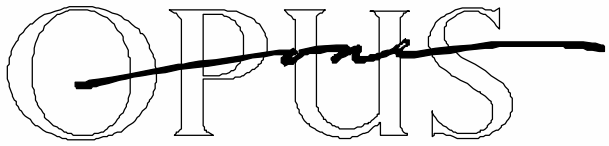
SearchFinancialSecurity.com
INFORMATION SECURITY
FINANCIAL
INFORMATION SECURITY DECISIONS

Five Myths of Threat Management

Joel Snyder
jms@opus1.com
Opus One



Myth 1

Intrusion Detection Systems Detect Intrusions

Reality: Intrusion Detection Systems Provide Visibility Into the Security Posture of Your Network

- If you're hoping that the IDS will "catch them in the act," you don't really understand what IDS is good at

SearchFinancialSecurity.com

INFORMATION SECURITY

FINANCIAL INFORMATION SECURITY DECISIONS

Message	Count
http_inspect: OVERSIZE REQUEST-URI DIRECTORY (119:15)	94852
smtp: Attempted response buffer overflow (124:3)	62304
MS-SQL version overflow attempt (1:2050)	55095
smtp: Attempted command buffer overflow (124:1)	19871
ftp_pp: Invalid FTP command (125:2)	16952
VOIP-SIP outbound 401 Unauthorized message (1:12007)	9173
VOIP-SIP inbound 401 unauthorized message (1:11969)	8706
SQL generic sql update injection attempt (1:13514)	
frag3: Fragmentation overlap (123:8)	
MISC source port 53 to <1024 (1:504)	
ftp_pp: FTP response length overflow (125:6)	
MS-SQL probe response overflow attempt (1:2329)	
smtp: Attempted data header buffer overflow (124:2)	
smtp: Attempted specific command buffer overflow (124:4)	
RPC portmap NFS request UDP (1:1959)	
SNMP trap udp (1:1419)	
SNMP missing community string attempt (1:1893)	190
SQL generic sql exec injection attempt (1:13512)	179
ftp_pp: FTP malformed parameter (125:4)	159
SQL generic sql insert injection attempt (1:13513)	141
frag3: Short fragment possible DoS attempt (123:3)	101
frag3: Teardrop attack (123:2)	59
BAD-TRAFFIC tcp port 0 traffic (1:524)	55
EXPLOIT RealVNC server authentication bypass attempt (1:13612)	40
ftp_pp: FTP parameter length overflow (125:3)	38

Here's a month's worth of events...

Message	Count
http_inspect: OVERSIZE REQUEST-URI DIRECTORY (119:15)	94852
smtp: Attempted response buffer overflow (124:3)	62304
MS-SQL version overflow attempt (1:2050)	55095
smtp: Attempted command buffer overflow (124:1)	19871
ftp_pp: Invalid FTP command (125:2)	16952
VOIP-SIP outbound 401 Unauthorized message (1:12007)	
VOIP-SIP inbound 401 unauthorized message (1:11969)	
SQL generic sql update injection attempt (1:13514)	
frag3: Fragmentation overlap (123:8)	
MISC source port 53 to <1024 (1:504)	
ftp_pp: FTP response length overflow (125:6)	
MS-SQL probe response overflow attempt (1:2329)	
smtp: Attempted data header buffer overflow (124:2)	
smtp: Attempted specific command buffer overflow (124:4)	
RPC portmap NFS request UDP (1:1959)	
SNMP trap udp (1:1419)	
SNMP missing community string attempt (1:1893)	
SQL generic sql exec injection attempt (1:13512)	179
ftp_pp: FTP malformed parameter (125:4)	159
SQL generic sql insert injection attempt (1:13513)	141
frag3: Short fragment possible DoS attempt (123:3)	101
frag3: Teardrop attack (123:2)	59
BAD-TRAFFIC tcp port 0 traffic (1:524)	55
EXPLOIT RealVNC server authentication bypass attempt (1:13612)	40
ftp_pp: FTP parameter length overflow (125:3)	38

Firewall Hole improperly opened or internal SQL Slammer infected system (not an intrusion)

Message	Count
http_inspect: OVERSIZE REQUEST-URI DIRECTORY (119:15)	94852
smtp: Attempted response buffer overflow (124:3)	62304
MS-SQL version overflow attempt (1:2050)	55095
smtp: Attempted command buffer overflow (124:1)	19871
ftp_pp: Invalid FTP command (125:2)	16952
VOIP-SIP outbound 401 Unauthorized message (1:12007)	
VOIP-SIP inbound 401 unauthorized message (1:11969)	
SQL generic sql update injection attempt (1:13514)	
frag3: Fragmentation overlap (123:8)	
MISC source port 53 to <1024 (1:504)	
ftp_pp: FTP response length overflow (125:6)	
MS-SQL probe response overflow attempt (1:2329)	
smtp: Attempted data header buffer overflow (124:2)	
smtp: Attempted specific command buffer overflow (124:4)	
RPC portmap NFS request UDP (1:1959)	
SNMP trap udp (1:1419)	
SNMP missing community string attempt (1:1893)	
SQL generic sql exec injection attempt (1:13512)	179
ftp_pp: FTP malformed parameter (125:4)	159
SQL generic sql insert injection attempt (1:13513)	141
frag3: Short fragment possible DoS attempt (123:3)	101
frag3: Teardrop attack (123:2)	59
BAD-TRAFFIC tcp port 0 traffic (1:524)	55
EXPLOIT RealVNC server authentication bypass attempt (1:13612)	40
ftp_pp: FTP parameter length overflow (125:3)	38

Hyperactive protocol decoder… make sure systems being ‘touched’ are patched; probably many false positives

SearchFinancialSecurity.com INFORMATION SECURITY FINANCIAL INFORMATION SECURITY DECISIONS

Message	Count
http_inspect: OVERSIZE REQUEST-URI DIRECTORY (119:15)	94852
smtp: Attempted response buffer overflow (124:3)	62304
MS-SQL version overflow attempt (1:2050)	55095
smtp: Attempted command buffer overflow (124:1)	19871
ftp_pp: Invalid FTP command (125:2)	16952
VOIP-SIP outbound 401 Unauthorized message (1:12007)	
VOIP-SIP inbound 401 unauthorized message (1:11969)	
SQL generic sql update injection attempt (1:13514)	
frag3: Fragmentation overlap (123:8)	
MISC source port 53 to <1024 (1:504)	
ftp_pp: FTP response length overflow (125:6)	
MS-SQL probe response overflow attempt (1:2329)	
smtp: Attempted data header buffer overflow (124:2)	
smtp: Attempted specific command buffer overflow (124:4)	
RPC portmap NFS request UDP (1:1959)	
SNMP trap udp (1:1419)	
SNMP missing community string attempt (1:1893)	
SQL generic sql exec injection attempt (1:13512)	179
ftp_pp: FTP malformed parameter (125:4)	159
SQL generic sql insert injection attempt (1:13513)	141
frag3: Short fragment possible DoS attempt (123:3)	101
frag3: Teardrop attack (123:2)	59
BAD-TRAFFIC tcp port 0 traffic (1:524)	55
EXPLOIT RealVNC server authentication bypass attempt (1:13612)	40
ftp_pp: FTP parameter length overflow (125:3)	38

Improperly configured VoIP system. Track down and fix. (not an intrusion)

Message	Count
http_inspect: OVERSIZE REQUEST-URI DIRECTORY (119:15)	94852
smtp: Attempted response buffer overflow (124:3)	62304
MS-SQL version overflow attempt (1:2050)	55095
smtp: Attempted command buffer overflow (124:1)	19871
ftp_pp: Invalid FTP command (125:2)	16952
VOIP-SIP outbound 401 Unauthorized message (1:12007)	
VOIP-SIP inbound 401 unauthorized message (1:11969)	
SQL generic sql update injection attempt (1:13514)	
frag3: Fragmentation overlap (123:8)	
MISC source port 53 to <1024 (1:504)	
ftp_pp: FTP response length overflow (125:6)	
MS-SQL probe response overflow attempt (1:2329)	
smtp: Attempted data header buffer overflow (124:2)	
smtp: Attempted specific command buffer overflow (124:4)	
RPC portmap NFS request UDP (1:1959)	
SNMP trap udp (1:1419)	
SNMP missing community string attempt (1:1893)	
SQL generic sql exec injection attempt (1:13512)	179
ftp_pp: FTP malformed parameter (125:4)	159
SQL generic sql insert injection attempt (1:13513)	141
frag3: Short fragment possible DoS attempt (123:3)	101
frag3: Teardrop attack (123:2)	59
BAD-TRAFFIC tcp port 0 traffic (1:524)	55
EXPLOIT RealVNC server authentication bypass attempt (1:13612)	40
ftp_pp: FTP parameter length overflow (125:3)	38

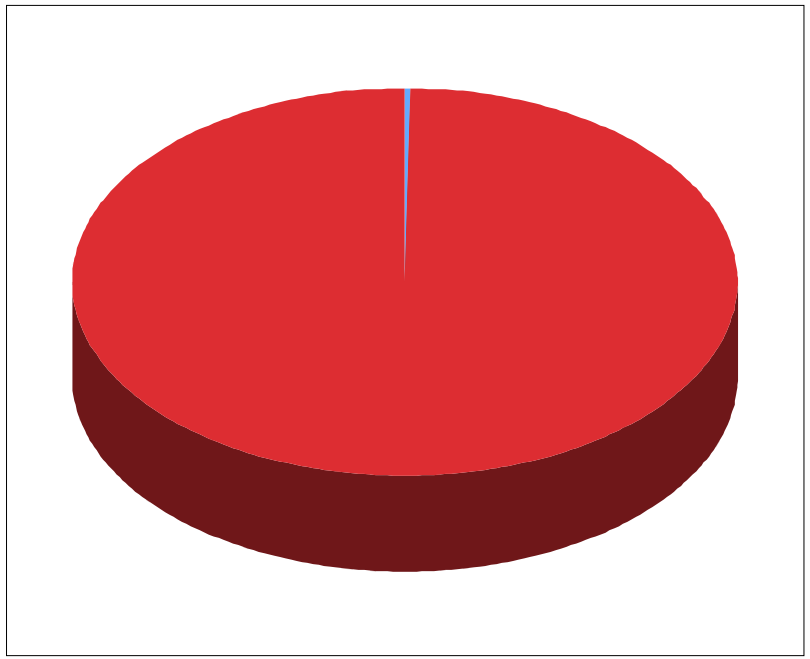
Policy issue. Is NFS allowed or isn't it? Is SNMP allowed or isn't it? (not an intrusion)

Message	Count
http_inspect: OVERSIZE REQUEST-URI DIRECTORY (119:15)	94852
smtp: Attempted response buffer overflow (124:3)	62304
MS-SQL version overflow attempt (1:2050)	55095
smtp: Attempted command buffer overflow (124:1)	19871
ftp_pp: Invalid FTP command (125:2)	16952
VOIP-SIP outbound 401 Unauthorized message (1:12007)	
VOIP-SIP inbound 401 unauthorized message (1:11969)	
SQL generic sql update injection attempt (1:13514)	
frag3: Fragmentation overlap (123:8)	
MISC source port 53 to <1024 (1:504)	
ftp_pp: FTP response length overflow (125:6)	
MS-SQL probe response overflow attempt (1:2329)	
smtp: Attempted data header buffer overflow (124:2)	
smtp: Attempted specific command buffer overflow (124:4)	
RPC portmap NFS request UDP (1:1959)	
SNMP trap udp (1:1419)	
SNMP missing community string attempt (1:1893)	
SQL generic sql exec injection attempt (1:13512)	179
ftp_pp: FTP malformed parameter (125:4)	159
SQL generic sql insert injection attempt (1:13513)	141
frag3: Short fragment possible DoS attempt (123:3)	101
frag3: Teardrop attack (123:2)	59
BAD-TRAFFIC tcp port 0 traffic (1:524)	55
EXPLOIT RealVNC server authentication bypass attempt (1:13612)	40
ftp_pp: FTP parameter length overflow (125:3)	38

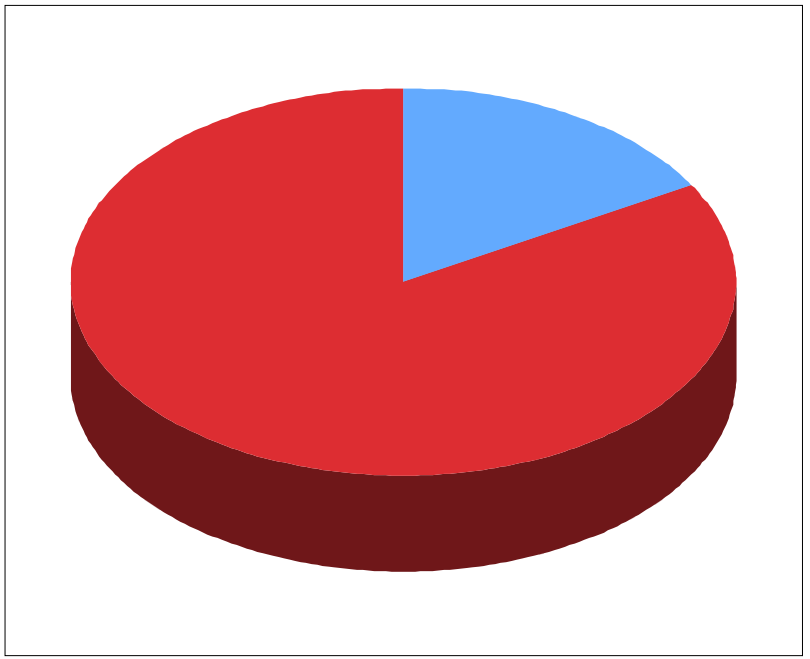
Why is VNC happening across this IPS? Policy problem or firewall hole! (attempted intrusion)

IDSes Can Help You With the Problems You Might Have Tomorrow

Chance of your company being "intruded" at random from the Internet

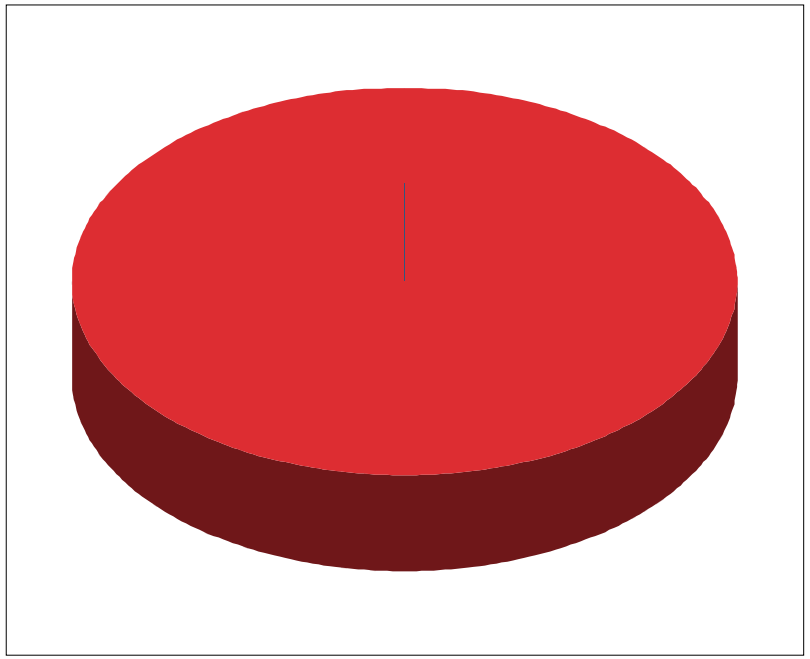


Chance of your IDS discovering the intrusion as it happens

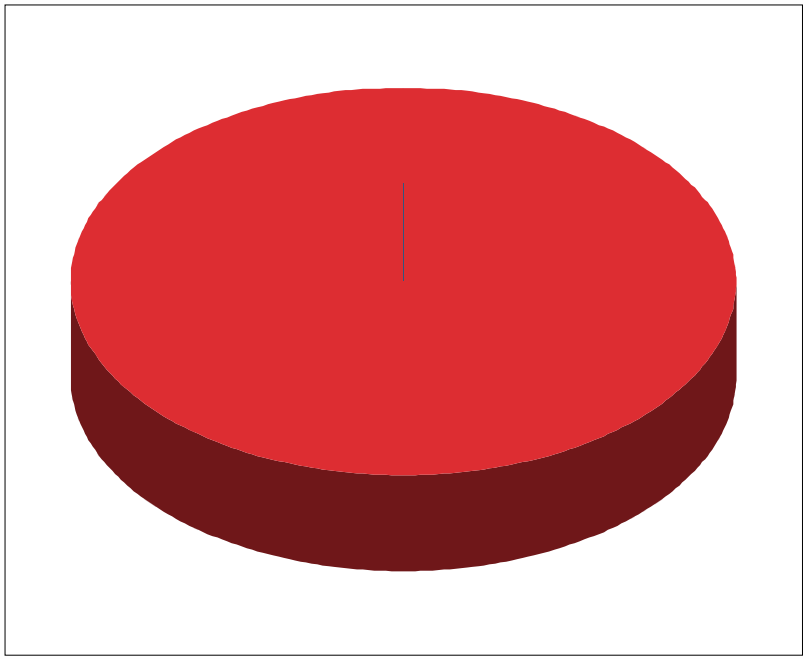


IDSes Do Help You With the Problems You Have Today

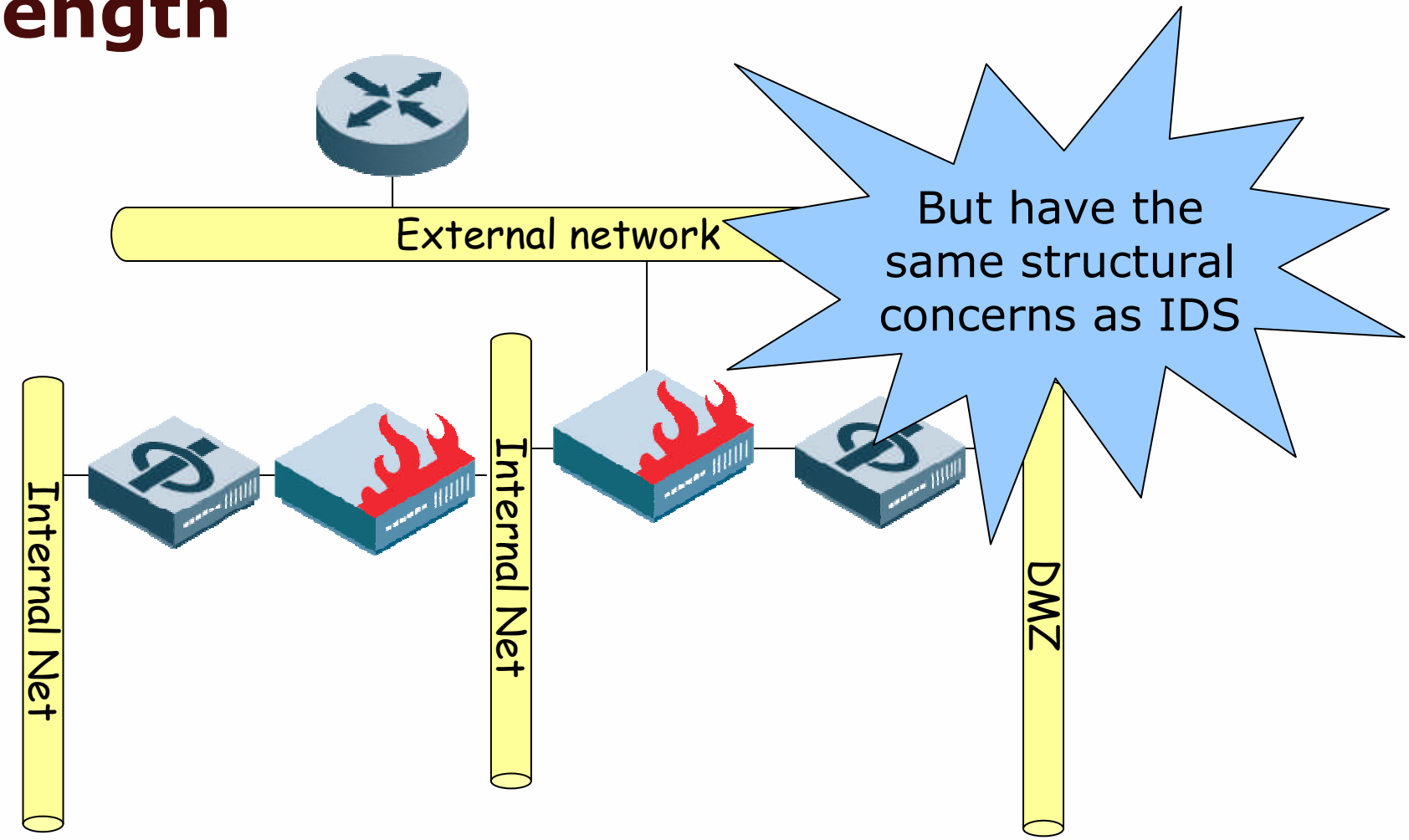
Chances your company has at least one network security problem



Chances of your IDS discovering network security problems



IPSes Also Have Their Area of Strength



Grain Of Truth: Use IDS and IPS Where They Make Sense

- **Your goal with an IDS should be improved network security visibility**
  - Which can help you dramatically increase total security!
- **Your goal with an IPS should be improved visibility and "narrowing" of patch window**
  - Which may or may not be redundant, but will add visibility in the same way IDS does

Myth 2

Unified Threat Management (UTM) Firewalls with Anti-Virus provide effective malware protection

Reality: UTM Firewalls Provide Secondary and Tertiary Protections

- **Desktop protection is required!**
- **Application-specific protection is required!**
  - Example: anti-spam/anti-virus email gateway
- **"Layer 7 aware" protection is strongly recommended!**
  - Example: web proxy for outbound

Real Testing Shows A/V Protection Only (Except for Sonicwall) on Standard Ports!

Vendor	Product	Protocols Covered	Catch Score
Astaro	ASG 425a	FTP, HTTP, SMTP, POP3	67%
Check Point	UTM-1 2050	FTP, HTTP, SMTP, POP3	70%
Crossbeam	C25	FTP, HTTP, SMTP, POP3	70%
Fortinet	FortiGate 3600A	FTP, HTTP, SMTP, IMAP, POP3, IM, NNTP	75%
IBM/ISS	Proventia MX5010	FTP, HTTP, SMTP, POP3	60%
Juniper Networks	SSG-520M	FTP, HTTP, SMTP, IMAP, POP3	72%
Nokia	IP290	FTP, HTTP, SMTP, POP3	75%
Secure Computing	Sidewinder 2150D with IPS accel.	FTP, HTTP, SMTP	75%
SonicWALL	PRO 5060	FTP, HTTP, SMTP, IMAP, POP3, CIFS, TCP	85%
WatchGuard	Firebox Peak X8500e	SMTP, HTTP, TCP	45%

Real Testing Shows IPS Protection by UTM Lower Than Standalone IPS

Vendor	Product	Version	Scenario Notes	Client Score	Server Score
Astaro	ASG 425a	v7.009	Recommended Settings	19%	36%
Check Point	UTM-1 2050	NGX R65	SecureDefense	27%	32%
Cisco	ASA5540	7.2.3	Block at 85% confidence	20%	30%
			Block at 55% confidence	37%	33%
Crossbeam	C25	NGX R65	SecureDefense	27%	32%
Fortinet	FortiGate 3600A	v3.00 MR4	major/critical severity	14%	23%
			all signatures	41%	24%
IBM	System x3650	NGX R65	SecureDefense	27%	32%
IBM/ISS	Proventia MX5010	v3.12	Recommended Settings	75%	44%
Juniper Networks	ISG-1000	6.0.0	IDP, high severity	42%	46%
			IDP all severities	87%	70%
			No additional protections	5%	17%
Juniper Networks	SSG-520M	6.0.0	Deep Inspection, maj/crit	19%	24%
			Deep Inspection, all sigs	21%	25%
Nokia	IP290	NGX R65	SecureDefense	27%	32%
Secure Computing	Sidewinder 2150D	v7.0	with IPS	22%	34%
			only proxy	7%	14%
SonicWALL	PRO 5060	v4.0.0.0	major/critical severity	22%	19%
			all signatures	45%	46%
WatchGuard	Firebox Peak X8500e	v9.0.1	major/critical severity	39%	30%
			all signatures	40%	31%

Don't Get Me Wrong: UTMs are Great!

Criteria	Notes
Cost	Long-term costs for UTM will likely be lower than individual point solutions
Performance	By intelligently routing traffic to different engines, performance of a single large box can exceed multiple small boxes
Complexity	High Availability and Scalability are dramatically simplified in UTM
Management	A single management interface reduces the possibility of mistakes
Flexibility	Ability to bring security services in and out of the equation quickly supports threat response requirements best

Grain of Truth: Use UTMs to Provide Both Primary and Secondary Security Services

- As border firewalls, UTMs provide the same protection you're used to
- Services such as content filtering and URL control are ideal at UTM firewalls
- Security services such as Anti-Malware help back-stop other technologies as a "defense in depth" strategy

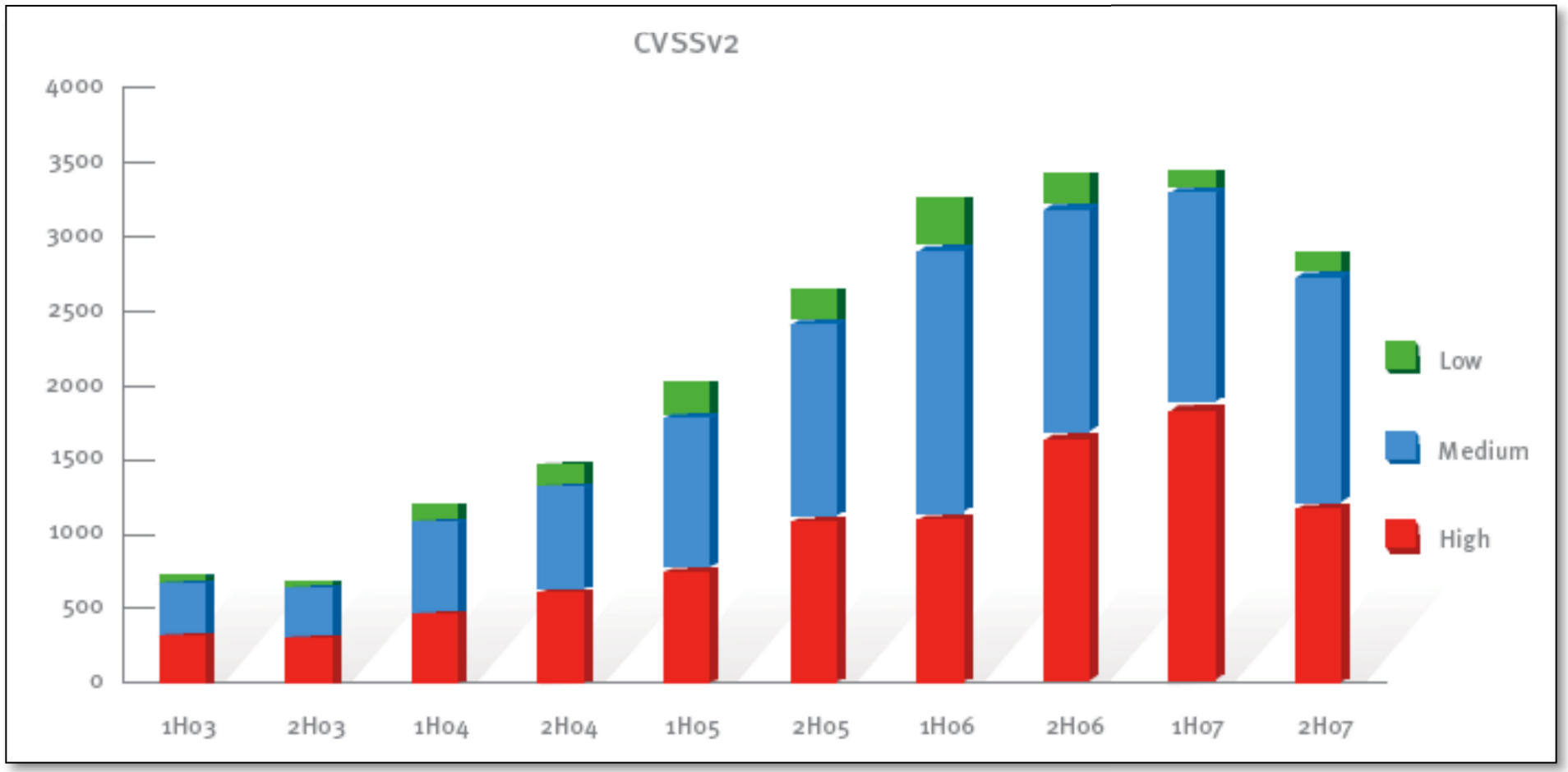
Myth 3

Updating Anti-Virus Signatures Every 30 Seconds Is The Best Protection Against New Threats

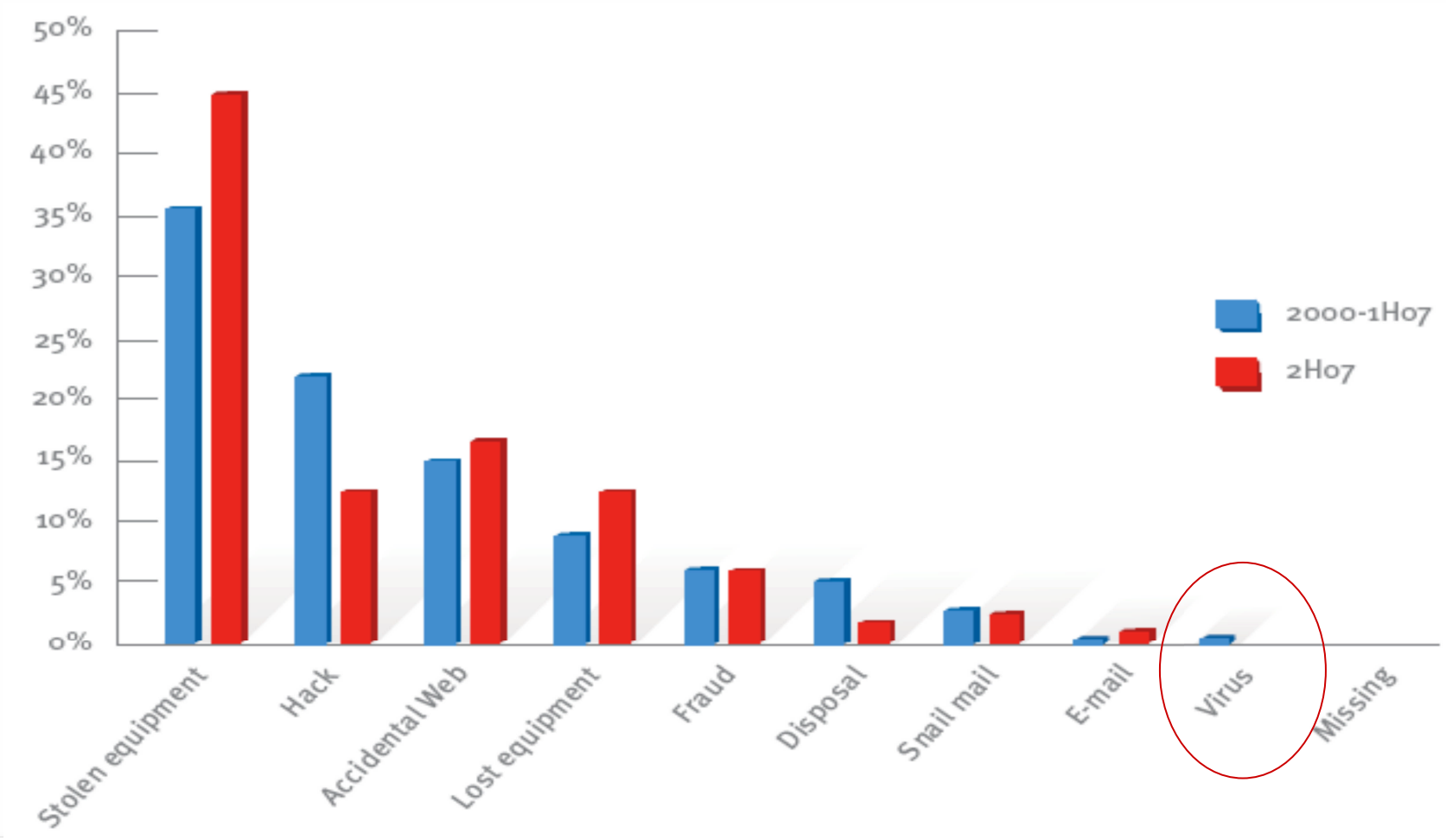
Reality: New Threats Are Application Layer Threats

- Focusing on viruses makes you lose sight of the larger threat landscape

CVSS Says: 6500+ Vulnerabilities in 2007. That's Not Viruses.



Attrition.ORG Says: Viruses the Least of Your Worries in 2007 for Breaches



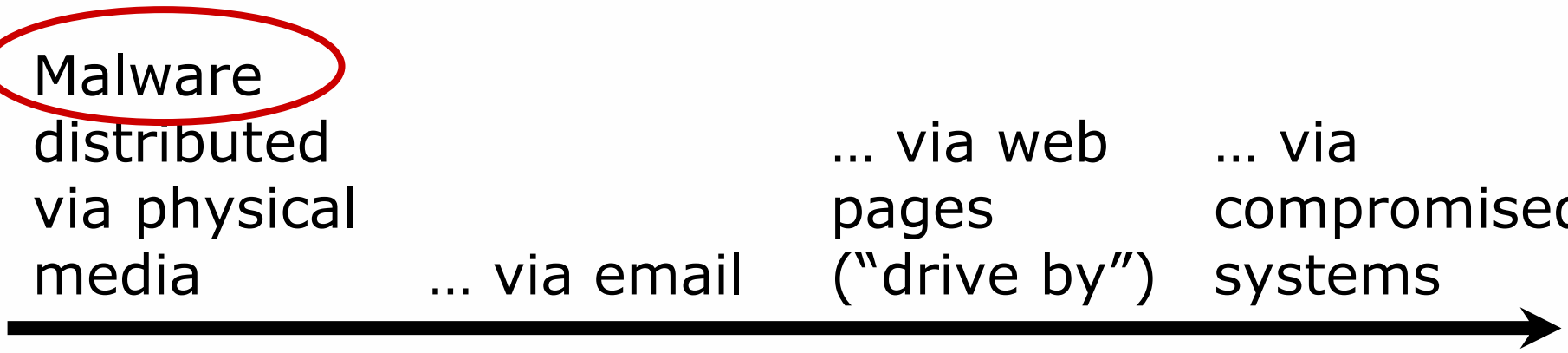
Look Beyond Yesterday's Threats **And Focus on Tomorrow's Threats**

Malware distributed via physical media

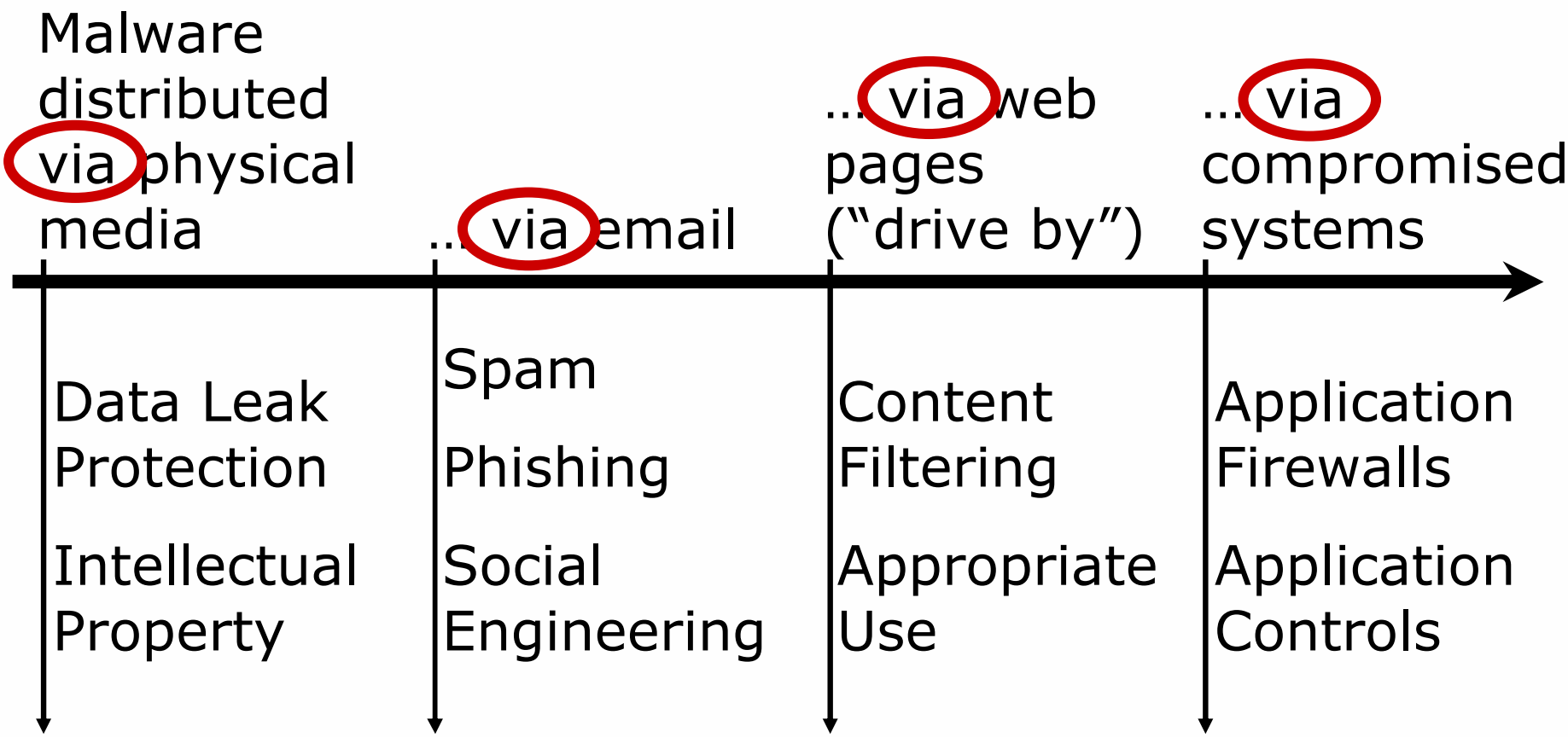
… via email

… via web pages ("drive by")

… via compromised systems

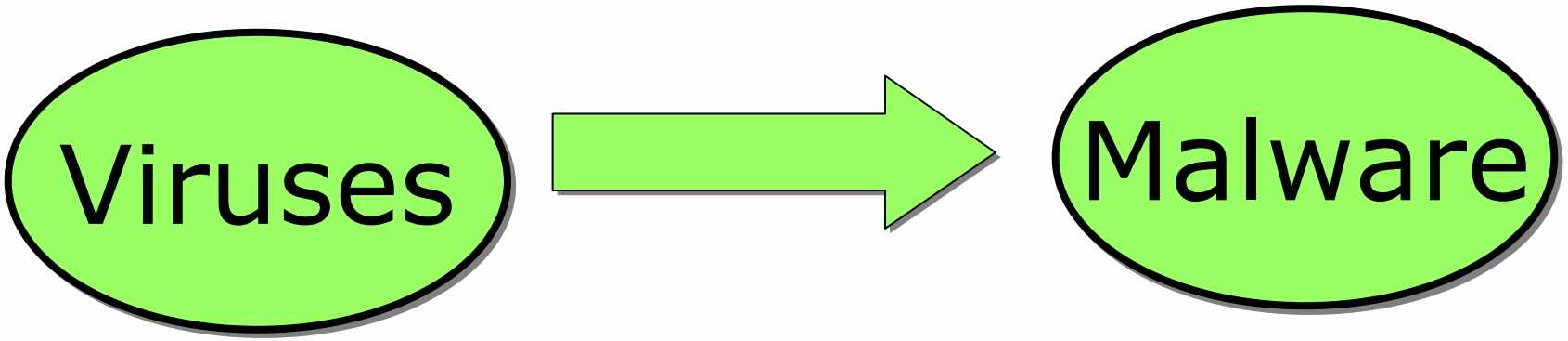


Look Beyond Yesterday's Threats And Focus on Tomorrow's Threats



Grain of Truth: Be Proactive In Responding To New Threats

- **But focus on the threat vector rather than on the threat *du jour***



Myth 4

Zero-Day Threats Are Your Biggest Problem

Reality: Old, Tired, Reliable Threats Are Your Biggest Problem

- You do have to worry about new threats
- But the greatest likelihood of a problem is going to come from old threats

Microsoft says: Oldies are Still Goodies

Rank	Malware Family	Added to the MSRT	Disinfections
1	Win32/Zlob	March 2006	14,351,774
2	Win32/Renos	May 2007	4,263,697
3	Win32/ConHook	November 2007	2,419,023
4	Win32/RJump	October 2007	2,268,529
5	Win32/Rbot	April 2005	2,257,546
6	Win32/Brontok	November 2006	1,767,449
7	Win32/Hupigon	July 2006	1,392,050
8	Win32/Jeefo	August 2006	1,358,413
9	Win32/Parite	January 2006	1,297,617
10	Win32/Nuwar, WinNT/Nuwar	September 2007	1,274,684

82% of detected malware by MSRT are more than 6 months old!

Rootkits are successful with old attacks

WebAttacker (9/06)	MPack V0.94	IcePack (9/07)
MS-DAC Vuln. (CVE-2006-0003); Windows VML Vuln. (CVE-2006-4868); MS Virtual Machine Vuln. (CVE-2003-0111); Windows Media Player Plug-In with Non-MS Internet Explorer Vuln. (CVE-2006-0005); Exploitable crash in InstallVersion.compareTo Vuln. (CVE-2005-2265)	MS-DAC Vuln. (CVE-2006-0003); Apple QuickTime RTSP URI Remote Buffer Overflow Vuln. (CVE-2007-0015); WinZip FileView ActiveX Control Multiple Vulns (CVE-2006-6884); MS WebViewFolderIcon ActiveX Control Buffer Overflow Vuln. (CVE-2006-3730); MS Management Console Vuln. (CVE-2006-3643); Windows Media Player MP Plug-In with Non-MS IE Vuln. (CVE-2006-0005)	MS-DAC Vuln. (CVE-2006-0003); WebViewFolderIcon ActiveX Control Buffer Overflow Vuln. (CVE-2006-3730); MS Management Console Vuln. (CVE-2006-3643); Vector Markup Language Vuln. (CVE-2007-0024); MS DirectX Media 6.0 Live Picture Corp. DirectTransform FlashPix ActiveX (CVE-2007-4336); Yahoo! Messenger Webcam ActiveX Remote Buffer Overflow Vuln. (CVE-2007-3147/3148); Yahoo! Widgets YDP ActiveX Control Buffer Overflow Vuln. (CVE-2007-4034); WMP Plug-In with Non-Microsoft IE Vuln. (CVE-2006-0005); JavaScript Navigator Object Vuln. (CVE-2006-3677)

Old Attacks Outnumber New

Microsoft Security Bulletin MS02-039

Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code Execution (Q323875)

Originally posted: July 24, 2002
Updated: January 31, 2003

Summary

Who should read this bulletin:
System administrators using Microsoft® SQL Ser
Engine 2000.

Impact of vulnerability:
Three vulnerabilities, the most serious of which could enable an attacker to gain control over an affected server.

Maximum Severity Rating:
Critical

SQL Slammer Attacks Per Hour at Opus One, May 2008: 810

Really Old Attacks are Still Around!

Microsoft Security Bulletin MS01-033

Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise

Originally posted: June 18, 2001
Updated: November 04, 2003

Summary

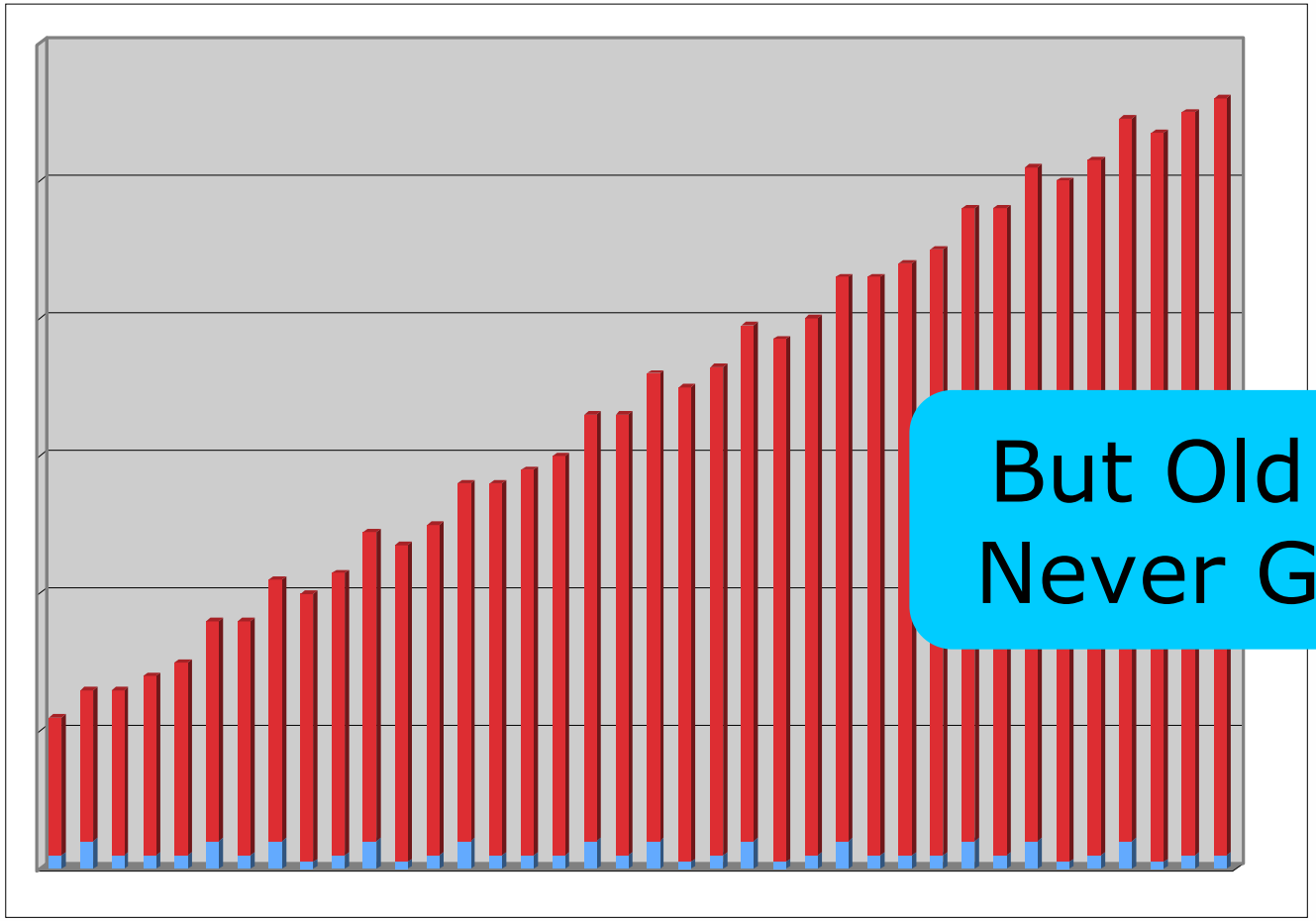
Who should read this bulletin:
System administrators of web servers using Microsof

Impact of vulnerability:
Run code of attacker's choice.

Recommendation:
Microsoft strongly urges all web server administrators to apply the patch immediately.

Code Red Attacks Per Hour at Opus One, May 2008: 4

Grain of Truth: There Will Be A New Attack Tomorrow



But Old Attacks Never Go Away!

Myth 5

I Can't Afford To Buy All The Products That Everyone Wants To Sell Me

Reality:
You can't afford to waste money

- **Many networks have security 20 layers thick in some places, and 0 layers thick in others**

Build Balance Into Your Threat Protection

Anti-Spam

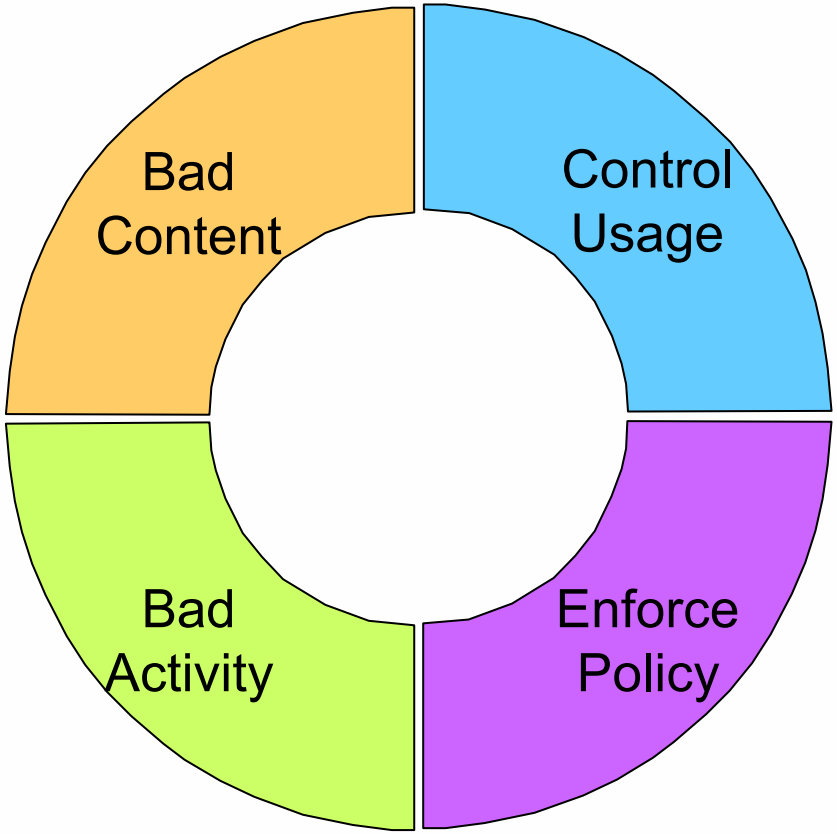
Anti-Virus

Anti-Spyware

Anti-Phishing

Intrusion Prevention

DoS/DDoS Mitigation



Content Filtering

Application Blocking

Bandwidth Management

Regulatory Logging/ Blocking

Grain of Truth: Security Companies Are There To Make Money First

- **… And To Protect You**

You have to take responsibility for a balanced and rational strategy!