Protecting Data From the Cyber Theft – A Virulent Disease

[1]Dr. S.N. Panda and [2]Vikram Mangla
[1]Professor & Principal, [2]Assistant Professor
[1] RIMT-IMCT, Mandi Gobind Garh, Punjab.
[2]Chitkara Institue of Engineering & Technology, Rajpura, Punjab.
[1] panda.india@gmail.com, [2] mangla.vikram@gmail.com

***Abstract* - Network security policies are essential elements in Internet security. Network security perimeter devices such as firewalls, IPSec, and IDS/IPS devices operate based on locally configured policies. Malware-related data breaches have reached pandemic proportions as criminals discover that Internet crime is easy to commit, highly lucrative, and largely under-policed. With a few hundred dollars, a cyber criminal can begin a career of breaking into computers to steal identity and confidential data for sale to the highest bidder. This paper will cover current and emerging trends of stealth malware, such as moving primarily to the Web since most organizations allow Web traffic into the network. It will also cover new advances in network security technologies that use multi-phase heuristic and virtual machine analysis to detect and mitigate the damages that result from malware-related data thefts.**

***Index Terms* - Network Security, Web Threats, Malware, Phishing**

I. INTRODUCTION

With the global connectivity provided by the Internet, network security has gained significant attention in research and Industrial communities. Due to the increasing threats of network attacks, network security devices such like firewalls and IPSec gatewaye have become important integrated elements not only in enterprise networks but also in small size and home networks. 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. Malware-related data breaches have reached pandemic proportions as criminals discover that Internet crime is easy to commit, highly lucrative, and largely under-policed. With a few hundred dollars, a cyber criminal can begin a career of breaking into computers to steal identity and confidential data for sale to the highest bidder. Fraudsters who purchase the data have developed a variety of schemes to monetize that information ranging from transacting unauthorized stock trades to transferring funds to offshore bank accounts. The cyber crime economy is so robust that there is a vibrant market for professional malware toolkits available for $500 to $1,000 and come pre-configured with a range of attack modules, exploit ‘maintenance’ updates, and 24 x 7 online technical support.

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, and 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.

In August 2007, a 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

doi:10.4304/jetwi.2.2.152-155

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.

II. 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 spy ware 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]

III. 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.

IV. Today's Insider - Threat Is Stealth Malware

Law enforcement, computer crime experts, and even the military are playing catch up to the threat posed to consumers, businesses, and national security as cyber criminals cash in on stolen identity data, fraudulent online transactions, and cyber espionage. It is no surprise that the rise in cyber crime has coincided with the increased use of the Internet and especially "Web 2.0" technologies.

Web sites and applications now support user-contributed content, syndicated content, iframes, third-party widgets (or applets), and convoluted advertising distribution networks into which 'stealth' malware can easily be injected somewhere along the line. In a 2007 USENIX paper, Google researchers determined that approximately 9% of all suspicious web sites launched "drive-by" downloads of stealth malware binaries[12]. Government studies[13] estimate that 65% of all exploits now enter via the Web and IBM Internet Security Systems (ISS) estimates that nearly 100% of Web attacks now utilize obfuscated JavaScript as a very effective technique to bypass antivirus and intrusion prevention.

Today, once a PC is infected with stealth malware, it typically opens two-way communications to a “command and control” (C&C) server to establish a channel back to the cyber criminal. This allows the “bot” (as in “robot computer”) to report status as well as any valuable information that is immediately accessible. Groups of these remotely controlled, malware-infected computers are commonly called botnets, and serve as the foundation of most cybercrime on the Internet.

How do victims get infected? A user may be drawn by a phishing e-mail to a Web site hosted on a hijacked server, which serves up a browser exploit; this downloads and installs a bot on the user’s PC. The bot then downloads more malware like “keyloggers” that silently record keyboard and mouse activities to execute further criminal activities, such as stealing user credentials and capturing other sensitive information. All of this takes place without the knowledge of the user or administrator. As their prevalence has increased, remote-control malware/botnets have become serious concerns for security administrators.

The recent January, 2009 malware-related data thefts at Heartland Payment Systems and earlier malware infiltrations at Hannaford Supermarkets, University of Florida Medical Center, and NASA underscore the escalating threat of malware-related data breaches. The Identity Theft Resource Center, a nonprofit group focused on understanding and preventing identity theft, reported that 656 known security breaches had taken place in 2008, reflecting a 47 percent increase over 2007’s total. As of March 17, 2009 the resource center had already reported 110 breaches in 2009.

Recent Research[14] Has Found:
11 % of the world’s computers are enmeshed in at least one botnet
23 % of home computers become infected despite having security enabled
72 % of corporate networks larger than 100 PC’s have an infection

V. Stealth Malware Attacks Are Outmaneuvering Conventional Defenses

Defending corporate networks from today’s malware-related data thefts requires modern protection that goes beyond current signature- and heuristic-based detection techniques. Modern threats exploit the inability of conventional network protection to provide a unified defense against a criminal who attacks on multiple fronts, from OS and browser vulnerabilities to social engineering. The anachronistic concept of detecting infections with a single technique, such as signatures, has left many businesses and consumers open to attack, despite their deployment of antivirus and IPS (intrusion prevention systems). The sheer volume and escalating danger of modern attacks are overwhelming limited IT resources and outmaneuvering conventional defenses that may already be in place. To enable a more efficient IT security process, accurate and timely identification of infected machines is the first step in preventing malware-related data breaches. And, the only viable solutions are those that provide thorough coverage across the many vectors that are used in attacks.

VI. 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.

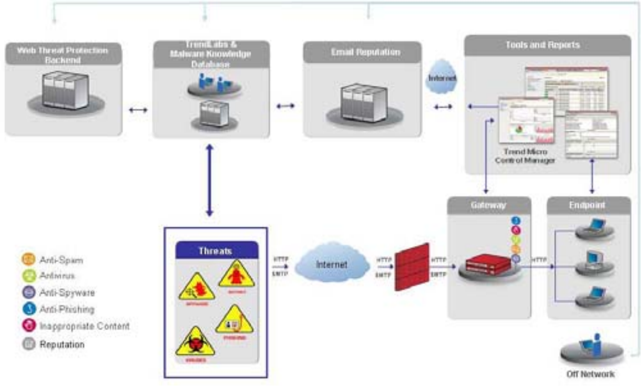
The large numbers of variants use multiple delivery vehicles (for example, spam, instant messaging, and Web sites), rendering the conventional sample collection, pattern creation, and deployment process insufficient. Another reason that conventional virus detection processes fall short involves a fundamental 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.

VII. Future work

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.



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

DNA of an Ideal Solution:

Dynamic, real-time detection of threat: Finds the latest stealth, 0-day attacks

Accurate detection: No false positives, and no false negatives

Return on security investment: Easy to install, manage, support and scale

VIII. 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.

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.
12. Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, and Nagendra Modadugu: The Ghost in the Browser Analysis of Web-based Malware, May 2007.
13 David Barroso, ENISA Position Paper No. 3: Botnets – The Silent Threat, November 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_botnets.pdf.
14 Panda Security, http://www.pandasecurity.com/homeusers/media/press-releases/viewnews?noticia=9077

Call for Papers and Special Issues

Aims and Scope

Journal of Emerging Technologies in Web Intelligence (JETWI, ISSN 1798-0461) is a peer reviewed and indexed international journal, aims at gathering the latest advances of various topics in web intelligence and reporting how organizations can gain competitive advantages by applying the different emergent techniques in the real-world scenarios. Papers and studies which couple the intelligence techniques and theories with specific web technology problems are mainly targeted. Survey and tutorial articles that emphasize the research and application of web intelligence in a particular domain are also welcomed. These areas include, but are not limited to, the following:

- Web 3.0
- Enterprise Mashup
- Ambient Intelligence (AmI)
- Situational Applications
- Emerging Web-based Systems
- Ambient Awareness
- Ambient and Ubiquitous Learning
- Ambient Assisted Living
- Telepresence
- Lifelong Integrated Learning
- Smart Environments
- Web 2.0 and Social intelligence
- Context Aware Ubiquitous Computing
- Intelligent Brokers and Mediators
- Web Mining and Farming
- Wisdom Web
- Web Security
- Web Information Filtering and Access Control Models
- Web Services and Semantic Web
- Human-Web Interaction
- Web Technologies and Protocols
- Web Agents and Agent-based Systems
- Agent Self-organization, Learning, and Adaptation
- Agent-based Knowledge Discovery
- Agent-mediated Markets
- Knowledge Grid and Grid intelligence
- Knowledge Management, Networks, and Communities
- Agent Infrastructure and Architecture
- Agent-mediated Markets
- Cooperative Problem Solving
- Distributed Intelligence and Emergent Behavior
- Information Ecology
- Mediators and Middlewares
- Granular Computing for the Web
- Ontology Engineering
- Personalization Techniques
- Semantic Web
- Web based Support Systems
- Web based Information Retrieval Support Systems
- Web Services, Services Discovery & Composition
- Ubiquitous Imaging and Multimedia
- Wearable, Wireless and Mobile e-interfacing
- E-Applications
- Cloud Computing
- Web-Oriented Architectrues

Special Issue Guidelines

Special issues feature specifically aimed and targeted topics of interest contributed by authors responding to a particular Call for Papers or by invitation, edited by guest editor(s). We encourage you to submit proposals for creating special issues in areas that are of interest to the Journal. Preference will be given to proposals that cover some unique aspect of the technology and ones that include subjects that are timely and useful to the readers of the Journal. A Special Issue is typically made of 10 to 15 papers, with each paper 8 to 12 pages of length.

The following information should be included as part of the proposal:

- Proposed title for the Special Issue
- Description of the topic area to be focused upon and justification
- Review process for the selection and rejection of papers.
- Name, contact, position, affiliation, and biography of the Guest Editor(s)
- List of potential reviewers
- Potential authors to the issue
- Tentative time-table for the call for papers and reviews

If a proposal is accepted, the guest editor will be responsible for:

- Preparing the “Call for Papers” to be included on the Journal’s Web site.
- Distribution of the Call for Papers broadly to various mailing lists and sites.
- Getting submissions, arranging review process, making decisions, and carrying out all correspondence with the authors. Authors should be informed the Instructions for Authors.
- Providing us the completed and approved final versions of the papers formatted in the Journal’s style, together with all authors’ contact information.
- Writing a one- or two-page introductory editorial to be published in the Special Issue.

Special Issue for a Conference/Workshop

A special issue for a Conference/Workshop is usually released in association with the committee members of the Conference/Workshop like general chairs and/or program chairs who are appointed as the Guest Editors of the Special Issue. Special Issue for a Conference/Workshop is typically made of 10 to 15 papers, with each paper 8 to 12 pages of length.

Guest Editors are involved in the following steps in guest-editing a Special Issue based on a Conference/Workshop:

- Selecting a Title for the Special Issue, e.g. “Special Issue: Selected Best Papers of XYZ Conference”.
- Sending us a formal “Letter of Intent” for the Special Issue.
- Creating a “Call for Papers” for the Special Issue, posting it on the conference web site, and publicizing it to the conference attendees. Information about the Journal and Academy Publisher can be included in the Call for Papers.
- Establishing criteria for paper selection/rejections. The papers can be nominated based on multiple criteria, e.g. rank in review process plus the evaluation from the Session Chairs and the feedback from the Conference attendees.
- Selecting and inviting submissions, arranging review process, making decisions, and carrying out all correspondence with the authors. Authors should be informed the Author Instructions. Usually, the Proceedings manuscripts should be expanded and enhanced.
- Providing us the completed and approved final versions of the papers formatted in the Journal’s style, together with all authors’ contact information.
- Writing a one- or two-page introductory editorial to be published in the Special Issue.

More information is available on the web site at http://www.academypublisher.com/jetwi/.

(Contents Continued from Back Cover)