Web Threats
Challenges and Solutions

Web Security

Web Threat Protection

A Trend Micro White Paper | March 2008

I. EXECUTIVE SUMMARY

Motivated by the lure of profits from the sale of stolen confidential information, cyber criminals today are shifting to the Web as their chosen attack vector, which provides an ideal environment for cyber crime. Many Web threats can be deployed unbeknownst to the user, requiring no additional action than merely opening a Web page. Large numbers of users, an assortment of technologies, and a complex network structure provide criminals with the targets, exploitable weaknesses, and anonymity required for large-scale fraud.

Web threats pose a broad range of risks, including financial damages, identity theft, loss of confidential business information, theft of network resources, damaged brand or personal reputation, and erosion of consumer confidence in e-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 personal and business information in a decade.

Web threats employ blended techniques, an explosion of variants, and targeted regional attacks often based on social engineering to defraud users. And these threats often use multiple protocols, such as an email that delivers a link to a dangerous Web site, using both the SMTP and HTTP protocols in the attack. Conventional 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; it explains why conventional methods fail to protect against these threats and describes the characteristics of a new approach required to ensure security, regulatory compliance, and business continuity.

II. INTRODUCTION: AN UNWELCOME SCENARIO

Robert, a Human Resources Director at a large law firm, arrives at his office on Monday morning, logs on to his computer, and scans his new email. He opens an email from a large employment site he uses frequently, clicks an embedded link, then logs on to the site to view his postings and responses. Robert's client status entitles him to access job seekers' personal information, which he uses to perform background investigations and credit checks. Unbeknownst to Robert, the email was actually fraudulent, spoofing the employment site. When his email client rendered the images in his message, malicious code contained in the .jpg file secretly downloaded an executable file, which ran automatically on his computer. This malware logged keystrokes on Robert's computer, capturing his login information when he accessed the job site and providing this information to the hacker.

In August 2007, a very similar scene played out as cyber criminals infiltrated the monster.com job site through "Monster for Employers" accounts, compromising the personal information of 1.6 million users. Many of these users then received official-looking emails, claiming to be from monster.com and encouraging them to download a "helper application" that turned out to be yet more malware. These attacks were well-researched, using familiar language and branding, and coded to transfer data slowly, under the radar of IT administrators looking for suspicious network traffic.[1]

Web threats also include malware that is downloaded from an email attachment, but accesses the Web to convey information to the hacker. In 2007, fraudulent emails were sent purporting to be from the Federal Trade Commission. These emails claimed that a complaint had been filed against the company and contained an attachment. If the recipient opened the attachment, a keylogging Trojan was deployed that attempted to steal login information from the user's computer and send it back to the hacker. [2]

Phishing is a prevalent Web threat, spoofing legitimate companies to trick people into providing confidential information. Consumer phishing is wide-spread, sending emails that spoof organizations like banks and on-line retailers. These phishing emails often use links to take recipients to Web sites where confidential information is gathered. Employees can fall victim to these consumer threats, but phishing can also affect corporations more directly. In 2005, phishing emails targeted CEOs and other high-level executives of US credit unions in an attempt to gain control of millions of personal financial records. The email messages contained a link to a Web site where a Trojan was downloaded. Even one successful infection could have caused millions of dollars of damage and caused irreparable harm to hundreds of thousands of users through identity and asset theft. [3]

But Web threats don't just steal confidential information; they can also steal network resources. Variations of e-greeting card spam were sent throughout 2007. These simple spam messages told recipients that a friend had sent them an e-greeting card and to follow the link in the email to view the card. If recipients followed the link, it took them to a Web site that downloaded malicious code. This code hijacked the computer, turning it into a "bot" and allowing the hackers to use the machine for their own purposes—sending spam, hosting malicious Web sites, and much more. Consumer and corporate computers were infected by the millions. Hackers network these infected computers to create botnets, stealing resources and further perpetuating their fraudulent activities.

Unfortunately, around the world, scenarios like these are unfolding at large enterprises and small businesses alike. A large and growing number of so-called "Web threats," like the ones described above but in an infinite number of varieties, are wreaking havoc, usually unbeknownst to the companies they affect. Cyber criminals are stealing lists of social security numbers from health care organizations, credit card numbers from financial institutions, proprietary information from technology companies, and resources from all industries. These compromised machines and identity thefts are eroding consumer confidence in the ability to maintain the privacy of their information, undermining online banking, transactions, and e-commerce.

III. WEB THREATS DEFINED

Web threats are any threat that uses the Web to facilitate cyber crime. They are sophisticated in their methods, using multiple types of malware and fraud, all of which utilize HTTP or HTTPS protocols, but can also employ other protocols as components of the attack, such as links in email or IM, or malware in attachments or on servers that access the Web.

The creators of such threats frequently update Web site content, variants, and malware types in order to evade detection and achieve greater success. Web threats based on malware are hidden within Web pages and victims are infected when they visit the page. Fraudulent sites mimic legitimate business Web sites and use social engineering to request visitors to disclose confidential information. Individuals once characterized as hackers, virus writers, spammers, and spyware makers are now simply known as cyber criminals with financial profit their primary aim.

Over the last 15 years, information security threats have evolved through a series of incarnations. In each case, malware writers and fraudsters sought out the medium that was most used and least protected (for example email). Today, a new wave of threats is emerging that uses the Web as a delivery vehicle. These Web threats are gaining traction at a time when the Web has become a major commerce engine as well as social networking vehicle, with usage continuing to grow. At the same time, the Web is relatively unprotected, compared to messaging for example, as a medium to deliver malware and conduct fraud. 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.” [4]

However, email is often a component of a Web threat attack, using social engineering to get users to follow links to dangerous sites. The growth of the Web 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, online banking, and e-commerce as well as the everyday lives of Web-savvy consumers.

Emerging Threats: Web 2.0

Web 2.0, the collection of next-generation interactive technologies bringing dynamic, rich content to social networking and information-sharing sites, provides many new threat vectors to cyber criminals. For example, the popular networking site facebook.com is a platform that allows third-party developers to create powerful scripted applications that can access user account details and execute within a browser window. Users can add additional applications and grant access permissions with just a few clicks, and when they do, on-site messaging encourages the user’s friends to do the same. This viral networking pattern opens the door for tremendously fast-spreading malware. The classic Web 2.0 exploit is the “Samy Worm” (JS.SPACEHERO) created by a teenager that infected over one million users in less than a day.

IV. WEB THREAT DELIVERY MECHANISMS

Web threats can be divided into two primary categories, based on delivery method – *push* and *pull*. Push-based threats use spam, phishing, or other fraudulent means to lure a user to a malicious (often spoofed) Web site, which then collects information and/or injects malware. Push attacks use phishing, DNS poisoning (or pharming), and other means to appear to originate from a trusted source. Their creators have researched their target well enough to spoof corporate logos, official Web site copy, and other convincing evidence to increase the appearance of authenticity.

Precisely-targeted push-based threats are often called “spear phishing” to reflect the focus of their data gathering (“phishing”) attack. Spear phishing typically targets specific individuals and groups for financial gain. In November 2006, a medical center fell victim to a spear phishing attack. Employees of the medical center received an email telling them they had been laid off. The email also contained a link that claimed to take the recipient to a career counseling site. Recipients that followed the link were infected by a keylogging Trojan. [5]

In other push-based threats, malware authors use social engineering such as enticing email subject lines that reference holidays, popular personalities, sports, pornography, world events, and other popular topics to persuade recipients to open the email and follow links to malicious sites or open attachments with malware that accesses the Web.

Pull-based threats are often referred to as “drive-by” threats, since they can affect any visitor, regardless of precautions. Pull threat developers infect legitimate Web sites, which unknowingly transmit malware to visitors or alter search results to take users to malicious sites. Upon loading the page, the user’s browser passively runs a malware downloader in a hidden HTML frame (IFRAME) without any user interaction.

Both push- and pull-based Web threat variants target infection at a regional or local level (for example, via local language sites aimed at particular demographics), rather than using the mass infection technique of many earlier malware approaches. These 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.

Case Study: “The Italian Job”
On June 15, 2007, a cyber criminal compromised nearly 6,000 Italian Web sites using three Trojans (software applications that claim to do one thing, but actually contain malicious code) that identified, stole, and uploaded personal information to a criminal network. The attack, which became known as “The Italian Job,” affected roughly 15,000 users over six days. While the damage caused by identity theft and fraud could easily reach millions of dollars, the cyber criminal who created the initial downloader used a malware kit (MPack v.86) that cost roughly $700 (USD).

V. BENEFITS FOR CYBER CRIMINALS

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 personally identifiable information (PII), data that can potentially be used to uniquely identify, contact, or locate a single person. Personally identifiable information is typically the precursor to identity theft, and therefore carries enormous value on the black market.

The other primary purpose of Web threats is the absorption of the infected PC into a criminal network (for example, a botnet), hijacking 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.

Of the 3.5 billion requests Trend Micro's Web Reputation™ service scans daily, nine million are malware-infected Web pages. According to Trend Micro research, while the number of conventional worms has grown only 22 percent since 2005, Web Threats have increased by 1,564 percent during the same period.

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. [6] Ivan Maksakov, Alexander Petrov, and Denis Stepanov extorted $4 million (USD) by unleashing a distributed denial-of-service attack on U.K. sports bookmakers. [7]

On the black market, cyber criminals typically pay $1,000-$5,000 (USD) for a Trojan horse, for example, that is able to steal online account information. [8] Yet, little is known about the scope of the profits in this sector, due to the underground nature of their behavior.

VI. WEB THREAT DAMAGES

Some aggregate data has been gathered on the financial impact of certain types of Web-based threats. For example, customers of various German banks remain victims of phishing despite using Transaction Authentication Numbers (TANs) in addition to user names and passwords. The Munich Police Department estimates that from January-July 2006 the damages due to online fraud exceeded 1 million Euro in that city alone. [9] The Gartner consultancy reports that phishing attacks cost consumers and businesses $3.2 billion in 2007, a cost of $886 per incident. [10] The same report shows a rise in phishing effectiveness as well, with the number of targeted victims losing money rising from 2.3 percent to 3.3 percent.

Trend Micro threat analytics shows that the growth in severe malware infections, such as viruses, Trojans, PHP scripts, VB Scripts, batch files, and rootkits, grew 200% throughout 2007, infecting more than one in eight PCs scanned. In addition to the potential data loss caused by these infections, “cleaning” infected machines requires substantial IT resources and lost employee productivity. Of the 3.5 billion requests Trend Micro’s Web Reputation™ scans daily, over nine million are for malware-infected Web pages.

9 million

Malware-infected Web pages scanned daily

Figure 1: Daily scans reveal a high number of malware infected Web pages

VII. CONVENTIONAL APPROACHES FAIL TO PROTECT AGAINST WEB THREATS

Web threat scanning has specific requirements that are not met by the traditional approach to virus scanning. Conventional 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. One reason is that the conventional approach to virus protection involves collecting samples of viruses, developing patterns, and quickly distributing these patterns to users. 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 (for example, spam, instant messaging, and Web sites), rendering the conventional sample collection, pattern creation, and deployment process insufficient.

Another reason that conventional virus detection processes fall short involves a fundamental difference between these viruses and evolving Web threats. Conventional viruses were fundamentally designed to spread as quickly as possible, and were therefore often easy to spot. With the advent of Web threats, malware has evolved from this outbreak model to stealthy “sleeper” infections that are therefore difficult to detect via conventional antivirus techniques.

Recovering from infections also presents new challenges. In some cases, Web threats may result in a system infection that is so extensive (for example, via a rootkit in which the system file is replaced) that conventional uninstall or system cleaning approaches become useless. Infected systems often require a complete system recovery, in which the hard drive is wiped and the operating system, applications, and user data are reinstalled.

Cyber criminals also take advantage of the need to keep port 80 open for legitimate traffic, which circumvents existing client and network firewalls. And some professional cyber criminals create exploits for unknown vulnerabilities, so that even on-time security patches are unable to prevent the impacts of these threats.

Profit-driven cyber criminals target and compromise not only the Windows Web server platform (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, may now be compromised.

Malware programs in Web threats also violate host intrusion prevention system (HIPS) rules. Once a malware program is installed, it continues to initiate other programs. Excessive false alarms annoy users to the point that they disable protection or allow the program to execute. In this way, the malware evades conventional HIPS techniques.

In addition, protecting against Web threats is more difficult than protecting against email-borne threats because of the much larger bandwidth needed to scan or filter the Web’s data stream. Email contains less than one thousandth the amount of data.

Web threats frequently combine a number of seemingly innocent programs to create a malicious result. Individual downloader programs – commonly used as part of Web threats – appear to be benign. In combination, 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 conventional means. For instance, a cyber criminal embeds a URL in an email 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 it detects a vulnerability, the malware attacks; if not, it downloads a file, tests for another vulnerability, downloads other files, and so on. Each session of the traffic appears to be benign, but the combined activities become a coordinated attack.

Web threats use a variety of tactics, for example, targeted local and regional attacks with customized spam language and Web sites. One security solution does not fit all threats; a sample collected for one targeted local attack, for instance, does not address other local attacks. The multiple delivery vehicles also render any solution that addresses only one vehicle obsolete. This means, for example, that URL filtering or spam filtering alone are insufficient. As a result, information security today is at a critical turning point: a new approach is needed to address the newest class of threats.

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

Clearly, users need a new approach to addressing Web threats that complements existing techniques. The most effective approach will employ multiple layers of protection and incorporate a range of protective measures. In addition, the evolving nature of the threat necessitates some form of information feedback and integration, in which information gathered in one portion of the protection network is used to update information in other layers. Any effective approach should also address all relevant protocols, because Web threats leverage multiple protocols in their attacks, in particular email as the initial delivery mechanism and the Web as the threat host. However, other mechanisms can also help perpetrate attacks such as links in IM and infected files. Coordinating measures requires efficient, centralized management of region-specific expertise to help address the regional, and even localized nature of many of the threats.

The key to effectively addressing Web threats is a multi-layered approach. The network points are categorized in four different layers (see Figure 2): 1) “in-the-cloud” (i.e. before the traffic reaches the Internet gateway), 2) at the Internet gateway, 3) across the network servers, 4) and at the endpoint (for example, the client). In the below example, the description uses the points in the network for high level organization and describes the protocol protection and security technologies that can be deployed at these points. The subsections on protocol protection and security technologies describe email solutions first, which is often the first step in a Web threat attack, followed by Web solutions that directly protect Web usage.

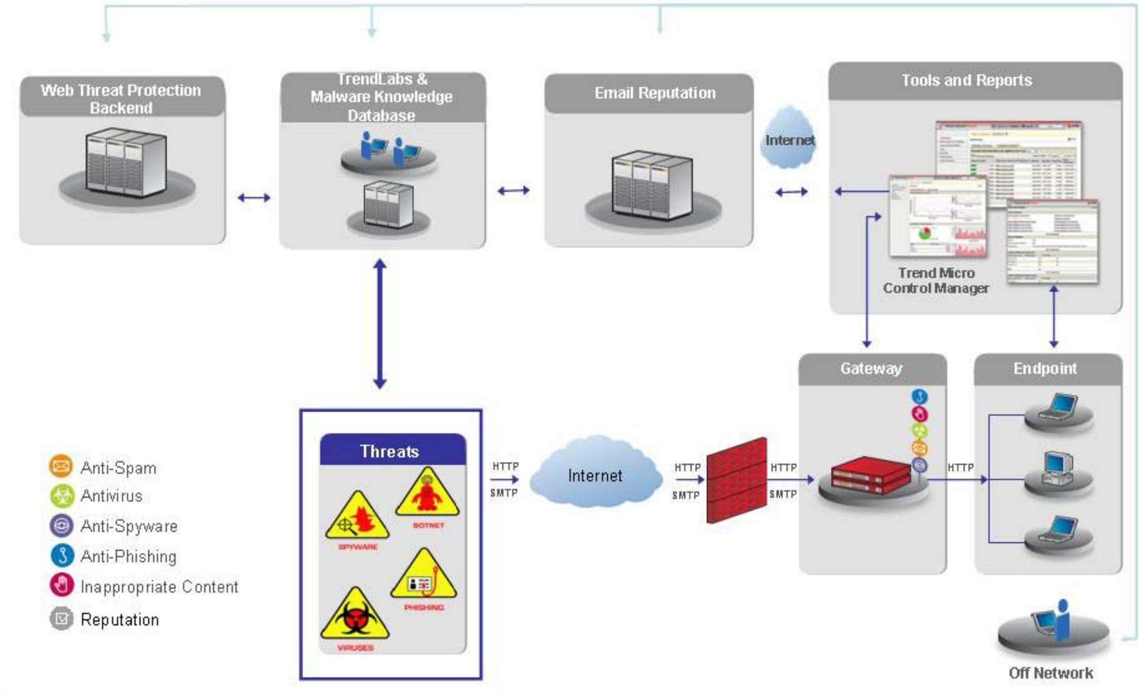

Figure 2. A multi-layered approach is needed to protect against the broad range of Web threats.

IN-THE-CLOUD

Internet-based “in-the-cloud” services can provide full security solutions or deploy specific technologies that supplement on-site products. These in-the-cloud services reduce the load on the network and enable the rapid exchange of information necessary to respond to threats as they appear.

IN-THE-CLOUD PROTOCOL PROTECTION

A comprehensive security solution can be provided in the cloud, similar to an on-site solution, but with the added benefit of keeping threats completely off the network. For example, a hosted email security solution removes all email threats in the cloud and only delivers legitimate email to the organization’s network, providing the following benefits: less email traffic to the gateway, no security hardware or software on site; less administration; more bandwidth, less processing power required, and less storage and archiving of emails necessary to comply with regulatory requirements. These benefits provide a more cost-effective solution. Web threats often use email as a medium to deliver an initial Web link. Hence, intercepting emails carrying Web threats in-the-cloud can prevent many Web threats from even entering the network.

IN-THE-CLOUD SECURITY TECHNOLOGIES

Even if security solutions are deployed on site, many of the security technologies can be housed in the cloud, enabling a smaller footprint on the network as well as real-time security updates based on global, integrated information queried through the in-the-cloud service. These services should include the following components (see Figure 3).

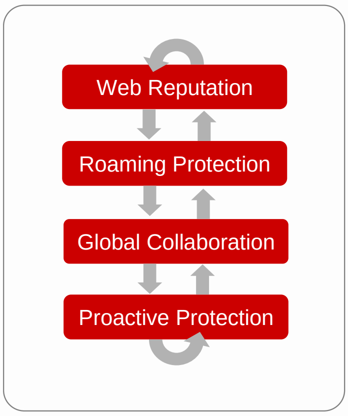

Figure 3: Key factors required for proper protection.

Email Reputation Services. Effective Email Reputation services can stop up to 80 percent of email-based threats, including emails with links to dangerous Web sites, before these threats reach the network based on the reputation of the sender. An extensive analysis of an IP addresses' behavior, scope of activity, and prior history is required. The service should reference email IP addresses against a database of known spam sources as well as provide a dynamic service that can assess email sender reputation in real-time, blocking threats from zombies and botnets when they first emerge. The reputation status must be continually updated ensuring that a good reputation is restored when infected zombies are cleaned and resume sending legitimate email.

Malware Knowledge Database. When security companies store their applications' malware databases locally at the client level, those clients are only protected against malware identified in the latest patch or system update. Conversely, moving the malware knowledge database to the Internet maintains a centralized repository of the most up-to-date threat information, guaranteeing that customers are protected against new malware as soon as it is discovered.

Web Reputation Services. Web Reputation services help protect against Web-based threats before they even touch the network. Web reputation assigns a relative reputation score to domains, based on a number of factors, including evaluation of a site's age, any historical location changes, and other factors that might indicate suspicious behavior. The service then builds on this assessment through malware behavior analysis, monitoring network traffic to identify any malware activity originating from a domain. It should also perform Web site content crawling and scanning to complement this analysis with a block list of known bad or infected sites. To reduce false positives and increase the accuracy of protection, Web reputation should assign reputations to specific pages or links, rather than an entire site, as sometimes only portions of a legitimate site are hacked.

Global Research and Support. A global network of research, service, and support centers that are committed to constant threat surveillance and attack prevention is another important component of in-the-cloud protection. An extensive global customer base combined with direct threat research and threat detection technologies are necessary to stop new attacks as they surface.

REAL-TIME SERVICE FEEDBACK AND INTEGRATION

Working together, these in-the-cloud services can provide continuous threat intelligence and a comprehensive threat assessment in real-time, with each service bolstering the others. For example, an email from a seemingly "good" IP address might pass an Email Reputation check, but Web Reputation might identify a download from a "known bad" Web site when a user clicks a link. When Web Reputation stops the malicious download before it hits the network, Email Reputation adds the email's IP address to its list of known bad senders.

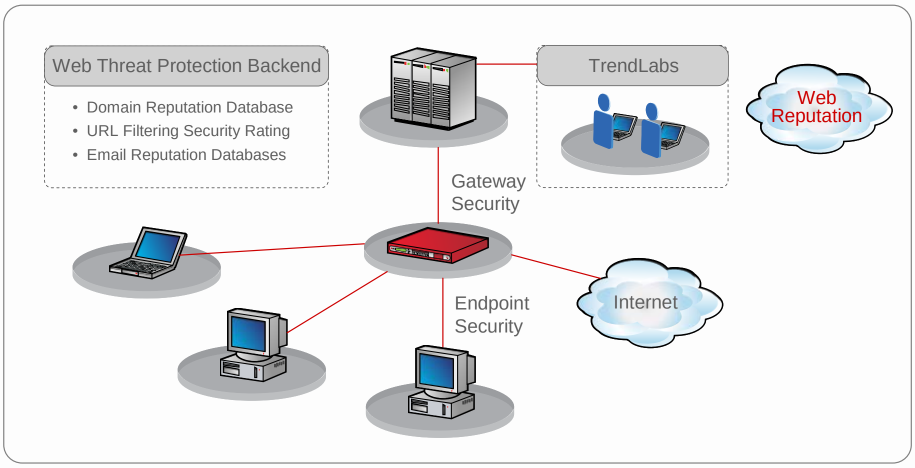
Web Threat Protection Backend
• Domain Reputation Database
• URL Filtering Security Rating
• Email Reputation Databases
TrendLabs
Web Reputation
Gateway Security
Endpoint Security
Internet

Figure 3. Working together, Trend Micro's in-the-cloud services provide a layer of comprehensive, updated protection.

AT THE INTERNET GATEWAY

Important functions are also needed at the second of the four levels, the Internet gateway. Gateway security solutions and technologies are critical to preventing threats from further permeating the network.

GATEWAY PROTOCOL PROTECTION

As the initial network entry point, the gateway is an ideal location to block Web threats. Security solutions should be implemented to block emails with links and attachments that are components of Web threats, as well as Web security that directly protects Web usage.

GATEWAY SECURITY TECHNOLOGIES

Just as sender or source based technologies are best placed in-the-cloud, content scanning technologies are most appropriately conducted in on-site solutions. The following technologies require content inspection. They are applied to gateway protection to stop threats at the earliest entry point.

Embedded Link Reputation. Web threats often use links embedded in emails to take users to malicious sites. Reputations can be assigned to URLs in links and can be used to block emails with links to malicious Web sites. This reputation information can also be integrated with the Email Reputation and Web Reputation information discussed above. If a bad reputation is assigned at any single point (email sender, embedded URL, or Web site), the bad reputation can be extended to all elements of the Web threat attack.

File Checking. Gateway capabilities should include file checking. For emails, any attached files should be scanned for malware, including antivirus, anti-spyware, and other malware protection. Malware in email attachments, if installed, can access the Web as an implementation mechanism. Files should also be checked on the Web itself. 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. A reputation may not yet be assessed for a Web site that contains a malicious file.

Behavior Analysis. The next form of protection from Web threats that is needed at the gateway is behavior analysis that can correlate combinations of activities to determine if they are malicious. Often a single activity or component of a Web threat may appear innocuous, but when several activities are used in conjunction, they create a malicious result. A holistic view across the different components may be required to determine if a Web threat is present. This approach is similar to the behavior analysis performed by virus scanners to locate new, undiscovered viruses. Behavior analysis should correlate activities of a single session on the same protocol (for example, an SMTP attachment with a suspicious double extension) as well as activities during multiple network connection sessions on the same protocol (for example, a downloader blended threat in which individual files that each appear to be innocent are downloaded, but together they form a malicious program). In addition, activities of multiple sessions and different protocols (for example, SMTP and HTTP) should be correlated to identify suspicious combinations of activities (for example, an email with a URL link to several recipients, and an HTTP executable file download from the linked Web page).

Across the Network Servers

For comprehensive Web threat protection, security solutions must be deployed across the entire network, including on network servers.

NETWORK SERVER PROTOCOL PROTECTION

The mail servers are another opportunity to block email and attachments that may be components of a Web threat. Security at the mail server is required to protect interoffice email, mail from remote users logging back onto the network, and the mail store. The emails may have dangerous links and the attachments and mail store may be harboring malware that access the Web.

Other servers may be infected with Web threat malware and other protocol protection can be deployed on network servers, including security that protects Instant Messaging (IM) with malicious links or downloads and collaborative environments that might share infected files.

NETWORK SERVER SECURITY TECHNOLOGIES

Some of the technologies deployed at the gateway are also used to secure other network servers with the technology targeted and customized for the specific protection point. For example, IM security should include link reputation and all network security should include malware protection with file checking and behavior analysis.

At the Endpoint

In addition to the other protection points, a fourth level of protection at the endpoint (the client) remains critical. Approximately two-thirds of recent U.S. computer retail sales are notebook computers. [11] 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.

A client can play many roles in a Web threat. The user can access their email or the Web through the client. In addition, if a notebook computer has been compromised 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 malware case, this activity can be detected and blocked, and a clean-up operation can be directed if needed. Therefore, a solution is needed that provides client-level prevention (e.g. access control and scanning), and in case of infection, cleaning and recovery.

ENDPOINT PROTOCOL PROTECTION

A single endpoint solution can provide protection for multiple protocols, securing the many uses of the client. In particular, endpoint security can provide safeguards during Web browsing, applying Web security policies both while a user is on and off the network, and can help to identify and clean up malware infections.

ENDPOINT SECURITY TECHNOLOGIES

Endpoint protection utilizes several of the technologies mentioned above, such as Web Reputation and malware scanning targeted for the client. However, additional technologies are required to meet the unique security needs of endpoint computers.

Virtual Environment. 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 and Recovery. 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 to allow only limited access to the network to complete cleaning. Complete system restorations are also needed in cases when clean-up is not feasible due to a rootkit infection, for example.

IX. INTEGRATING THE LAYERS: FEED-THROUGH AND LOOP-BACK

Figure 4 illustrates this multi-layered approach, and also shows an important and much needed aspect of its implementation: Incorporating layers of protection in-the-cloud, at the gateway, across the network servers, 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 provide Web Reputation with site-threat correlation data and update Email Reputation’s list of known bad IPs and domains. Similarly, information acquired at the endpoint can be looped back to the file scanning capability at the gateway, network servers, and the Web reputation capability in-the-cloud. Both feed-through and loop-back techniques are needed to ensure real-time, Web threat protection across the entire network. The greater the number of customer sensors providing threat content, the stronger the protection becomes, creating “better together” security through a strong neighborhood watch.

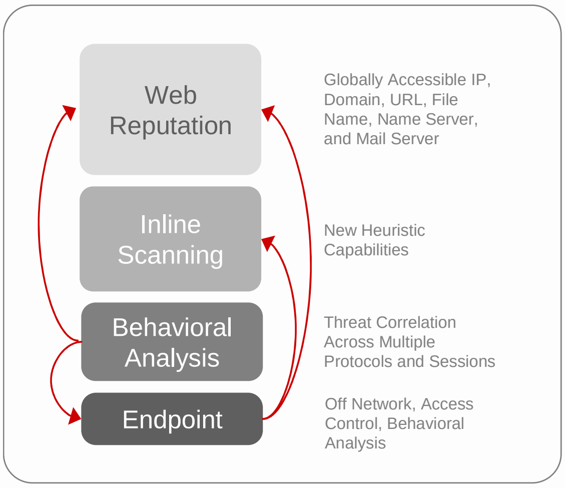
Web Reputation
Globally Accessible IP, Domain, URL, File Name, Name Server, and Mail Server
Inline Scanning
New Heuristic Capabilities
Behavioral Analysis
Threat Correlation Across Multiple Protocols and Sessions
Endpoint
Off Network, Access Control, Behavioral Analysis

Figure 4. 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.

X. TREND MICRO WEB THREAT PROTECTION

TREND MICRO PROTECTION NETWORK

Trend Micro's Protection Network incorporates multi-layered information protection technologies in the cloud, at the gateway, within the network, and on the client PC, all working seamlessly together to proactively respond to internal and external threats (see Figures 6 and 7). The real-time, in-the-cloud nature of much of the Trend Micro Protection Network technologies reduces the reliance upon conventional pattern files and the protection delays conventionally associated with updates. Built-in feedback loops and communication between Trend Micro products ensures rapid and optimal protection against the latest threats and provides "better together" security. Not only does adding more Trend Micro products protect additional points in the network, each additional product enhances the protection provided by all deployed Trend Micro solutions.

With accurate, real-time data provided by components of Trend Micro's Protection Network, TrendLabs staff of more than 1000 security experts detects, pre-empts, and eliminates threats. TrendLabs operates 24/7, with offices in the Philippines, United States, Japan, France, Germany, and China. Trend Micro uses a combination of technologies and data collection methods including "honey pots" for email and network worms, Web crawlers, and its IP reputation services to proactively gain intelligence about the latest threats. And its global, multi-lingual staff can respond in real-time, providing constant threat surveillance and attack prevention and minimizing the damages and costs of new Web-based threats.

Trend Micro supplements TrendLab's proactive identification of Web threats in the wild with feedback from its extensive global network of users, providing a comprehensive, up-to-date threat index. By allowing its users to opt into a global collaboration system, Trend Micro can use real-time information from infected users to isolate threats as they appear and push updates to all levels of its protection tiers. Trend Micro uses that information in the cloud in real-time in its industry-leading Web Reputation, which maintains risk profiles of Web pages. This information is also used to support Email Reputation which applies over a decade of reputation information with ratings assigned to over 1.6 billion IP addresses. The data from TrendLab's research and the user network also supports embedded URL reputation, which is used to block dangerous links in email as well as IM security. And all of these types of reputation protection communicate with each other to provide a bad reputation across all elements of a Web threat attack.

TREND MICRO PRODUCTS AND SERVICES

Trend Micro provides solutions that, when used together, provide Web threat protection across the network. Trend Micro behavior monitoring technology scans the entire network detecting threats across nearly 50 different protocols within a single session, helping to trace the root cause of the original threat to identify potential security risks. Patent-pending technology correlates independent events to identify the sources of malicious threats, such as tracing a malicious URL to its origin in an IM session.

Comprehensive gateway Web threat protection is provided by combining InterScan Messaging Security and InterScan Web Security solutions. Together these solutions stop Web threats at all points of the attack—in email links, attachments, and the browser. These solutions are offered as software or as an appliance. The InterScan Messaging Security solution is also available as an in-the-cloud hosted service, keeping all email threats off the network.

Several products are available to protect the various servers across the network. ScanMail provides security for the mail server, both for Microsoft Exchange and Lotus Domino environments. Instant Messaging Security protects IM for Live Communications Server and PortalProtect safeguards the SharePoint environment, providing layered protection for Windows solutions. ServerProtect secures a variety of server platforms.

At the endpoint, Trend Micro offers its award-winning OfficeScan integrated client and server security solution. OfficeScan provides access control, safe Web browsing with Web Reputation, malware protection for viruses, spyware, and rootkits, as well as security even for roaming users when they are both on and off the network.

Trend Micro's Worry-Free Security Solutions provide all-in-one integrated protection against Web and other emerging threats in solutions specifically designed for businesses with limited IT resources.

Trend Micro also provides cleaning and recovery services, feed-through and loop-back mechanisms between these capabilities, and centralized management via Trend Micro Control Manager. Trend Micro provides these capabilities in form factors that suit consumers and organizations of all sizes—small and medium businesses, enterprises, and service providers.

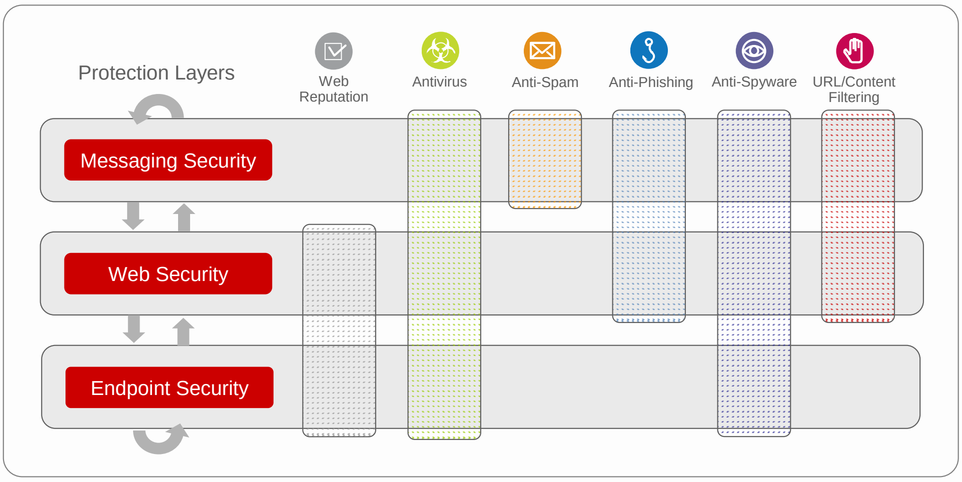

Figure 6. Trend Micro offers best-in-class defense technologies that protect against Web threats in a multi-layered deployment.

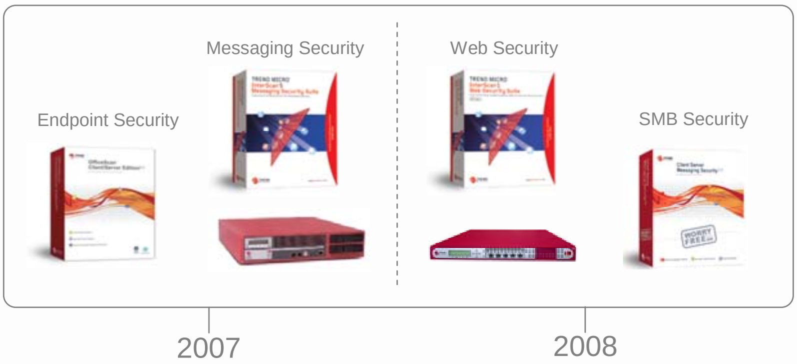

Figure 7. Timeline for commercial availability of enhanced Trend Micro protection against Web threats

XI. CONCLUSION

Web threats are prevalent 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 - the Web - make Web threats the most challenging threat that consumers, businesses, and services providers, have faced in a long time. Potential costs associated with these threats include confidential information leakage and theft of network resources, with the adverse impact of erosion of customers, trust, and brand reputation; regulatory and legal implications; negative public relations; and loss of competitive advantage. Because conventional 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 real-time, comprehensive protection against these threats.

XII. REFERENCES

1. Gregg Keizer, Computerworld, August 19, 2007, “Identity attack spreads; 1.6M records stolen from Monster.com,” http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9031418&pageNumber=1.

2. Dan Kaplan, SC Magazine, October 30, 2007, “FTC Spam Contains Keylogging Trojan”, http://www.scmagazineus.com/FTC-spam-contains-keylogging-trojan/article/58273/

3. Paul F. Roberts, eWeek.com, December 16, 2005, “Spear Phishing Attack Targets Credit Unions,” http://www.eweek.com/article2/0,1895,1902896,00.asp.

4. 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.

5. Cara Garretson, NetworkWorld.com, January 11, 2006, “Spam that Delivers a Pink Slip” http://www.networkworld.com/news/2006/110106-spam-spear-phishing.html

6. Gregg Keizer, TechWeb Technology News, January 24, 2006, “Botnet Creator Pleads Guilty, Faces 25 Years,” http://www.techweb.com/wire/security/177103378.

7. 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.

8. 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-hackerforums_x.htm.

9. Police of the City of Munich, August 25, 2006, http://www.sueddeutsche.de/,tt3m3/muenchen/artikel/612/83529.

10. Avivah Litan, “Phishing Attacks Escalate, Morph, and Cause Considerable Damage,” Gartner, December 12, 2007.

11. 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.

TREND MICRO INCORPORATED

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

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1 +800-228-5651
phone: 1 +408-257-1500
fax: 1 +408-257-2003
www.trendmicro.com

TREND MICRO™