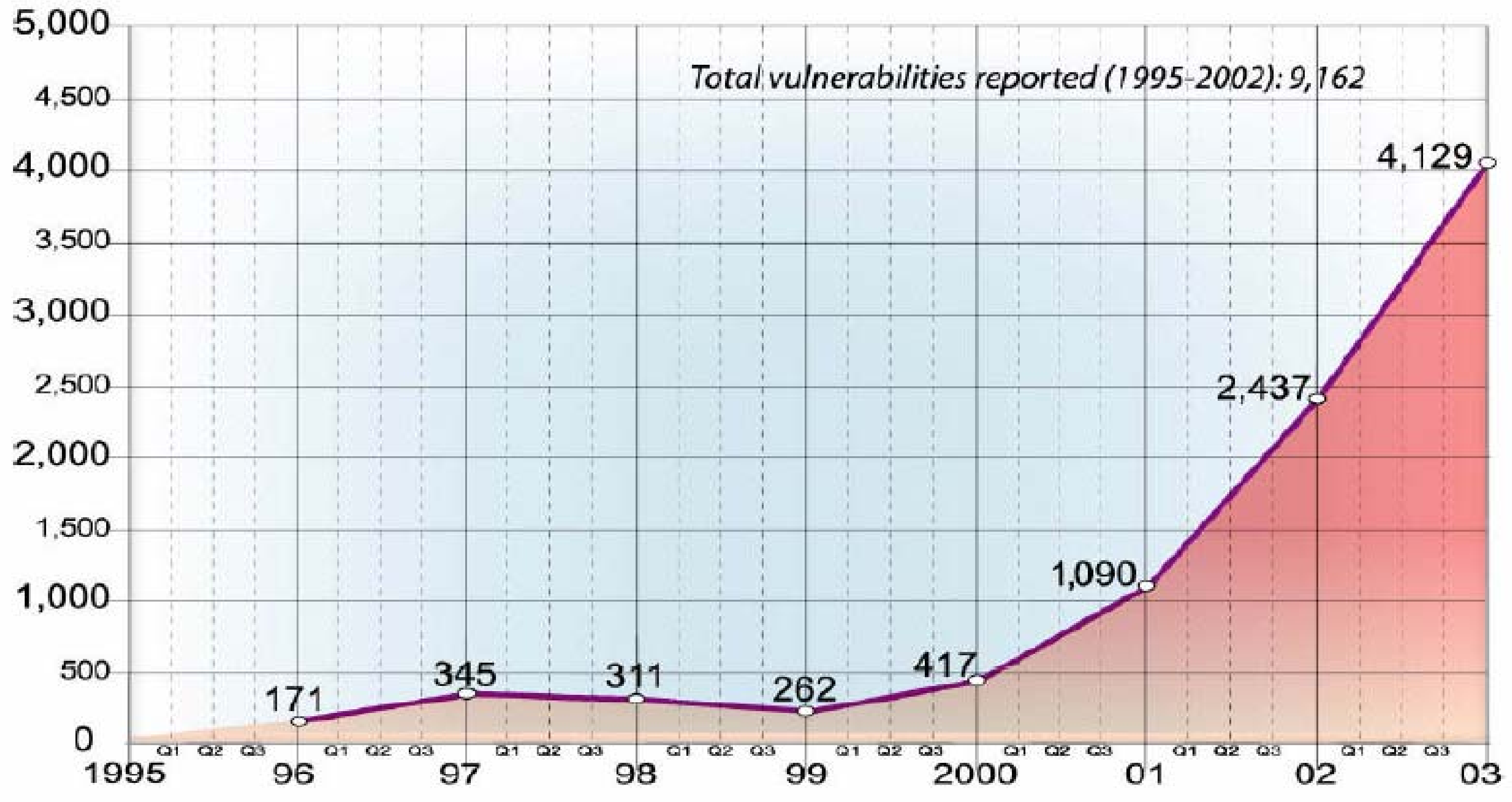
- System and network administrators are either not prepared or overloaded
- Vendor turn off security features in default setting
- Vendor put products to market without fully tested
- End-users disable/bypass security functions deliberately

Facts and Threats (3)

- Critical infrastructures increasingly rely upon the Internet for operations
- Internet attacks are more easy and hard to trace than the old days
- Global cooperation is difficult as different countries have different computer laws.
- Intruder tools are increasingly sophisticated, easy to use, designed to support large-scale attacks, and can be downloaded from the Internet

Security Vulnerabilities Reported

Source: CERT



Top Twenty Internet Security Vulnerabilities

Source: SANS

Windows Stream

1. Internet Information Server (IIS)
2. Microsoft SQL Server
3. Windows Authentication
4. Internet Explorer
5. Windows Remote Access Services
6. Microsoft Data Access Components (MDAC)
7. Windows Scripting Host (WSH)
8. Microsoft Outlook -- Outlook Express
9. Windows Peer to Peer File Sharing (P2P)
10. Simple Network Management Protocol (SNMP)

Unix Stream

1. BIND/DNS
2. Remote Procedure Call (RPC)
3. Apache Web Server
4. General UNIX Authentication
5. Clear Text Services
6. Sendmail
7. Simple network Management Protocol (SNMP)
8. Secure Shell (SSH)
9. Misconfiguration of Enterprise Services (NFS/NIS)
10. Open Secure Sockets Layer (SSL)

Changes in Intrusion Profile

Source: CERT

1988

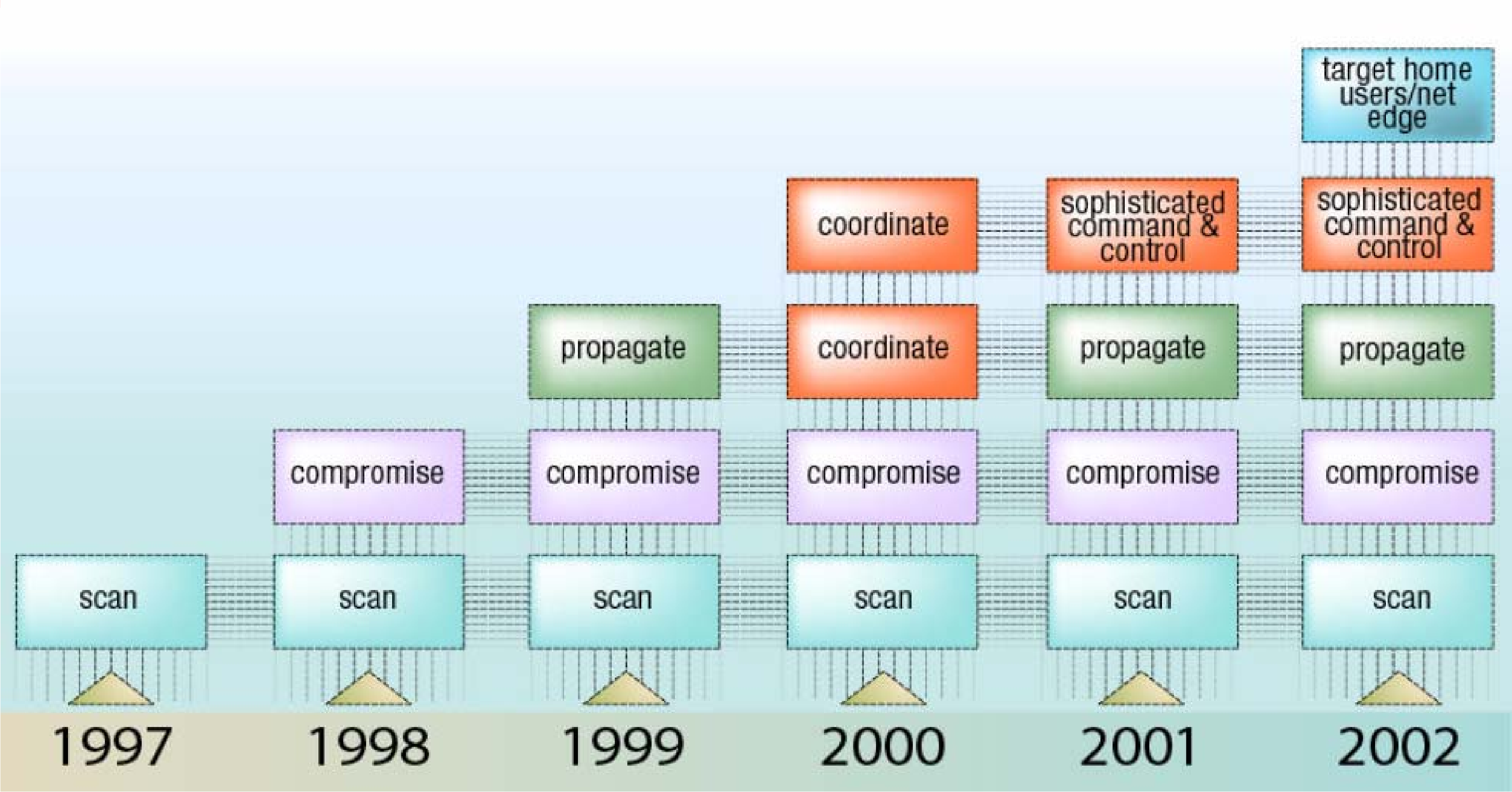
- Exploiting passwords
- Exploiting known vulnerabilities

Today

- exploiting passwords
- exploiting known vulnerabilities
- exploiting protocol flaws
- examining source and executable files for new security flaws
- defacing web servers
- installing sniffer programs
- IP source address spoofing
- denial of service attacks
- widespread, automated scanning of the Internet
- distributed attacks
- building large networks of compromised computers
- developing command and control networks to use compromised computers to launch attacks

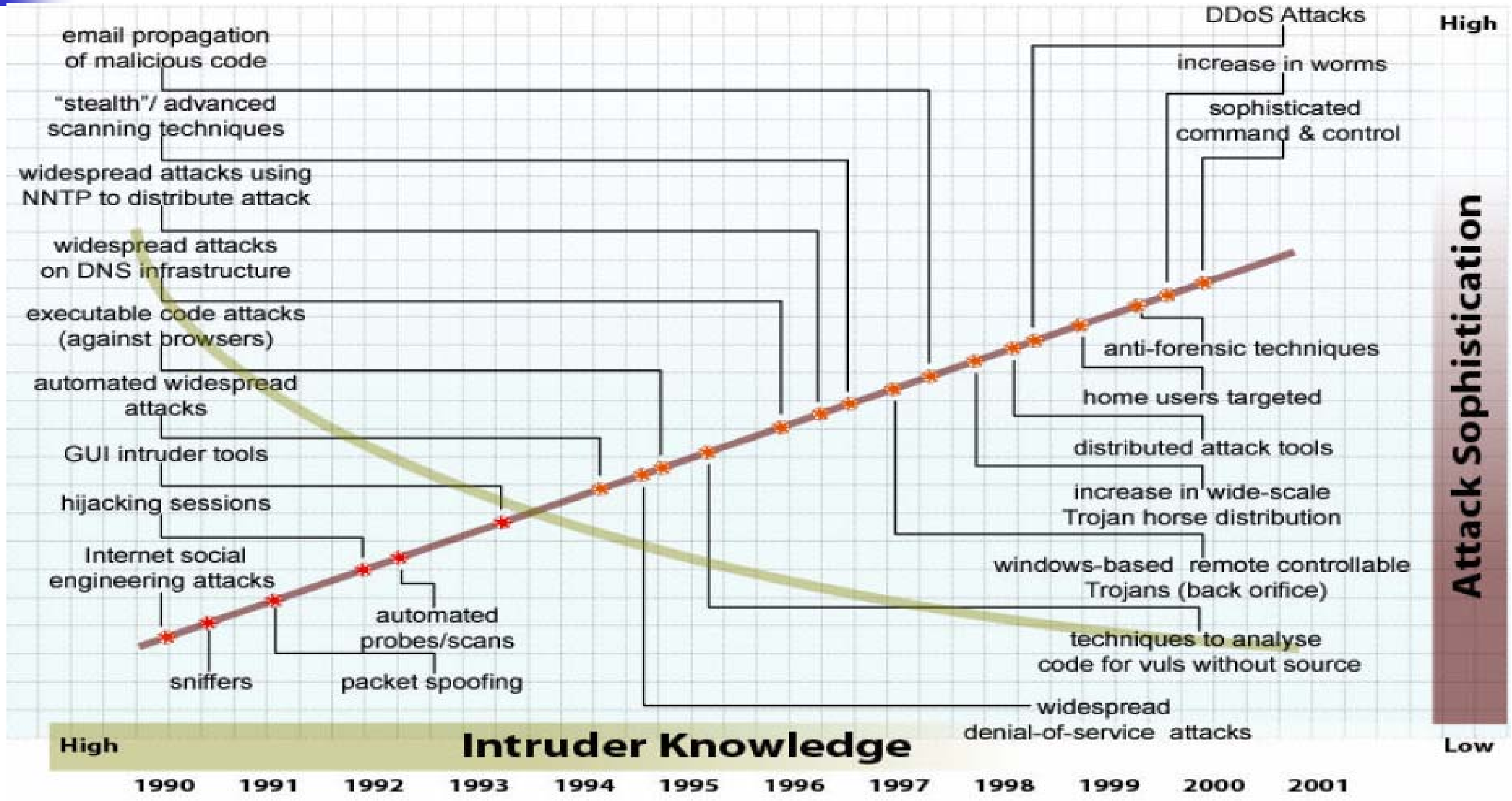
Attacker Technology

Source: CERT



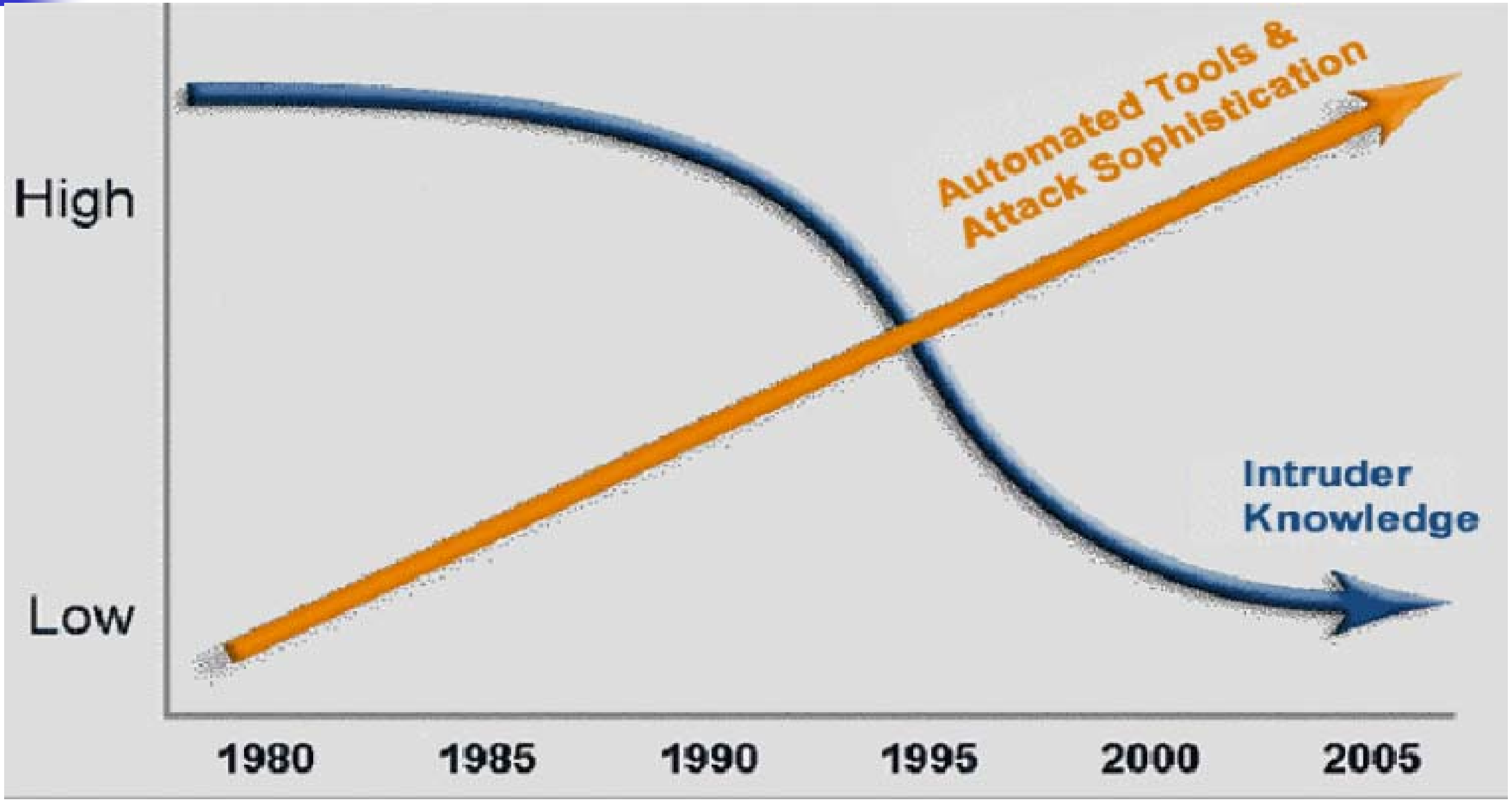
Attack Sophistication vs. Intruder Knowledge

Source: CERT



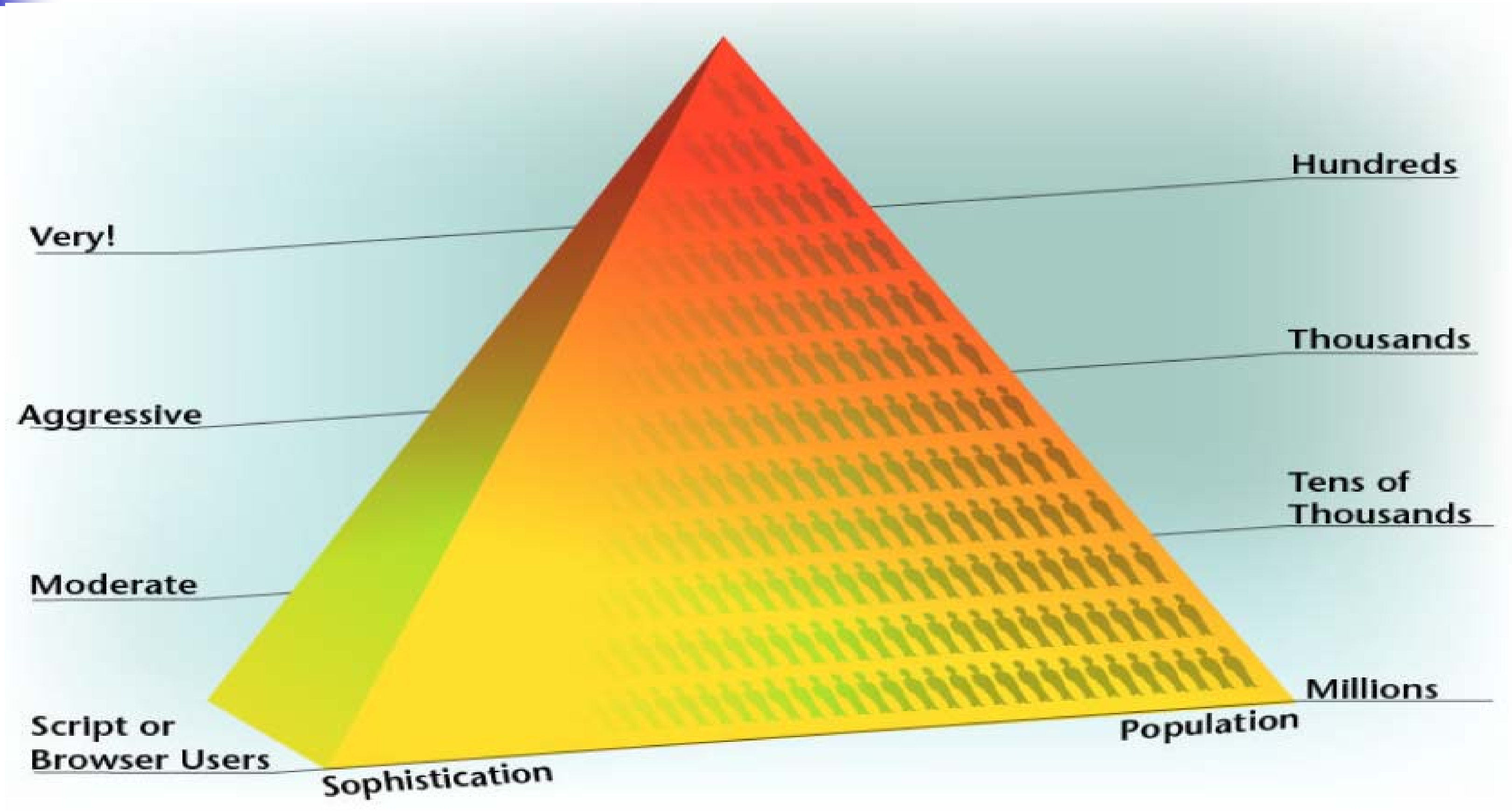
Less Knowledge Required to Attack

Source: Symantec



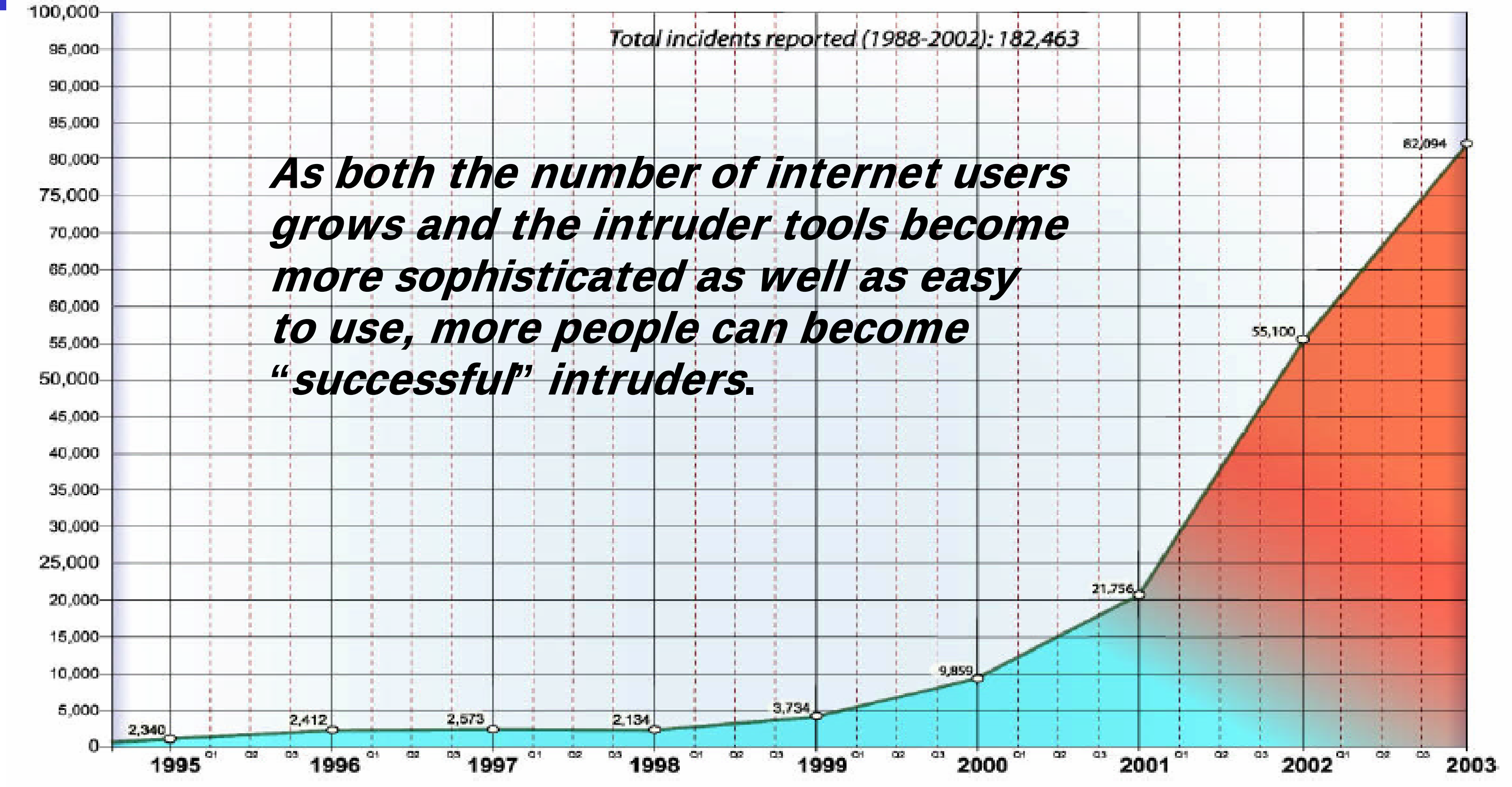
Sophistication VS Population

Source: CERT



Security Incidents Reported

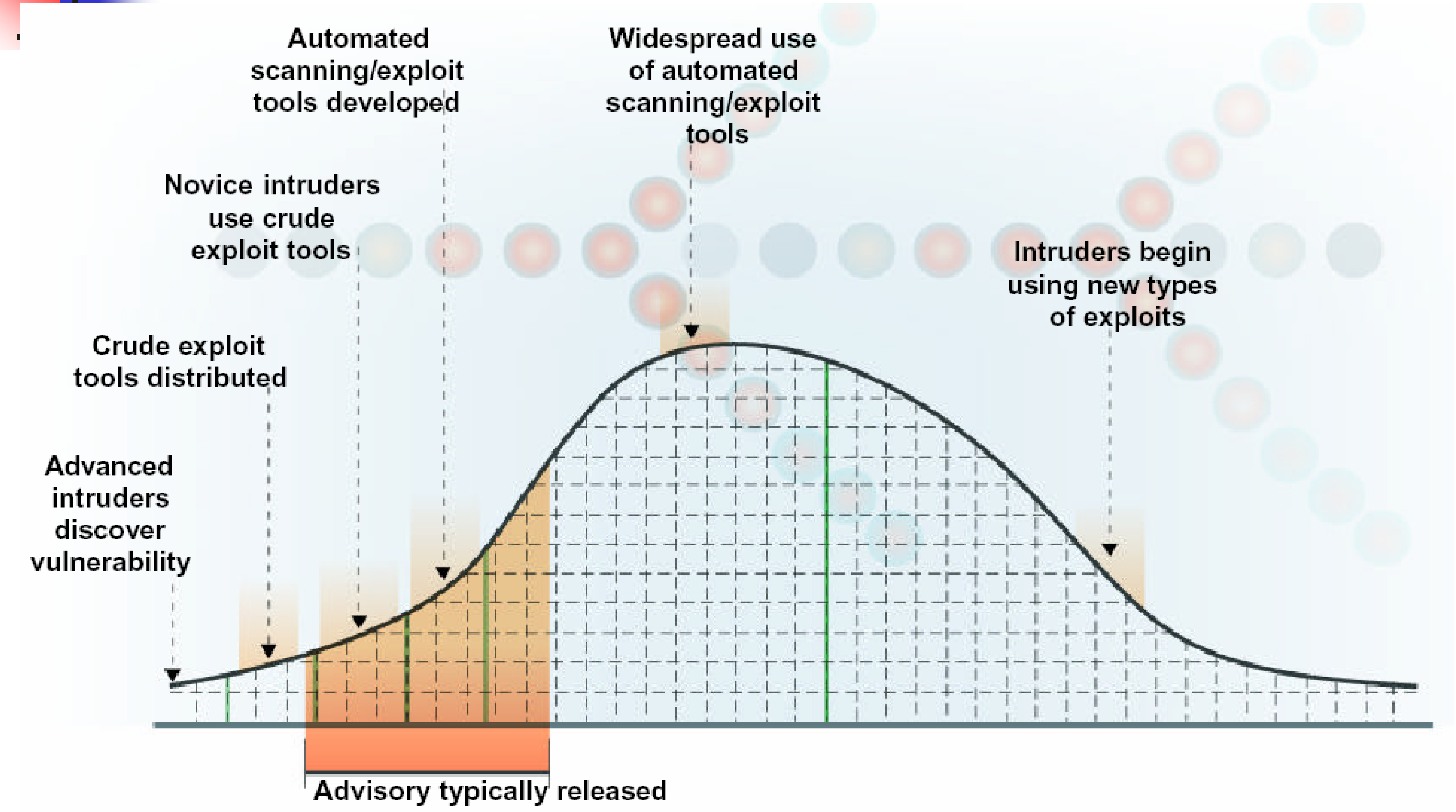
Source: CERT



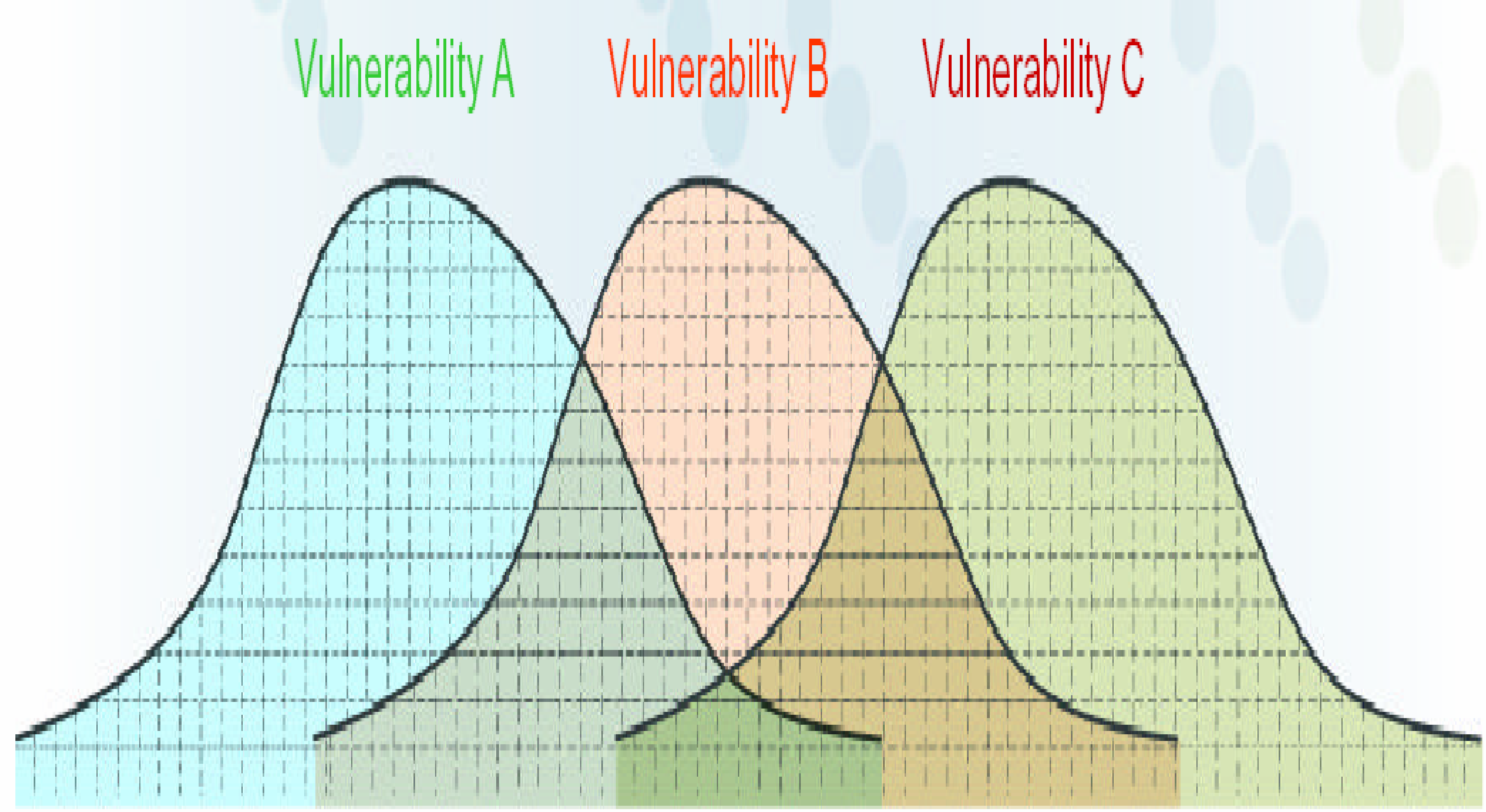
As both the number of internet users grows and the intruder tools become more sophisticated as well as easy to use, more people can become "successful" intruders.

Vulnerability Exploit Cycle (1)

Source: CERT

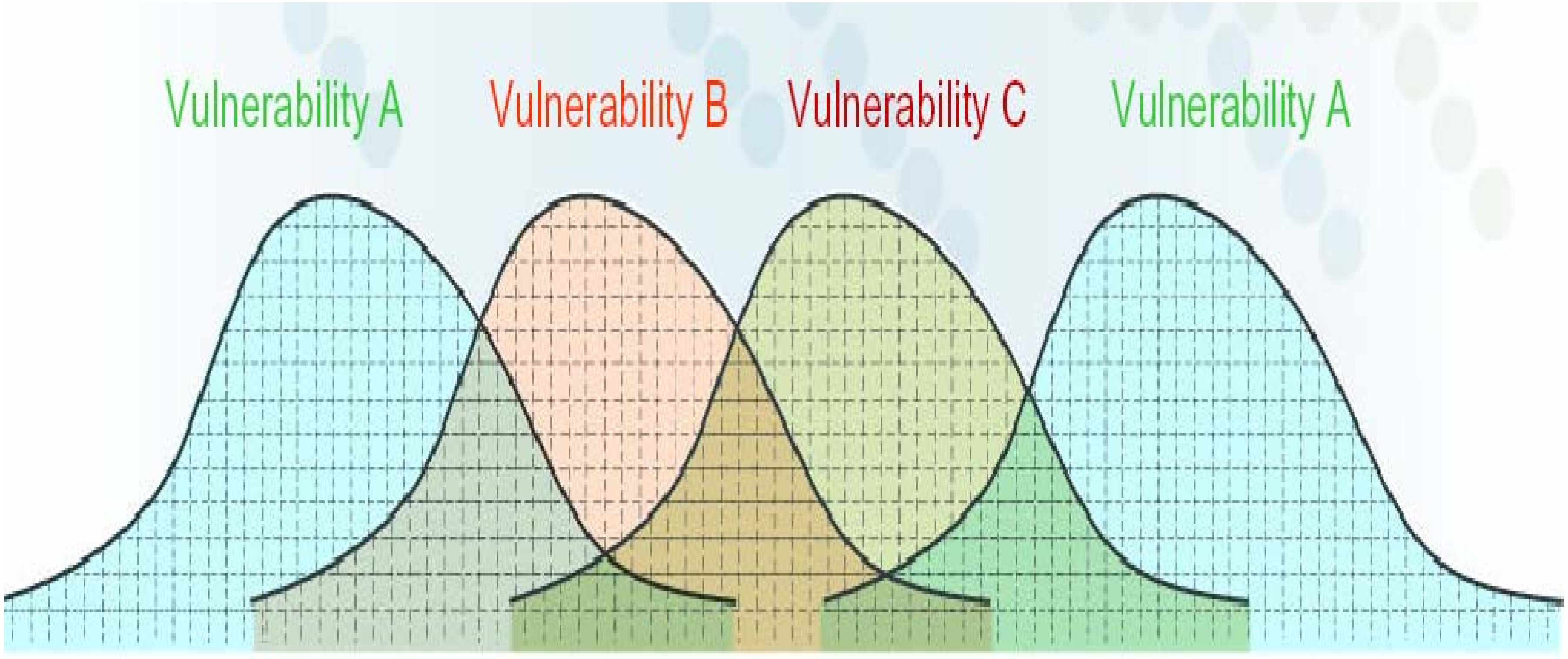

Automated scanning/exploit tools developed
Widespread use of automated scanning/exploit tools
Novice intruders use crude exploit tools
Intruders begin using new types of exploits
Crude exploit tools distributed
Advanced intruders discover vulnerability
Advisory typically released

Vulnerability Exploit Cycle (2)



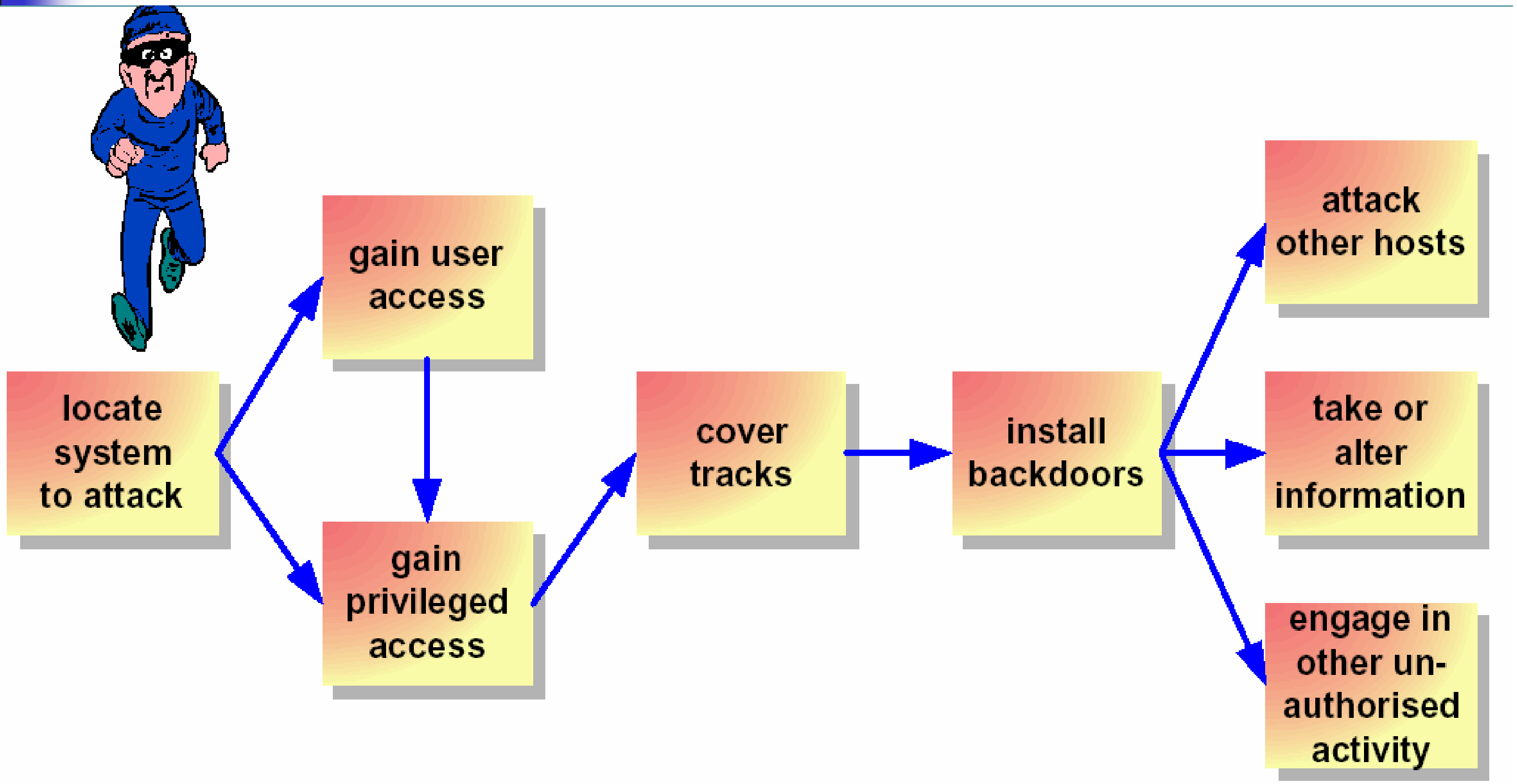
Vulnerability Exploit Cycle (3)

For some vulnerabilities, there may be a resurgence in its exploitation



Typical Network Attack

Source: CERT



locate system to attack

gain user access

gain privileged access

cover tracks

install backdoors

attack other hosts

take or alter information

engage in other un-authorised activity

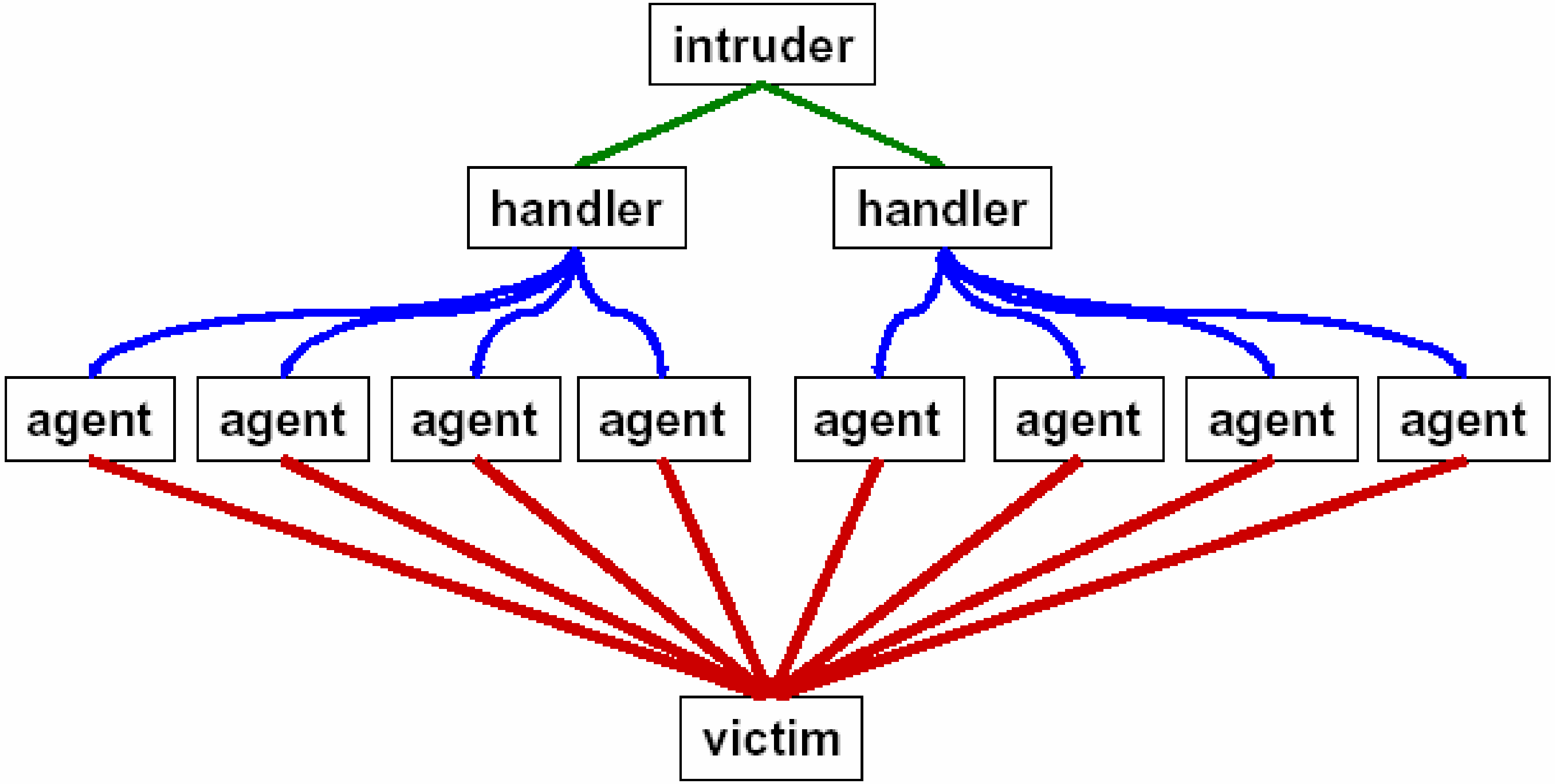
Attack Trends (1)

1. **Automation; speed of attack tools**
   - *Scanning for potential victims*.
   - *Compromising vulnerable systems*.
   - *Propagate the attack*.
   - *Coordinated management of attack tools*.
2. **Increasing sophistication of attack tools**
   - *Anti-forensics.*
   - *Dynamic behavior.*
   - *Modularity of attack tools*.

Attack Trends (2)

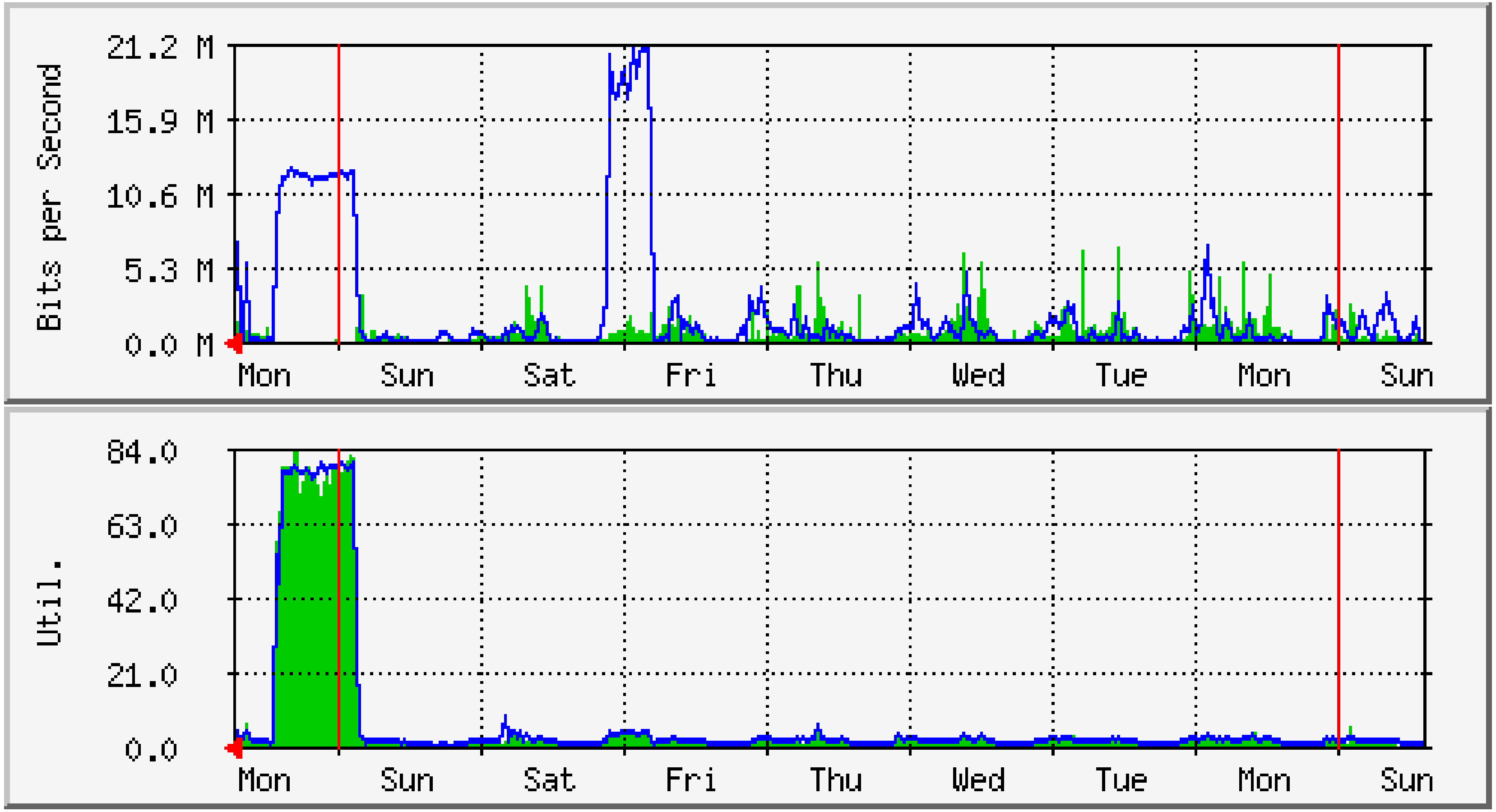
3. **Faster discovery of vulnerabilities**
4. **Increasing permeability of firewalls**
5. **Increasingly asymmetric threat**
6. **Increasing threat from infrastructure attacks**
   - **Distributed denial of service (DDOS)**
   - **Worms**
   - **Attacks on the Internet Domain Name System (DNS)**
   - **Attacks against or using routers**

The Classic DDoS model



DoS Impact to Infrastructure

Traffic VS router CPU Loading



Attack Trends (3)

Potential Impact

- Denial of service
- Compromise of sensitive information
- Misinformation
- Time and resources diverted from other tasks

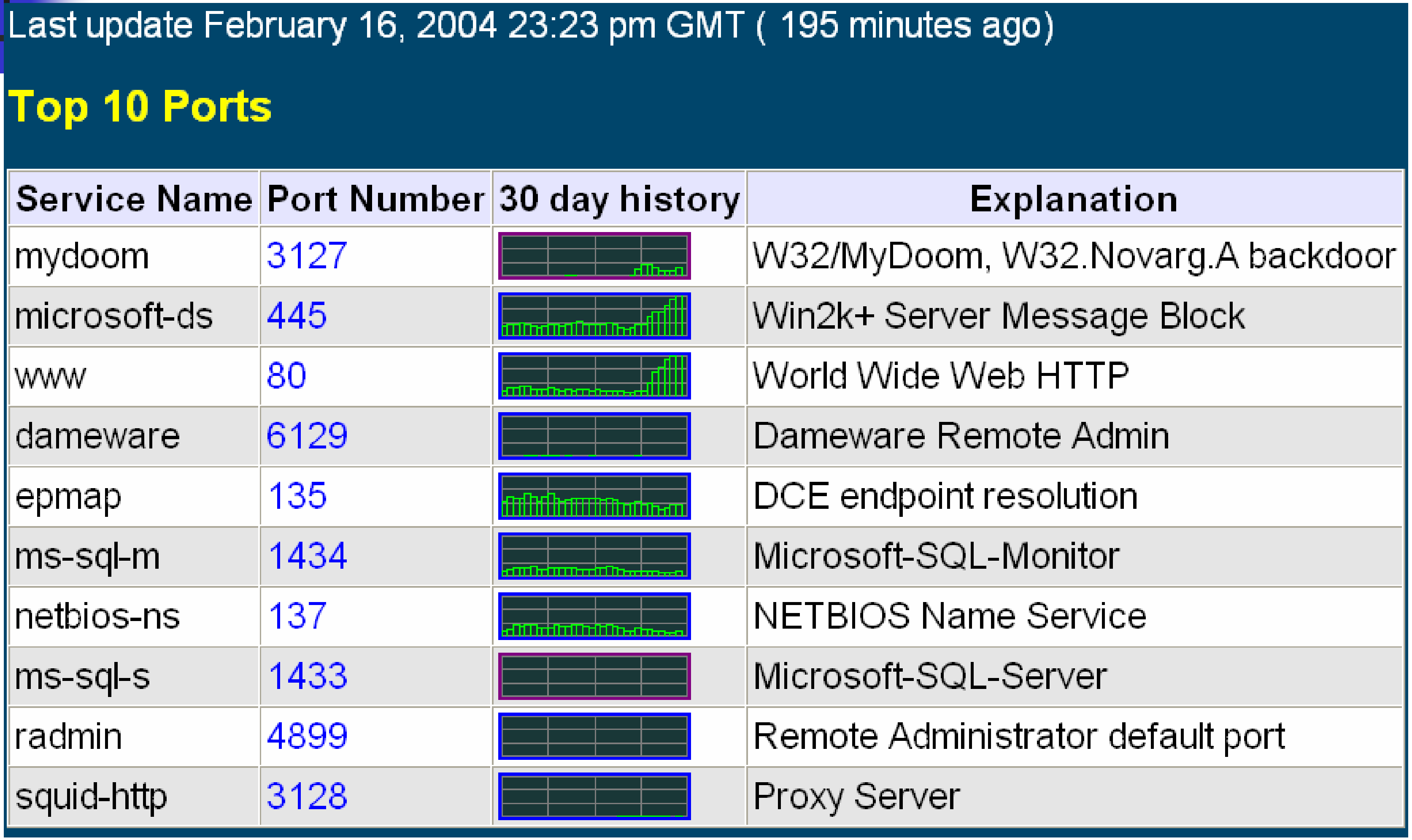
Economic Impact

Source: Computer Economics

Date	Code Name	Worldwide Economic Impact (USD)
1-2/2004	MyDoom	$4.00 billion
8-9/2003	Blaster	$500 million
2003	Slammer	$1.00 billion
2001	Nimda	$635 million
2001	Code Red	$2.62 billion
2001	SirCam	$1.15 billion
2000	Love Bug	$8.75 billion
1999	Melissa	$1.10 billion
1999	ExploreZip	$1.02 billion
2001	9/11 attack to WTC	$15.8 billion (to restore IT and communication capabilities

Top Ten Network Scans (on Feb16)

Source: SANS



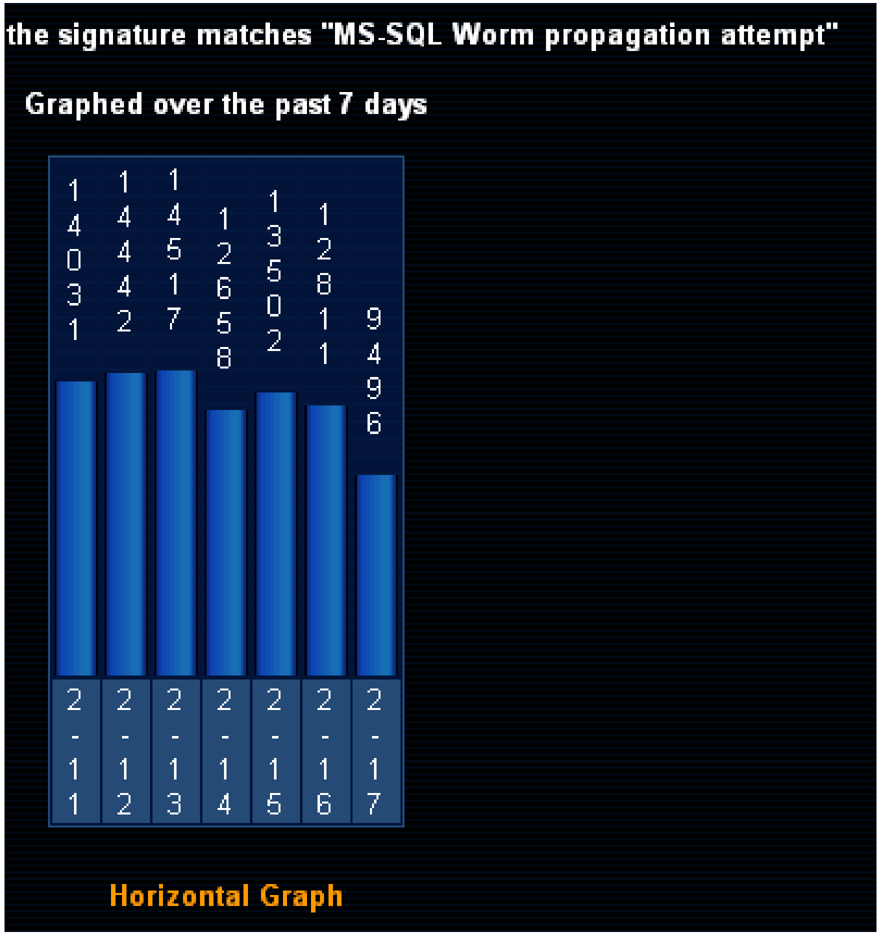
Last update February 16, 2004 23:23 pm GMT (195 minutes ago)

Top 10 Ports

Service Name	Port Number	30 day history	Explanation
mydoom	3127		W32/MyDoom, W32.Novarg.A backdoor
microsoft-ds	445		Win2k+ Server Message Block
www	80		World Wide Web HTTP
dameware	6129		Dameware Remote Admin
epmap	135		DCE endpoint resolution
ms-sql-m	1434		Microsoft-SQL-Monitor
netbios-ns	137		NETBIOS Name Service
ms-sql-s	1433		Microsoft-SQL-Server
radmin	4899		Remote Administrator default port
squid-http	3128		Proxy Server

Slammer Propagation

Our IDS still detects over 10 K slammer worm propagation each day in Feb 2004

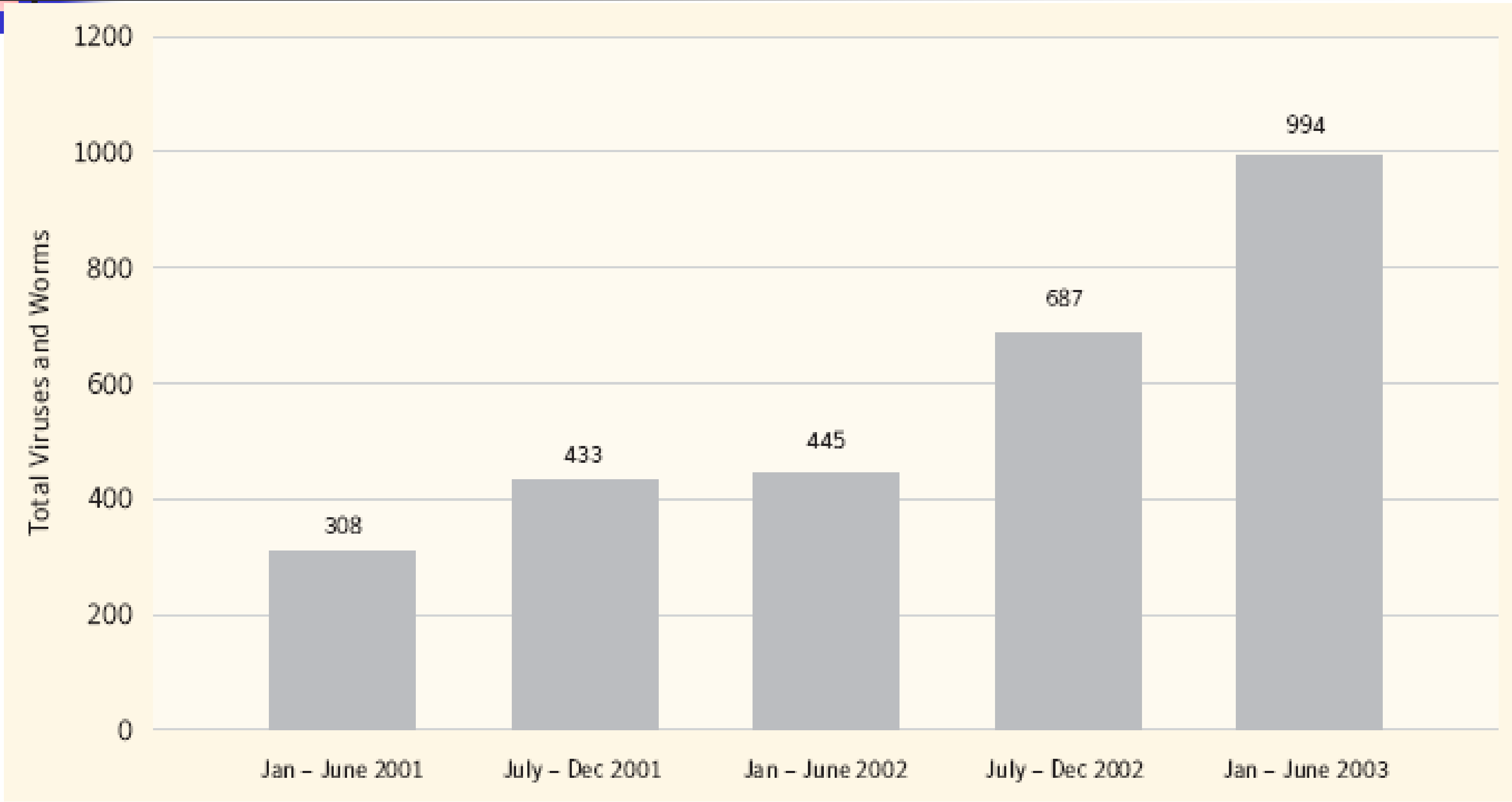


the signature matches "MS-SQL Worm propagation attempt"

Graphed over the past 7 days

New Documented Win32 Viruses and Worms

Source: Symantec



Recent Virus/Worm Review (1)

Code Name	Outbreak Date	Comment
Nachi.B	Feb 2004	Make use of RPC DCOM vulnerability and the IIS WebDav vulnerability
Doom Juice	Feb 2004	Make use of the backdoor left by MyDoom and set to perform a DDOS against www.microsoft.com
MyDoom	Jan 2004	People still love to open unexpected attachments
Swen	Sep 2003	Forge to look like Microsoft safety updates
Sobig.F	Aug 2003	Virus and spammer work hand-in-hand

Recent Virus/Worm Review (2)

Code Name	**Outbreak Date**	**Comment**
Nachi	Aug 2003	A worm to clean Blaster
Blaster	Aug 2003	Make use of the RPC DCOM vulnerability
Bugbear.B	Jun 2003	Try to steal information from banks
Slammer	Jan 2003	It jammed Internet within a matter of minutes
Nimda	Sep 2001	Propagate through different channels
Code Red	Aug 2001	Make use of IIS Vulnerability

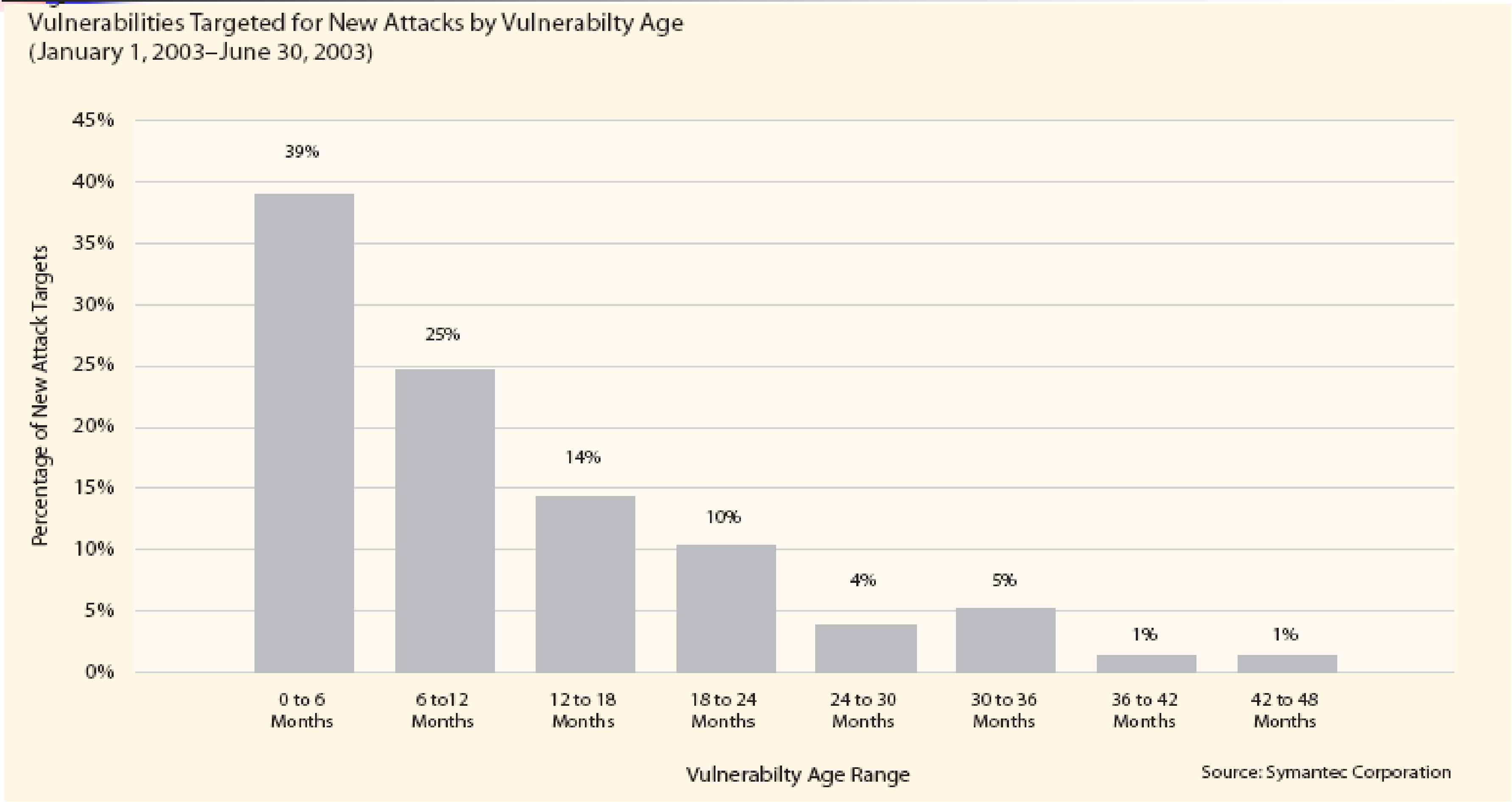
Recent Virus/Worm Review (3)

Tendency to Zero-Day Exploit

Code Name	**Worm / virus released**	**Vulnerability discovered and patch released**
Code Red	July 2001	June 2001
Slammer	Jan 2003	July 2002
Blaster	Aug 2003	July 2003
MyDoom	Jan 2004	Jan 2004
DoS exploit using ASN.1 bug	Feb 14, 2004	Feb 10, 2004

Vulnerabilities Targeted VS Vulnerability Age

Source: Symantec



Prediction: Next attack in Internet (1)

- Close to Zero-day exploit
  - systems which cannot catch up with the latest patch will be the victims in no time
- Virus/worm keep mutating, one after another, and in great speed
  - One wave after another, anti-virus tools hardly keep up with the new viruses or worms
- Make use of other attacker works, e.g. backdoor left behind in infected hosts
  - There will be lots of scan hunt for these infected hosts

Prediction: Next attack in Internet (2)

- Networks of captured hosts will be the resource which the attackers will battle for
  - These networks will be highly stealthy, coordinated and self-managed
  - Attackers use these networks to collect sensitive information, launch DDoS attacks, or set up proxy servers to cover up their trace
  - These networks will be the war zone among the attackers who try to keep others out of these networks

Prediction: Next attack in Internet (3)

- Spammers, criminals, and industrial spies are working together
  - The attacks will be more purpose oriented rather than just for fun or proof-of-concept motivation
  - As motivated by great profit opportunity, more resources will be allocated for the attacks to make them more well-planned, effective and professional
  - Corps, organizations or Institutions which are against these group of people will be on the target list

Prediction: Next attack in Internet (4)

- Recovery of an inflected or break-ins hosts will be much more difficult
  - Trojan horse programs will be difficult to spot or clean
  - Patch or backup could be unreliable
- Main corps and Internet Infrastructures will be on the target lists
  - The attacks to these targets will cause tremendous impact and chaos in the Internet so that the attackers can make use of these advantages to get what they want

How we counteract

- Patch! Patch! Patch!!!
- Act proactively before we need to pay for the lessons
- Need co-operation of
  - High management level
  - System and Network Administrators
  - Vendors and Government
  - Institutes managing Internet Infrastructure
  - End users themselves

Q&A

Where are we now and what will be the next?

Question, Comments, and Suggestions

Thank You