The Emergence of Web-based “Super Attacks”
and ZoneAlarm ForceField’s Virtual web Surfing Solution

By Jordy Berson,
ZoneAlarm Group Product Manager
Introduction

The dominant type of cyber attack consumers face today combines the most effective strategies and characteristics of historical attacks to form a “Super Attack.” This Super Attack is more difficult to stop and more serious in its consequences than previous attacks. It is all of the following:

- Often web-, not PC-, based
- Financially motivated
- Silent
- Socially engineered
- Viral
- Rapidly morphing

This paper discusses the emergence and character of these modern web-based Super Attacks on consumers and the reasons that these attacks are dominant today.

It then discusses how traditional security is mostly ineffective against such attacks because it:

- Focuses on protecting the PC, not the user. Your PC may be protected, but what good is that if you have just accidentally given your username and password to a phishing site?
- Focuses on the PC, not the web. Since the web browser has become the major path for modern attacks, more attention needs to be devoted to browser security.
- Relies too heavily on signature lists. There is too much malware and too many dangerous sites being created too quickly to possibly track.
- Relies too heavily on removing malicious software instead of blocking it. When just one web page can silently make over 1,000 registry changes and download hundreds of executables, you can’t rely on antivirus to detect and remove these attacks. You must stop the attacks before they can infect your operating system.
- Is too heavy and disruptive to the user. If security requires the user to behave differently, or frequently interrupts the user, or generally gets in the way, the user will just not use it.

Finally, the paper discusses Check Point’s consumer solution to these web-based Super Attacks: ZoneAlarm® ForceField™.

Problem Statement

Hackers are waging war against consumers to exploit their web surfing, steal their data, and target their PCs. With every move a consumer makes, hackers are uncomfortably close behind and doing everything they can to exploit even the slightest misstep.

Today, consumers are using the Internet more than ever before, and in dramatically different ways than they did just a couple years ago. Here are a few examples:

> More people of all ages are surfing the web. Home broadband penetration rose 40% between early 2005 and early 2006, according to a survey conducted by the Pew Internet & American Life Project.¹ Another Pew survey revealed that 73% of American adults go online to surf the web or use email.² 93% of teens are online (21+ million teens) according to a Pew survey.³

> E-commerce transactions have become more commonplace. Approximately eight in ten...
Americans use the Internet to conduct online financial transactions, including banking, stock trading, and filing taxes, according to the NCSA Online Fraud Report (May 2006), sponsored by the National Cyber Security Alliance.

Web-based applications are on the rise, including office productivity software, Voice-over-Internet Protocol, and video conferencing. Companies are bringing more web-based services to market than ever before. Yet generally, the resultant security implications to the consumer of this rapid growth are not being adequately addressed. As consumers embrace the new ease and functionality of the Internet, they often do so without awareness of the potential threats. Furthermore, up to this point, most security companies have not provided consumers with dedicated protection against web-based threats. These conditions create ripe opportunity for hackers, who’ve found their own ways to embrace the web platform. As Ed Skoudis, Senior Security Analyst for the SANS Institute, proclaimed, “Unfortunately, this rush to the convenience and lower cost of web-based transactions has brought with it massive vulnerabilities.”

The following is a small sampling of recent incidents in which criminal hackers used the Internet as a platform to distribute their wares:

> In August 2007, researchers discovered a Trojan that was being delivered most often via phishing attack. The Trojan captured the identities of hundreds of thousands of people from job sites including Monster.com.

> In April 2007, it was discovered that anyone who Googled the term “betterbusinessbureau” saw a sponsored link to “www.bbb.org.” Though that site is legitimate, a thief had purchased the sponsored link. Anyone who clicked on it was taken to a server in Russia, which captured the sensitive data PC users typed on subsequent webpage forms they visited.

> A security flaw on eBay in April 2007 enabled a scam in which consumers were unknowingly redirected to a spoofed eBay site and tricked into providing their personal information.

> The websites of the 2007 Super Bowl hosts, the Miami Dolphins, and Dolphin Stadium were hacked in January 2007. The sites were used for at least a week to infect visiting PCs with a password-stealing program.

> In early December 2006, hackers compromised the MySpace.com social networking site and infected hundreds of user profiles with a worm. The malicious code exploited a known vulnerability to replace legitimate links on user profiles with links to a phishing site, where victims were asked to submit their user name and password. What’s more, the worm embedded infected video within user profiles.

> Last year, an online banner ad on MySpace.com and other sites exploited a security flaw in non-patched versions of Windows to install adware, keystroke loggers and other malware for at least seven months. Over one million users were affected.

> In 2006, approximately 109 million U.S. adults received phishing emails, up from 57 million in 2004, according to research firm Gartner. The average financial loss per victim grew from $257 in 2004 to $1,244 in 2006.

The Evolution of Hacking

Since the advent of the Internet, hacking has evolved from the attention-grabbing viruses of nearly a decade ago to the more covert and dangerous affair it is today. The result: consumers, businesses and governments face more daunting online threats today than ever before and they are often less equipped to handle those threats.

A Drive for Glory

A decade ago, hacking was generally characterized by a drive for glory, not financial motivation. Though sophisticated Trojan and other attack technology was around, it was rarely deployed – especially not for the financial gain for which such technology is used today. Email viruses such as the “I Love You” and “Melissa” were the norm, and they were widely reported in the press. This type of hacking had three key properties:

a) Threats were noticeable. If you were hit, you generally knew it.

b) Threats were widespread and viral. Millions of people fell victim to a single attack.

c) Financial motivation wasn’t yet common. So though attacks were
expensive for industry, consumers usually escaped without serious financial consequences such as identity theft.

To react to these threats, consumers, small businesses and corporations adopted security applications such as anti-virus signature solutions in response. The proactive realized the need for firewalls. And still others remained under-protected or not protected at all.

A Drive for Profit

Around 2001, a new era in hacker motivation was born — hacking for profit. This largely came about through the culmination of these things: first, the Internet had reached a critical mass in terms of the number of people online and the number of people making financial transactions online. This made individual home PCs attractive targets in the same way that corporations were already attractive targets.

Second, anonymous money transfers became not only possible but downright easy through services like PayPal. For these and other reasons, criminals awoke to the relative ease of committing crime on everyday people, through the Internet, using available and emerging hacking technologies. Thus the for-profit era was born, and organized crime began hiring hackers and utilizing hacking tactics to augment or even take the place of higher risk and higher cost traditional tactics. As their profit increased, so too did the motivation. Hacking for a profit became lucrative and blended threats became the norm. Blended threats combine: viruses, Trojans, worms, file, program, and operating system exploits all in a single attack. Consequently, the character of hacking shifted. Various types of spyware ruled the day, ranging from benign adware to dangerous key loggers and root kits. This type of hacking created a dramatic change in the three key properties:

a) Threats were much less noticeable because they were designed to be silent on the victim PC. A loss of PC performance or stability was often the only noticeable result.

b) Threats were targeted and sent in small batches to avoid detection. No longer were there major headlines accompanying each threat.

c) Consequences were serious and included personal data loss/identity theft as well as the silent takeover of individual PCs to create botnets — thousands of computers that can be controlled at once to launch large-scale attacks.

The damage from these attacks was severe and ranged from individual identity theft to systematic large-scale attacks on people and institutions. PC performance was also a major casualty. Users quickly responded to visible computer slow-downs and instability by installing signature-based anti-spyware. The more savvy users again reached for more proactive security, available this time from just a few solutions, such as the ZoneAlarm Operating System Firewall™.

Today: A Super Attack

The motivation for today’s hacking remains primarily financial. And the targeted silent attacks continue. But two important changes have conspired to make today’s attacks the most threatening yet.

First, through increased use of web-based attacks such as drive-by-downloads, PHP and AJAX exploits, threats have taken on all of the worst characteristics of the recent past. They remain financially motivated, extremely damaging, and relatively silent and unnoticeable. But like earlier threats, they are once again viral and widely distributed.

Second, many consumers assume they already have sufficient Internet security and remain unprotected. Regardless, most consumers are unaware that web sites are more susceptible to hacking than ever before; thus consumers haven’t reached out for appropriate protection. This fact itself is perhaps the most serious threat of all. To make matters worse, most software companies haven’t yet provided the appropriate protection against today’s web-based threats.

In summary, today’s threat environment has these characteristics:

a) Threats are even less noticeable than before because not only are they designed to be silent, they may no longer cause the loss of PC performance or instability that used to make consumers aware of the threats on their PC.

b) PC-based threats are still targeted and sent in small batches to avoid detection. But web-based threats are often massively deployed and viral, like the first wave of virus-based hacking.

c) Consequences are just as serious as before and include personal data loss/identity theft as well as the silent takeover of individual PCs to create botnets.

d) Consumers are complacent about threats on this new web platform; hackers have refined their social engineering and technology; and most security companies haven’t yet created the new layers of security necessary to fend off these new attacks.

Previous Options

PC-based security remains critical today but is no longer enough to combat the new web-based Super Attacks. Each type of solution falls short in at least one important way, as we’ll see here.

Signature Solutions

This category of solutions includes PC-based forms of security such as antivirus, anti-spyware and signature-based intrusion protection systems.

As we discussed earlier, signature solutions had difficulty keeping up with attacks a decade ago; this was before modern automated, morphing and small-batch custom attacks were available. In the face of such robust, modern attackware, it is no wonder that experts and analysts have written hundreds of
articles concluding the decline and death of antivirus.14

The problem is simple: since antivirus software reacted too late for the “Morris” worm in 1998, “Melissa” in 1999, and “I Love You” in 2000 – all of which were mass-mailed, relatively low-tech (slowly morphing) viruses – how can antivirus (and its cousins anti-spyware, IDS and similar) keep up with today’s viruses and worms that are blended, and more advanced? Indeed, they cannot. As we’ve seen with more recent threats that come out in small batches (thousands, not millions), they constantly morph, change their signature on every PC they hit, and stay hidden instead of drawing attention to themselves.

While antivirus, anti-spyware and similar security solutions are useful for “cleanup duty” in the aftermath of an attack, they are certainly ineffective as a defense for Super Attacks.

Firewalls
Firewalls shine where signatures don’t: they are effective against zero-hour, morphing, and targeted attacks. This is because they follow a simple and elegant rule: do not allow anything onto the PC unless the user specifically allows it.

This “reject all unless known good” rule is in direct opposition to the signature rule of “allow all except known bad.” It is easy to see why firewalls are more effective than signature solutions at preventing threats and protecting PCs.

However, there are a couple of downsides to firewalls. First, they allow user-solicited traffic on HTTP port 80, the web surfing port. When the user initiates web surfing, the firewall acts as a wide-open highway that brings traffic straight onto the PC. In fact, most studies show that spyware and other malware exists on over 80% of PCs running firewalls.15

Second, firewalls are focused on protecting users’ computers, not users’ behavior. They do little to prevent direct online contact with malware. What good does it do for the firewall to filter traffic to the PC if the user goes online and encounters a web site with a drive-by-download or a phishing attack?

Finally, firewalls tend to be rather heavy and ungainly and can interfere with computer usage, either by slowing computer performance or interrupting the user with questions. Though today’s firewalls do try to address both issues, the fact remains that firewalls — while a critical security layer — are not the only layer needed today.

Web “Transaction” Security
In the face of modern web attacks, new signature-based security solutions have emerged that try to protect users online. These new transaction security products use signatures of known bad websites, including phishing sites and spyware distribution sites. Some also contain signatures of malicious website behaviors; thus, they are able to identify and prevent users from visiting websites at a more general level and keep a more secure environment than they could otherwise.

As in the past, while these signature solutions are the first response to the new attack types, they are not the most effective. Though they are excellent as partial solutions, they are no match for the threat environment described earlier wherein armies of hackers design dynamic, morphing threats that get past signature systems. Just as today’s viruses can bypass antivirus systems, modern web attacks evade these signature-based web transaction security products.

NATs (New Advanced Technologies)
There are several technologies that have emerged to fight web-based Super Attacks without the use of signatures. These can be classified in a few ways:

1) Manual virtualization systems: these systems virtualize all or a part of the host computer, and require that all changes from the Internet to the PC take place in the virtualized system. In this way, nothing harmful can transfer from the Internet to the PC. While this seems like an elegant solution, it requires users to maintain both a virtual machine/file system and an actual one, and make ongoing decisions about each – something that an average user is unwilling or unable to do. Indeed, no company has yet been able to successfully sell such a system to a non-technical consumer.

2) Method-blocking systems: this technology focuses on one or more known browser vulnerabilities that allow hackers to target users with malicious code. For example, Internet Explorer natively allows cross-site scripting. This feature presents a vulnerability that enables a hacker to inject malicious code into other people’s webpages. A method-blocking system actually interferes with this feature, thus removing the method by which these attacks can be carried out. While these systems are important and necessary, their shortcoming is that they block only some methods of attack (usually just one), and therefore cannot stand on their own against the sheer breadth of tactics that web-based Super Attacks employ.

ZoneAlarm Solution
Unlike previous security options, web “transaction” security or NATs, ZoneAlarm ForceField has been created exclusively to protect users against the full breadth of web-based Super Attacks. Its main technology is a virtualization engine that surrounds users from all
sideways in a “bubble of security” as they surf the web. Its main goal is to make it simple and seamless for the consumer.

**Precision Emulation**
ZoneAlarm ForceField’s virtualization engine is similar in function to “manual virtualization systems” such as that used in VMware® and similar products. But through its precision emulation, ZoneAlarm ForceField virtualizes only those parts of the operating system that the Internet writes to. It also automatically maintains the virtual system it creates. *The result is the first virtualization system that adapts to how users work rather than forcing changes onto the user.* This means that there is no large installation, much less system memory use and associated performance degradation, and no need for the user to keep track of two separate operating systems or even two separate filing systems.

The virtualization engine works in two directions, protecting the PC from threats on the Internet but also protecting the web session (such as banking, shopping and other vulnerable activity) from threats that may lurk on the PC.

**How ZoneAlarm ForceField Works**
Each time you surf the web, a number of changes — most of them innocuous — are made to your computer system. For instance, when you fill out an online form to become a registered user of a website, the site’s server creates a cookie, which is downloaded onto your computer.

But not all changes made to your computer when you surf the web are useful or benign. For instance, keyloggers downloaded from a web server to your PC can record everything you type without your knowledge and transmit it to criminals.

ZoneAlarm ForceField software protects you from such threats at both the operating system and browser levels, without the need for signatures.

**Protecting PCs from Internet Threats**
The ZoneAlarm ForceField virtualization engine operates as a very simple, firewall-like rule. All unsolicited downloads from the Internet write to the computer just like normal. But all unsolicited downloads, such as drive-bys, write to the emulation layer, never touching the computer.

The result: Users can surf to any web site and click on any link without worry, because all unknown or unwanted changes (from browser exploits and drive-by downloads, spyware, viruses, and junk files) are made to a virtualized file system that disappears once the user is finished surfing. Only the items the user purposely downloads make it onto the computer itself.

**Active Safety Features**
At the same time the virtualization layer is working to protect users, the active safety features are offering redundant or altogether new layers of protection aside from what the virtualization layer provides.

To protect users while they surf, **dual-mode anti-phishing** uses both advanced heuristics and the best spyware signature database available to prevent users from visiting fraudulent versions of real websites.

Meanwhile, ZoneAlarm ForceField **rates each site visited** to warn users if a site has weak or suspicious credentials. ZoneAlarm ForceField also searches for and warns users about websites that distribute spyware.

Virtualization in ZoneAlarm ForceField blocks all unsolicited downloads. But what about the files the user knowingly downloads? The ZoneAlarm ForceField’s **Dangerous Download Detector** feature automatically checks all Internet-related downloads and activities against the ZoneAlarm spyware database. Any download that’s potentially dangerous or useless is deleted before it can run. Conversely, any download that is found to be valuable and legitimate is saved to the user’s computer just like normal.

ZoneAlarm ForceField supplements the inherent protection of the virtualization layer by automatically flushing away auto-executing files such as spyware and other dangers each time a user finishes a surfing session.

In addition, ZoneAlarm ForceField jams **keyloggers and screen grabbers**, thwarting these programs’ attempts to record users’ keystrokes or take screen grabs. No keystrokes are recorded and all screen grabs are blacked out.

**Essential Security Layer**
By adding a new security layer, ZoneAlarm ForceField software, which works with Microsoft® Internet Explorer® and Mozilla Firefox®, provides the strongest protection yet from phishing sites, spyware sites, keyloggers, malicious drive-by-downloads, unauthorized registry changes, adware, spy cookies, clutter, and more. ZoneAlarm ForceField is designed to supplement the ZoneAlarm line of products (ZoneAlarm; ZoneAlarm Pro; ZoneAlarm Antivirus; ZoneAlarm Anti-Spyware; ZoneAlarm Internet Security Suite) as well as other vendors’ security products.

**Precision Emulation Technical Details**
ZoneAlarm ForceField’s precision emulation is based on intercepting Windows’ own interfaces for working with files and registry keys. As such, the ForceField download is limited to a single driver and few other files along with some advanced rules and interaction with Windows; making it lightweight. As shown in Diagram 1, ForceField creates two major components:

1) A virtualization engine, which implements a duplicate Windows file and registry system
2) A hooking engine, which selectively redirects NT kernel calls to the virtualization engine.

**Without ForceField**
Normally a user account runs with administrative privileges and gives applications the freedom to read and write to the operating system and kernel. This allows malicious code to harm the operating system.

**With ForceField**
The ForceField hooking engine intercepts indiscriminate NT kernel calls. At this point, it decides if a kernel...
call was solicited by the user or was automatic, as in a drive-by-download. It determines this based upon whether or not expected UI calls were made (user initiated) or not (automated, drive-by). User-solicited calls are made to the native system component as always, so as not to interrupt the user’s normal workflow. Unsolicited calls, however, get applied to the virtualization engine and virtual file and registry system, therefore never reaching the actual computer. At the end of each browsing session, the dangerous virtual files are deleted.

**Summary of ForceField Benefits**

**Signature Independent**
As discussed in this paper, signature systems alone are not sufficient to combat today’s web-based Super Attacks. While advanced signatures certainly have their place, they must be coupled with a zero-hour system that, like ForceField, employs the simple firewall-like rule: Reject all changes to the user’s PC unless the user specifically solicits them.

**Protects At All Times**
Because web-based Super Attacks can occur the moment the user encounters a website, ZoneAlarm ForceField does not passively wait for malware to transfer from the Internet to the PC. Its virtualization layer and active security layers proactively protect the user at all times.

**Lightweight and Non-intruding**
ZoneAlarm ForceField is less than 5MB. It can be deployed within seconds and requires one simple step for installation. No setup or maintenance is required. Its interface is designed to protect the user without interruption; all virtualization activity is invisible to the user and requires zero maintenance. Only when data loss is imminent will ForceField interrupt the user.

**Conclusion**
The emergence of web-based Super Attacks, combining the most effectively malicious strategies and characteristics of historical attacks, has changed web-based interaction and transaction forever. Traditional security, while effective against aspects of today’s threats, cannot effectively protect a PC or a user’s private information from Super Attacks.

Today’s Super Attacks require a third generation solution; one that goes beyond the best of the New Advanced Technologies (NATs), the newest signature-based security and the latest tried-and-true virus and spyware eradication mechanisms and new generation firewalls.

Technologies that offer easy-to-implement, cutting-edge precision emulation that virtualize those parts of the operating system to which the Internet writes, layered over existing security products, represent today’s most effective means for thwarting Super Attacks.

ZoneAlarm ForceField is the only solution to provide this exciting and effective new integrated technology.