



Hack in Paris
International IT Security Conference
June 14-17 2011

The logo features a stylized green figure with a white lightning bolt in its center, set against a black background with radiating lines.

Proactive Security Through Vulnerability Management

by Gary S. Miliefsky, FMDHS, CISSP®



Agenda

- Learn about Common Vulnerabilities and Exposures (CVEs) and how hackers, viruses, worms, spyware, botnets, rootkits, Trojans, cybercriminals and cyberterrorists use CVEs to exploit networks. Over 95% of successful attacks are exploits of these CVEs.



About Me

- ✓ ***Fellow CISSP®***
- ✓ ***Founder & CTO, NetClarity, Inc.***
- ✓ ***Founding Member, US DHS***
- ✓ ***Founding Board Member of NAI SG.org***
- ✓ ***Frequent Cover Story Writer for Hakin9 Magazine***
- ✓ ***Advisor to Norwich University's Cyberwarfare Labs***



About My Company – NetClarity, Inc.

“Most Innovative New Security Product for 2011”

- Award during RSA2011 by InfoSec Products Guide

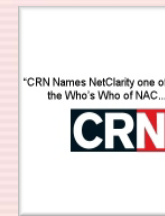
“NetClarity Picks Up Where Firewalls, Anti-virus, Intrusion Detection Systems and Intrusion Prevention Systems Leave Off”

— John Gallant, President, Network World



“The Most Innovative NAC Vendor in the World”

– Network Products Guide, Hot Companies, 2009, 2010, 2011



What is Cybercrime?

Traditional criminal techniques

Burglary: Breaking into a building with the intent to steal.



Deceptive callers: Criminals who telephone their victims and ask for their financial and/or personal identity information.



Extortion: Illegal use of force or one's official position or powers to obtain property, funds, or patronage.



Fraud: Deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage.



Identity theft: Impersonating or presenting oneself as another in order to gain access, information, or reward.



Child exploitation: Criminal victimization of minors for indecent purposes such as pornography and sexual abuse.



Cybercrime

Hacking: Computer or network intrusion providing unauthorized access.



Phishing: A high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.



Internet extortion: Hacking into and controlling various industry databases (or the threat of), promising to release control back to the company if funds are received or some other demand satisfied.



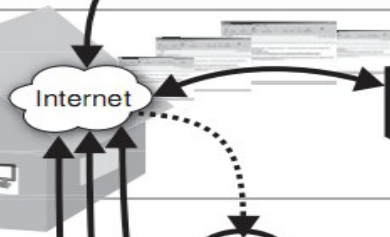
Internet fraud: A broad category of fraud schemes that use one or more components of the Internet to defraud prospective victims, conduct fraudulent transactions, or transmit fraudulent transactions to financial institutions or other parties.



Identity theft: The wrongful obtaining and using of another person's identifying information in some way that involves fraud or deception, typically for economic gain.



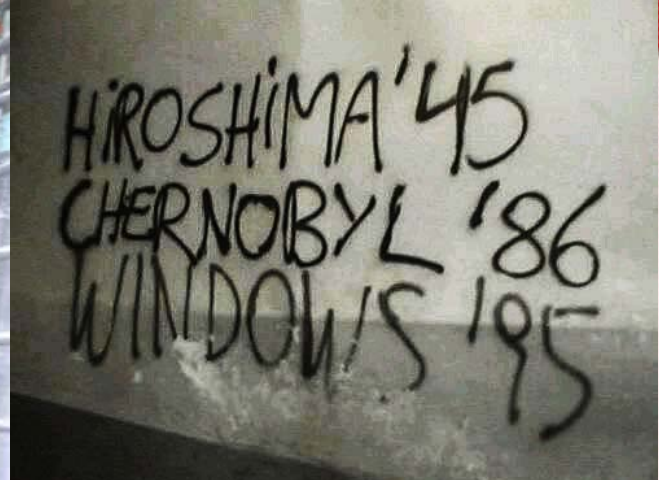
Child exploitation: Using computers and networks to facilitate the criminal victimization of minors.



Cybercrime – Purely “Digital” Paradigm



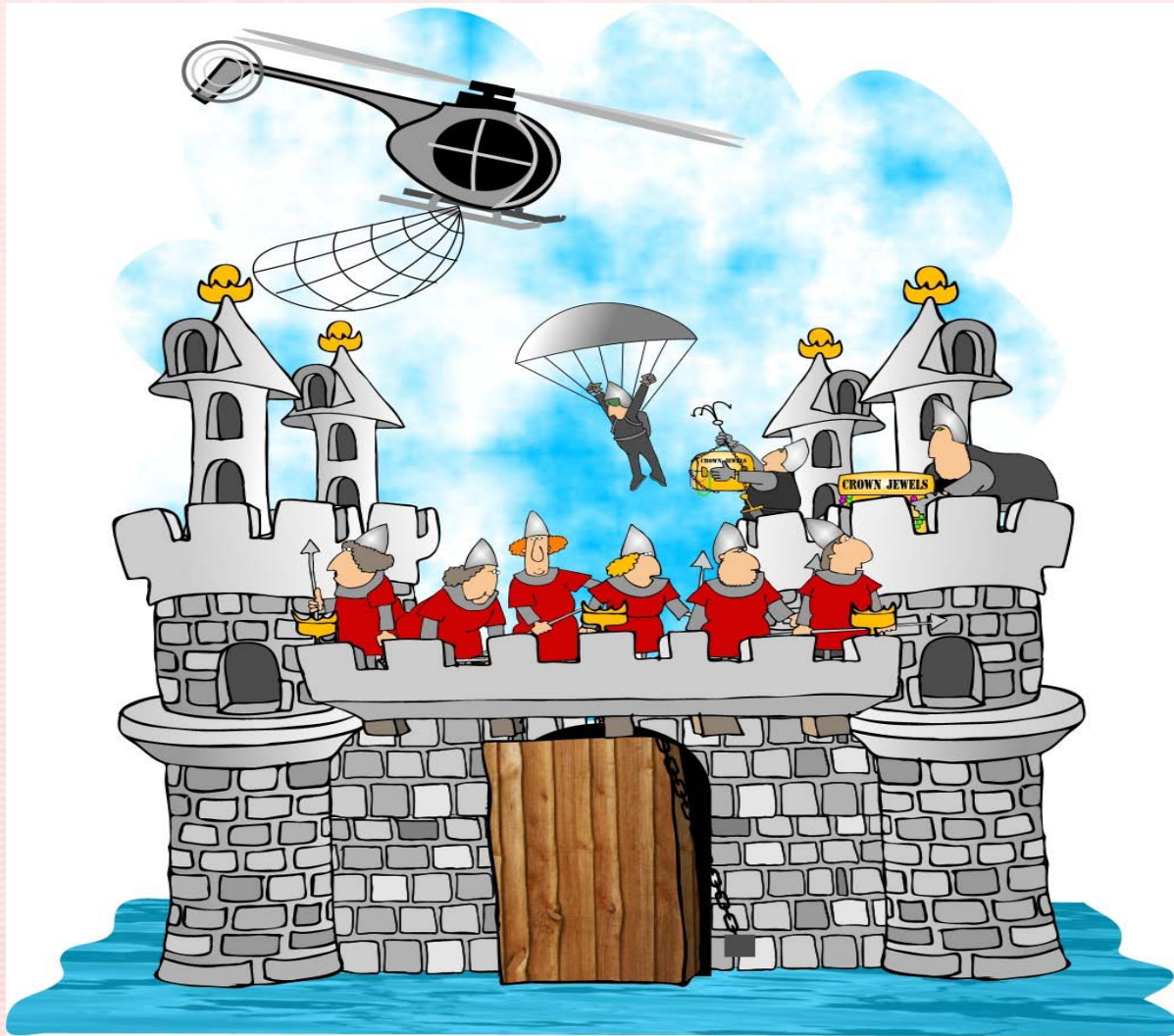
What is Cyberwar?



Trust me...you'll love this gift...



Looking outward with old tools...



“over 80% of successful exploitation happens from the inside, behind the firewall”

- SANS.org

Today's Giveaway....PRIZES!!!

- Stay Awake, Sharp and Focused!
- Ten of you who are able to answer my questions correctly will win...
- ONE YEAR OF HAKING MAGAZINE on USB STICK



Fact: Nothing with an IP Address Is Secure

- No device is safe – all IP-based devices are exposed to exploitation:

It is a target

It can be spoofed

It can be infected

It can be remotely controlled

It is probably already infected



Fact: Wireless Will Never Be Secure!

- **WEP was easy to crack; now WPA is also...**

Recently deployed tools such as Back Track v4.0 allow you to break wireless encryption by attacking the smaller 24-bit session initiation key and then gaining full “trusted” access to a wireless router.

- **Wireless Routers have Critical Flaws (CVEs)**

Now you can break into the admin interface of a wireless router by sending malformed packets from your laptop and pringles can...not worrying about the encryption, see NVD.NIST.GOV and type in “wireless”



Fact: VoIP is Insecure

VoIP is at very high risk of attack, including Eavesdropping and Denial of Service(DoS) attacks, as well as exploitation of CVE®s.

Eavesdropping:

Would you make a purchase over a VoIP connection, giving your credit card information out over the VoIP phone? (over 100M credit card numbers stolen over the IP protocol)

Denial of Service:

What happens when you need to place an emergency phone call (E911)? Can you do it with VoIP? Not today and not guaranteed (without copper wire backup connection).

Exploiting CVE®s: More on that to follow...





VoIP Communications

- Dozens of voice over IP (VoIP) holes....known as Common Vulnerabilities and Exposures (CVEs)
- Take over the administrative console remotely by exploiting one of many CVEs
- Launch a Man in the Middle attack:
Voice over Misconfigured IP Telephony (aka VOMIT)
– use a TCP/IP wireshark/ethertrace:
 - a) save a “dump” file of network traffic
 - b) then run the file through this tool and get a .WAV file to play back conversations...

<http://hakin9.org/magazine/1255-securing-voip>



Sample VoIP Vulnerabilities

- **Confidentiality and Privacy**
 - Switch Default Password
 - Classical Wiretap
 - ARP Cache Poisoning
 - ARP Flooding
 - Web Server Flaws
 - IP Phone Netmask Vulnerability
 - Extension to IP Address Mapping
- **Integrity Vulnerabilities**
 - DHCP Server Insertion
 - TFTP Server insertion
- **Availability and Denial of Service Issues**
 - Account Lockout
 - CPU Resource Consumption
 - Buffer Overflows and Improper Packet Handling

Exploitable VoIP CVE[®]s (see cve.mitre.org)

CAN-2005-2181

- **Summary:** Cisco 7940/7960 Voice over IP (VoIP) phones do not properly check the Call-ID, branch, and tag values in a NOTIFY message to verify a subscription. This allows remote attackers to spoof messages such as the "Messages waiting" message.

CVE-2002-0835

- **Summary:** Preboot eXecution Environment (PXE) server allows remote attackers to cause a denial of service (crash) via certain DHCP packets from Voice-Over-IP (VOIP) phones.

CAN-2002-0882

- **Summary:** The web server for Cisco IP Phone (VoIP) models 7910, 7940, and 7960 allows remote attackers to cause a denial of service (reset) and possibly read sensitive memory via a large integer value in (1) the stream ID of the StreamingStatistics script or (2) the port ID of the PortInformation script.



Sorry if you just ate lunch...

VoMIT—Voice over Misconfigured Internet Telephone:

- The vomit utility converts a Cisco IP phone conversation into a wave file that can be played with ordinary sound players.
- Vomit requires a tcpdump output file.
- Example of how to run VoMIT
 - `$ vomit -r phone.dump | waveplay -S8000 -B16 -C1`



Fact: Anti-virus is dead!

No One Can Keep Up With New Malware

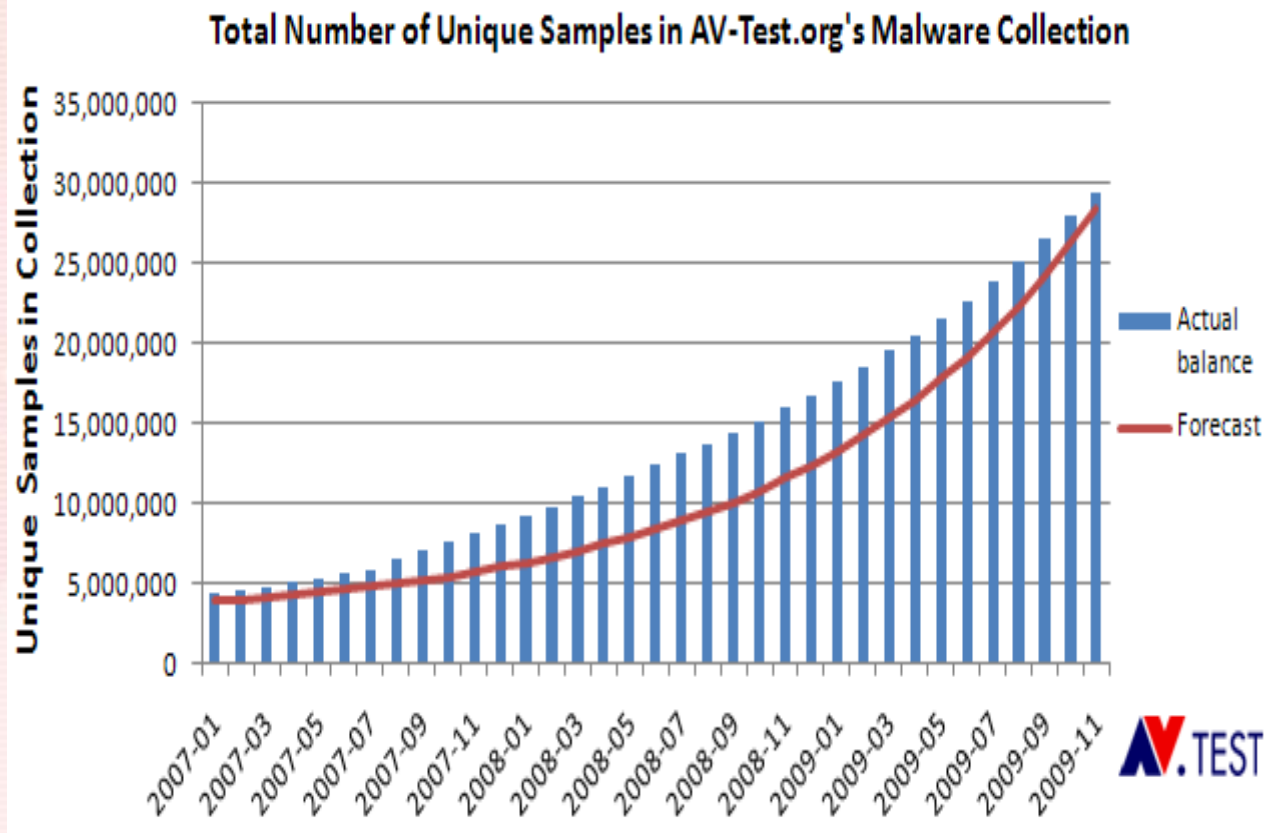
According to independent malware test labs, ALL ANTI-VIRUS software agents FAILED to stop ALL new threats, known as zero-day malware.

See:

<http://www.anti-malware-test.com>

<http://blogs.zdnet.com/security/?p=5365>

<http://av-test.org>



Report: 48% of 22 million scanned computers infected with malware



Fact: Your Identity Was Stolen!

~350M Americans & 516M records stolen

PrivacyRights.org



- More than 516M Personally Identifiable Information (PII) records for more than 350M citizens in America. How many have been lost, hacked and stolen?

According to PrivacyRights.org, the total number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005:

**516,942,944 RECORDS BREACHED
from 2,392 DATA BREACHES made public since 2005**

- Still think you are secure?
- Still believe your anti-virus and firewall can truly secure your network or your personal computer?





Retail and E-tail #1 Target

Retail and E-tail Outlet Attacks will Outpace Attacks Targeting Banks

- ***Banks are getting much more secure***
- ***Banks are audited regularly by the FDIC (in the USA)***
- ***Cybercriminals are finding it harder and harder to break into the bank***
- ***Retail and E-tail are easy targets***
 - ***Wireless routers***
 - ***Wireless CVEs***
 - ***Spoof-able Barcode Scanners***
 - ***Spoof-able Cash Registers***
 - ***Real-time Connections to MONEY (Visa Payment Gateway, etc...)***





Hospitals #1 Exploitable

Hospitals will become the Most Exploitable of All Vertical Markets

- *Hospitals are run by committees*
- *Committees are slow to make decisions*
- *No one from H&HS enforced HIPAA*
- *Therefore, HIPAA had NO TEETH!*
- *Finally, you're looking at older, less updated equipment*
- *More Wireless, More Vulnerabilities*
- *NOT ENOUGH ENCRYPTION*
- *NOT ENOUGH SELF-ASSESSMENT*
- *Can be exploited from the parking lot...*





The “Cloud” Is a Cybercrime Magnet

- **Cloud computing has shifted the paradigm for risk.**
- **The Cloud offers low overhead in return for powerful remote business functionality.**
- **In return, you face the risk of data leakage, Cloud attacks and Cloud infections.**
- **You won't know if and when it happens because of the remote aspects and the pervasive nature of the Cloud.**





Clouds & VMs Will Be Attacked!

Cloud Computing and Virtual Machines (VM) are specifically targeted by Cybercriminals and Cyberterrorists resulting in VM Malware and Cloud Downtime and Cloud Data Theft.

- *Holes are being discovered monthly on VMs*
- *The Cloud enables one infected VM to infect another VM*
- *Through distributed denial of service (DDos) attacks, exploiters can cause a new 'elasticity' attack on your Cloud resources, leaving you with a HUGE bill from your provider.*
- *There is so much more I could share in this area, I recommend you read my article about Securing the Cloud in Hakin9 Magazine, here:*

<http://hakin9.org/magazine/1296-securing-the-cloud>





Critical Infrastructure – Bullseye!

New and Innovative Attacks will be launched against Critical Infrastructure by Rogue and Competitive Nations.

- ***Transportation is a major target***
- ***Power grids are now under attack***
- ***Defense Departments will continue to be hit***
- ***Some of these attacks are well crafted (like Stuxnet)***
- ***Some will take advantage of weak assets***
- ***Some Countries (like USA, China, North Korea, and last week, Iran, have announced they have teams working on this or are now hiring teams of cyber experts)***
- ***Google...HILF, EMP, HERF and CEE or read this article:***

<http://www.scmagazineus.com/hired-guns-whats-in-the-name-cyberpmc-or-cyberpsc/article/193959/>





Blackberry? iPhone? iTouch? iPad?

- Do they really belong on the “corporate” network?
- How do you know when they come and go?
- How do you stop them from bringing malware into the network?
- How do you stop them from being used to steal or leak confidential data?



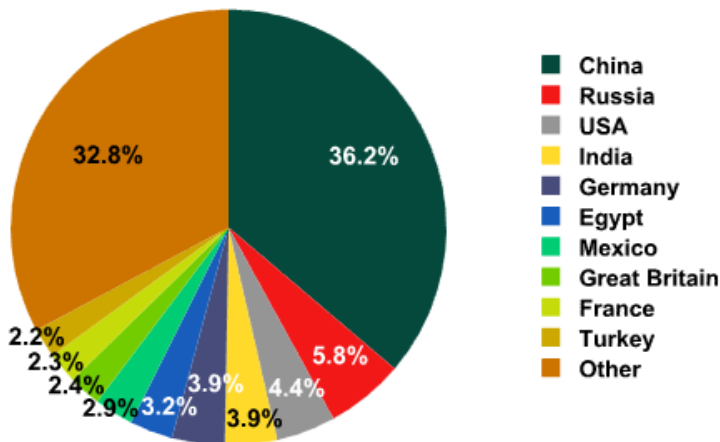
Cell Phones and PDAs – Target!

- ***Apple admits there's no way to guarantee an iTouch or iPhone Application DOES NOT contain malware.***
- ***Google admits there's no way to guarantee an Android Application DOES NOT contain malware.***
- ***Blackberry devices have 9 known CVEs (and more coming)....Android based on Linux OS (which also has known vulnerabilities)***
- ***Most Users CLICK "OK" almost every time when warned that "This application can use the internet, track your location, utilize other phone and data resources..."***



Zero-Day Malware Is Running Rampant

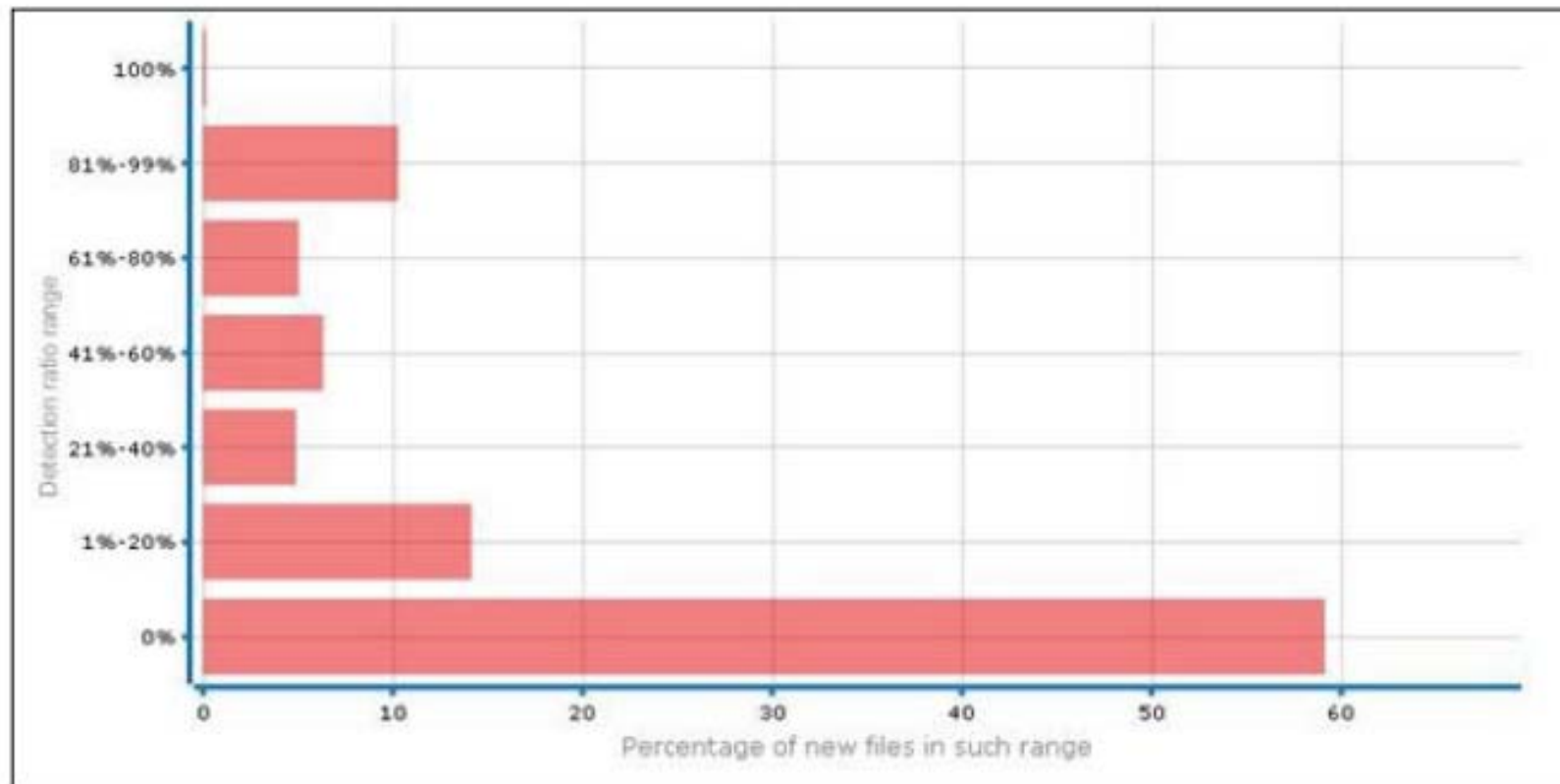
New Malware that exists without a known signature is Zero Day. Sometimes it takes weeks before major vendors have fully tested samples and written a signature test.



Position	Change in position	Name	Number of infected computers
1	0	Net-Worm.Win32.Kido.ir	276021
2	0	Net-Worm.Win32.Kido.iq	197376
3	▲ 1	Virus.Win32.Sality.aa	169101
4	▼ -1	Net-Worm.Win32.Kido.ih	164421
5	0	Worm.Win32.FlyStudio.cu	109898
6	▲ 21	Trojan-Downloader.JS.Zapchast.m	65476
7	▲ 21	Trojan-Downloader.JS.Small.oj	64767
8	▲ 1	Trojan-Downloader.WMA.GetCodec.s	63266
9	▼ -1	Trojan-Downloader.Win32.VB.eql	61852
10	▲ 2	Virus.Win32.Virut.ce	51944
11	▼ -4	not-a-virus:AdWare.Win32.Boran.z	51868
12	▲ 1	Virus.Win32.Induc.a	44432
13	🐾 New	Trojan.Win32.AutoRun.sj	39530
14	🐾 New	Packed.Win32.Krap.l	38944
15	🐾 New	Trojan.Win32.AutoRun.sl	38742
16	▲ 1	Worm.Win32.Mabezat.b	37365
17	🐾 New	Worm.Win32.AutoIt.tc	36162
18	🐾 New	Trojan.Win32.AutoRun.ws	36149
19	▼ -5	Trojan-Dropper.Win32.Flystud.yo	35883
20	▼ -4	Packed.Win32.Black.a	35462



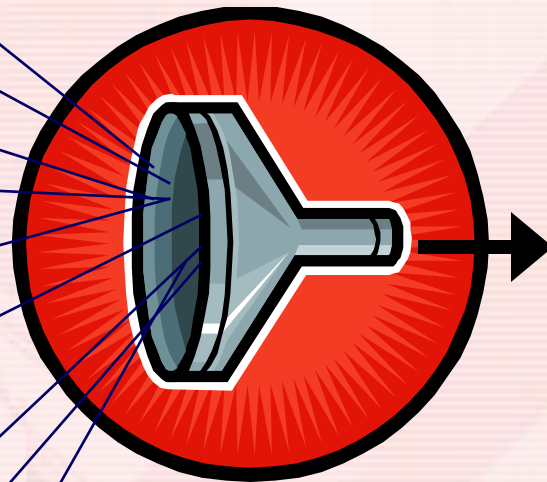
Exponential Growth of New Malware!



Virus Total has nearly 60% undetectable malware samples, each day

What Is Malware?

- Virus
- Trojan
- Worm
- Rootkit
- Botnet
- Zombie
- Keylogger
- Adware
- Spyware

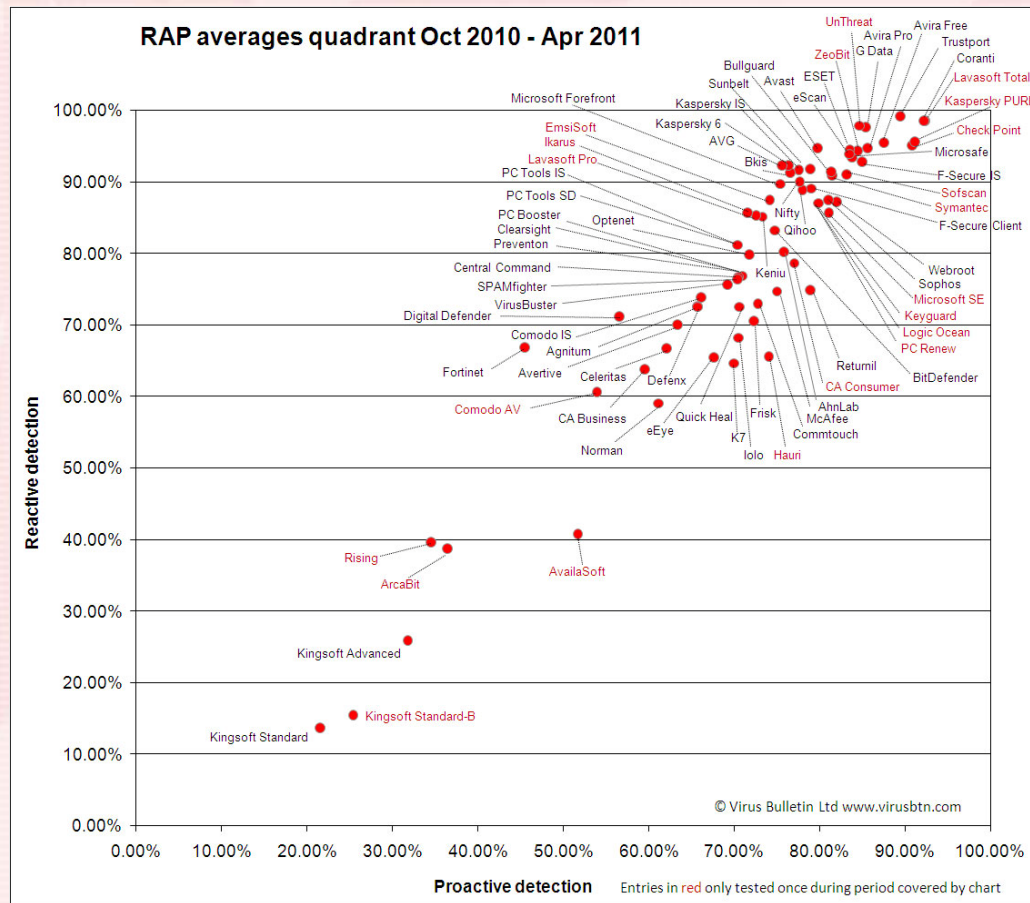


BLENDED THREATS

*...designed mostly for Cybercrime
and Cyberterrorism....*

What are the real stats for AVS?

- Visit <http://www.virusbtn.com>





Malware Root Cause - CVEs

- **Common Vulnerabilities and Exposures (CVEs)**
 1. Although there might be 9,000,000 signatures in your McAfee or Symantec anti-virus scanner database (and growing exponentially), there are only 46,000 CVEs. If you close just one CVE, for example, you can block more than 110,000 variants of the W32 malware.
 2. If you aren't visiting <http://nvd.nist.gov> to see what kind of exploitable holes you have in your network, cyber criminals CERTAINLY are...
 3. Everything with an IP address has a CVE, you need to figure out which ones are critical holes and how to patch, reconfigure and remove them—i.e. system hardening.

...and MALWARE LOVES TO EXPLOIT THESE HOLES...



Exponential Growth of New Malware!

Exponential Growth of More Intelligent Zero-Day Malware both for Cybercrime and Cyberwar.

- *Vulnerabilities (CVEs) are uncovered daily*
- *Software is JUST NOT SECURE!*
- *Professional “TIGER” teams are writing new malware*
- *Some of them do it for their local ‘mob’ boss*
- *Others do it for their Government’s defense department*
- *Either way, Stuxnet was only the beginning*
- *The wave has begun.*
- *There are over 30M samples of malware in AV-Test.org’s database growing at over 400,000 new samples per month.*
- *The problem is now Exponential.*



Traditional Countermeasures All Fail!

- **Anti-virus** = One to seven days BEHIND the current malware threat. Usually infected without knowing it.
- **Firewall** = Easily circumvented or used as part of an exploit because of their exploitable holes (CVEs)
- **Intrusion Detection System (IDS)** = Detects odd or mal traffic AFTER the infected system or hacker system has breached the gates.

Note: Both IPS or UTM Firewall both use similar technology for 'deeper packet inspection'



DECEMBER 2010 IPS GRADE IS A “D-”

NSS Labs Inc. tested 13 of the world's most powerful IPS products in December 2010. They caught 62% of the attacks, missing 38%.

While the NSS Labs test is revealing, most of the attacks don't come through the front door (the firewall or IPS) anyway, they come through the back door.



UTM Firewalls and IPS Exploits!

New Sophisticated UTM Firewall and IPS Exploits are being launched...

- These devices are running too many 'add-on' services.*
- All it takes is one running service to be exploitable.*
- If you can take control of the Firewall or IPS, you have hijacked the entire network.*
- It's easy to eavesdrop and steal data where all network traffic flows.*
- If you use a VM deployment firewall, it may be at risk of "hyperjacking" – Hijack the hypervisor and you own the firewall. Look for VM CVE's at <http://nvd.nist.gov>*



Microsoft Windows App Layer Holes

Increases in Microsoft Windows Application Layer Vulnerabilities Lead Towards Their Rapid Exploitation.

- ***MITRE'S OVAL Database is Growing Significantly***
- ***OVAL was designed to help you track and fix host-based vulnerabilities, mostly at the application layer.***
- ***There are 2645 new Windows XP Application holes in all major apps – Apple iTunes, Adobe Acrobat, Internet Explorer, Microsoft Word, etc. Windows 7 already has 1096 application layer vulnerability entries and growing...***
- ***Apps are growing in size, complexity and release cycle deployments – this means HOLES, HOLES and more HOLES to exploit.***
- ***Learn more at <http://oval.mitre.org>***



A New Paradigm in Proactive Defense

- **Understanding The Risk Formula**

$$R = T \times V \times A$$

(R)isk = (T)hreats x (V)ulnerabilities x (A)ssets

Threats = Cybercriminals, malware, malicious insiders

Vulnerabilities = Weaknesses that threats exploit

Assets = People, property, your network, devices, etc.



Proactive Defense Continued

- **Threats** need to be detected, deterred, defended against and defeated in real time or expect DOWNTIME.
- **Vulnerabilities** need to be detected, deterred, defended against and defeated (i.e. removed – system hardening, reconfiguration, patching, etc.) as quickly as possible or expect to be EXPLOITED.
- **Assets** need to be controlled – which ones gain access to your network/infrastructure and those that are trusted but weak or infected need to be quarantined in real time or expect MALWARE PROPAGATION.

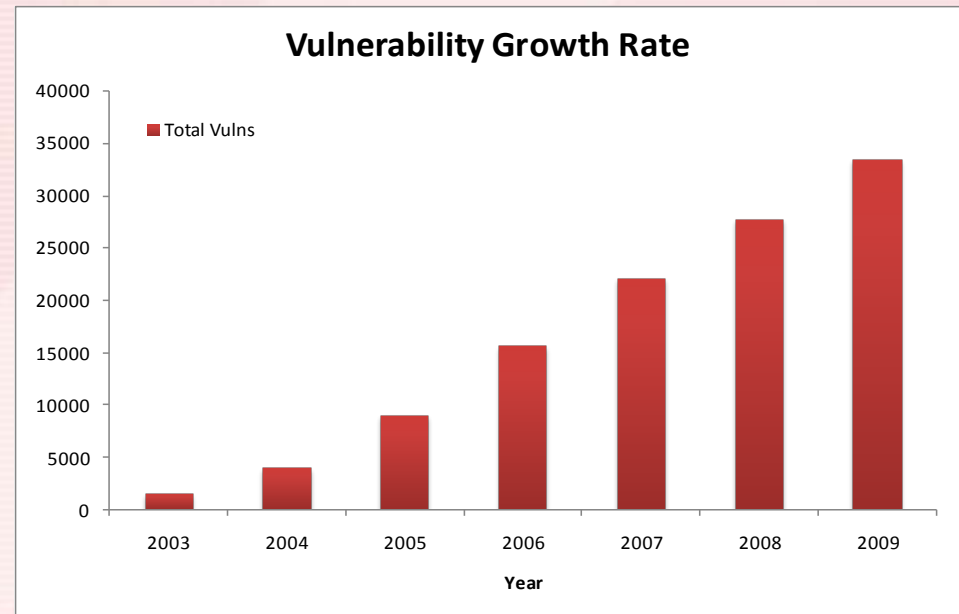


Fact: Everyone can be exploited!

All of our Systems have Holes! (CVEs)

According to the USCERT, SANS, FBI and MITRE, over 95% of security breaches are a direct result of exploiting a Common Vulnerability and Exposure (CVE®).

See: <http://nvd.nist.gov>



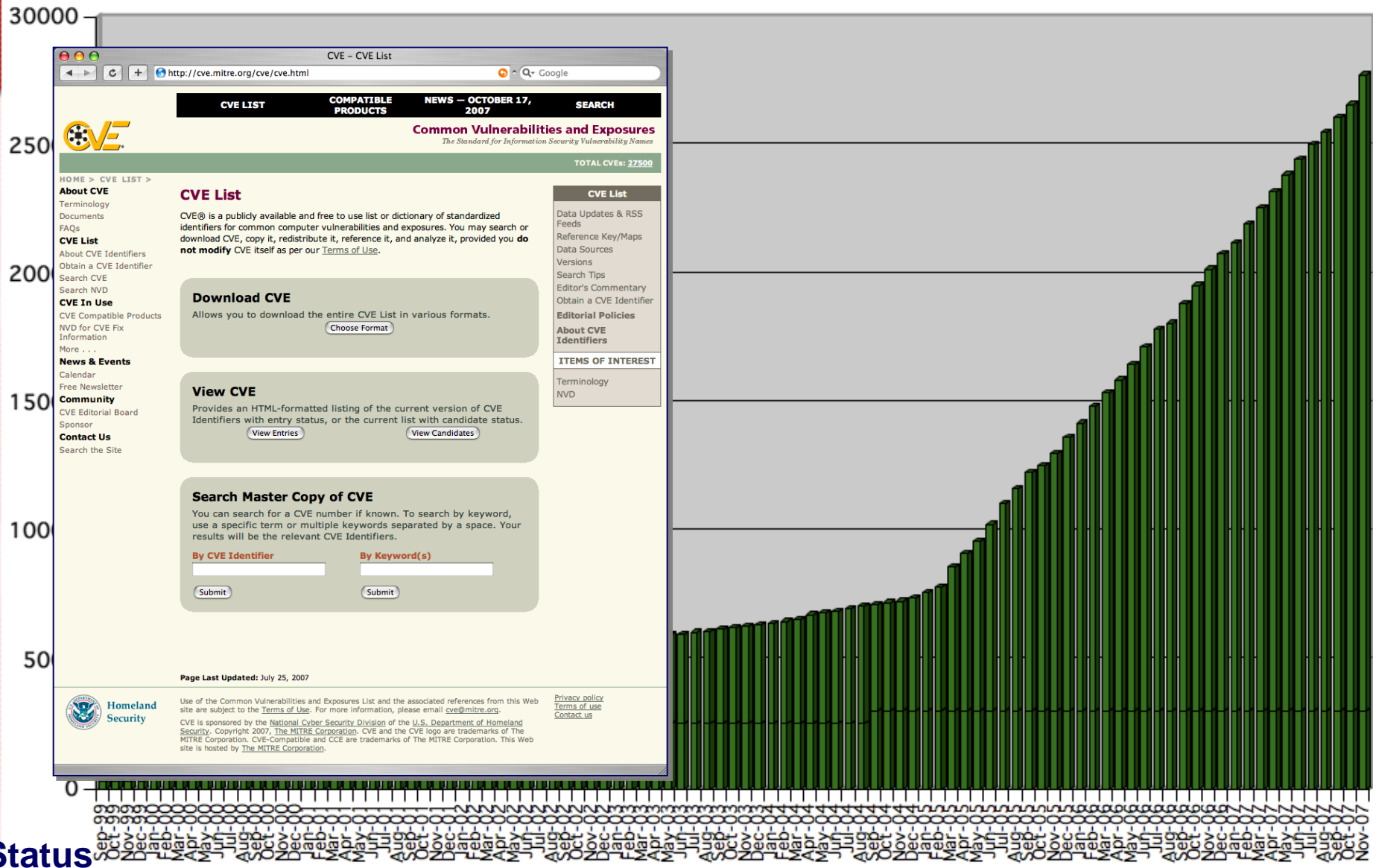
In addition, 80% of all successful attacks occur from the inside (malicious insider, rogue wireless, the 'cleaning company' tapping of your network with an unknown and untrusted laptop)

Common Vulnerabilities and Exposures (CVE)

- CVE: Enabling fast, accurate correlation of vulnerability information across the security industry
- Key tenets
 - one identifier for one vulnerability
 - dictionary of standardized descriptions for vulnerabilities and exposures
 - publicly accessible for review or download from the Internet
 - **international** scope
 - **industry participation** in open forum (editorial board)
 - **compatibility program** for products & services



CVE Growth

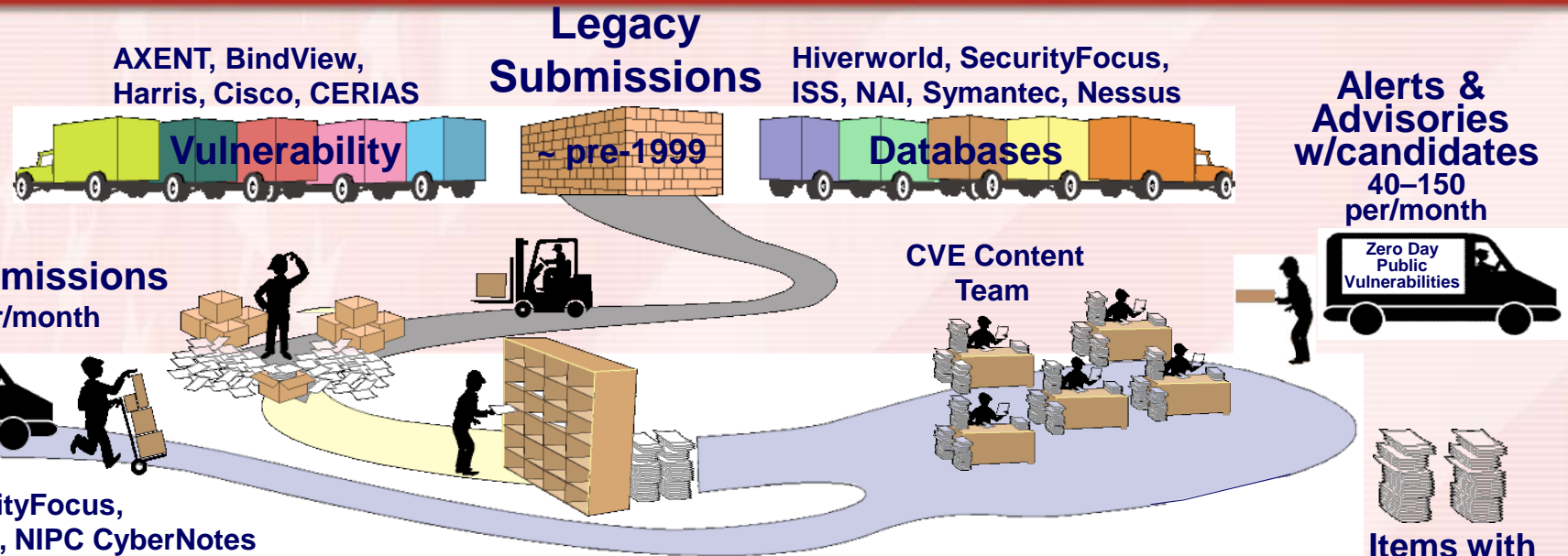


Status

+46,000 unique CVEs



Where the CVE Items Come From



CVE Editorial Board



Open Vulnerabilities and Assessment Language (OVAL.mitre.org)

- OVAL Language
 - express specific machine states
 - standardize the transfer of information
 - XML based defined by XML Schema
 - compatibility program for products & services
- OVAL Repository
 - promote open and publicly available content
 - central meeting place
- open community standard
 - to facilitate sharing
 - open up the details
 - utilize community expertise

XCCDF-OVAL Connection

XCCDF

<Rule id="RequireCTRL_ALT_DEL" >

<Title>

Interactive logon:
Require CTRL+ALT+DEL

<Reference> CCE-133

<Description>

Disabling the Ctrl+Alt+Del security
attention sequence can compromise ...

<Check>

oval:gov.nist.1:def:69

OVAL

<definition id="oval:gov.nist.1:def:69">

<metadata>

<title> Require CTRL_ALT_DEL

<reference> CCE-133

<criteria>

Windows family, Windows XP, SP2, 32 bit

HKLM\Software\Microsoft\Windows\
CurrentVersion\Policies\System\
DisableCAD = 0

[makingsecuritymeasurable.mitre.org]










Making Security Measurable

A Collection of Information Security Community Standardization Activities and Initiatives

Home | Current Collection | Feedback Requested

Measurable security pertains at a minimum to the following areas:

- Vulnerability Management
- Asset Security Assessment
- Configuration Guidance
- Malware Response
- Threat Analysis
- Intrusion Detection
- Asset Management
- Patch Management
- Incident Management

Enumerations	Languages	Repositories
 Common Vulnerabilities and Exposures (CVE®) - common vulnerability identifiers	 Open Vulnerability and Assessment Language (OVAL™) - standard for determining vulnerability and configuration issues	 OVAL Repository - community-developed OVAL Vulnerability, Compliance, Inventory, and Patch Definitions
 Common Weakness Enumeration (CWE™) - list of software weakness types	 Common Result Format (CRF™) - standardized assessment result format for conveying findings based on common names and naming schemes	National Vulnerability Database (NVD) - U.S. vulnerability database based on CVE that integrates all publicly available vulnerability resources and references
 Common Attack Pattern Enumeration and Classification (CAPEC™) - list of common attack patterns	Extensible Configuration Checklist Description Format (XCCDF) - specification language for uniform expression of security checklists, benchmarks, and other configuration guidance	NIST Security Content Automation Protocol (SCAP) - security content for automating technical control compliance activities, vulnerability checking, and security measurement
 Common Malware Enumeration (CME™) - common identifiers for viruses, worms, and other malicious code	Common Vulnerability Scoring System (CVSS) - open standard that conveys vulnerability severity and helps determine urgency and priority of response	Red Hat Repository - OVAL Patch Definitions corresponding to Red Hat Errata security advisories
 Common Configuration Enumeration (CCE™) - common security configuration identifiers	Common Announcement Interchange Format (CAIF) - XML-based format created to store and exchange security announcements in a normalized way	Center for Internet Security (CIS) Benchmarks - best-practice security configurations accepted for compliance with FISMA, the ISO standard, GLB, SOX, HIPAA, and FIRPA, and other regulatory requirements for information security
 Common Platform Enumeration (CPE™) - common platform identifiers	OMG Semantics of Business Vocabulary and Business Rules (SBVR) - language for interchange of business vocabularies and rules among organizations and software tools	DISA Security Technical Implementation Guides (STIGS) - U.S. Defense Information Systems Agency's (DISA) STIGS are configuration standards for DOD information assurance and information assurance-enabled devices and systems
SANS Top Twenty - SANS/FBI consensus list of the Twenty Most Critical Internet Security Vulnerabilities that uses CVE-IDs to identify the issues		
OWASP Top Ten - ten most critical Web application security flaws		
WASC Web Security Threat Classification - list of Web security threats		

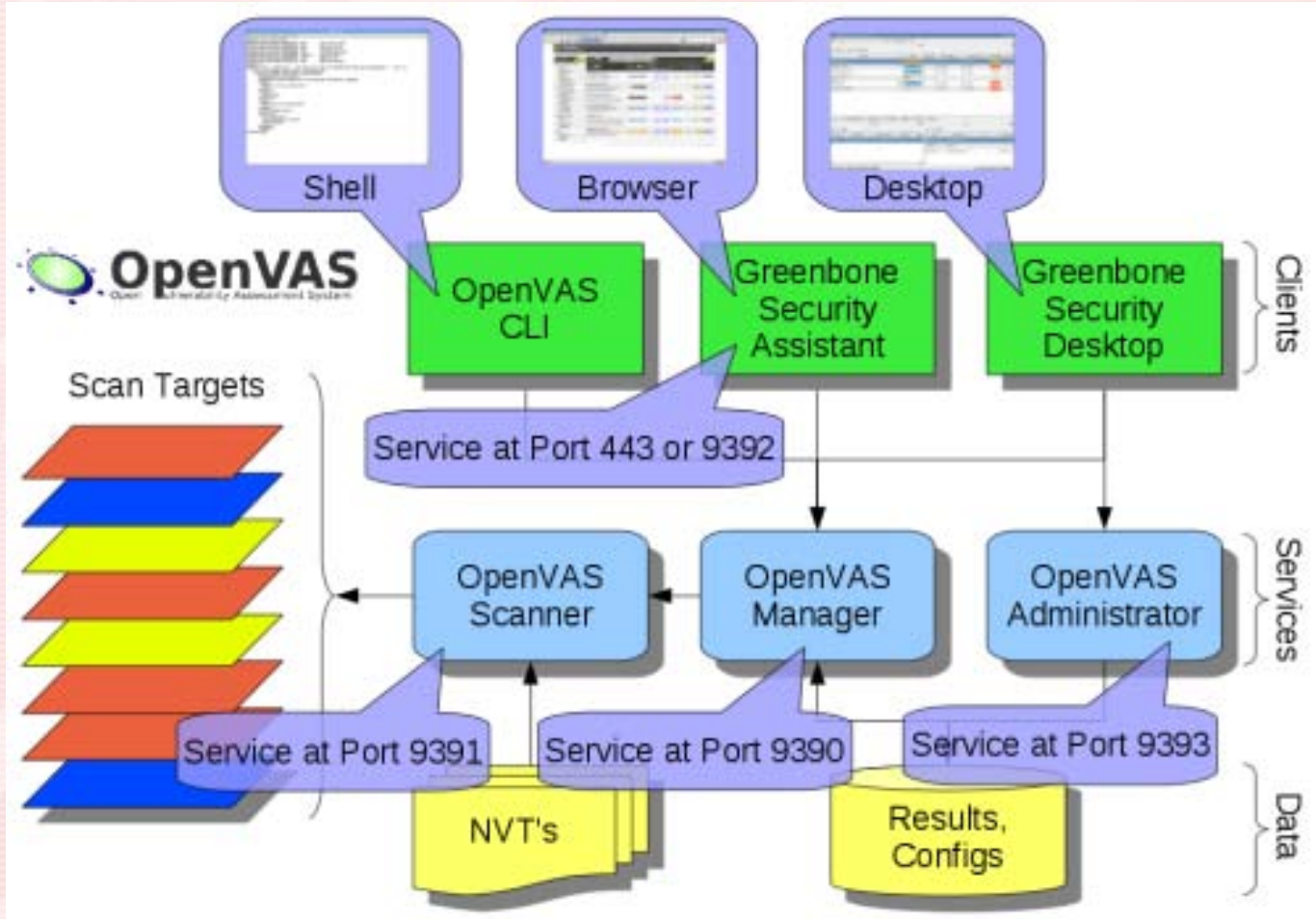
[View the current collection of organizations, activities, and initiatives.](#)

[Disclaimer](#)

This Web site is hosted by [The MITRE Corporation](#). © 2007 The MITRE Corporation. CVE is a registered trademark and the Making Security Measurable logo, CCE, CME, CWE, CPE, and OVAL are trademarks of The MITRE Corporation. All other trademarks are the property of their respective owners. Contact us: measurablesecurity@mitre.org

Page Last Updated: September 14, 2007

OpenVAS



Let's Play

- Let me show you:
 - HOW WOULD A HACKER EXPLOIT A CVE (DON'T DO THIS FOR REAL – IT'S ILLEGAL!!!)
 - [NVD.NIST.GOV](https://nvd.nist.gov) (CVE SEARCH ENGINE)
 - [NETCRAFT.COM](https://netcraft.com) (FINGERPRINT ENGINE)
 - [OVAL.MITRE.ORG](https://oval.mitre.org) (HOST-BASED CVEs)
 - [OPENVAS.ORG](https://openvas.org) (NETWORK-FACING CVEs)
 - HOW TO BUY SOME TIME WITH HIPS (WHILE YOU ARE FIXING YOUR CVEs)



BEST FREE CVE SCANNING TOOLS

- OpenVAS for tests across networks

<http://www.openvas.org>

- OVAL for host-based tests

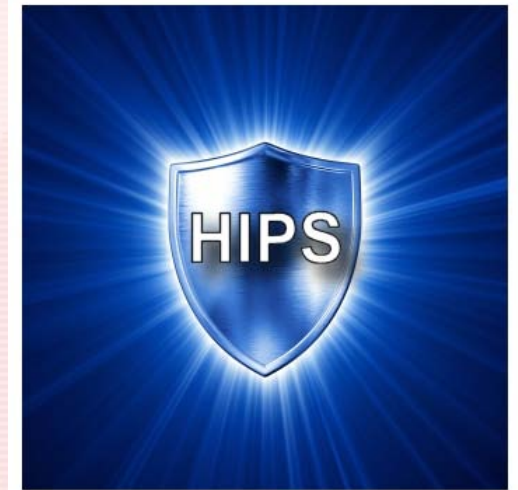
<http://oval.mitre.org>



Your First Line of Defense: HIPS

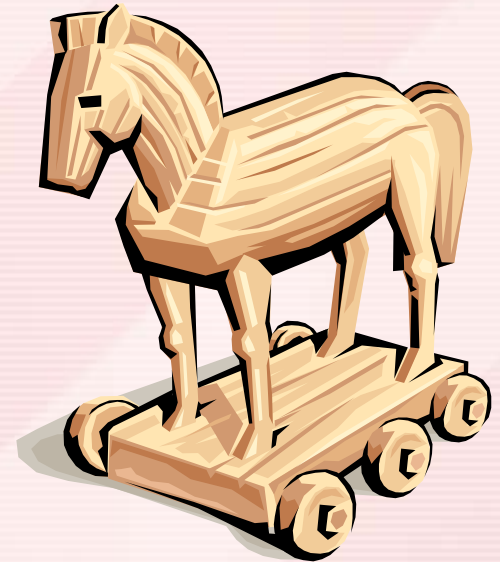
- **Host-based Intrusion Prevention System (HIPS)**

- **PREVX:**
<http://www.prevx.com/event>
- **THREATFIRE:**
<http://www.threatfire.com>
- **WINPATROL:**
<http://www.winpatrol.com>
- **COMODO FIREWALL:**
<http://www.comodo.com>



Thoughts for the Day...

- Find and fix your vulnerabilities...
- Document your security activities...be vigilant!
- Be preemptive, be proactive—get one step ahead of the next threat...





Hack in Paris

International IT Security Conference
June 14-17 2011



QUESTIONS?

Thank you.

Gary S. Miliefsky, FMDHS, CISSP®
NetClarity, Inc. <http://www.netclarity.net>

