

Blended Threats: Sophisticated, Elusive, and Dangerous

Blended Threats: Sophisticated, Elusive, and Dangerous.

In 1939 Winston Churchill described the Soviet Union's elusive military strategy as, "...a riddle wrapped in a mystery inside an enigma." Nearly seventy years later, that description could easily be applied to a new kind of stealth computer warfare; blended threats.

Overview

A blended threat is an attack on a single computer or a network that uses multiple malicious techniques in order to maximize the severity of the harm it causes and the speed with which it infects as many users as possible. Blended threats defy simple categorization. They often combine the attributes of viruses, worms, and denial-of-service attacks while also exploiting vulnerabilities in physical systems.

In response to the proliferation of blended threats, iS3 has enhanced STOPzilla's detection capabilities and upgraded its SITEguard™ functionality which now uses multiple technologies to protect users from malicious Web sites of all kinds.

The Nature of the Beast

Blended threats have become the preferred weapon of hackers because they can be both elusive and smart. For example, e-mail blended threats use active content such as Java, JavaScript, or ActiveX, or embedding URLs in the e-mail to link the user to Web sites where malicious programs can be downloaded in the background. These attacks are missed by anti-virus products looking for malware as e-mail attachments, and by Web filters that focus on content, not viruses and spyware. Programmed to be smart, blended threats will attempt to attack a system in a number of different ways. One of the most successful blended threats, Nimda, injected malicious code into each .EXE file on the system, created read-and-writable network shares worldwide, made numerous registry changes, and injected script code into HTML files. Damage was inflicted at multiple points throughout the victims' systems.

Some blended threats do not even require the user to click on links in the e-mail or visit a site. Content embedded in the e-mail can be activated via the preview panel of the user's e-mail program.

Mostly, a blended threat is distinguished by its intention to cause real harm to the recipient. As such, it differs from early malware which was written primarily to showcase the technical prowess of its creators. The newest blended threats invariably include crimeware; a class of malware designed specifically to automate financial crime; stealing sensitive data such as passwords, logins, bank credentials, and other personal identifiers that can be used for identity theft and other fraudulent activities. Perhaps most troublesome of all, blended threats are not one-time attacks. While the malicious program is installing a keylogger on the PC to capture data that the user enters via the keyboard, that machine is also being turned into a spam zombie capable of launching thousands of unsolicited spam e-mails.

The Tools

The following are a few of the techniques that hackers use to cause widespread damage:

Spamming: Spam is anonymous, unsolicited bulk e-mail. It is estimated that at least 85% of all e-mail worldwide is spam. In addition to wasting people's time, this electronic junk mail also eats up a lot of network bandwidth. While the most widely recognized form of spam is e-

mail spam, spam is also found in other media, such as instant messaging, Web search engines, blogs, wikis, etc. In addition to advertising questionable goods and services, spam is often used for financial scams, so-called charities, chain letters, and vehicles for spreading malware. Spamming techniques are often used for phishing.

Phishing: Phishing is a technique to obtain personal data. Typically, the phisher sends a spam e-mail that appears to come from a legitimate business — most often a financial institution — requesting "verification" of information or warning that the user's account has been frozen, or some other extreme action has or will take place unless the user acts immediately. The letter usually contains a link to a fraudulent Web page that looks legitimate — with company logos and content — and displays fields for inputting personal data such as account number, PIN, social security number, credit card number, etc. Phishing in itself is a blended threat. It uses social engineering techniques to manipulate people into performing actions and divulging confidential information, in combination with technical subterfuge, the creation of a fraudulent Web site used to capture this sensitive information. More than 90% of phishing attacks involve counterfeiting the Web sites of financial institutions. Security in this market sector is improving and users are becoming suspicious of e-mail from financial institutions. Hackers are expanding their horizons accordingly, now beginning to focus their efforts on social networking sites, healthcare sites, education sites, and special interest sites of all kinds.

Botnets: A botnet is a number of computers with Internet access that have been programmed in stealth to forward transmissions (including spam or viruses) to other computers on the Internet. This is done without the knowledge or consent the computers' owners. Botnets infect thousands of computers and turn them into zombies that are remotely controlled by "bot herders." Using the aggregate computing power of hundreds or even thousands of infected machines, spammers can send out hundreds of thousands of unsolicited bulk e-mails, many of which are phishing e-mails. Blended threats can be designed to spread via botnets, without any human interaction, which accounts for the speed with which they infect enormous numbers of users. The hacker who sells a user's personal data also makes money selling a percentage of that computer's processing power to spammers. Many ads for "Viagra," counterfeit high-end watches, or solicitations for pump-and dump stock scams are sent out by unsuspecting computer owners whose machines have been turned into zombies without their knowledge or consent. Zombies are also used to host phishing sites; fraudulent sites that counterfeit the look and feel of legitimate sites.

Spyware: Spyware is potentially unwanted software that gathers information from a user's computer without knowledge or consent; reports the information to the creator of the software or to one or more third parties; is installed on a user's computer without having given adequate notice to the user; and provides the user with little or no control over removing the software.

Blended threats reach their targets because many individuals and businesses implement only one form of computer security, such as a firewall, anti-spam or antivirus. When a sophisticated blended threat encounters an obstacle posed by a security application, it is smart enough to try another venue of attack.

Protecting Your System

One weak link in your security perimeter can compromise your entire system. Therefore, the best defense against blended threats is unified threat management; the broad, robust protection provided by multiple security products such as anti-spyware, firewall, anti-virus, anti-spam, and phishing protection.

Simple, basic Internet services such as Web access, instant messaging and peer-to-peer file sharing networks provide the majority of security holes for attackers to exploit. However, with each new technology comes a new means of attack and potential vulnerabilities.

STOPzilla provides best-of-breed protection against blended threats because it detects, blocks, and quarantines a broad range of malware in real time, including executables, DLLs, operating system settings, and connections.

STOPzilla versions 5.0.6 and later are particularly effective against botnets. The software inspects all incoming and outgoing e-mail traffic. When it detects a volume of e-mails that could not be sent by a human user, it severs the connection. Likewise, when it detects multiple open mail server connections, it severs those connections, shutting down those vectors of vulnerability.

About iS3

iS3 was incorporated in Florida in 1991 as International Software Systems Solutions, Inc. In 2001, our founders set out on a bold experiment, convinced that there was a place for superior technology and service in Web-based commerce. It's flagship product, STOPzilla, an anti-spyware application was launched to rave reviews in 2002. STOPzilla's award-winning technology and ease of use continues to raise the standard in computer security. It has protected more than 15 million users in more than 60 countries. Our proprietary technology and free, unlimited customer support has garnered a high level of customer satisfaction, a growing subscriber base and solid long-term relationships with our retail partners and online affiliates.

iS3 security software products currently include the following:

ANTIfraud protects against ID theft with powerful 5-in-1 protection. Secure Password Protection, SITEguard™ to protect against phishing and other malicious Web sites, Automatic Intelligent Form Filler, and keylogger attack protection. Combined, these features offer users powerful protection against ID theft. All data stored in ANTIfraud are 128-bit AES encrypted.

iS3 ANTIvirus puts a friendly face on the most sophisticated technology available. iS3 ANTIvirus' advanced heuristics and NTFS data streams scanning takes a predictive approach to detecting viruses, worms, and Trojans; even those not yet identified. It's economical, easy to install, and easy to use.

MAXpc scrubs Windows registries clean, stabilizes systems to prevent freezes and crashes, and creates backups in minutes. A quick easy tune-up with MAXpc boosts PCs' lost processing power dramatically.

Into the Future

iS3 is poised to launch a comprehensive suite of security products throughout 2008 and 2009. Identity theft is one of the fastest growing crimes worldwide. As new, ever more complex online threats emerge, iS3 will develop the products and services to provide our customers with the highest level of protection available.

Our dedication to continuous improvement and passion for exceeding customer expectations has driven us to create the most trusted and effective products for businesses and consumers.