

A background image showing a laptop on a desk with a speedometer overlay. The speedometer has a needle pointing towards the 40 mark, with numbers 10, 20, 30, 40, 50, 60, and 70 visible. The scene is dimly lit, suggesting an office environment.

# Threat Management

Challenges and Solutions ↩

## ➔ Web Threats

*A Trend Micro White Paper | February 2007*

## ➔ TABLE OF CONTENTS

<b>Executive Summary</b> .....	3
<b>Introduction: An Unwelcome Scenario</b> .....	3
<b>Background</b> .....	4
<b>Web Threats Defined</b> .....	4
Forms of Web Threats .....	5
Sophisticated Methods .....	5
<b>Impacts and Extent of Web Threats</b> .....	5
<b>Traditional Approaches Fail to Protect Against Web Threats</b> .....	8
<b>A New Approach is Needed: Integrated, Multi-Layered Protection</b> .....	8
In-the-Cloud .....	9
At the Internet Gateway .....	10
At the Endpoint .....	11
Feed-Through and Loop-Back .....	11
<b>Extending this Approach to Email Security</b> .....	12
<b>Conclusion</b> .....	13
<b>References</b> .....	14

## EXECUTIVE SUMMARY

Motivated by the lure of profits from the sale of stolen confidential information, cyber criminals today are shifting to the Web as the medium for their malicious activities. Characterized by blended techniques, an explosion of variants, and targeted regional attacks, Web threats pose a broad range of potential costs, including identity theft, loss of business confidential information, damaged brand reputation, and erosion of consumer confidence in Web commerce. These high stakes, the pervasive use of the Web, and the complexity of protecting against Web threats combine to form perhaps the greatest challenge to protecting the privacy of personal information and the confidentiality of business information in a decade. Traditional means do not provide adequate protection from these threats, and no single method or technology will improve this situation. Instead, a multi-layered, comprehensive set of techniques must be brought to bear. This white paper describes Web threats, how they function, and their impacts; explains why traditional methods fail to protect against these threats, and describes the characteristics of a new approach that are needed.

## INTRODUCTION: AN UNWELCOME SCENARIO

Robert, an attorney in the legal department of a major pharmaceutical company, arrives at his office Monday morning, logs on to his computer, and as is his habit, first scans his new email. A basketball fan, Robert had watched a game the previous evening on television. Still thinking about the game, he notices a brief email from a friend. The email mentions a link to a new Web site with information on one of his favorite basketball players. So Robert clicks on the link, which takes him to a fascinating site with photos, videos, and other information on the player. But unbeknownst to the attorney, when his browser renders one of the photos, malicious code contained in the jpg file issues a command to download an executable file, which runs automatically on his computer. This malware then captures pre-defined types of files stored on Robert's hard drive, compresses and encrypts them, and sends them to a third-party email address – the address of a cyber criminal. Some of these files contain highly confidential information about several patent cases in which Robert is involved. By sending this same email to a list of employees at various pharmaceutical companies, the cyber criminal specifically targets the pharmaceutical industry to gain information like this and subsequently sell it for profit. Hence, by simply clicking on the seemingly innocuous link to the Web site, Robert has unintentionally set in motion a process that allows confidential corporate information to fall into the wrong hands. This potentially exposes his company to loss of competitive patents, legal entanglements, and other costs.

That same Monday morning, an IT administrator at the pharmaceutical company is monitoring network traffic. Confident in the knowledge that the company has recently supplemented its client-based virus protection with list-based URL filtering, the administrator sees no unusual activity on her screen. The malware download and subsequent theft of Robert's files escape her detection for a number of reasons that involve common practices of today's cyber thieves. First, the malware writer had just established the new Web site with the malicious content that morning, so that it would not be included on the list of sites in URL filtering software. Second, the cyber criminal incorporated instructions in the malware to gradually export Robert's files, thus avoiding any spikes in network traffic that the administrator might notice. Since the pharmaceutical company has not installed any software at the gateway that includes behavior analysis, the emails with attachments that trickle out of the attorney's computer do not seem out of the ordinary.

Unfortunately, around the world, scenarios like this one are unfolding at large enterprises and small businesses alike. A large and growing number of so-called "Web threats," like the one described above but in an infinite number of varieties, are wreaking havoc. Cyber criminals are stealing lists of social security numbers from health care organizations, credit card numbers from financial institutions, and proprietary information from technology companies. In addition to facilitating identity theft, this thievery is eroding consumer confidence in the ability to maintain the privacy of their information, while undermining online banking, transactions, and ecommerce.

## BACKGROUND

Over the last 15 years, information security threats have evolved through a series of incarnations. Viruses embedded in downloaded executable files gave way to Macro viruses in document files, followed a few years later by email-delivered threats (e.g., the “I Love You” and “Melissa” viruses). In each case, malware writers sought out the medium that was most used and least protected. While malware continues to exploit the pervasive use of email, this vector is becoming increasingly protected, in response to growing understanding of the need for such protection. Today, a new wave of threats is emerging that uses the Web as a delivery vehicle.

Consistent with the evolution of past threats, Web threats are gaining traction at a time when use of their medium – the Web – is at an all-time high, has become a major engine of commerce, and continues to grow. Most office workers open a browser at their desktop first; this is where most people start their work. Social trends such as Myspace and YouTube and growing regionalized Internet user behavior are important contributors to this Web use.

At the same time, the Web is relatively unprotected, compared to messaging for example, as a medium to deliver malware. According to IDC, “Up to 30% of companies with 500 or more staff have been infected as a result of Internet surfing, while only 20%-25% of the same companies experienced viruses and worms from emails.” [1] The Web is more difficult to protect because of the much larger bandwidth needed to scan or filter its data stream, compared to email, which contains less than one thousandth as much data. Traditional antivirus software installed on client machines, for example, while crucial to the protection of these machines from a variety of threats, does not adequately protect against the evolving set of Web threats. This creates a “perfect storm” for the advance of Web threats: a relatively unprotected, yet widely and consistently used medium that is crucial to business productivity. As a result, information security today is at a critical turning point: a new approach is needed to address the newest class of threats.

## WEB THREATS DEFINED

Web threats encompass a broad array of threats that originate on the Internet. Using a combination of various files and techniques, rather than a single file or approach, Web threats are sophisticated in their methods. For example, Web threat creators constantly change the version, or variant, used. Because the Web threat is stored in the fixed location of a Web site, rather than on an infected user’s machine, its code must be constantly modified to avoid detection.

In recent years, individuals once characterized as hackers, virus writers, spammers, and spyware makers are now known simply as cyber criminals. These criminals unleash Web threats primarily for reasons of financial gain. They achieve this by causing infections simply via user visits to targeted Web pages, and subsequently using various stealth techniques to hide on a computer or on the Web. Once in place, the malicious code slowly and surreptitiously steals the user’s files and consumes CPU power.

*A “perfect storm” for the advance of Web threats: a relatively unprotected, yet widely and consistently used medium that is crucial to business productivity.*

# CHALLENGES AND SOLUTIONS: WEB THREATS

## ➔ Forms of Web Threats.

Following is a few examples of this group of threats, categorized according to various portions of the threat lifecycle:

- How the Web links are delivered
  - Spam, phishing-attack emails, “get rich quick” scams, and any other targeted emails that contain URLs and direct the user to a malicious site
  - A poisoned Domain Name Server (DNS, i.e., via pharming) or compromised Web sites that redirect the user to a fraudulent Web site (instead of the legitimate one) or proxy server to either steal information or expose the user to infection
  - Social networking sites and various other circumventions to infect the user
- The Web site experience
  - Browser rendering exploits in media files (e.g., image, animation, video, and audio files) that either drop malicious files or download malicious files
  - ActiveX controls or drive-by downloads that either force the user to download to continue viewing or automatically push down a malicious file if an unpatched browser is used
- Infection routine
  - Infection arrival in applications that introduce malicious files to a system
  - Web threat frequent self-updating via update downloading on the Web of multiple sets of codes to avoid detection with traditional scanners
- Payload after infection
  - Spyware or applications that steal data or information from a system and send it to a third party
  - Adware, data miner, or pop-ups that serve commercial interests
  - Browser Helper Objects that taint search engine results or monitor user browsing habits to collect info about user interests (e.g., goods or services) and feed them marketing ads
  - Bots (code that can be remotely controlled to take malicious actions) or zombies that receive commands through the Web

## ➔ Sophisticated Methods.

Web threats typically take advantage of internet port 80, which is almost always open to permit access to the information, communication, and productivity that the Web affords to employees. (The earlier example illustrates this approach.) Web threat variants target infection at a regional or local level (e.g., via local language sites aimed at particular demographics), rather than using the mass infection technique of many earlier malware approaches. Malware authors also use social engineering such as enticing email subject lines (which often provide a URL to a site that downloads malicious code) that reference holidays, popular personalities, sports, pornography, world events, and other popular topics.

## IMPACTS AND EXTENT OF WEB THREATS

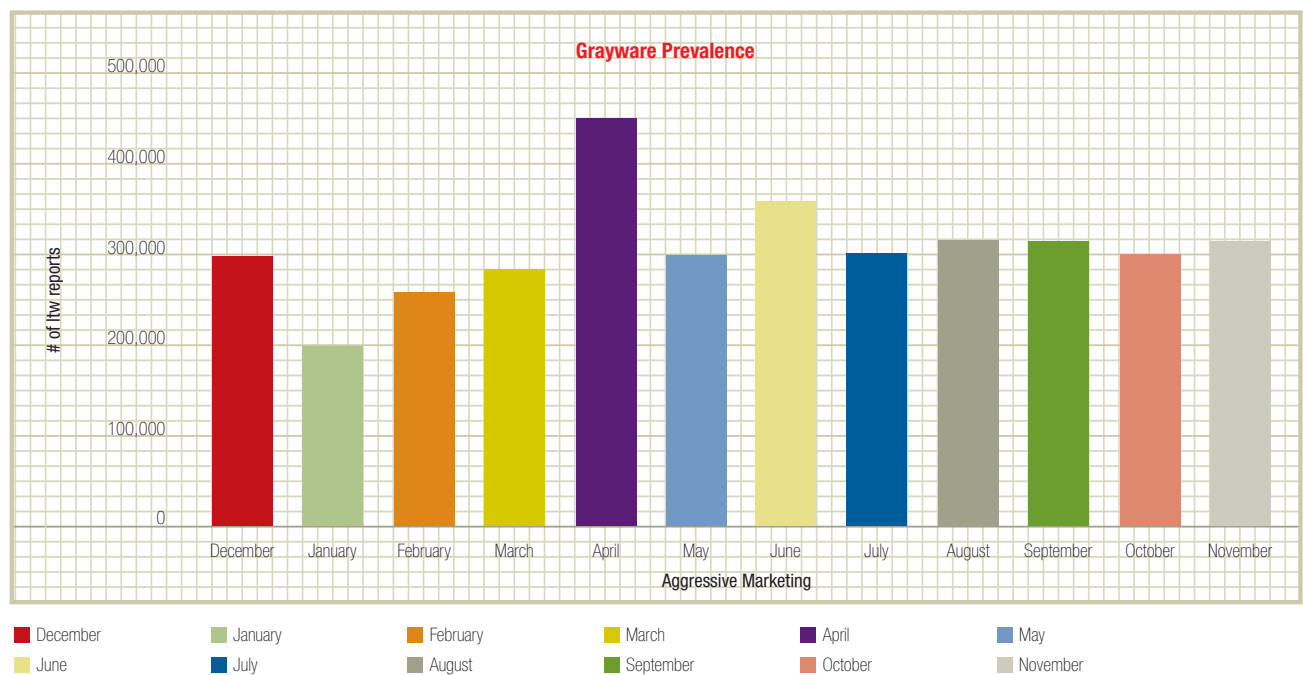
Web threats help cyber criminals pursue one of two goals. One goal is to steal information for subsequent sale. The resulting impact is primarily confidential information leakage in the form of identity loss or use of the infected user as a vector to deliver phishing or other information capturing activities. Among other impacts, this threat has the potential to erode confidence in Web commerce, corrupting the trust needed for Internet transactions. The second goal is to hijack a user’s CPU power to use it as an instrument to conduct profitable activities, such as sending spam or conducting extortion in the form of distributed denial-of-service attacks or pay-per-click activities.

# CHALLENGES AND SOLUTIONS: WEB THREATS

Profits gained from a variety of Web threats are significant. Jeanson James Ancheta, for example, earned \$60,000 USD by managing a 400,000-PC Botnet [2]. Ivan Maksakov, Alexander Petrov, and Denis Stepanov extorted \$4 million (USD) by unleashing a distributed denial-of-service attack on U.K. sports bookmakers [3]. On the black market for malware like this, \$1000-\$5000 (USD) is typically paid for a Trojan horse, for example, that is able to steal online account information [4]. Yet, little is known about the scope of the profits in this underground sector, due to the underground nature of their behavior.

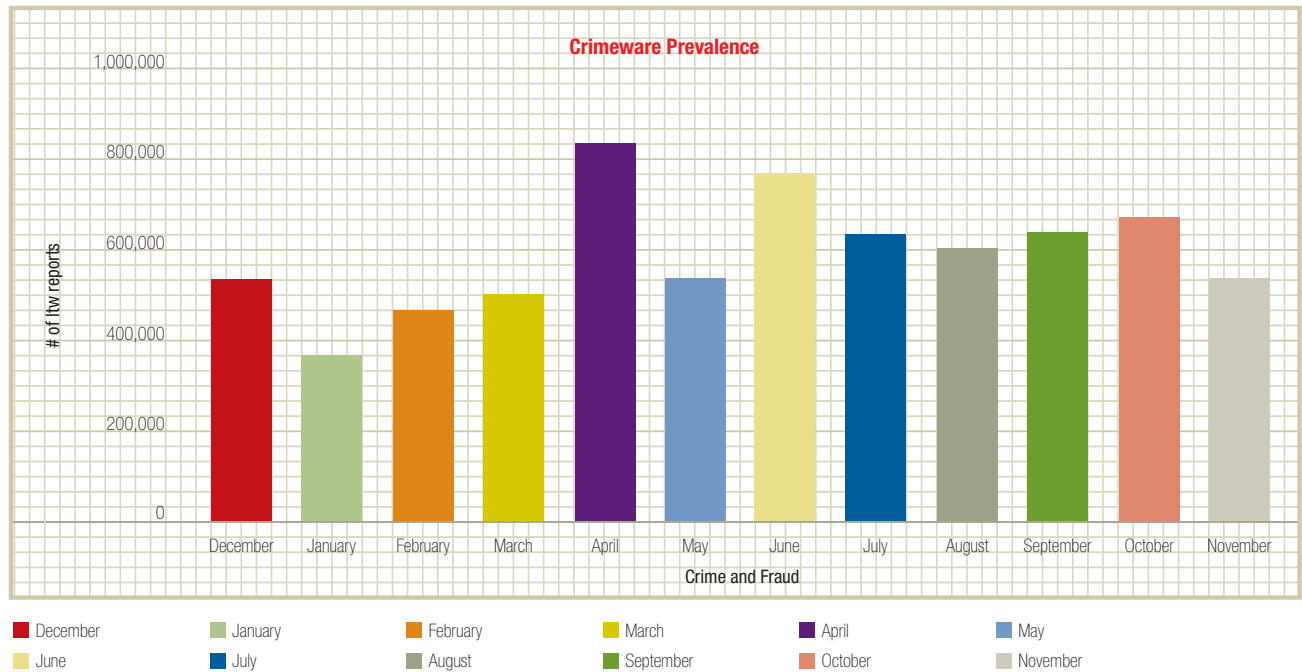
Some aggregate data has been gathered, however, on the financial impact of some types of Web-based threats. For example, Consumer Reports USA reports that phishing attacks on U.S. citizens generated \$630 million (USD) in 2005 [5]. Despite using Transaction Authentication Numbers (TANs) in addition to user names and passwords, customers of various German banks remain victims of phishing. The Munich Police Department estimates that damage due to online fraud (January – July 2006) exceeded 1 Million Euro in that city alone [6]. According to Asia.Internet, Gartner Group reports that total losses from phishing attacks in 2006 were \$2.8 billion [7].

Figures 1 and 2 provide estimates of the extent of various types of Web threats. At the same time, data indicates that Web threats are growing (see Figure 3). The Standard Bank estimates a 50 percent growth in spyware in the past 18 months, and a 16-fold increase in virus creation over the past three years [8]. One study showed that phishers might be successful with as many as 14 percent of their trick messages in only 24 hours – much higher than previous estimates by network security watchers [9].

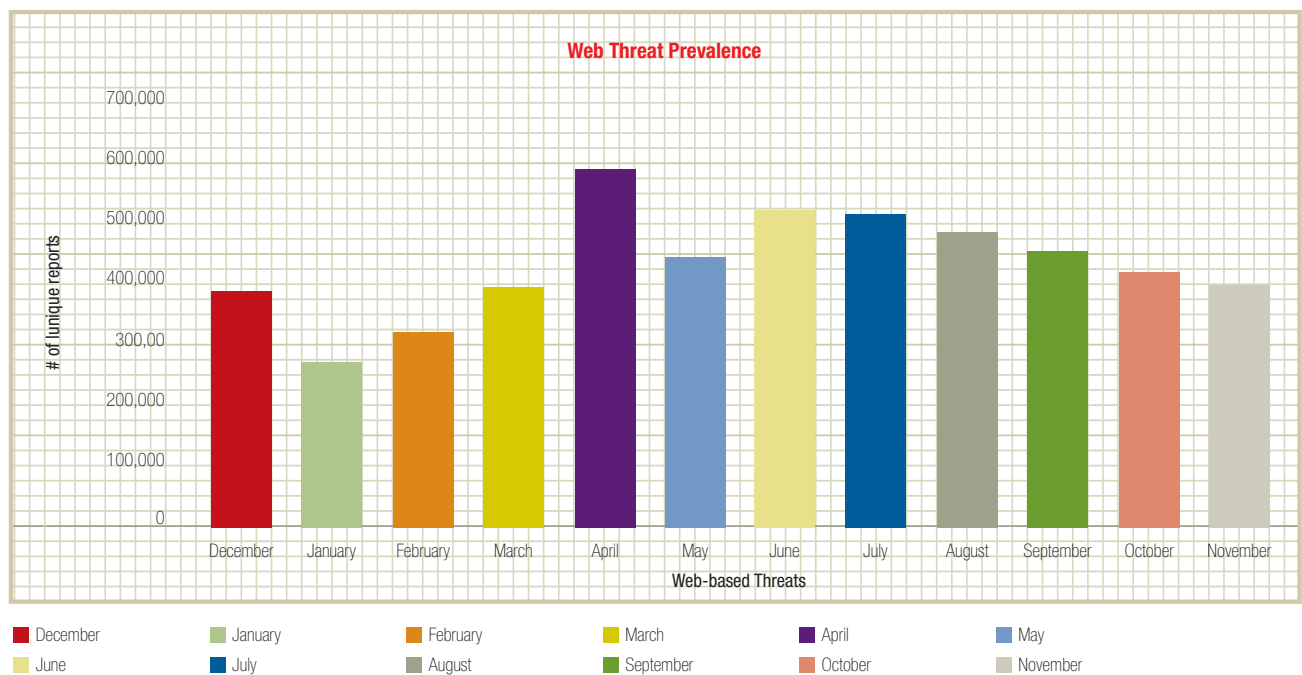


**Figure 1.** Grayware – while considered non-malicious – rose significantly in 2006. This is a concern, as Trend Micro has noticed a move toward malware as a means of generating click-through revenues. *Source: Trend Micro*

# CHALLENGES AND SOLUTIONS: WEB THREATS



**Figure 2.** In 2006, the prevalence of crimeware – malicious software designed to automate financial crime – rose significantly. Source: Trend Micro



**Figure 3.** In addition to email, the second most prevalent means of malware distribution is via the Web. Source: Trend Micro

## TRADITIONAL APPROACHES FAIL TO PROTECT AGAINST WEB THREATS

The traditional approach to virus protection involves collecting samples of viruses, developing patterns, and quickly distributing these patterns to users. This is insufficient to address Web threats for various reasons.

For example, because many Web threats are targeted attacks and span many variants, collecting samples is almost impossible. The large numbers of variants use multiple delivery vehicles (e.g., spam, instant messaging, and Web sites), rendering the traditional sample collection and pattern creation process insufficient. Because Web threats use a variety of tactics (e.g., targeted local and regional attacks, local/regional language spam, and Web sites), one security solution does not fit all threats; a sample collected for one targeted local attack, for example, does not address other local attacks.

Fundamentally, Web threats aim to hide instead of explore and spread, and hence are difficult to detect via traditional antivirus techniques. In some cases, Web threats may result in system infection that is so extensive (e.g., via a rootkit in which the system file is replaced) that traditional uninstall or system cleaning approaches become useless. A total recovery – in which the hard drive is wiped, and the operating system, applications, and user data are reinstalled – is often needed. Cyber criminals also take advantage of the need to keep port 80 open for legitimate traffic, which circumvents existing client firewalls. And some professional cyber criminals use the “pre-zero” day vulnerability, so that even on-time security patches are unable to prevent the impacts of these threats.

At the same time, profit-driven cyber criminals target and compromise not only the Windows Web server platform (e.g., so it can spread a downloader source), but also other platforms. In fact, Web threats are operating system independent, targeting Web servers of all types. This means that even Linux-based Web servers, once thought to be less vulnerable to security threats, are now compromised. Once a malware program is installed, it continues to initiate other programs to violate host intrusion prevention system (HIPS) rules. Excessive false alarms annoy users to the point that they disable protection or allow the program to execute. In this way, the malware evades traditional HIPS techniques.

Individual downloader programs – commonly used as part of Web threats – appear to be “innocent.” Yet when they are combined, they become malicious, making file-based heuristic scanning prone to false positives or useless. Web threats often expand this technique to include multi-layered, multi-protocol coordinated attacks to avoid detection via traditional means. For example, a cyber criminal embeds a URL in a Web mail or instant message. The user clicks on the link to a legitimate URL that was hijacked by the cyber criminal for a few days or hours. Then an ActiveX control tests the vulnerability of the user’s browser. If a vulnerability is detected, the malware attacks; if not, it downloads a file, tests for vulnerability, downloads other files, and so on. Each session of the traffic appears to be benign, but the combined activities become a coordinated attack.

## A NEW APPROACH IS NEEDED: INTEGRATED, MULTI-LAYERED PROTECTION

Clearly, a new approach is needed to address Web threats that complements existing techniques. The most effective approach will employ multiple layers of protection and incorporate a range of protection measures. In addition, the evolving nature of the threat necessitates some form of feedback, in which information gathered in one portion of the protection system is used to update information in other layers. Any effective approach should also address all relevant protocols, because of the ability of Web threats to leverage these protocols. Coordinating these measures requires some sort of efficient centralized management, and of course, targeting specific regions of the world with regional expertise would help address the regional and even localized nature of many of the threats.

# CHALLENGES AND SOLUTIONS: WEB THREATS

The key to effectively addressing Web threats is a multi-layered approach. This can be accomplished by implementing measures at three different layers (see Figure 4): 1) “in-the-cloud” (i.e., before the traffic reaches the Internet gateway), 2) at the Internet gateway, 3) and at the endpoint (i.e., the client). Web threats often use email as a medium to deliver an initial Web link. Hence, intercepting Web threats in-the-cloud reduces email traffic to the gateway, frees up bandwidth, consumes less processing power, requires less storage and archiving of emails and other information to comply with regulatory requirements, and hence, is more cost effective.

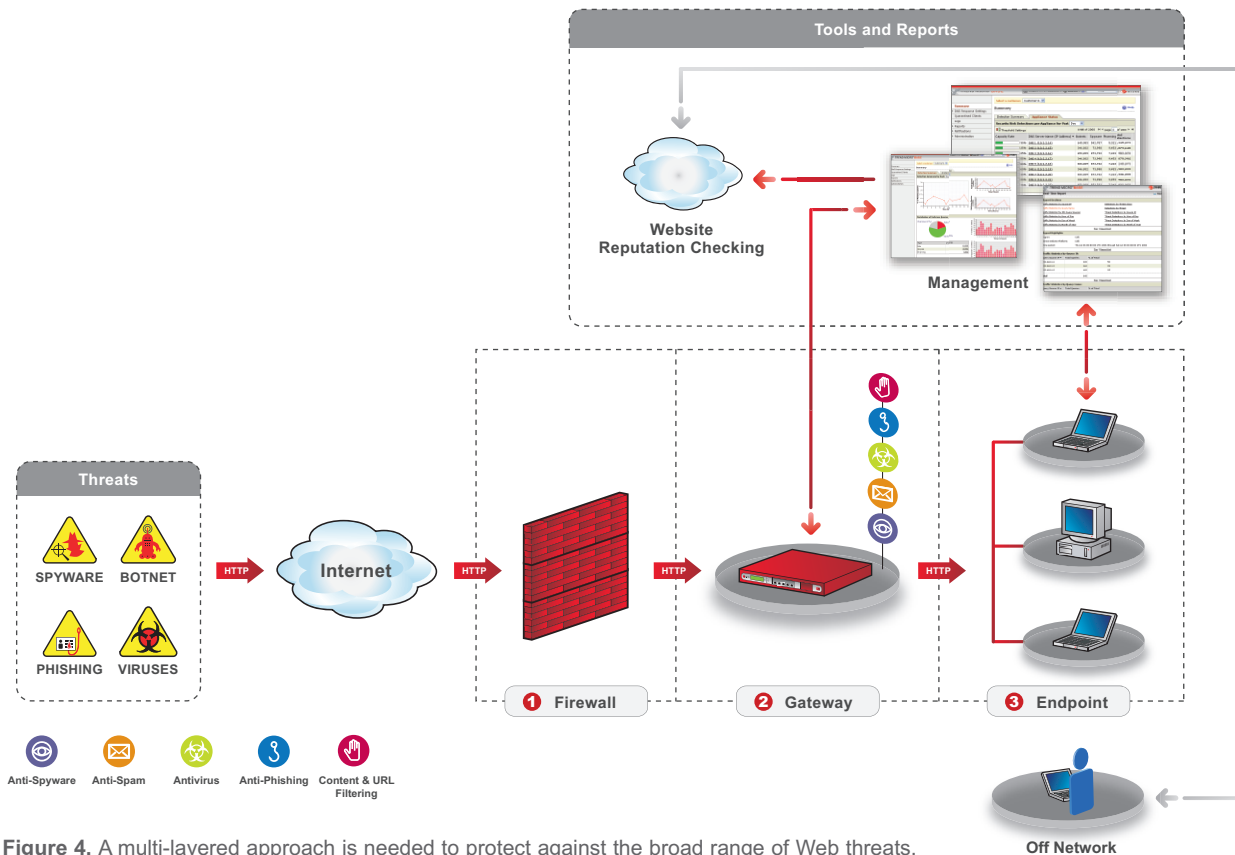


Figure 4. A multi-layered approach is needed to protect against the broad range of Web threats.

## ➡ In-the-Cloud.

At this level, the primary function is to check the “reputation” of each Web site before allowing user access. This is analogous to performing a “credit check” before consummating a financial transaction. A Web reputation check involves a URL filtering database; however, the addition of approximately 5000 new domains per day means that additional measures are needed to complement this important element. These measures should include checking a database of “security ratings” that are developed based on a periodic data crawl of Web sites to check for malware, and a database of known phishing and pharming URLs. Cyber criminals often change the physical locations of IP addresses to evade detection; hence, an additional measure in-the-cloud should perform an IP location check in which IP locations are correlated with URLs. For maximum effectiveness, an analysis of all top level domains (i.e., the letters in a URL to the right of the last dot, including country codes) is also recommended (see Figure 5).

# CHALLENGES AND SOLUTIONS: WEB THREATS

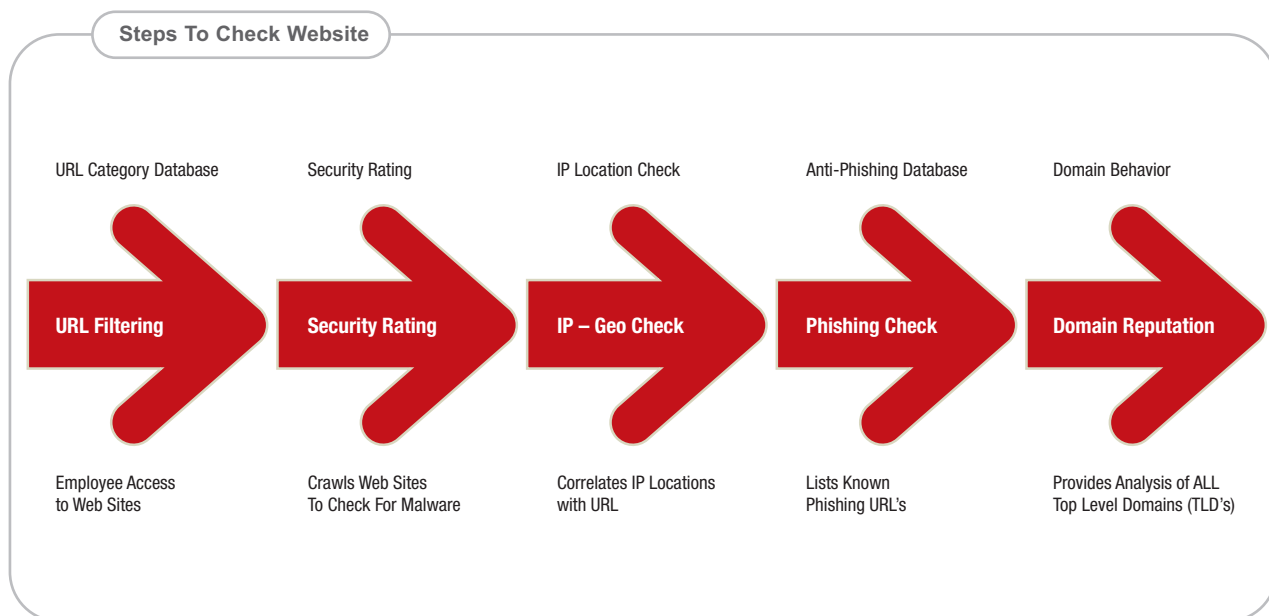


Figure 5. In the cloud, the key is to check the “reputation” of each Web site via a comprehensive set of steps.

## ➔ At the Internet Gateway.

Important functions are also needed at the second of the three levels, the Internet gateway. Performed via either software or a hardware appliance, gateway capabilities should include file checking. The file checking function essentially checks the reputation of each file before permitting the user to download it. To do this, a data crawl of each file at the Web site and an assessment of each file’s “reputation” are periodically performed to establish and maintain a database of file reputation. This file checking is needed, in addition to the Web reputation function in-the-cloud, because cyber criminals can easily move individual files with malicious content from one Web site to another.

The second form of protection from Web threats needed at the gateway is some form of behavior analysis that can correlate combinations of activities to determine if they are malicious. This analysis can develop a score for each combination of activities and block the combination if the score exceeds a threshold level. This approach can also identify triggers, which are evidence or clues in session data or a protocol property that can be used to help identify suspicious activity. Further, this approach can implement rules, which are a correlation of triggers that match defined conditions of malicious activity, at the gateway.

This approach should correlate, for example, activities of a single session on the same protocol (e.g., an SMTP attachment with a suspicious double extension). The approach should also correlate activities during multiple network connection sessions on the same protocol (e.g., a downloader blended threat in which individual files that each appear to be innocent are downloaded, but together they form a malicious program). Activities of multiple sessions and different protocols (e.g., SMTP and HTTP) should even be correlated to identify suspicious combinations of activities (e.g., an email with a URL link to several recipients, and an HTTP executable file download from the link).

## ➔ **At the Endpoint.**

Despite implementation of these measures in-the-cloud and at the gateway, a third level of protection at the endpoint (i.e., the client) remains critical. Approximately two-thirds of recent U.S. computer retail sales are notebook computers [10]. These machines require protection because they connect to multiple networks, and visitors and contractors physically carry them past the company gateway; corporate Web security policy must be enforced whether the user is on or off the network. Therefore, a solution is needed that provides client-level prevention (e.g., access control and scanning), and in case of infection, cleaning, and recovery. So, for example, if a notebook computer has been compromised elsewhere and is part of a botnet, the notebook could attempt to connect back to the bot herder (the botnet originator). Another example is phone-home spyware, which periodically attempts to transfer information captured on the infected host back to the spyware owner. In either case, this activity can be detected and blocked, and a clean-up operation can be directed if needed.

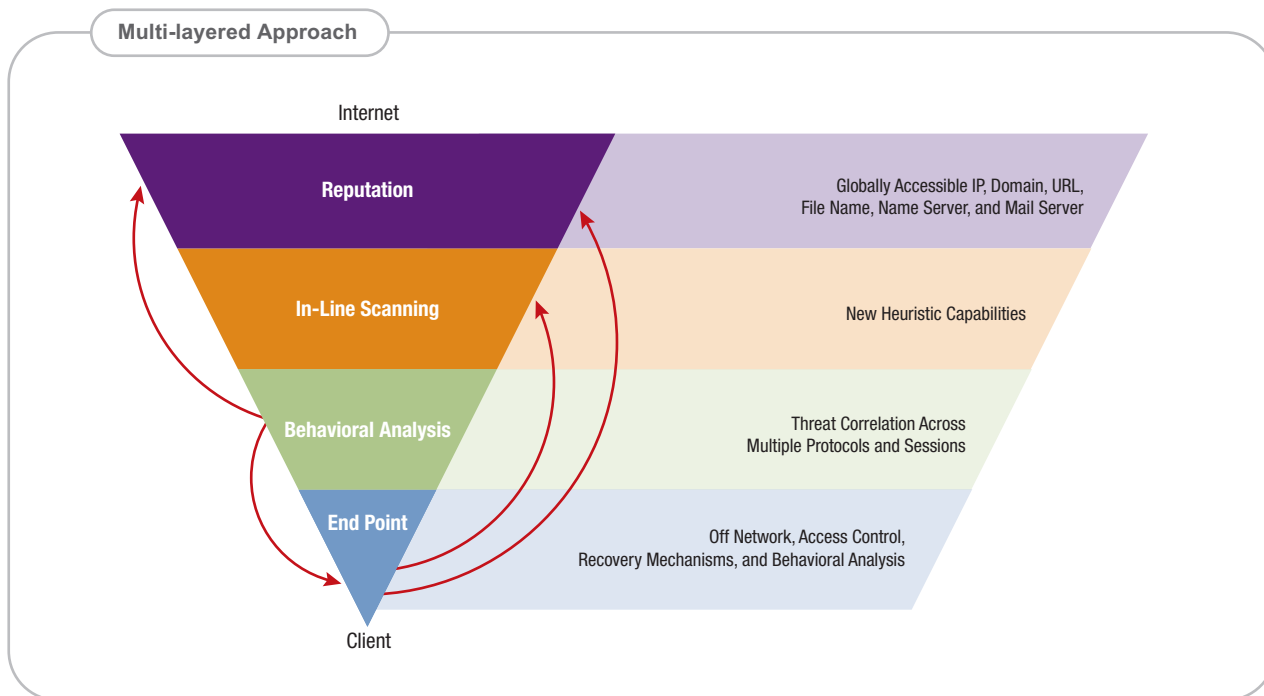
Endpoint-based prevention should consist of URL filtering, Web site reputation capabilities, and use of a “restore point” for the machine that is saved prior to Web surfing. Using the latter, if the user detects any abnormal activity after downloading a file or browsing the Web, the machine could be returned to the restore point. Other prevention options should include establishing a “virtual environment” for the user to surf the Web; in this arrangement, Web threats reach only the virtual environment and do not penetrate the user’s actual environment.

Clean up capabilities should assume two forms: agent-based cleaning, and non-agent-based cleaning. Using agent-based cleaning, an agent that is centrally managed resides on the laptop computer, coordinating activities. Non-agent-based cleaning applies to the situation in which an agent is not installed on the notebook computer of a visitor or contractor; in this case, cleaning is accomplished on-demand with network access control (i.e., that allows limited access to the network to complete cleaning). Total recovery is also needed in cases when cleanup is not feasible due to a rootkit infection, for example.

## ➔ **Feed-Through and Loop-Back.**

Figure 6 illustrates this multi-layered approach, and also shows an important needed aspect of its implementation. Incorporating layers of protection in-the-cloud, at the gateway, and at the endpoint is a “feed-through” mechanism. In addition, feeding back information from one layer to another is a “loop-back” mechanism. For example, information learned in the behavior analysis function at the gateway can be looped back to update the Web reputation databases, as well as the endpoint capabilities. Similarly, information acquired at the endpoint can be looped back to the file scanning capability at the gateway and the Web reputation capability in-the-cloud. Both feed-through and loop-back techniques are needed to ensure adequate protection on an ongoing basis.

All of these capabilities and relevant policies need to be monitored and managed from a centralized console. At the same time, specific teams need to target specific regions of the world. These teams should be at the forefront of intelligence gathering, sample sourcing, mitigation and prevention, and coordination with local security groups and law enforcement agencies in the fight against Web threats. This approach is likely to result in faster response, customized solutions, and cultural awareness.



**Figure 6.** Feed-through (top to bottom) and feedback (arrows) capabilities complement a multi-layered approach that begins in-the-cloud, and continues at the gateway, in the network, and at the endpoint.

## EXTENDING THIS APPROACH TO EMAIL SECURITY

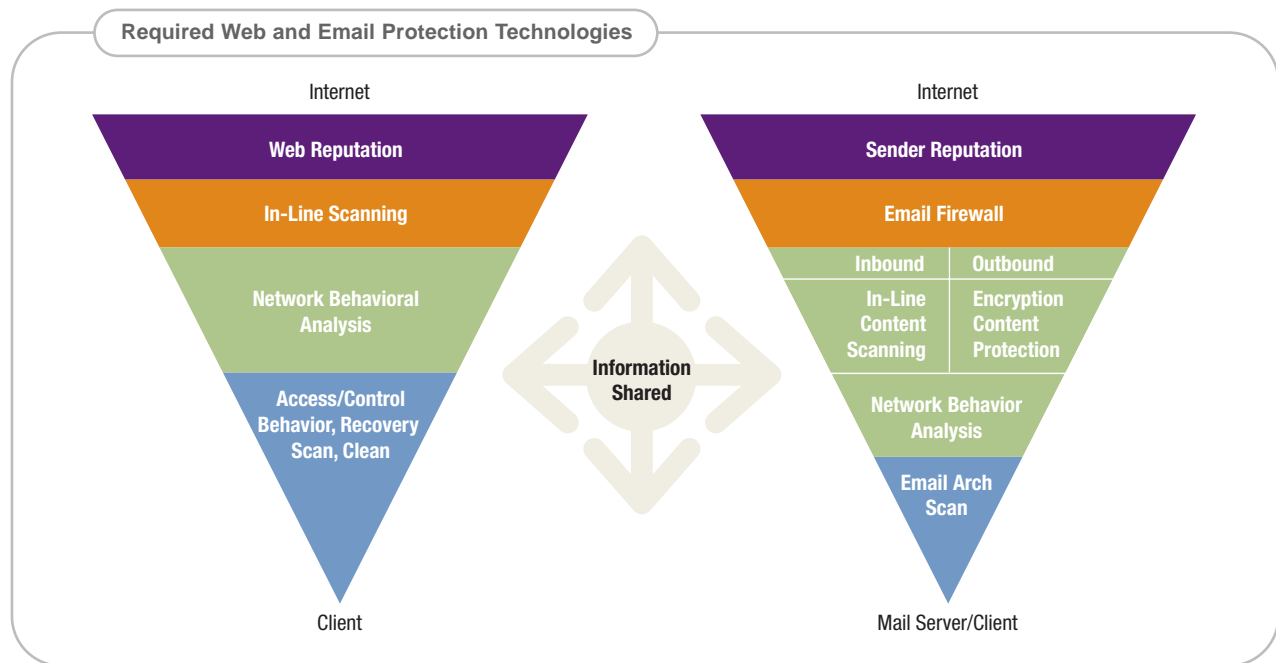
This multi-layered approach can also be extended to email security. Active protection in-the-cloud is important in the messaging realm because once email reaches the Internet gateway, regulatory requirements mandate email retention for as long as ten years. Hence, prefiltering email in-the-cloud saves bandwidth, reduces storage and maintenance costs, and aids protection. At this layer, protection should include email sender IP reputation checks, domain IP reputation checks, an email firewall, and anti-spam and anti-virus filtering (with zero false positives in this layer). The email firewall should be hosted outside of the email server to prevent distributed denial-of-service attacks and directory harvest attacks (i.e., attacks that randomly search for valid email addresses).

At the Internet gateway, anti-spam and anti-virus software should include attachment scanning to detect attachment spam – a relatively new form of bot-generated spam that is difficult to identify, uses images to conceal spam, consumes storage, and usually contains malware. At this level, a policy engine is also needed that links to the directory (e.g., LDAP) from email servers. Here, behavioral analysis technology is used to detect, for example, that a user never replies to a repeated email, labeling it spam so it can be returned. Email content scanning can also be performed at this level to ensure that employees and others do not reveal confidential information in email or attachments to unauthorized parties. This functionality should also enable encryption for outgoing email, and email archiving to comply with regulatory requirements.

# CHALLENGES AND SOLUTIONS: WEB THREATS

In the messaging environment, the third level (the endpoint level) is the email server itself, because mailboxes reside on this server. The email server needs to run security software and also allow end users to manage utilities such as end user quarantine mailboxes where spam is sent. This additional layer of security is important to counter internal messaging threats.

Because email and Web threats are merging, solutions that provide feedback between these two vectors and centrally manage networks from all of these threats are needed (see Figure 7). Essentially, IT administrators need to know how malware enters their networks. Additional media that need to be protected include instant messaging and collaboration tools.



**Figure 7.** Trend Micro recommends solutions that provide feedback between required Web and email protection technologies, and centrally manage networks from all of these threats.

## CONCLUSION

Web threats exist today and are growing in numbers and impact. Their complexity, large number of variants, and use of multiple vectors, combined with their exploitation of the most commonly used medium today, make Web threats the most challenging threat that enterprises, services providers, and consumers have faced in a long time. The cost of these threats assumes the form of confidential information leakage, with the consequent impact on brand reputation, regulatory and legal implications, and cost of loss of confidentiality to competitors. Because traditional approaches fail to protect against Web threats, the information security industry is at a crossroads. Businesses of all sizes, as well as service providers, need to deploy solutions via an integrated, multi-layered approach to provide adequate protection against these threats.

## REFERENCES

1. IDC, press release, July 18, 2006, "Private Internet Use by Staff Threatens IT Security in Danish Companies, Says IDC," [http://www.idc.com/getdoc.jsp?containerId=pr2006\\_07\\_14\\_125434](http://www.idc.com/getdoc.jsp?containerId=pr2006_07_14_125434).
2. Gregg Keizer, TechWeb Technology News, January 24, 2006, "Botnet Creator Pleads Guilty, Faces 25 Years," <http://www.techweb.com/wire/security/177103378>
3. Marius Oiaga, Softpedia, October 4, 2006, "Hacking Russian Trio Gets 24 Years in Prison," <http://news.softpedia.com/news/Hacking-Russian-Trio-Gets-24-Years-in-Prison-37149.shtml>.
4. Byron Acohido and Jon Swartz, USA TODAY "Cybercrime flourishes in online hacker forums," October 11, 2006, [http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-10-11-cybercrime-hacker-forums\\_x.htm](http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-10-11-cybercrime-hacker-forums_x.htm)
5. Consumer Reports, "Don't bite at phishers' e-mail bait," September 2006, [http://www.consumerreports.org/cro/personal-finance/news/september-2006/dont-bite-at-phishers-e-mail-bait-9-06/overview/0609\\_dont-bite-at-phishers-email-bait\\_ov.htm](http://www.consumerreports.org/cro/personal-finance/news/september-2006/dont-bite-at-phishers-e-mail-bait-9-06/overview/0609_dont-bite-at-phishers-email-bait_ov.htm).
6. Police of the City of Munich, August 25, 2006, <http://www.sueddeutsche.de/tt3m3/muenchen/artikel/612/83529/>
7. "Scammers Hooking Bigger Phish," Asia.Internet, November 9, 2006, <http://asia.internet.com/news/article.php/3642971>.
8. Herman Singh, Standard Bank, "Next Generation Internet Fraud and Techniques to Combat This," BMI-T Annual Banking Forum, October 19, 2006, Johannesburg, <http://www.bmi-t.co.za/presentations/bf/links/presentations/Herman%20Singh.pdf>.
9. Markus Jakobsson, Jacob Ratkiewicz, "Designing Ethical Phishing Experiments: A study of (ROT-13) rOnI query features," International World Wide Web Conference Committee, WWW 2006, May 23-26, 2006, Edinburgh, Scotland, ACM 1-59593-323-9/06/0005, [http://www.informatics.indiana.edu/markus/papers/ethical\\_phishing-jakobsson\\_ratkiewicz\\_06.pdf](http://www.informatics.indiana.edu/markus/papers/ethical_phishing-jakobsson_ratkiewicz_06.pdf).
10. Tom Krazit, Cnet, "Two in three retail PCs are notebooks," December 20, 2006, [http://news.com.com/Two+in+three+retail+PCs+are+notebooks/2100-1044\\_3-6144921.html](http://news.com.com/Two+in+three+retail+PCs+are+notebooks/2100-1044_3-6144921.html).

### TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at [www.trendmicro.com](http://www.trendmicro.com).

### TREND MICRO INC.

10101 N. De Anza Blvd.  
Cupertino, CA 95014  
USA toll free: 1+800-228-5651  
phone: 1+408-257-1500  
fax: 1+408-257-2003  
[www.trendmicro.com](http://www.trendmicro.com)

