

# Computer Viruses Have Grown Up

*Why CIOs Must Start Defending Against  
Endpoint Attacks*

*A Zellerent White Paper*

# Computer Viruses Have Grown Up

## *Why CIOs Must Start Defending Against Endpoint Attacks*

The first infectious computer virus appeared in 1982, ran under Apple DOS 3.3 and was transmitted by floppy disk. Called Elk Cloner, it stopped a game and then read a poem. Its author was a high school student.

25 years later, we wish all viruses were good for a laugh. But instead, they're financially destructive and deadly serious. Viruses have indeed grown up. Juvenile delinquents no longer, they today pack the muscle of organized crime (in fact, global organized crime syndicates may be their authors). Consider:

- The Melissa Virus, which shut down email systems across the globe
- The fast and furious Slammer worm, which brought down the Internet in 15 minutes
- The Bagle worm, which heralded the era of Botnets.

Unfortunately, many corporate executives still think they're dealing with teenagers instead of syndicates run by global Godfathers. The belief that viruses are mere annoyances that are globally broadcast is thus far more than a mistaken one; it is pernicious, because it results in companies' ignoring or dismissing strategic threats.

The good news is that there is a solution. A large part of it involves what we term peer-to-peer transmission. Our model suggests that enterprises divide threats into two distinct categories:

- Infrastructure Attacks. Those targeting the enterprise infrastructure, and which firewalls, anti-virus applications and other conventional Internet security applications are reasonably good at handling (provided the applications are chosen correctly, installed properly, and updated and monitored at an enterprise level).
- Endpoint Attacks. Those targeting the endpoints of the enterprise, such as browsers, workstations, email clients, PDAs, and the hardware and software that end users interact with. Endpoint Attacks are often transmitted on a peer-to-peer basis. One of the most damaging beliefs in the modern corporation is that by securing the perimeter, creating a moat as it were, the firm will be safe. What actually happens is that people get lulled into a false sense of security. In the meantime, inside your enterprise, right under your nose, it's carte blanche.

Only by acknowledging the legitimacy of Infrastructure and Endpoint Attacks can one begin to develop and deploy a security architecture that protects the corporation from all invaders: those intended to wreak havoc on anyone in their path and those intended specifically to attack your company and/or harvest your confidential information and intellectual property.

In this white paper, you'll learn:

- I. The true nature of the threat today
- II. Spurious threats that can lead you astray
- III. Why you need to focus attention on Endpoint Attacks
- IV. 10 Myths and Truths you must know

- V. Why installing anti-virus applications won't solve the problem
- VI. Why security matters when it comes to Sarbanes-Oxley and other IT compliance mandates
- VII. How to protect against threats against the infrastructure and the endpoints
- VIII. How to design and deploy commonsense defenses: An 8-Point Plan
- IX. How not to become a victim of Viral Myopia

## I. The Threat Today

### Legitimate Threats--Overview

We begin by examining the most prevalent threats to an enterprise's IT infrastructure today.

- **Malware.** So-called because its primary intent is malicious. Malware consists of code-based attacks that seek to steal confidential business information, trade secrets and intellectual property.
- **Ransomware.** Imagine finding your most valuable data encrypted and not having the key to unlock it. Unless, of course, you pay the kidnapper (usually based in a foreign country) a ransom.
- **Botnets.** When you read about yet another company's losing millions of credit card records and personal information to an unidentified third party, Botnets were probably involved. They can also be used to launch coordinated spamming, phishing and denial of service attacks.
- **Embedded Spyware and Trojan Horses.** It's reasonably well known that opening attachments from unsolicited email is not a good idea, lest you unleash a Trojan Horse. Even with this knowledge, it seems as though some employee is always doing it. But the problem gets worse, particularly because of web surfing. Today, spyware and Trojan Horses are spread when someone visits a compromised website, uses an RSS feed, or clicks on a hyperlink in an email or an instant message.

Today's threats don't announce themselves. Authors gloat after they have your money or information, rather than by flashing obscene messages on your monitor. So once a PC or notebook in your enterprise (or at an employee's home) has been infected, you no longer own it. Control has been ceded to a Botnet that could be transmitting personal information to the malware's author, or key-logging passwords or even packet sniffing (i.e., reading everything in and out of your network). Even if we ignore the damage wrought by such infections, the cost last year of simply replacing or repairing infected PCs neared \$4 billion.

### Legitimate Threats—Differentiating Viruses from Trojan Horses & Worms

Viruses, Trojan Horses and Worms are all forms of malware, but they are not the same. This section explains their differences.

#### Viruses

Computer viruses vary as much as real viruses. Some are like Ebola; they destroy data almost instantly, rendering the computer under attack useless in hours or even minutes.

Others are like HIV, unnoticeable at first, but then over long periods of time, causing irreparable, severe damage to a computer's files and disks. All viruses, benign and malignant, work the same way: they are applications consisting of executable code. The virus first infiltrates an existing application. Once it's accomplished that mission, it has effectively hijacked the application, just as a real virus hijacks a living cell in order to do its dirty work. The virus, in other words, acts as a parasite. If the virus doesn't have a real application to insert its "code DNA" into, it can use one of many other vectors, from boot sectors to email attachments. But once the virus is doing that dirty work, it can then reproduce itself at will, all while the user remains blissfully ignorant.

### **Trojan Horses**

Trojan Horses are named after the story told by Virgil in the *Aeneid*. The Achaeans, seeking victory in their 10-year-long war with the Trojans, retreated, but only after leaving a large wooden horse outside the fortresses of Troy. The Trojans, thinking the horse to be an offering from the defeated, then brought it inside their gates when, stealthily, in the middle of night, there emerged from within its hollow shell Achaean warriors, led by Odysseus. The warriors then staged a surprise attack on the Trojans, thus winning the war. Trojan Horses of the malware variety are not nearly as heroic, but they are often as crafty as their Greek counterpart. Often appearing as appealing attachments to emails (e.g., the infamous Anna Kournikova Trojan Horse, where the "attachment" was ostensibly a picture of the comely Ms. Kournikova), they are actually independent applications that run upon activation by the user (e.g., by clicking to see the picture of Ms. Kournikova). While only some Trojan Horses destroy data, many seek to shut down systems and servers by overwhelming them with pointless requests (such as sending the Kournikova email and attachment to everyone in one's address book). Always, the Trojan Horse requires a user to do something to activate it; it does not hijack an existing application as does a virus, but rather performs its own set of malefic actions once a user has set it in motion.

### **Worms**

Worms are applications that inhabit a netherworld between viruses and Trojan Horses. They are not viruses, because they are not parasites and do not attach themselves to a host application. They are not Trojan Horses because they do not require user activation; they can reproduce all by themselves. Unlike viruses or Trojan Horses, their targets are rarely individual computers, but instead the network itself. The worm's goal is to so overwhelm the network with traffic that everything grinds to a halt. Sometimes, however, a worm is spread via a Trojan Horse tactic, and since the definitions of some of these terms are not universally agreed upon, one can find numerous references on the Internet to both an Anna Kournikova Trojan and an Anna Kournikova worm.

## **II. Spurious Threats**

Living in the past can be dangerous. This is particularly true when it comes to Internet security. For example, large scale virus attacks used to be common. These viruses had no particular target: the goal was to cause the greatest amount of disruption in the shortest period of time to the greatest number of users. Today, most attacks have a particular target, use fewer hosts and occur over a shorter period of time. It's passé to crash remote hosts or deface websites and, when either does occur, you can be sure amateurs are behind it.

Now, here's the problem. While enterprise need firewalls, intrusion detection systems and antivirus software, they are fighting the last war. They simply aren't capable of thwarting today's sophisticated attacks. The reason is that today's ingenious attackers hijack protocols and ports through which firewalls permit traffic, they embed pernicious code in innocent messages that intrusion detection or content filtering systems won't pay heed to, and they do their devil's work without the fireworks. As for antivirus systems, the new attacks mutate on-the-fly, so they aren't recognized as viruses. In fact, most attacks are "zero day" ones: the same day security holes are found in applications like browsers, malicious code gets released. That's because, by day one, there will already be fixes to the holes, so the window of opportunity will have been closed.

The result of this dichotomy between past and present is that many CIOs are caught in a infrastructure-focused time warp, filtering inappropriate content, blocking dating sites and preventing misuse of company printers. In the meantime, the really bad malware has already infiltrated their enterprises to do its dirty work in silence.

### III. The New Kid On The Block: The Endpoint Attack

Today, the biggest threats to any enterprise are attacks against the endpoints. These are attacks launched against normal end users via email and through their browser. Even if 99% of the users don't bite, all it takes is one employee or contractor who does. These attacks redefine the importance of buttressing the weakest link and of never underestimating how weak that link can be.

What does this mean? Network administrators need to concentrate significantly more effort on preventing Endpoint Attacks than on building the next battle-hardened server. We almost have the latter issue won, yet our end users keep inviting ever-worsening spam and phishing attacks. But winning this battle first means not being mesmerized by myths. Next, we'll look at some of the most pervasive ones.

### IV. Ten Myths & Truths You Must Know

1. *Myth 1: Dedicated and dangerous human hackers are pervasive.*  
Truth: This one is simply not operative, unless your information is so precious that competitors or foreign governments deem you worthy of that attention. Otherwise, you may be hacked, but the hacker still won't be posing a major threat. Much, much more likely is inanimate malware, like viruses, worms, and Trojan horses.
2. *Myth<sup>1</sup>: Anti-virus software and firewalls are 100% effective.*  
Truth: Anti-virus software and firewalls are important elements for protecting your information. However, neither of these elements is guaranteed to protect you from an attack. Combining these technologies with good security habits is the best way to reduce your risk.
3. *Myth: Once software is installed on your computer, you do not have to worry about it anymore.*  
Truth: Vendors may release patches or updated versions of software to address

---

<sup>1</sup> Numbers 2, 3, 4, 5 and 6 of the "myths & truths" are from the US Government's Computer Emergency Readiness Team (content edited from <http://www.us-cert.gov/cas/tips/ST06-002.html>):

problems or fix vulnerabilities. You should install the patches as soon as possible; some software even offers the option to obtain updates automatically. Making sure that you have the latest virus definitions for your anti-virus software is especially important.

4. *Myth: There is nothing important on your machine, so you do not need to protect it.*  
Truth: Your opinion about what is important may differ from an attacker's. If you have personal or financial data on your computer, attackers may be able to collect it and use it for their own financial gain. Even if you do not store that kind of information on your computer, an attacker who can gain control of your computer may be able to use it in attacks against other people.
5. *Myth: Attackers only target people with money.*  
Truth: Anyone can become a victim of identity theft. Attackers seek the biggest reward for the least amount of effort, so they typically target databases that store information about many people. If your information happens to be in the database, it could be collected and used for malicious purposes.
6. *Myth: When computers slow down, it means that they are old and should be replaced.*  
Truth: It is possible that running newer or larger software programs on an older computer could lead to slow performance, but you may just need to replace or upgrade a particular component (memory, operating system, CD or DVD drive, etc.) Another possibility is that there are other processes or programs running in the background. If your computer has suddenly become slower, you may be experiencing a denial-of-service attack or have spyware on your machine.
7. *Myth: Viruses have magical properties that allow them to wreak havoc unlike anything else in the computer world.*  
Truth: Viruses are computer software – no more, no less. Software doesn't cause viruses; people do. Viruses are thus no more or less magical than word processing, spreadsheet, email or database software (and "magical" is not the word typically used to describe these types of applications). The only difference is intent and, in the case of viruses, it's bad. They can delete files, format hard drives, or scramble or encrypt data on them. But viruses cannot damage your CPU, physically harm your hard disk or RAM, or make your PC explode.
8. *Myth: Most virus warnings are true.*  
Truth: If you received a warning about a virus via email from someone with no ill intent, you still should probably not believe it. Typically, the person will have forwarded you a dire pronouncement that some email will erase your disk and/or destroy your computer. But unless the person is a security expert on retainer, chances are that it's a hoax and that the person who sent it to you just fell victim to it. But how can you be sure? If you receive such a message and become worried, there are online sites which you can immediately reference<sup>2</sup>. In addition, there's an even simpler solution. Search Yahoo! or Google for the supposed virus's name.

---

<sup>2</sup> In particular, look at any of these sites: <http://www.viruslist.com>, <http://hoaxbusters.ciac.org>, <http://www.symantec.com/avcenter/hoax.html>

Then look in your search results for a site run by a reputable antivirus company. If you can find multiple reputable sites that say the virus is a hoax, then it almost certainly is<sup>3</sup>.

9. *Myth: I am completely safe, because I have the most up-to-date firewall and malware protection.*

Truth: With infrastructure, you may very well be safe. But at the endpoints, it's a whole different story. Back in the days when computers were not portable, network-level protection would protect all the computers connected to that network. But today, portable notebooks have changed all that. Worms still arrive via email and peer-to-peer mechanisms. The primary culprit is the unprotected, unmanaged notebook. Infrastructure protections, such as router ACLs and firewalls, won't help. What's needed today is to lock down the endpoints, and to take measures to protect desktops, laptops and portable devices against malware. Correctly blocking the right ports not only protects the network, but also protects every local node against infections spread through the network.

10. *Myth: We've looked everywhere, protected against Infrastructure and Endpoint Attacks, and found nothing. Therefore, we're safe.*

Truth: Technologies like steganography enables messages to be hidden inside JPGs and other files. Except for the recipient, no one can even tell anything is amiss. No wonder steganography is a favorite of terrorists worldwide. Of course, it can also be used to steal company secrets and get them into the hands of competitors. But steganography requires tools, ones which have to be installed at the endpoints and, in particular, on an individual PC or laptop. Looking for steganographs won't help, but preventing or detecting steganographic tools can and does.

## V. Why Installing Anti-Virus Applications Won't Solve The Problem

Antivirus tools can do a lot. They can provide protect against viruses, worms and Trojan Horses. They can remove outdated antivirus and security applications and prevent users from changing settings. They can implement network worm blocking and, because of product bundling, often protect against firewall intrusions, spam, phishing and spyware.

But antivirus applications can't do it all. Most require "training" by the end user in order to know what to allow and what not to allow. The typical end user is not an IT expert. He is often playing roulette when he says "allow" or "disallow." In fact, it is entirely inappropriate to expect even an advanced user to understand the full implications of "allowing" a particular application to connect to a given server on the Internet through a specified port. And even if this hole is closed, these products will still be unable to prevent infections due to users' clicking on a malicious website. And these problems don't even take into account the entirely human factor. Suppose the responsible person, the one who is supposed to understand what to allow and disallow, is improperly trained or incompetent? Worse, what if that person is a malcontent or has specific malicious objectives?

---

<sup>3</sup> Why look for multiple sites? Because a malicious person could potentially get you to "phish" to an illegitimate site that looks real at first glance (e.g., [www.symantec.com](http://www.symantec.com)... – note the 2 "t's") and that says the virus is not dangerous.

## **VI. Why Security Matters When It Comes To Sarbanes-Oxley and Other IT Compliance Directives**

Does your company need to comply with Sarbanes-Oxley (SOX), the Health Insurance Portability & Accountability Act (HIPAA), 21CFR11 or other major Federal or state regulations, laws and standards? Are you aware that the applicable security standards are equally true for data being transmitted and for data that is stored (i.e., "at rest")? The fact is that having either infrastructure or endpoint security problems could expose you to major risks.

All major regulations and standards mandate that IT data be protected from viruses and other malware. Your failure to comply (even if such failure is not willful) could lead to very serious civil--and even criminal--legal consequences should any virus or malware compromise others' private data stored on your computer systems. At the endpoints, your largest risks are in the areas of unauthorized access to records and identity theft.

In terms of public relations, the consequences are equally dire. Even something not covered by SOX, HIPAA, or 21CFR11 could make national news and expose your company to worldwide ridicule. In contrast, deploying the right security procedures puts you in the position of being able to comment on why other companies should be doing what you already practice.

## **VII. How to Protect Your Infrastructure And Endpoints**

While proper protection starts with the best possible applications, those aren't enough. Zellerent offers the following guidelines (but note that if you have outsourced any applications, then you must ensure that your outsourcing provider has implemented the same protections and controls):

### **Infrastructure**

- Install firewalls to limit inbound and outbound traffic to allowed ports and protocols only.
- Implement intrusion detection/prevention to detect and block network based attacks in real time.
- Install a content filtering gateway for Web/IRC/IM-based malicious code, spam and phishing filtering, and antivirus applications to implement content filters that protect users from malicious web sites, and to filter messages (e.g., email, IMs, VoIP) for malicious code and against spam and phishing attacks.

### **Endpoints (Desktop/Laptop/PDA)**

- Harden your operating systems to securely configure systems in environments with the minimum level of required services.
- Install host-based antivirus/firewall/anti-malware to detect and prevent malicious code from being installed or executed and to ensure frequent scans and automatic updating that will stop damage in its tracks.
- Secure portable media interfaces (USB, Firewire, Bluetooth, etc.) to prevent hosts from being infected with viruses transmitted through portable media devices.

- Use log monitoring to detect unusual or abnormal system activity (which might be due to malicious code).
- Periodically scan for vulnerabilities to verify that all systems have been patched against known vulnerabilities and to detect malware infections.
- Continuously enforce security policies to ensure that corporate level security best practices are being implemented and adhered to. These policies must include user training.

## VIII. How To Design and Deploy Commonsense Defenses: An 8-Point Plan

- **Inventory and classify assets**  
First, you must know precisely what you need to protect. Don't forget to include all electronic media and assets, from cellular phones and Blackberries to notebook computers and removable storage media.
- **Identify who owns each asset and who requires access privileges to that asset**  
From a security point of view, every person must be viewed as a potential threat. This does not mean invoking conspiracy theories and building underground shelters. It simply means identifying, for each asset, every person who should or could have access to it, directly or indirectly.
- **Identify your existing information architecture**  
Once you know what your information assets are and who can access them, you will want to see how these assets fit into the framework of your enterprise and network architecture. In order to do this, you must first specify the precise nature of that architecture.
- **Conduct a vulnerability assessment: identify your defenses, weaknesses and points of failure**  
To plug holes in your architecture, you must understand where you are most vulnerable and what those vulnerabilities are. This means identifying how each node in your architecture (and each asset class associated with a given node) is presently defended and then analyzing how and where that defense could fail. To protect against infiltration, you must understand fully the points and methods of infiltration.
- **Identify potential threats: who or what could be infiltrating your organization**  
Having identified how your enterprise's security can be compromised, you must next determine who or what is likely to be doing the actual infiltrating. You must know the nature of your enemies in order to confound and defeat them.
- **Conduct a risk assessment and formulate a remediation strategy**  
By this point, you should understand where your architecture is weak, how those weaknesses could be exploited and who the exploiters are likely to be. This knowledge enables you to remediate the architecture to address these weaknesses. Be careful to consider not just current infiltrations, but also the potential nature of future ones. An architecture designed for today will be obsolete by the time you have implemented it. In an ideal scenario, design your architecture to support your security requirements for at least a year after you have finished implementation.
- **Establish an ongoing monitoring program to prevent unauthorized access and to detect all unauthorized attempts at access**  
Never assume that everything you have done will work. Instead, be on guard and institute a program of continuous monitoring. Ideally, you will discover that your system works perfectly. But if it does not, or if a "mad genius" develops a new method of infiltration, you will be able either to observe and recognize the attempted

infiltration or, in the worst case, to see the evidence that something bad has occurred, which will enable you to investigate it. You should use a combination of signature-based and anomaly detection techniques to identify such intrusions.

- **Be prepared for even more sophisticated Endpoint Attacks based on social engineering<sup>4</sup> or new technology**

Social engineering is “a term used among [malicious hackers—i.e., ‘crackers’] for cracking techniques that rely on weaknesses in [human beings] rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a mark who has the required information and posing as a field service tech or a fellow employee with an urgent access problem.” In the context of this white paper, consider a malicious internal user who creates malware and then posts an apparently innocuous message on the company's internal blog or classified bulletin board. Or consider an outside user who submits a fake job application with an infected or malware-based Word document. The advent of user defined/controlled applications (e.g., Web 2.0 apps) means that malware and phishing techniques will continue to evolve. Second, when deploying new technologies, such as RFID, use these steps as a guide for evaluating the pros and cons of deployment. Keep in mind that, when it comes to technology, malicious users demonstrate greater creativity than technology architects or business users.

## IX. Conclusion: Don't Be A Victim of Viral Myopia

In 1960, Theodore Levitt wrote an article for the *Harvard Business Review*. Entitled “Marketing Myopia,” it told the early 20<sup>th</sup>-century story of how the railroads, when faced with competition from the trucking industry, decided they were in the railroad industry. The trucking companies thought differently and realized they were in the transportation industry. The myopic railroads never again regained their dominance and, to this day, trucking is the leading means of moving freight across the country. “Marketing Myopia” also became the most popular article ever published in the *Review*.

Now, in the early 21<sup>st</sup> century, many enterprises are suffering from Viral Myopia. They believe that, by defending their enterprise against viruses, Trojan Horses and worms, they are protecting their security. But actually, they are only protecting them from Infrastructure Attacks. On the other hand, other firms believe that they are not fighting viruses, but rather strategic, ever-evolving threats to their public reputation and intellectual property.

While the first set of firms will continue to exist, their ultimate fate will be that of the railroads. But those who understand the long-term competitive advantage of protecting themselves against Endpoint Attacks will have a far different future, one with a greater market share and a superior reputation.

---

<sup>4</sup> “social engineering.” *The Free On-line Dictionary of Computing*. Denis Howe. 20 Mar. 2007. <[Dictionary.com http://dictionary.reference.com/browse/social\\_engineering](http://dictionary.reference.com/browse/social_engineering)>

## About the Authors:

**Roby Jacob** is the CEO of Zellerent and has over 20 years of international IT leadership, project management and engineering experience gained through working with organizations and clients that include IBM's prestigious Thomas J. Watson Research Center, Unisys, Olivetti and Dialogic. His technical expertise includes software design and development, networking, network and systems management, protocol development and relational databases. He holds Master's and Bachelor's degrees in electrical engineering. He may be contacted at [roby@zellerent.com](mailto:roby@zellerent.com).

**Kalyan Dishingia**, CISA, CISSP, is the Vice President of Professional Services and a Principal Consultant for Zellerent. He has directed security and compliance engagements with organizations such as ING, Columbus Regional Hospital, Toyota Financial Services, and Fidelity. A trained ISO17799 Lead Auditor, he was also the Delivery Manager for the North American eSecurity Practice of an international IT services leader. He may be contacted at [kalyan@zellerent.com](mailto:kalyan@zellerent.com).

## About Zellerent:

Zellerent was formed by a team of seasoned industry executives whose combined experience spans several continents, multiple Fortune 500 companies and hundreds of successful engagements over two decades. Zellerent offers Business-Driven consulting expertise in the areas of IT Compliance, IT Security and IT Risk Management. Our practices include Regulatory Compliance (SOX, HIPAA, 21CFR11), Standards Compliance (ISO 27001, PCI DSS/VISA CISP), Security Deployments and Security Monitoring.

Zellerent's Business-Driven Compliance™ practice first assesses where you stand. Having identified the gaps between your current compliance status and your compliance and business imperatives, *remediation* can help you close that gap. With that problem solved, the solution, its associated controls and the in-compliance status need to be *documented*. Nevertheless, compliance that works today will not necessarily work tomorrow. *Monitoring* ensures that you will be prepared to address new regulations as they are introduced. Finally, *audit readiness* exercises give you a "dry run" before the auditors come calling.

Zellerent's Business-Driven Security™ practice *audits and assesses* the internal and external security threats to your organization. Next, armed with the proper requirements, we create an optimal security *architecture* for your enterprise, select the appropriate applications, and deploy your controls across it. As part of this effort, we also provide *awareness training* to ensure that your employees and stakeholders understand their responsibilities. Finally, we recognize that security threats change constantly, so we continuously *monitor* your deployed applications and controls to ensure they function as intended.

Zellerent is strictly vendor agnostic, identifying and deploying scalable best-of-breed solutions regardless of their source (public domain, 3rd party vendors, custom implementations).

**Zellerent Inc.**

39355 California St., Suite 309  
Fremont, CA 94538

510-742-7400

[www.zellerent.com](http://www.zellerent.com)

[security@zellerent.com](mailto:security@zellerent.com)

*Copyright ©2007 Zellerent Inc. All rights reserved. Reproduction or transmission without this notice is expressly prohibited. Zellerent, Business-Driven Compliance and Business-Driven Security are trademarks of Zellerent Inc. All other trademarks are the properties of their respective companies.*