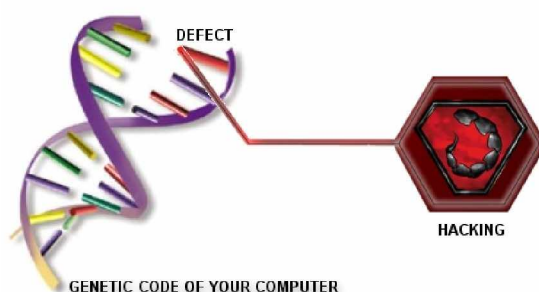


**PROTECTING AGAINST  
AGAINST HACKERS,  
VIRUSES AND WORMS**

**A CVE<sup>®</sup> WHITEPAPER**

November 17, 2005



A handwritten signature in black ink, appearing to read "Gary S. Miliefsky".

Gary S. Miliefsky, CISSP<sup>®</sup>

**NetClarity**

54 Middlesex Turnpike, Bld. C  
Bedford, MA 01730  
781-276-4555 or 877-677-3328  
[www.netclarity.net](http://www.netclarity.net)

The CVE Standard – Funded by the U.S. Department of Homeland Security and Operated by MITRE Corporation.

CVE and the CVE logo are registered trademarks of The MITRE Corporation. Use of the Common Vulnerabilities and Exposures List and the associated references from MITRE are subject to the Terms of Use. For more information, please visit <http://cve.mitre.org> or email [cve@mitre.org](mailto:cve@mitre.org)

# CONTENTS

THE DISCOVERY .....	3
HACKING IS EASY .....	5
THE METHODOLOGY .....	7
PROTECT AGAINST CVE EXPLOITERS .....	8
DETECT AND TRACK ASSETS.....	8
AUDIT YOUR NETWORK FOR CVES .....	8
LOCK THE DOORS AGAINST CVE EXPLOITS .....	8
CLEANUP YOUR CVES .....	8
CONCLUSION .....	9
CREDITS: .....	9

# THE DISCOVERY

After years of R&D, in early 2005, NetClarity uncovered a methodology to protect against hackers, viruses and worms. First, you need to understand the Defects in the genetic code of your computer and how hacking takes advantage of those Defects.

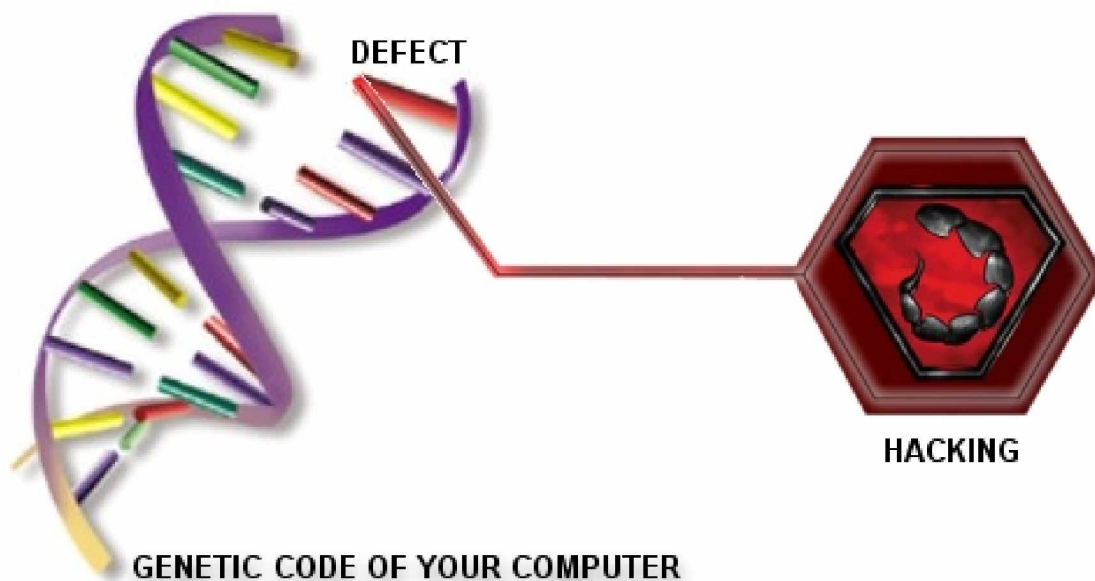


Figure 1: Genetic Code of your Computer, Defect Discovered, Successful Hacking (Exploit)

According to our research, every computer and every piece of networking equipment (VoIP telephones, Wireless Routers, Laptops, Desktops, Servers, Firewalls, SmartSwitches, etc.) has its own Genetic Code.

For example, the Genetic Code of your office computer might read as follows:

1. Ethernet (NIC) Card, Ethernet Driver – for Internet access
2. Bios – for hard drive, operating system (OS) and peripheral device access
3. CPU – the brain, with RAM, memory
4. Operating System – Windows, Macintosh, Linux, Novell or Unix, etc.
5. Device Drivers – loaded into memory and used to access your devices such as your monitor, floppy drive, CD-ROM, etc.
6. Services or Background Tasks – such as your printer queue, anti-virus scheduler, software updater, instant messenger listener, etc.
7. Applications – such as your favorite word processor or e-mail program or web browser.

These seven components make up the *Genetic Code* of your office computer. Within each component, there may reside a *Defect* that is exploitable by a Virus, Worm or *Hacker*. The Hacker might use this Defect to install a worm or backdoor on your computer, take control of your system, change or delete your files, remotely, over the internet or from within your internal network.

The number of Defects that has been uncovered in the genetic code of computer equipment has been growing exponentially. These Defects are also known as Vulnerabilities.

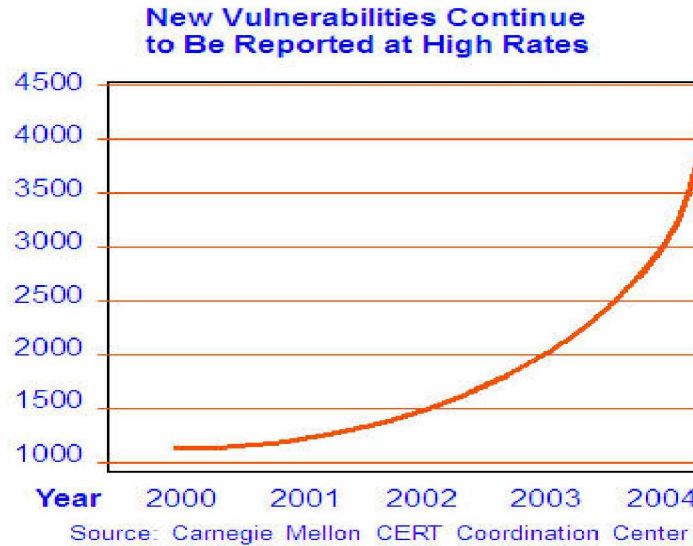


Figure 2: Genetic Defects Continue to be Discovered at High Rates

As a result of so many Defects, literally thousands, the volume of successful Hacker attacks against those Defects continue to rise dramatically.

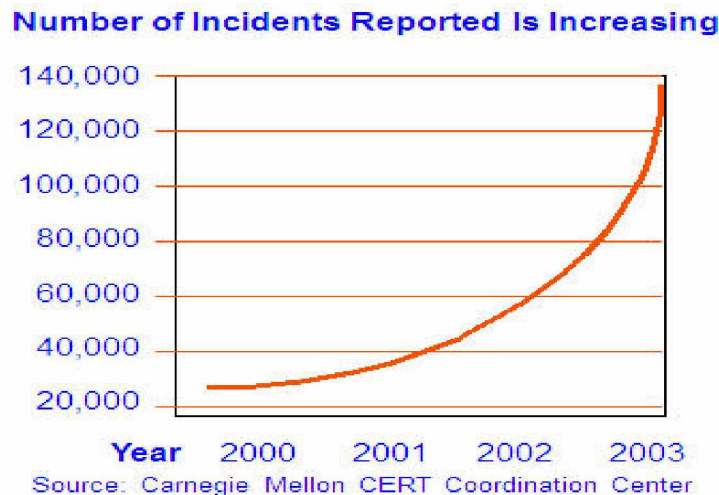


Figure 3: Hacking Attacks against Genetic Defects on the Rise

So Hackers write viruses, worms and other malicious computer code or 'bots' that attack the weaknesses at the heart of your computer – your genetic Defects. These Defects, known as Vulnerabilities are more accurately called CVE<sup>®</sup>s, which stands for **C**ommon **V**ulnerabilities and **E**xposures.

If you didn't know that CVEs are what allow Hackers to be so successful, you are not alone. Most people are unaware that CVEs, rather than viruses, are at the root of 95%

of all security breaches. Firewalls can't stop most CVE Exploiters. Anti-virus software can't get rid of CVEs. Anti-virus software only cleans up viruses, while doors and windows are still open to attack because of CVEs.

Hackers and their automated tools are CVE Exploiters – taking advantage of the Defects in your Computer's Genetic Code.

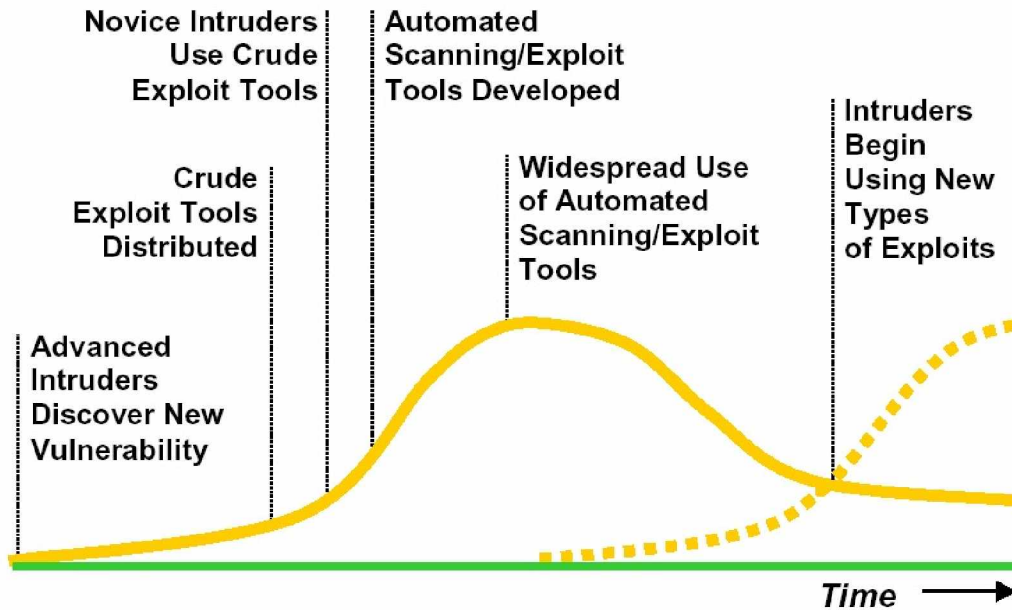


Figure 4. CVE Exploiters use the Window of Vulnerability

## HACKING IS EASY

There are thousands of free Hacker tools available freely online by visiting a search engine such as AltaVista, Google or Yahoo, typing in a few keywords and following the links. The amount of damage Hackers may cause depends on how far they or their tool goes and the CVEs they find and exploit. All Hackers and the automated tools they have created use the same methodology:

1. Footprint your servers, desktops and network infrastructure.
2. Scan for numbers of computers, open ports, services running.
3. Enumerate those servers and services they can find.
4. Penetrate those systems that have high-risk CVEs.
5. Escalate their privileges to become a super-user or administrator.
6. Pillage your information and customer records.
7. Get interactive including installing helper software to let them in later.
8. Expand influence by replacing trusted programs with backdoors.
9. Cleanup their tracks including firewall and server logs.

And if they want to disrupt your business, they will perform:

10. DoS (Denial of Service) attacks against you or others, using your resources.

Sometimes they install software known as Zombies, which are used as remotely controlled or preconfigured DoS attacking tools that use your resources against another target, such as your customers, partners or even an online bank.

How hard is it to Exploit your CVEs? Just look at the following steps a Hacker took at an online bank:

- The Hacker found an online bank web site running a version of Microsoft IIS (Web Server) that contained a genetic Defect.
- The Defect is in the printer service, which is turned on by default. By sending a simple message over the Internet, with too much data, the printer service crashes, allowing an attacker to gain root privileges and take remote control of the bank server.

You would think that the online bank would be more secure or could have ‘patched’ the problem. A patch is exactly that – it’s a Band-Aid that may or may not work. In fact, many patches open up new Vulnerabilities. Here are some other interesting Hacker attacks that caused embarrassment and billions of dollars in damages:

**Paris Hilton’s cell phone was hacked because of a CVE.** *How? Hackers used a CVE (Common Vulnerability and Exposure) to break into T-Mobile’s user website for Hilton’s Sidekick phone-computer and stole her personal data.*

**MyDoom takes advantage of a hole in your network that is a CVE** *(Common Vulnerability and Exposure). The worm looks for machines that have certain files installed and uses a particular port to communicate. Machines that have any CVEs are vulnerable to attack. Removing the worm alone is not enough to fix the problem. MyDoom can return to successfully attack those machines again and again, unless you remove the underlying Vulnerability.*

**Sasser is another intruder that takes advantage of a CVE.** *The truth is that Sasser uses a CVE that was around long before the worm was born.*

**You may never know your data has been hacked.** The only way to be sure your network is safe is to lock the doors—eliminate the Vulnerabilities—the CVEs – the weak spots – before the attackers strike.

*CVEs can be repaired.*

*With our discovery, through continuous detection and remediation, you can do for your computer and network equipment, what Science has not yet been able to do for humanity – you can remove your genetic Defects – your CVEs – from most and possibly all of your computers and networking equipment.*

*Quarantine & Repair of your CVEs is a methodology to protect against hackers, viruses and worms.*

Today’s networks are at critical risk. Not just because Hackers are out there, but also because in a mobile world, any device can pick up a virus or Trojan or have a Vulnerability that opens just enough of a window to your network that a Hacker can exploit it to gain access. Just one CVE® in your network and you may be in trouble.

# THE METHODOLOGY

**Repairing your CVEs is the litmus test by which all information security professionals will be judged against regulatory compliance** including GLBA, HIPAA, 21 CFR FDA 11, E-Sign and SOX-404 as relates to information assets.

CVE Management is the key to hardening your network assets and removing genetic Defects in your computer and networking equipment. Three types of solutions that claim to help you harden your assets are:

1. Configuration Management
2. Patch Management
3. Vulnerability Management

If you find a solution that helps automates this process for you, make sure it helps find and fix CVEs. If the solution you choose has not been vetted by MITRE, then it may not be compatible with the CVE standard. MITRE is funded by the U.S. Department of Homeland Security to manage this industry standard – the Code of Genetic Defects in all networking equipment and computers. Look for this logo to accompany the product or service in question – verify it at <http://cve.mitre.org>.



Every day there is a new CVE so keep an eye on <http://cve.mitre.org>. As you now know, this website is the homepage for helping you stop Hackers and harden your assets. Why? By knowing the CVEs, if you find a system with a CVE, then you can find a way to block an exploit that would impact this asset.

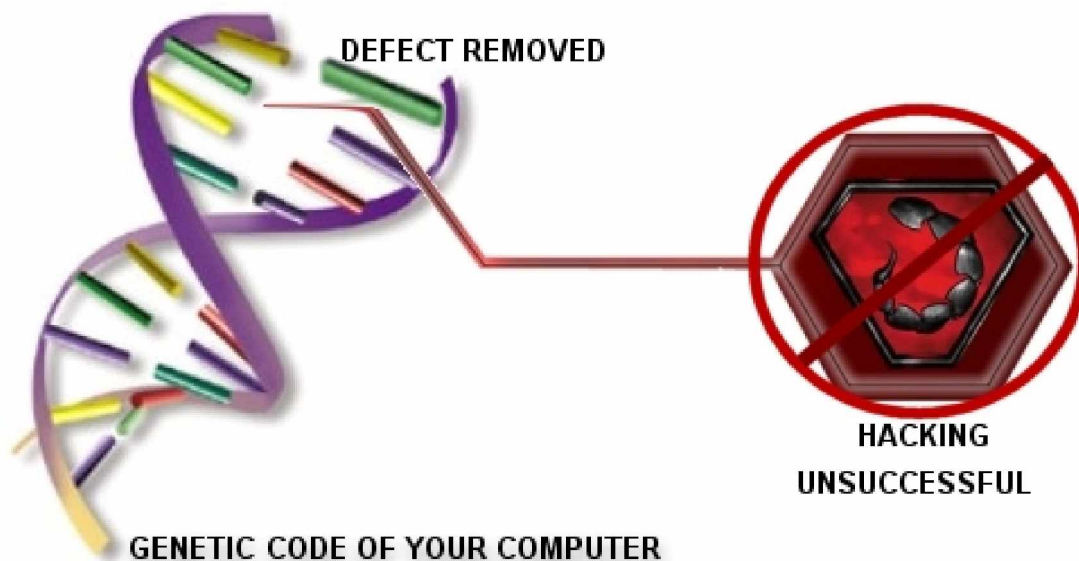


Figure 5. Removing Defects Is A Methodology To Protect Against Hackers, Viruses And Worms

## **PROTECT AGAINST CVE EXPLOITERS**

There are four key things you can do to protect yourself against CVE Exploiters:

- 1. Detect and Track Assets**
- 2. Audit your Network for CVEs**
- 3. Lock The Doors against CVE Exploits**
- 4. Cleanup your CVEs**

### ***DETECT AND TRACK ASSETS***

Do you have policies and systems in place to track all of your network-based assets? Do you allow laptops in and out of the office? Are laptops a company asset or a personal computer that can be used at home? Do you require firewall, antivirus, antispymware and patches to be installed on each host and up to date? What about wireless routers and ad-hoc wireless LANs – have you sniffed the airwaves and port connections to see if there are any new wireless devices or servers connected to your network? Answering these questions is critical in the protection of these assets against CVE Exploiters.

### ***AUDIT YOUR NETWORK FOR CVEs***

Find a tool you like. Google “Laptop Auditor” or “Security Auditor” or use similar keywords and you’ll find companies and products in this marketplace. Do an evaluation of open source versus commercial products. If you built your firewall from scratch – go for open source, otherwise find a company you can work with and trust. Make sure to pick a tool that doesn’t take any assets offline and scans and reports on CVEs.

### ***LOCK THE DOORS AGAINST CVE EXPLOITS***

Your firewall is your best countermeasure. Make sure to review logs – look for suspicious traffic. Also make sure you setup the VPN interface properly and know who’s using it and if they are coming in through a secure tunnel on an insecure or ‘sick’ computer. By reconfiguring your rules table around CVE Exploits, you might be one step ahead of the Hackers. For example, why not block ports for all inbound/outbound traffic that you don’t use – 445 was exploited by MSBlast and Sasser. Do you need to keep this port open at the firewall? Look at the computers that have CVEs – how long to fix and what port is it on? Update your rules table until it is fixed. Don’t trust all patches. Reinspect for same or new CVEs and the affected ports and services. Keep repeating this process, daily.

### ***CLEANUP YOUR CVEs***

Does your vendor offer patches? Did the patch fix the CVE? Yes, good. No? Then, why not shut off the service or feature that harbors the CVE – one quick configuration change and there won’t be a CVE to exploit. Some CVEs can be patched while others require intelligent reconfiguration. Cleanup your CVEs on the most important systems and highest risk of attack. Keep repeating this process, daily.

If you don’t have time to do this yourself, find a security appliance, service or consultant who will do it for you. It’s easy to find them, now that you know what to look for and where to look.

# CONCLUSION

It is crucial today to prevent Vulnerabilities across the enterprise and remove your Genetic Defects. Knowing what they are, where they are on your network, and how to remove them is more important than sniffing packets and listening for burglars.

Take this opportunity to harden your network assets by using the following formula:

1. Visit <http://cve.mitre.org>  
Some CVEs are currently Candidates (CANs) – keep an eye out on both CVEs and CANidate CVEs.

**Example CANDidate CVE:**

CAN-2003-0352 (under review)

Buffer overflow in a certain DCOM interface for RPC in Microsoft Windows NT 4.0, 2000, XP, and Server 2003 allows remote attackers to execute arbitrary code via a malformed message.

**What exploited this CVE?** Blaster, Msblast, LovSAN and the Nachi and Welchia worms causing massive downtime and financial losses.

2. Visit <http://nvd.nist.gov> – the U.S. National Vulnerability Database powered by CVE®
3. Keep an eye on the CVEs contained on the SANS/FBI top 20 list  
<http://www.sans.org/top20/>
4. Test for the latest CVEs on a daily basis
5. Report on your CVEs on a daily, weekly or monthly basis (DUE DILIGENCE)
6. Remove all CVEs that you possibly can (DUE CARE)
7. Block at the Firewall and at the SmartSwitch (INCREASE UPTIME)

Hackers, viruses and worms cause Billions in damages by using CVEs against us and the damages are growing annually (Source: CSO Magazine). How many CVEs do you have in your Network? Is your computer network taking you out of compliance? Knowing if you have any CVEs is the only way to find out and is considered Due Diligence. Removing critical CVEs is considered Due Care. Frequent and consistently scheduled security audits for CVEs and their removal is the only prudent thing to do as a proactive information security manager.

**CREDITS:**

Thanks to numerous NetClarity, Inc. customers for their time in reviewing this document and for offering their suggestions.

Many thanks to the MITRE CVE team, <http://cve.mitre.org>, for their work in creating and standardizing CVEs.

CVE® and the CVE logo are registered trademarks of The MITRE Corporation. Use of the Common Vulnerabilities and Exposures List and the associated references from MITRE are subject to the Terms of Use. For more information, please email [cve@mitre.org](mailto:cve@mitre.org)

CVE® is sponsored by U.S. Department of Homeland Security. For more information, please visit <http://www.us-cert.gov>

For information on NetClarity's patented CVE® Auditing system, email inquiries to: [sales@netclarity.net](mailto:sales@netclarity.net) or call us toll free at 877-677-3328.



Gary Miliefsky has over 20 years of experience as an entrepreneur, computer scientist and trained security professional. He has been CEO and/or CTO of 3 start-up ventures. At QuickBuy, Inc. he raised over \$10M in strategic and venture funding, personally recruited key team members, filed 6 patents, sold a \$0.5 million technology license deal to the president of Computer Associates, Inc. and drove revenues to over \$1M in the first year. At Netwave Technologies, he co-developed an Internet security technology that was licensed to N2H2, subsequently acquired by Secure Computing (NASDAQ:SCUR).

Mr. Miliefsky has also successfully brought new products and technologies to market for Fortune 500 companies, including a multi-million dollar executive information system for AIG, Lotus and DEC. At Wang Laboratories, Inc. he led a team to deliver in record time his new Internet fax invention for the Wang Open/image product line, deployed in over 40 countries in 14 languages and subsequently acquired by Kodak.

Mr. Miliefsky received his undergraduate degree from UMASS Lowell in Computer Science, and has subsequently earned certification as a CISSP®. He helped the White House develop their Internet Safety program for families and the recent National Strategy to Secure CyberSpace, advising the President's Critical Infrastructure Board. He is a Founding Member of the Department of Homeland Security and a member of MITRE's CVE/OVAL advisory team. He holds six e-commerce patents and has 3 network security patents pending. He has been written about twice in *Fortune magazine*, and has been seen and heard in *CIO magazine*, *Red Herring*, *Information Week*, *USA Today*, *the Washington Post*, *Washington Times*, *the New York Post*, *ZDNet*, *PCWeek* and *PCWeek Radio*, *Into Tomorrow* radio talk show, *the Boston Business Journal*, and *Mass High Tech*.

NetClarity | 54 Middlesex Turnpike | Bedford, MA U.S.A. | 01730 | [www.NetClarity.net](http://www.NetClarity.net) | [support@netclarity.net](mailto:support@netclarity.net)  
International (and U.S.) Telephone: 781-276-4555  
SKYPE Voice Over IP (8:30am until 5:30pm EDT): netclarity  
U.S. & Canada Toll Free: 877-677-3328  
Fax: 781-276-1569