



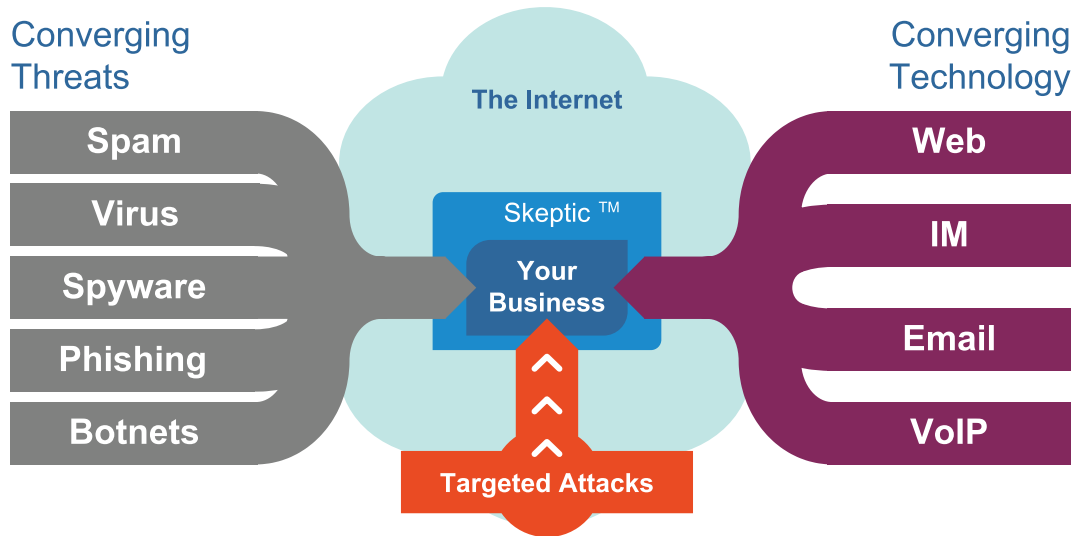
MessageLabs | Now part of Symantec

Converged threats on the security landscape

A MessageLabs Whitepaper – June 09

Understanding converged threats

The pervasive presence of malware on the Internet today creates more opportunities for mixing and matching dangerous content than has ever been possible. The essence of a converged threat is the combination of viruses, spyware, phishing, spam and other attempts at attack or exploitation of vulnerabilities that can disrupt networks and/or lead to theft or unwanted disclosure of sensitive information. These threats are no longer specific to particular channels for information delivery: They can come from e-mail, Web, and instant messaging (IM), and even Voice over IP (VoIP) applications and environments.



The obvious solution is to sever all ties with the Internet—disallowing Internet access drastically reduces a user’s exposure to threat and attack. But that strategy simply won’t work in today’s business climate. Companies and organizations can’t function without Internet access because it provides inputs—information, commercial transactions, supplier and customer communications—as well as outputs—information, products or services, sales and finance—for the whole working world.

Because this essential connection to the digital world must be maintained, it must therefore also be protected. The emerging consensus on proper protection methods depends on a global awareness of the current threat landscape from moment to moment, an ability to block, foil or avoid potential threats, and speedy (hours to minutes) reactions to new threats as they’re discovered. Additionally, aggressive use of proactive technologies to evaluate potential threats and block potentially dangerous behaviors is becoming increasingly important in managing a hostile threat landscape in real time. Finally, sharp sensitivity to sources of threats, including well-known “bad actors” and possible malefactors, can also head off potential threats and attacks before they begin to probe targets. Welcome to the 21st Century Internet!

How e-mail, web, and IM act as threat vectors

The simplest take on the threat issue is that all of these mechanisms provide ways for files or so-called “active content” (packages of information that a

computer can execute) to show up on a computer. E-mail includes message content and can also accommodate many kinds of attachments. Likewise, IM includes mechanisms for file transfer and attachments as well. And finally, visiting a Web page can trigger the execution of all kinds of code, some of which is downloaded to the client machine and run locally. Web pages also support a wide variety of file and data transfer mechanisms so that pages can deliver almost any imaginable form of computer program, active control, script and so forth to a visitor's desktop environment.

From a statistical standpoint in evaluating the likelihood of delivering questionable or hostile material to users and their systems and networks, here's how these three vectors stack up based on the MessageLabs Intelligence: 2008 Annual Security Report:

- E-mail malware traffic flourished in 2008. The high point occurred in September, with nearly 1 in 80 messages containing malware. The low point occurred in May, with approximately 1 in 220 messages containing malware. The average for the year was 1 in 143.8 messages contained malware.
- Web threats were up in 2008 by about 55 percent—the average number of new malicious sites blocked each day rose to 2,290, up from 1,253 in 2007. Lows at the beginning of 2008 were between 100 and 200 new sites blocked per day. By October 2008, new sites with viruses exceeded 5,000 per day, though sites with spyware were still between 100 and 200.
- Instant messaging threats also increased in 2008, where over 1 in 200 URLs sent in instant messages pointed to malicious sites during the second half of the year. In addition, recent advances in breaking Completely Automated Public Turing test to Tell Computers and Humans Apart (CAPTCHA) technology has allowed spammers to create countless numbers of social networking and IM accounts. If these accounts can make “friends” with real humans, they can often broadcast messages to their unwitting victims' entire address books.

Even at the current somewhat reduced levels, e-mail remains an active and dangerous threat vector for malware and other forms of malicious behavior or solicitation (phishing, social engineering, 419/Nigerian scams and so forth). And with Web and IM threats growing, it's clear that some form of protection against all these vectors is urgently necessary.

Top recent threats from e-mail, web and IM

What is at times interesting and always frightening is the incredible ingenuity that malware creators often manifest in creating new threats or variations on existing themes. In the following sections, we'll review some of the most ingenious and dangerous of newer features on the threat landscape. As a general principle, readers would do well to remember the old saying “If it looks too good to be true, it probably is.” Some of the most injurious threats to appear recently have conned users into responding to offers of free services, goods or money, which does nothing more than to let the bad guys know “there's a live one over here!”

Malware mashups

On the Web, a mashup is a page that combines multiple sources of content into a single seemingly unified online presence. A malware mashup represents a combination of attacks and threats in a single blitz against users. Thus, for example, resume and job hunting sites provide information about individuals via resumes and application forms users happily post there. Armed with user contact information extracted from such documents and forms, attackers can launch phishing attacks against those individuals simply by posing as legitimate employers in search of candidates.

Blogs can also serve as ready sources of e-mail addresses and other details about posters for those unprepared to fend off attack. User-generated content often isn't tightly policed, either, so unwitting bloggers can include apparently benign but actually malign links and information in their blogs or in blog comments. When CAPTCHA is easy to break, or spammers can otherwise gain posting rights on blog or forum sites, opportunities to post poison links explode.

At times these attacks simply foist adware on unwitting participants. But often, users are fooled into installing Trojans or backdoors that attackers use to locate and steal identity, account and other potentially valuable information.

Images with embedded scripts

Since March 2009, there has been a spike in the number of images that contain embedded or injected scripts (usually VBScript or JavaScript code is involved). Although this technique is not new, it has not been widely used until recently. It seeks to exploit older Web browsers whereby HTML or script code is appended to the end of the image's binary code. When a user displays the image, the HTML or script material is parsed and executed. This is often used to display online advertisements invisibly so that malefactors get credit for bogus click-throughs, or to invoke free online tracking tools to let creators know that the image has been opened and viewed.

The images used generally appear innocuous, such as flowers, nature scenes or landscapes. The primary purposes for such scripts include monitoring of related user activity—opening or viewing, user IP and location, number of accesses—or serving up pop-up advertisements. The interesting aspect of this threat, which does not yet pose significant security risks, is that many e-mail messages that incorporate such images originate from free online Web mail accounts, presumably created using CAPTCHA breaking tools. Some Web sites that have been compromised via SQL injection attacks use this type of image to foist pop-up advertisements on visitors.

SQL injection and cross-scripting attacks

Early 2009 witnessed a spate of SQL injection attacks whereby attackers exploit vulnerabilities in the SQL database engines so often used in conjunction with Web servers to add malicious links and content to otherwise legitimate (or seemingly legitimate) Web sites. Attackers insert SQL code into Web forms and end up communicating directly with the underlying database if developers don't have proper safeguards in place. This lets attackers update and add content to Web pages using SQL, and explains the name given to this type of attack.

Risk from SQL injection is increasing thanks to automated tools attackers employ

to exploit this vulnerability. Because such tools are now widely used, attackers can mount many more SQL injection attempts than if they did so manually. This not only increases the likelihood of eventual success, it also increases the damage attackers can do once an attempt succeeds because such tools enable them to quickly download and run complex, sophisticated scripts on vulnerable Web sites.

Cross-scripting attacks, also known as cross-site scripting or XSS, involve an attacker inserting malicious code into a link that apparently originates from a trustworthy source. If a user clicks such a link, the embedded code gets inserted into the user's Web request and can execute on his computer. This enables attackers to run programs on or steal information from that computer. Like SQL injection, XSS threats can materialize when Web application or server software fails to enact proper controls to validate user input and check the veracity or validity of URLs—if not filtering them outright—before executing them.

Reputation attacks

In the August 2008 Black Hat meetings, security researcher Dan Kaminsky reported numerous vulnerabilities and potential attacks that use the DNS protocol to poison servers that resolve address requests from users looking for Web sites, mail servers and other Internet resources.¹ Carefully crafted, such exploits can redirect users to malicious or improper addresses instead of those actually requested, a technique often called DNS poisoning or DNS cache poisoning. By the end of 2008, numerous such attacks had been documented in the wild, and legitimate companies or service providers were suffering from damaged reputations resulting from user reactions to such exploits. Even though the apparently culpable organizations are neither at fault nor completely responsible for such redirection, user ire can be a potent force for harm as well as good.

Kaminsky also described methods whereby similar attacks could be used to compromise e-mail messages, software update systems or password recovery systems on widely used Web sites. Even the use of Secure Sockets Layer (SSL) certificates to confirm Web site validity could be vulnerable to this type of attack. So far, no instances of such attacks have been reported in the wild, and vendors are working feverishly to patch such vulnerabilities. Currently, the potential danger remains unresolved.

Indirect references in search engine links

The recession has spawned a new flavor of spam that seeks to entice readers interested in saving money. Part of the spam content includes links to a well-known search engine, pre-configured to search for the spammer's own domain. The idea is to provide an indirect link to a suspect or malicious domain without actually including that link in the message content verbatim. This makes it much more difficult for URL filtering techniques to detect the bad or questionable reference they would otherwise identify and block immediately.

In response, search engine providers changed their link referencing technology to make it much more difficult for spammers to exploit this to their advantage. Likewise, anti-spam technology quickly adapted to recognize these types of links by equating such reference strings with undesirable content or disallowed links.

¹McMillan, Robert, "Kaminsky: Many ways to attack with DNS," ComputerWorld.com, August 6, 2008, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9111882>.

Black Hat Webcast No. 2, July 24, 2008, <http://www.blackhat.com/html/webinars/kaminsky-DNS.html>.

Spam obfuscation techniques

Spammers have long included various types of randomly generated text in their messages to attempt to foil or fool spam recognition techniques. They also include standard e-mail text such as unsubscribe opt-outs and privacy links to try to make the message appear legitimate and compliant with anti-spam legislation (such as CAN-Spam in the United States, PIPEDA in Canada and the EU Privacy and Electronic Communications of 2002). Often, these techniques are combined with indirect link methods that depend on search engine links like those described for reputation attacks, or multiple indirect Web server references to obscure the actual source for images and other linked items.

HTML tags may be inserted into the middle of bad or questionable domain strings so that literal recognition techniques don't work. The browser doesn't display such inserted text on-screen, so users see apparently well-formed domain names (which can be cut and pasted but aren't clickable) while unsophisticated spam screening tools see only apparent gibberish. Fortunately, statistical analysis helps to ferret out such misdirection because a large number of occurrences—an unavoidable characteristic of spam messages, which fly out by the millions—will soon make such unwanted message traffic identifiable by its frequency and other readily identifiable text characteristics.

Social networking vulnerabilities and “bogus updates”

Because of CAPTCHA compromise, fake identities and programming tools for Facebook™, LinkedIn®, MySpace™ and other popular sites, it's become alarmingly easy for attackers to generate bogus friend or buddy requests in large volumes. Some types of friend access on social networks not only allow a “friend” to interact with an individual user, it also grants that friend (bogus or legitimate) access to the user's entire friend list. This is a powerful and dangerous mechanism for propagation and for generation of social-network spam.

Another interesting wrinkle to this play is to inform users that they need to download an “update” to their social networking environment. Instead of a legitimate update from the site operator or provider, malware gets installed, often with Trojan, backdoor and information theft or keylogger components. This kind of malware mashup looks completely legitimate and may even be subject to forced installation by credulous users. The results can be disastrous.

In recent months, in fact, various Adobe products—especially Adobe® Flash® and Shockwave®—have fallen prey to the same kind of enticement technique. When informed that they must install an update, many users will simply click the link and take whatever shows up as a consequence. As an alternative, administrators should create Group Policy objects that prevent users from downloading and installing updates on their own recognizance.

Use of malicious URLs

Whether in e-mail text, on Web pages or in instant messages, sharing of URLs is pervasive and constant. When malicious URLs enter the mix the chances for trouble skyrocket. We've discussed how subverting CAPTCHA can create bogus e-mail or IM accounts, which can then flood their respective recipients with messages of all kinds, many of which include malicious URLs. Likewise, unmoderated postings, forum comments and SQL injection can festoon pages on the most legitimate of sites with malicious URLs as well.

Whether in e-mail text, on web pages or in instant messages, sharing of URLs is pervasive and constant. When malicious URLs enter the mix the chances for trouble skyrocket.

The only appropriate response is to create multiple levels of URL screening and filtering. Users can opt into many kinds of white and black lists or reputation-based URL ratings and rankings to decide what to click and what not to click, but the action doesn't stop there. Network administrators and service providers can screen URLs at their firewalls and further block or filter access using the same kinds of techniques. Hopefully, the net effect through a combination of user education and filtering or screening technology can help users avoid visiting links they really should not.

Appropriate countermeasures

Information security is often and correctly compared to a game of “cops and robbers.” In this version of the game, the robbers keep coming up with new and ingenious ways to perpetrate mischief, mayhem and other dastardly deeds, while the cops keep coming up with new ways to foil them. This is also a case where the best offense is a good defense. Detection, prevention and proactive engagement are all key ingredients in winning the game—or at least in limiting losses as much as circumstances will permit.

The importance of countermeasures is also hard to overstate. Given that many attacks are known, and therefore such malware can be recognized and filtered, it requires only simple prudence and the right tools and techniques to fend them off. Nevertheless, a complete battery of countermeasures is an essential ingredient in maintaining peace and security in the face of today's threat landscape. We'll review some of the most important elements in that collection in the sections that follow.

Heuristics augment signatures and content analysis

Known and potentially dangerous items can often be recognized as such. That's why the foundation for most anti-malware countermeasures rests on inspection of incoming materials and comparison with libraries of identifying characteristics or content patterns, often known as signatures. When it comes to spam, malicious URLs and suspect or dangerous Web sites, simple lookups by name, address and other text and data characteristics often signal which items can be granted safe passage across the periphery and which items should be left outside.

On the other hand, new threats continually present themselves and must be carefully inspected and monitored in terms of their structure, content and behavior to determine what's fair and what's foul. This is where heuristics come into play. By definition, a heuristic is a kind of educated guess that infers intent from behavior. Threat-oriented heuristics watch how suspect or unknown software behaves, and then permit only safe behaviors to proceed while blocking unsafe, suspect or questionable behaviors.

Signatures and content-pattern matching work very well to detect and block what's known and recognizable. Heuristics, however, allow the unknown or unrecognized to be monitored carefully and managed closely enough to proactively prevent most unwanted outcomes from occurring. Just as no single signature can capture all threats, no heuristic can foil all bad behavior. A judicious combination of both techniques can provide organizations with reasonable assurance that their systems, networks and information assets are safe.

The best offense (in the information security game) is a good defense. Detection, prevention and proactive engagement are all key ingredients in winning the game — or at least in limiting losses as much as circumstances will permit.

**MessageLabs
has a 100%
guarantee
Service Level
Agreement
against all
known and
unknown
viruses.**

Detailed file analysis techniques

As described previously, malware and spam use all kinds of obfuscation and obscurity techniques to make detection or recognition more difficult; malware files do likewise with different file-oriented techniques. They will compress malignant payloads to change their obvious characteristics and make them harder to inspect. Alternatively, they will encrypt their payloads to make them as opaque to content analysis as possible. They may even break up payloads into bits and pieces and distribute them inside valid, benign files in attempts to avoid detection and to seek opportunities to execute.

Here, appropriate countermeasures include an arsenal of tools designed to reverse or remove the obscurity techniques. Thus you'll find a battery of compression/decompression tools and encryption/decryption tools in the file inspection and analysis toolbox brought to bear on incoming files to look for and block potential threats.

This is also a case where the good guys have a significant advantage. They can trace incoming traffic back to its most recent forward, and carefully and closely examine previous stops in the forwarding chain from purported sender to receiver. Even though origination addresses can be spoofed and intermediate hops in the forwarding chain forged, recurring analysis of similar traffic often reveals patterns that allow detection and rejection to occur easily and automatically, no matter how cleverly the actual sender may have tried to disguise or recast that chain of transmission. Distribution mechanism analysis and detection of known patterns in the transmission chain are often enough to permit savvy threat analysis tools to block otherwise completely innocuous-seeming payloads from crossing the digital transom.

Detailed content analysis

In the same vein as the chain of transmission evidence mentioned in the preceding section, careful analysis of e-mail and instant message structure can often reveal suspicious or outright malign forces at work. In particular, message header and message content structure can often tell stories that senders may never realize they were sharing, and attach the digital equivalent of the old mapmaker's motto "here there be dragons" to certain forms of content.

Even more revelatory is the presence of certain types or instances of content, especially embedded scripts, specific code elements and embedded URLs. Where signatures alone aren't enough to separate the good from the bad, content analysis comes into play. Threat analysis software looks for various specific commands or sequences of actions known to pose security threats. Then, too, it's often possible to pick out suspicious uses of indirection if not outright references to known malicious sites.

All of these analytical techniques supply values that add up to provide a threat index for specific messages. If that value stays below a certain threshold, it is allowed to pass; once that value jumps beyond the threshold, it will be blocked.

Malware DNA

Over time, analysis of malware leads to a set of recognizable patterns—of code, structure, behavior, delivery mechanisms and so forth. These patterns constitute a kind of "malware DNA" so that new threats can be analyzed for occurrence of

such patterns or degrees of similarity to them. In many cases, a near-hit is as good as a perfect match when it comes to identifying and deflecting potential threats.

Absolving indirection

Given that clever techniques to present malicious links in seemingly innocuous or even trustworthy-appearing forms is a common practice, it stands to reason that analytical tools should seek to resolve suspect links to determine by execution where they actually lead. The best of the threat analysis tools perform such checks on all URLs whose formats or structure indicates that they are not the final stopping point for a linked reference. This approach permits absolute certainty about identifying where links lead, makes it easier to separate the good from the bad, and helps to keep the list of known bad sites current and up to date.

Threat analysis is never done

The real value of deep threat analysis is that it is comprehensive and ongoing. Properly done, threat analyses not only point out current threats, they also describe trends, reveal techniques and point back to their makers. Modern threat analyses and countermeasures take place 24/7/365.

Because monitoring is continuous, patterns emerge as new threats appear on the scene. In a fairly short time, it becomes apparent where the threat is coming from and where it is directed. As incidents occur and frequencies increase, it becomes possible to assess a corresponding index to measure the severity of the threat while work gets underway to create appropriate countermeasures, including patches, signatures and updates to routing tables and black lists.

Modern service providers maintain teams around the globe to provide continuous coverage and response to threats whenever and wherever they emerge. When threat assessments are high and the time to devise a countermeasure appears longer than a few hours, advisories begin to fly to inform clients about appropriate workarounds or defensive postures to adopt before countermeasures become available. If interim solutions are called for they will be supplied, until more permanent measures are ready for distribution.

These approaches enable service providers to implement zero-hour protection mechanisms as soon as threats are recognized. When clients present their message streams and Web traffic for analysis and protection to these providers, they can be assured of rapid and effective response.

Along the way, threat custodians maintain a complete and thorough library of known patterns, signatures, behavior and content as they maintain the DNA databases for the threat genomes under their purview. This approach to threat analysis and recognition not only helps to deal with known and identifiable threats, it also creates a set of heuristics that permits development of proactive and preemptive mechanisms to foil hitherto unknown threats.

Best methods to reduce or mitigate risk

Above and beyond applying the best tools and services available to help identify and manage threats, organizations should take important steps to reduce the risks in today's and tomorrow's threat landscape. The following list of items and

In many cases, a near-hit is as good as a perfect match when it comes to identifying and deflecting potential threats.

Modern threat analyses and countermeasures take place 24/7/365.

activities can significantly lower exposures to threats and vulnerabilities simply by avoiding them:

- **User education:** A set of clear messages to network and Internet users can be very beneficial, especially in concert with a well-defined and well-articulated Acceptable Use Policy (AUP). Communicate with employees what they can and cannot do with e-mail, IM and the Web. Teach them about “safe computing.” Enforce this policy and training with technology at all available levels.
- **Establish official sources for software and updates:** Too many unsuspecting users get tricked into applying bogus updates from questionable sources that end up installing malware on their machines. Explain to users where to go for official software and updates, telling them to avoid all other sources, and use automated policy tools (such as Group Policy objects in Active Directory environments) to enforce these restrictions whenever possible.
- **Establish ubiquitous Web anti-virus and anti-spyware protection:** Aside from blocking bad and suspect URLs, equip all e-mail servers and computers with anti-virus and anti-spyware protection that blocks unwanted active content from the Web from taking up residence on those machines. Complete coverage will reduce the number of incidents tremendously, as long as that software is kept patched and its data files and signatures are kept up to date.
- **Block non-business-related Web sites:** As an extension of the AUP, company firewalls and proxies should use a black list or some other source of “bad site information” to block access to unwanted, undesirable, unsavory, suspect and dangerous Web sites.
- **Filter all content for unwanted files:** Whenever a file or any active content arrives at the network periphery, it should be inspected deeply and thoroughly. Because it’s better to err on the side of caution, it’s also best to block anything that can’t be positively identified as 100% benign from crossing the network boundary. If you can keep the bad files and active content out, you can usually do likewise for malware.

Combined with a professional and thorough message handling service, with deep threat analysis, these techniques should help you keep your networks and information assets safe and sound.

About MessageLabs | Now part of Symantec

MessageLabs, now part of Symantec, is the world’s leading provider of managed messaging and Web Security Services. Over 21,000 organizations and over 9 million end users in 99 countries employ MessageLabs services to protect against viruses, spam, phishing, inappropriate Internet use, spyware and other business damaging threats.

For more information on MessageLabs, now part of Symantec, Email and Web Security Services, contact us at (866) 460-0000 or visit us at www.messagelabs.com.

Americas**AMERICAS HEADQUARTERS**

512 Seventh Avenue
6th Floor
New York, NY 10018
USA
T +1 646 519 8100
F +1 646 452 6570

CANADA

170 University Avenue
Toronto, ON M5H 3B3
T: 1 866 460 0000
F: +1 646 452 6570

Asia Pacific**HONG KONG**

1601
Tower II
89 Queensway
Admiralty
Hong Kong
T +852 2111 3650
F +852 2111 9061

AUSTRALIA

Level 14
90 Arthur Street
North Sydney
NSW 2060
Australia
T +61 2 9409 4360
F +61 2 9955 5458

SINGAPORE

Level 14
Prudential Tower
30 Cecil Street
Singapore 049712
T +65 6232 2855
F +65 6232 2300

Europe**HEADQUARTERS**

1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
T +44 (0) 1452 627 627
F +44 (0) 1452 627 628

LONDON

40 Whitfield St
London W1T 2RH
United Kingdom
T +44 (0) 207 291 1960
F +44 (0) 207 291 1937

NETHERLANDS

Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands
T +31 (0) 20 491 9600
F +31 (0) 20 491 7354

BELGIUM / LUXEMBOURG

Culliganlaan 1B
B-1831 Diegem
Belgium
T +32 (0) 2 403 12 61
F +32 (0) 2 403 12 12

GERMANY, AUSTRIA, SWITZERLAND

FeringasträÙe 9
85774 Unterföhring
Munich
Germany
T +49 (0) 89 189 43 990
F +49 (0) 89 189 43 999

