Volume 2, No. 3, May-June 2011

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# Challenges and Countermeasures for Web Applications

Mayank Sharma
Associate Professor (IT),
Aurora's Engineering College
Bhongir, Andhra Pradesh, India
Mayank_sharma04@yahoo.com

Pragati.G
Aurora's Engineering College
Andhra Pradesh, India
Pragati_g@yahoo.co

O.Nagamani*
Aurora's Engineering College
Bhongir, Andhra Pradesh, India
nagmani53@gmail.com

***Abstract:*** A web threat is any threat that uses the internet to facilitate cybercrime. Web threats use multiple types of malware and fraud, all of which utilize HTTP or HTTPS protocols, but may also employ other protocols and components, such as links in email or IM, or malware attachments or on servers that access the Web. They benefit cybercriminals by stealing information for subsequent sale and help absorb infected PCs into botnets.nature system for which signing ensures. Web threats pose a broad range of risks, including financial damages, identity theft, loss of confidential information/data, theft of network resources, damaged brand/personal reputation, and erosion of consumer confidence in e-commerce and online banking. Cyber crime is the latest and perhaps the most complicated problem in the cyber world. "Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime", "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime"

***Keywords:*** Web Threat, Cyber Crime, Security.

## I. INTRODUCTION

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. 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.

## II. DEFINING WEB THREATS

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.

## III. WEB THREAT DELIVERY MECHANISMS

Web threats can be divided into two primary categories, based on delivery method – *push* and *pull*. Pushbased 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, 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.

## IV. 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. 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.

## V. NTIONAL 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 vulnerability, 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.

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.

## VI. NEW APPROACH:INTEGRATED, MULTI-LAYEREDPROTECTION

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.

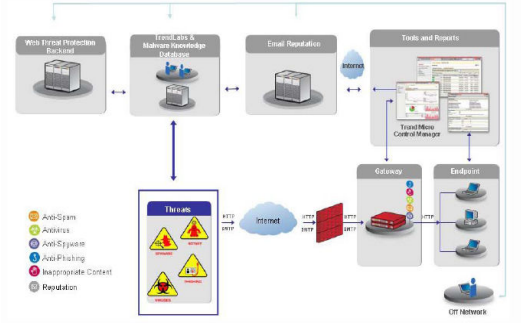


**Figure 1: A Multi Layered Approach**

The key to effectively addressing Web threats is a multi-layered approach. The network points are categorized in four different layers (see Figure 1): 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. 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,

### *A. 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.

### *B. 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.

### *C. 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 for Protection**

## VII. CONCLUSION

Web threats are prevalent today and are growing in umbers and impact. Their complexity, large number of variants, nd 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, usinesses, 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.

## VIII. 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.