PUBLISHED BY CISCO AND IRONPORT

2008 INTERNET SECURITY TRENDS

A REPORT ON EMERGING ATTACK PLATFORMS FOR SPAM, VIRUSES AND MALWARE

TABLE OF CONTENTS

IronPort is now part of Cisco.

“YOU HAVE TO LOOK AT THE TRENDS OF THE NEXT DECADE AND PLAN FOR IT. WE ALL UNDERSTAND THE **TREND**—

Security incidents are getting worse.

YOU CAN’T PREDICT **when** AND **where** THINGS WILL HAPPEN, SO YOU’LL HAVE TO UNDERSTAND THE **how.**”

JOHN CHAMBERS
CHAIRMAN AND CEO
CISCO SYSTEMS

Introduction

2007 marks a turning point. Amateur hour is over. Just when malware design seemed to have reached a plateau, new attack techniques have burst forth, some so complex – and obviously not the work of novices – they could have only been designed by means of sophisticated research and development. But, these advancements are not happenstance; they are actually a product of the security industry's own success.

For a time, security controls designed to manage spam, viruses, and malware were working. Loud, high-impact attacks abated. But, as a result of this success, the threats they protected against were forced to change. In 2007, many of these threats underwent significant adaptation. Malware went stealth, and the sophistication increased.

These changes were illustrated by the discovery of self-defending bot networks, and malware designed as a reusable attack platform. New terminology referring to these adaptations also appeared, including terms like: "fast-flux," "decentralized command and control" and "rotating exploit packs." Attackers created back-end malware management systems to maintain infection statistics and monitor exploit effectiveness – proving that Unified Threat Management (UTM) is apparently a two-way street.

This report is designed to help highlight the key security trends of today and suggest ways to defend against the sophisticated new generation of Internet threats certain to arise in the future.

TRENDS OVERVIEW

The overall trends in spam and malware can be characterized by a larger number of more targeted, stealthy and sophisticated attacks. Specific observations include:

- **Spam volume increased 100 percent,** to more than 120 billion spam messages daily. That's about 20 spam messages per day for every person on the planet.
- **Spam has become more dangerous.** Past spam attacks were primarily selling some type of product. In 2007, more than 83 percent of spam contained a URL. In accordance with a trend towards the blending of different malware techniques, URL-based viruses increased 256 percent.
- **The "Self Defending Bot Network" was introduced.** The Storm Trojan is perhaps one of the most sophisticated botnets ever observed. The quality and technical sophistication reflect that these threats are being developed by professional engineers.
- **Viruses no longer make headlines,** because virus writers have evolved from the previous mass distribution attacks, viruses where much more polymorphic and typically associated with the proliferation of very sophisticated botnets such as *Feebs* and Storm.

“SPAM…CONTINUES TO DEGRADE THE **INTEGRITY OF EMAIL.**

Some **55 percent** of email users say they have lost trust in email because of spam.”

—THE PEW INTERNET AND AMERICAN LIFE PROJECT

Spam Trends

2007 Trends: Testing New Techniques

The cyclical holiday spam surge pushed 2006 volumes to record highs and, by the end of the year, many companies were seeing spam messages making up as much as 90 percent of their inbound mail flow.

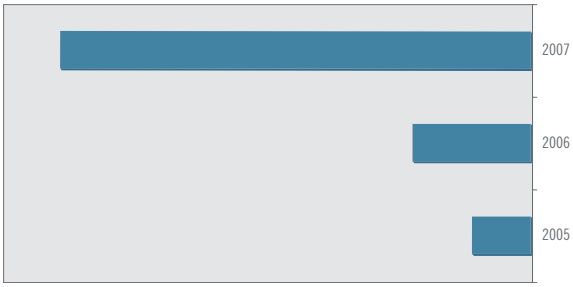
As image spam defenses got better and this technique lost its effectiveness, spam volumes throttled back somewhat—presumably because attackers saw the drop in results from their spam campaigns, and focused their resources on finding a new way to get their message through.

A Proliferation of Attachments

When image spam first appeared in 2005 it was the first time spammers tried using message attachments to get their pitch across. Usually consisting of a GIF or JPEG file, and often touting low-priced stocks to buy or a toll-free number to call for ordering drugs, these non-text attachments easily slipped by anti-spam engines that relied on keywords and text classification to sort out good content from bad.

2007 has seen a proliferation of different attachment types used in spam. Spammers are using these different attachments in order to try and get past email security gateways that are unable to look into complicated file types like PowerPoint and Zip files. Where in 2005 and 2006 there were only a couple of different attachment types seen overall, in 2007 there have been outbreaks of spam campaigns using at least twenty different attachment types.

Volume of Spam with Attachments



2007 HAS SEEN A SIGNIFICANT INCREASE IN THE TYPES OF ATTACHMENTS USED IN SPAM

SPAM ATTACHMENT TYPES BY YEAR

2007	2006	2005
image/gif	image/gif	image/gif
application/pdf	image/jpeg	image/jpeg
image/jpeg	image/png	
image/png	application/msword	
application/x-msdownload		
application/msword		
application/vnd.ms-excel		
image/pjpeg		
image/bmp		
audio/mpeg		
application/zip		
text/calendar		
application/rtf		
application/x-zip-compressed		
application/vnd.ms-powerpoint		
image/x-png		

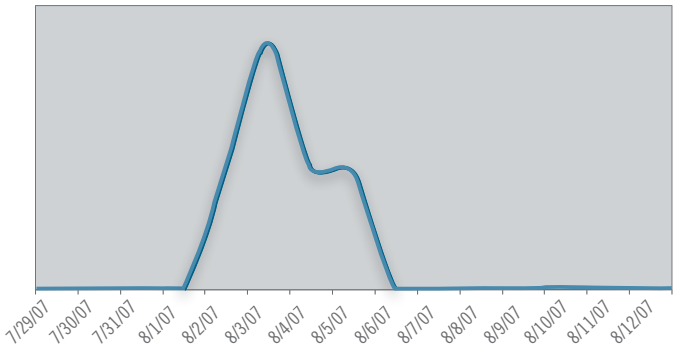
Testing the Waters: Excel and MP3 Spam

Spammers use different attachment types for one reason: to get their messages through spam filters. But the message delivery must still be easy for end-users to read, and so spammers experiment to find what is the best approach.

These graphs track the spike and quick decline of two of the most unique attachment-based spam attacks of 2007. In August there was a dramatic growth in the use of Excel files in spam messages, and then an equally quick decline over a period of six days. In October, there was a spike of spam using an MP3 attachment that was just as large, but it only lasted three days. At the peak of these outbreaks however, both of these spam types represented double-digit percentages of worldwide spam traffic, showing that the attackers are willing to put enormous resources into trying to find their next way to sneak into your inbox. The Excel outbreak totaled more than one billion spam messages sent worldwide!

These attachment types slipped through all but the most advanced email security systems. Since the spam content was encapsulated in a hard-to-parse Excel format or in an audio file that can only be listened to, traditional content-based scanning engines failed to protect their users – just as they had with image spam the year before. However, advanced spam defenses were able to stop these outbreaks.

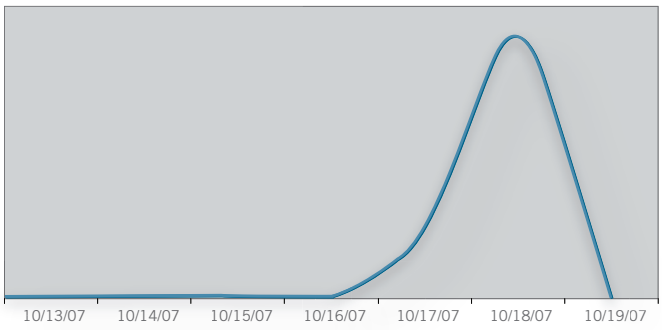
Excel Spam Magnitude



August 2007

IN AUGUST, THERE WAS DRAMATIC GROWTH IN THE USE OF EXCEL FILES IN SPAM MESSAGES, FOLLOWED BY SHARP DECLINE

MP3 Spam Magnitude



October 2007

OCTOBER BROUGHT A SPIKE OF SPAM USING MP3 ATTACHMENTS

By looking at factors not related to the message content such as the reputation of the IP sending the message, the structure created by automatic spam engines, and any URLs the message tries to get users to click on, third generation spam engines can detect and block many kinds of attachment spam, even if the text of the attachment is unreadable.

These messages did get through in large numbers; large enough to be noticed by the press.

eWeek

"Spammers have taken to using MP3 attachments in emails named after recording artists as part of a pump-and-dump stock scam… When recipients click on the attachment, a voice relays a message promoting stock for a particular company."

— **Brian Prince,** eWeek, October 18, 2007

Ultimately these campaigns were unsuccessful though, because users have learned not to click on strange attachment types, and spammers moved on to trying new techniques.

PDF: The new GIF

In 2007 there was one new attachment type that was extremely effective however. PDF-based attachment spam first appeared in June of this year. Like GIF-based spam, PDFs were touting low-priced stocks that the spammers were trying to manipulate the price on in order to make money in a "pump and dump" scheme. Unlike the GIF-based attacks however, these PDF messages looked extremely professional, in an attempt to gain people's trust that this was a worthwhile stock tip.

German Stock Insider - OYQ.F (TKMD.F)

Thursday 20-JUN-2007

Talktech Telemedia, Inc - HUGE GAINS EXPECTED!

Volume 4, Issue 6

Talktech Telemedia expects gains of 300% in next 5 trading sessions!

TOP REASONS TO CONSIDER OYQ.F:

- Top management team in place.
- Huge Investor Awareness mar-

In this edition of German Stock Insider we are featuring our winning pick of Talktech Telemedia, Inc (Frankfurt: OYQ.F).

With an excellent management team and a huge marketing campaign starting next week, we are expecting our German

before next week as we are expecting this to start trading up as early as Thursday 20-JUN -2007.

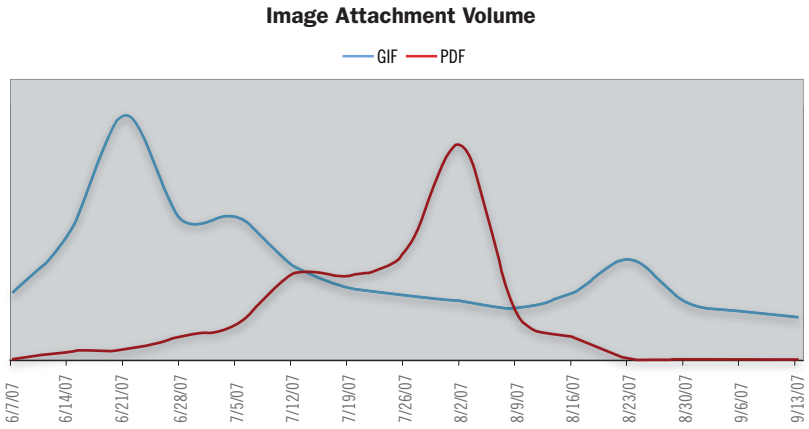
We strongly urge you do your own research on Talktech Telemedia before making any investment decisions. We feel

has to offer. We strongly urge you to call your stock broker and ask them about OYQ.F (TKMD.F). Add it to your portfolio today.

300% gains are expected on this one - **DON'T LET IT PASS YOU BY!**

IN AN ATTEMPT TO GAIN RECIPIENT TRUST, PDF-BASED ATTACHMENT SPAM IS DESIGNED TO APPEAR PROFESSIONAL

The PDF attachments had a high success rate for spammers, measured in the same way that many legitimate marketing campaigns would be: by the number of users that click-through to buy. For a three-month period PDF spam actually increased to levels above traditional image-based spam, some days accounting for *tens of billions* of individual messages.



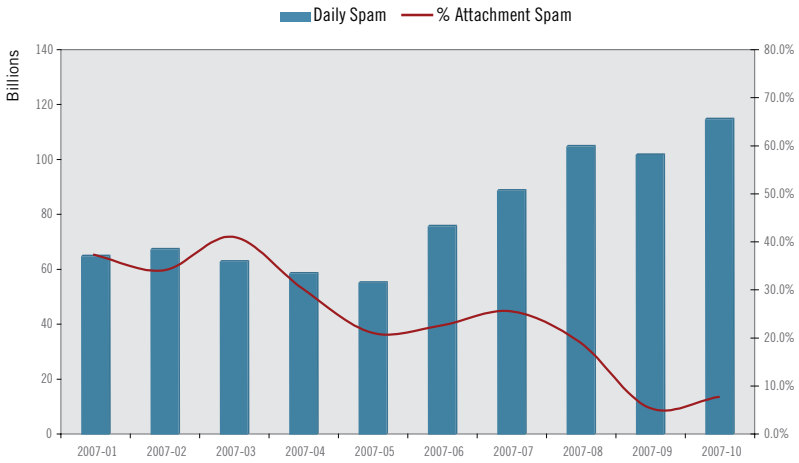
From Pictures to Links

For the three months before October, spam volume overall began to increase sharply. This is actually not surprising as there is a cyclical increase in spam every year just before the holiday season. It is surprising however that that the percent of spam messages that contain an attachment (image or otherwise) began to fall dramatically in the same period.

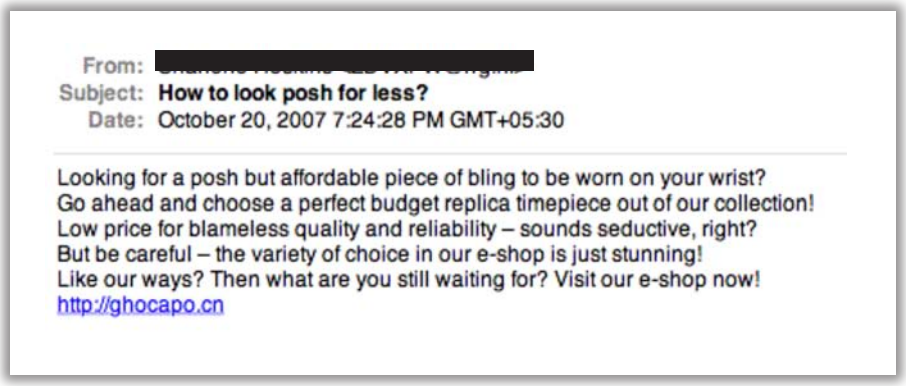
In the most recent measurements, attachment-based spam accounts for less than ten percent over overall spam volume, while the total number of spam messages sent worldwide has doubled to more than 120 billion per day.

The large number of text-only messages being sent today contain a different payload – one that, in many ways, is much more dangerous than graphics files imploring you to invest in cheap stocks. The predominate form of spam today is nothing more than a few simple words and a link, usually to a temporary webpage whose only purpose is to infect a computer with a malware Trojan.

Spam has become much more dangerous, because instead of just trying to sell useless products or services, it is now trying to infect computers with malicious software. These types of Trojan horse programs used to be sent in executable or Microsoft Office files as attachments to email, but attackers are now sending a seemingly benign spam message through and tricking recipients into reaching back out to them so they can infect computers through a weakness in Web browsers.



BEFORE EACH HOLIDAY SEASON THERE IS CYCLICAL INCREASE IN SPAM. HOWEVER, IN 2007, THE PERCENT OF SPAM MESSAGES THAT CONTAIN AN ATTACHMENT BEGAN TO FALL DRAMATICALLY DURING THE SAME PERIOD.

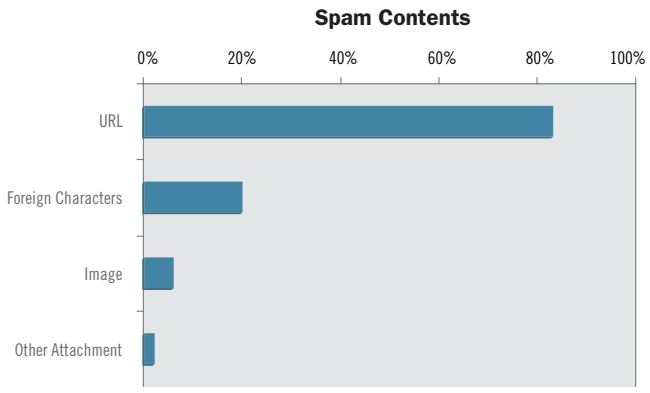

From: [redacted]
Subject: **How to look posh for less?**
Date: October 20, 2007 7:24:28 PM GMT+05:30

Looking for a posh but affordable piece of bling to be worn on your wrist?
Go ahead and choose a perfect budget replica timepiece out of our collection!
Low price for blameless quality and reliability – sounds seductive, right?
But be careful – the variety of choice in our e-shop is just stunning!
Like our ways? Then what are you still waiting for? Visit our e-shop now!
http://ghocapo.cn

EXAMPLE LINK-SPAM, CONTAINING A FEW SENTENCES AND A URL

Today, approximately 83 percent of spam contains a URL. This has increased greatly from 2005 and 2006 when a majority of spam contained only the image that conveyed the call to action ("buy this stock" or "call this phone number").

Now, coordinated and self-propagating botnets such as the Storm platform will send multi-phase attacks that use short spam messages point a user's Web browser right back at other systems in the Storm cloud for the sole purpose of infecting their machine with the Storm Trojan and expanding the network's numbers.



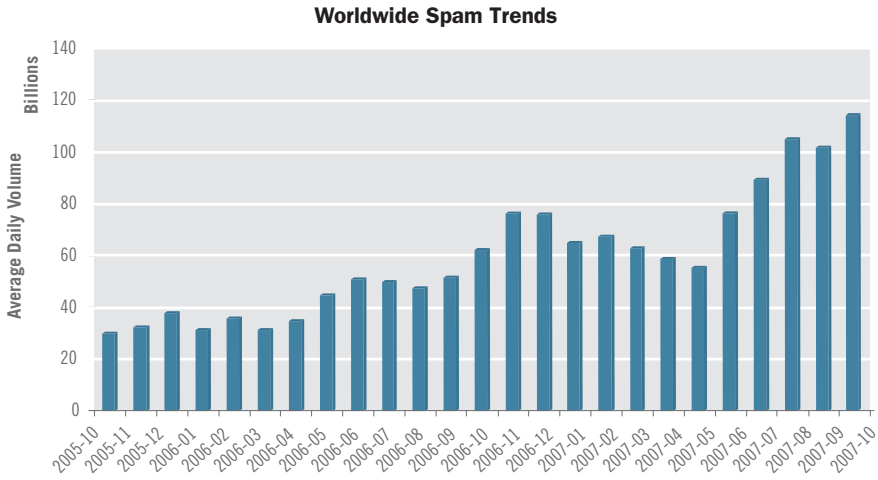
SPAM CONTAINING A URL FAR SURPASSES OTHER SPAM TECHNIQUES

Keeping the Vigil

Spam is at an all-time high. Spammers have reacted to the increased defenses that have been deployed over the past 24 months by simply cranking up the sheer number of messages they send. Since individual spam messages are nearly free to send after the campaign has been created, spammers have realized that as spam engines reach 99 percent effectiveness, they must send an order of magnitude more traffic to have the same number of messages end up in people's inboxes. The effectiveness of spam prevention systems is more critical than ever.

It is critical that spam defenses are able to adapt to new tricks in spam as well. Attachment spam is changing so quickly that merely being able to detect image-specific spam is not enough. The source of the message and the history of the URL it tries to draw you to is critical. Spam engines must look beyond a content of a message in order to accurately gauge its intent, reputation of the source and the target is key.

Companies must secure both email and Web traffic in order to fully defend against this new breed of blended threats. Attackers have realized that they no longer need to get their entire Trojan payload through in one message. Today's



A STEADY INCREASE IN SPAM VOLUMES HAS CONTINUED OVER THE PAST TWO YEARS

attacks come in multiple phases, starting off with the most innocuous message possible, only to trick the user into going out and actually infecting themselves.

2007 has been a year of trial and refinement for spammers. While the first half of the year did not bring a remarkable increase in the number of spam messages sent, spammers showed incredible persistence in testing and refining their attacks. Now that they have found significant weaknesses in the way that many spam engines handle URL-only messages, there will be an explosion on the order of the three-fold image spam increase seen in 2006. In fact, the past few months have already seen considerable uptick in worldwide spam volume. This trend is expected to continue through the holiday season, making the total amount of spam sent in 2007 larger than possibly all email sent in total since the medium was invented.

“TEN YEARS OF COMPELLING DATA CLEARLY INDICATES THE VIRUS PROBLEM SHOWS NO SIGN OF ABATING.

REAL PROGRESS

will be made when companies rely less on defensive technologies and more on **proactive security polices and practices.**”

LARRY BRIDWELL
CONTENT SECURITY PROGRAMS MANAGER
ISCA LABS

Virus Trends

While 2007 saw a new and virulent type of blended threat emerge with a preponderance of "link spam" that pointed to an attacker website, purely meant to infect a user's computer, traditional email-born viruses were still very prevalent and in fact showed a similar amount of experimentation and refinement throughout the year.

Virus outbreaks in 2005 and 2006 were dominated by variants of the *Bagle* and *Mytob* Trojans. These malicious payloads were delivered in executable files, Zip archives and other binary attachments – attempting to exploit flaws in popular mail clients in order to install their botnet payload onto a computer. The purpose of these botnets were to create specific-use attack platforms meant for sending even more spam, disguising phishing sites used to steal personal information, or executing distributed denial of service attacks (DDoS) against large corporate websites.

Shockingly, *Bagle* and *Mytob* have all but disappeared in 2007, being replaced by new and more devious botnets that try to spread through many more channels than just email. Storm, *Feebs* and *Clagger* variants top the list of this year's most frequent virus outbreaks.

TOP VIRUS OUTBREAKS

2005	2006	2007
Mytob	Stration	Storm
Bagle	Bagle	Feebs
Sober	Mytob	Clagger

THE *FEEBS* MASS MAILING WORM

"*Feebs*" is the research name for a self-propagating email worm that gives attackers remote access to infected computers for the purposes of stealing personal information.

The *Feebs* worm is particularly dangerous because it watches a system for outgoing SMTP connections and will transparently inject an infected Zip file into the system's own messages – increasing the likelihood of them being opened by the recipient because they are coming from a trusted source.

Once it is present on an infected computer, the worm will listen for incoming connections, accept commands to retrieve files from the local computer, upload new virus templates to propagate and retrieve new executable programs to run.

Like the experimentation with attachment spam in 2007, email viruses have seen a large amount of change and refinement, sometimes resulting in new variants of a virus being released in the wild even before traditional signature-based virus scanners have published rules to catch the first variants.

Take for example the Feebs virus, a particularly nasty threat which many researchers believe to be building a network as large and powerful as the oft-mentioned Storm virus, but doing so quietly in order to not attract attention to its growth.

During one week in 2007, the IronPort® Threat Operations Center detected six distinct outbreaks of different *Feebs* variants, each expanding exponentially for several hours before the first virus signatures were published. There was even a day when two completely different strains of *Feebs* were released at exactly the same time, with one of them taking nearly a full day for inoculations to be developed, twice as long as its sibling.

Zero-day virus protection is an essential layer of protection to guard against these rapidly changing attacks.

Feebs Outbreaks – October 2007

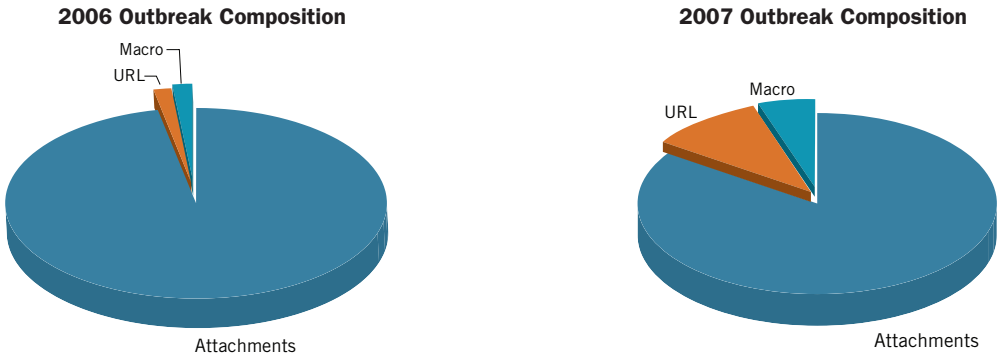
FREQUENCY OF CHANGING FEEBS VARIANTS DETECTED BY IRONPORT'S THREAT OPERATIONS CENTER
OCT 13, 2007 - OCT 22, 2007

FEEBS OUTBREAK TIMELINE

Sophos Virus Name	Outbreak First Reported	First Signature Published	Virus Outbreak Duration (Hours)
W32/Feebs-Fam	10/13/2007 4:00	10/16/2007 1:49	69:49
W32/Feebs-BW	10/17/2007 4:00	10/17/2007 14:36	10:36
W32/Feebs-BX	10/17/2007 4:00	10/18/2007 1:52	21:52
Mal/Feebs-B	10/19/2007 8:00	10/19/2007 13:19	5:19
W32/Feebs-BY	10/20/2007 1:00	10/20/2007 15:25	14:25
Mal/Feebs-C	10/22/2007 4:10	10/22/2007 11:17	7:07

Tremendous Growth in URL Outbreaks

While attachment outbreaks like the above *Feebs* variants still constitute the lion's share of zero-day virus threats, 2007 saw a significant increase in the number of outbreaks that were spread by URLs instead of through a traditional email attachment.



2007 SAW A SIGNIFICANT INCREASE IN THE NUMBER OF OUTBREAKS THAT WERE SPREAD BY URLS

Up 253 percent 2006, URL-classified outbreaks represented a disturbing trend in the evolution of multi-phase attacks that try multiple ways to deliver seemingly innocuous messages such as link-only email, but that can result in a significant security compromise when that URL points to a malware-infected Web server that is designed to compromise and enslave a passing computer.

LOOKING CLOSER AT A NEW CLASS OF INTERNET THREATS.

The "Storm" Network: Introducing Social Malware

In 2007, the "Storm" class of malware introduced new, and combined existing, technologies to create highly sophisticated social malware that borrows attributes from the social networks of Web 2.0. Storm did this by combining disparate techniques into a larger system that is difficult to track, fast-moving and dynamic in both source and size. As a blended threat, it uses both email and Web to conduct a two-stage attack.

Storm introduced new types of spam attacks carrying out large-scale PDF, XLS attacks and the smaller MP3 outbreak.

Over the course of 2007, the Storm Trojan grew from nonexistent to what some researchers estimate from one to ten million infected systems. First detected on January 17, 2007, Storm has reportedly grown to sizes never before seen and raised claims that the collective computing power has surpassed even the largest supercomputers. The significant variation in Storm size estimates may indicate inaccurate counting techniques or gross over-estimation of power.

STORM-CLASS MALWARE: KEY CHARACTERISTICS

- **Self-Propagating** – Storm sends massive amounts of spam to spread. Users are directed to multiple changing HTTP URLs, which serve Storm malware. If infected, the system then becomes part of the Storm network.
- **Peer-to-Peer** – Where previous botnets were controlled from centralized locations through a hierarchical management structure, Storm nodes communicate through a unique peer-to-peer communication protocol. This makes it difficult to track the total size.

A STORM BY ANY OTHER NAME

Storm has been called:

- Storm Trojan
- Storm Botnet
- Storm Worm
- Storm Spam Engine
- Storm Distributed Denial of Service (DDoS) network.

The many names are an indication of the number of features Storm provides and the fact it is a new class of malware – the reusable attack platform.

- **Coordinated** – Storm will send spam campaigns that point to webpages hosted by other Storm computers, showing amazing sophistication in the way the network creates its attacks.
- **Reusable** – Storm can be used for many kinds of attacks: spam, phishing, DDoS, it has even been known to compromise IM networks and post blog spam, making it a threat to many different protocols.
- **Self-Defending** – Storm watches for signs of reverse engineering or analysis. It repeatedly launched massive denial of services attacks against researchers and anti-spam organizations.

USERS ARE THE TARGET

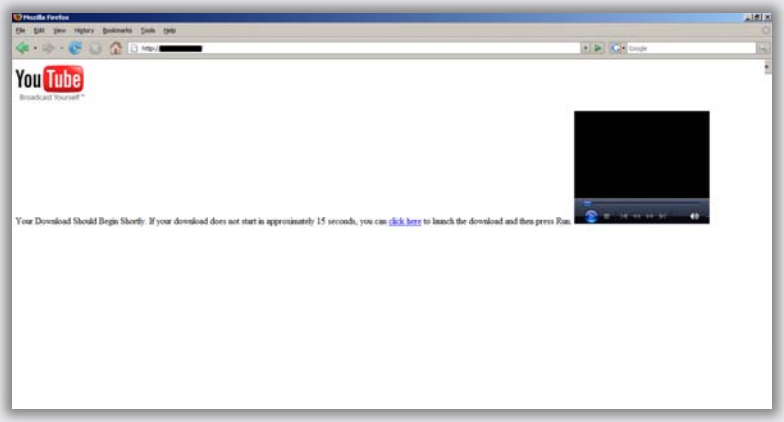
Storm requires user intervention and assistance to spread and relies on a simple attack technique – social engineering of the victim. To obtain new victims, Storm sends out enormous amounts of email.

NEW LEXICON

Storm has expanded the malware vocabulary by combing new or existing techniques into a larger system:

- **Fast-flux:** designed to thwart tracking and provide redundancy.
- **P2P botnet:** Allows systems to communicate and coordinate attack.
- **Decentralized Command and Control:** Prevents direct attack on the controlling systems, disguises controller network.
- **Self-protection:** Launching (possibly) automated attacks on researchers probing the Storm network.

THE EMAIL MESSAGES ARE DECEPTIVELY SIMPLE, AND CONTAIN ONE OR TWO LINES OF TEXT WITH A URL APPENDED TO THE END



AS IS OFTEN THE CASE, THE WWW.YOUTUBE.COM LINK ACTUALLY DIRECTS THE VIEWER TO A STORM NODE ACTING AS A WEB SERVER. WHEN THE VICTIM CLICKS THE LINK, THEY ARE PRESENTED WITH A PAGE THAT USES A SIMPLE YOUTUBE LOGO.

TWO-STAGE ATTACK

Storm coordinates the email and Web attacks into a two-stage system. This represents an interesting synchronization between the Storm bots sending spam and the other bots serving malicious webpages.

To make Storm even more virulent, the designer included "drive-by" browser exploits – a class of exploits that can infect a vulnerable, un-patched computer simply by means of viewing the webpage – no download of any executable file required.

PEER-TO-PEER AND SELF-DEFENDING

Once compromised, Storm-infected systems connect into a Peer-to-Peer (P2P) network to maintain redundancy and de-centralize communication. Prior to Storm, botnets relied on a centralized command and control structure. They often used IRC channels, awaiting commands from the operator. However, this older design presented a weakness; blocking access to, or shutting down the central IRC channel would effectively "cut off the head" of the botnet, rendering it useless. Storm learned from these weaknesses and moved to a decentralized command and control structure.

To maintain longevity and prevent reverse engineering, Storm contains self-defense features; launching (possibly automated) Distributed Denial of Service (DDoS) attacks if examined too closely. During the initial outbreak, Storm repeatedly attacked researchers who, while investigating the botnet, accidentally triggered a retaliatory attack. This DDoS attack capability has also been used against multiple anti-spam and computer security organizations.

RECYCLE, REUSE AND COORDINATE

When a new system joins the ranks of the Storm network, it can be directed to carry are different types of attacks:

- Sending Storm recruiting spam to grow the Storm network
- Serving malicious webpages
- Attacking Instant Messaging clients
- Providing fast-flux and DNS resolution
- Posting blog spam on websites

Storm bots can be repurposed as-needed to cycle these attacks. The entire network can be synchronized and coordinated to ensure the spam relates to the Web-based landing pages.

ATTACK CAMPAIGNS

The open nature of Storm allows the operator to redirect the computing resources and create "campaigns" by updating the infected systems with new instructions.

There are two primary types of attacks the Storm systems conduct:

- Spam advertising
  - PDF spam outbreaks
  - XLS spam outbreaks
  - MP3 spam outbreaks
  - Text spam for Pharma and stock "pump-and-dump" scams
- Recruiting of new Storm systems

The spam-sending side of this attack sends email to millions different address. The spam messages are simple and direct. The recruiting side is responsible for adding new systems to the Storm network and allows Storm to refresh itself and grow. It uses infected systems to host specific landing pages, directly related to the content contained in the spam.

In the fall of 2007, Storm began a series of recruiting campaigns that progressively increased in sophistication.

STORM RECRUITING ATTACKS

This timeline shows recent Storm campaigns and the effective lifespan of each. These examples show how Storm recruits new systems into the Storm network. Each of these webpages is loaded with a drive-by exploit and downloadable executable. Storm recruiting attack webpages are synchronized with the distribution of malicious emails. If the attack is successful, the infected computer will become part of the larger Storm network. As Storm progresses, the sophistication of each page increases.

YOUTUBE

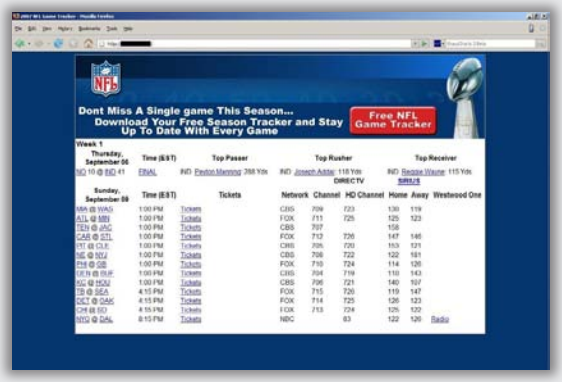
8/24/07 - 9/07/07

FREE GAME

9/14/07 - 9/28/07

9/7/07 - 9/14/07

NFL GAMETRACKER
[NFL SEASON OPENED 09/06/07]



STORM RECRUITING ATTACK WEBPAGES ARE SYNCHRONIZED WITH STORM MALICIOUS EMAILS.

ROTATING THE ATTACK

The progression in sophistication and design is clear. Each new Storm campaign looks more professional and refined than the last. Furthermore, all systems are updated and synchronized to ensure coordination during the attack. The spam and landing pages are always related to the same content and the whole system is cycled in unison.

The different landing pages show that Storm is marketing itself to a victim demographic. Each of these campaigns target different segments or even age groups during the attack. The NFL campaign is obviously directed toward football fans (and was timed to coincide with the NFL season opening), while the Free Games and Psycho Kitty campaigns were probably more successful among younger users. The length of the campaign may also indicate how successful it is; the more successful campaigns running longer while those not getting a good attach and infection rate being swapped out more quickly.

STORM RECRUITING ATTACK WEBPAGES

EACH OF THESE WEBPAGES IS LADEN WITH A DRIVE-BY EXPLOIT AND DOWNLOADABLE EXECUTABLE.

IF THE ATTACK IS SUCCESSFUL, THE VICTIM COMPUTER WILL BECOME PART OF THE LARGER STORM NETWORK.

KRACKIN

10/16/07 - 10/21/07

10/10/07 - 10/24/07

Note: Searches on these dates not exhaustive.

PSYCHO KITTY

NOTE THE INCREASING SOPHISTICATION OF EACH PAGE AS STORM PROGRESSES.

REUSABLE ATTACK PLATFORM

Previous malware was designed kamikaze-style. Once launched, it would run until out of fuel and crash – ultimately melting back into the Internet. Storm, however, is not single-use malware. It is designed as an adaptable, extensible and reusable platform. This adaptation has allowed Storm to last (and grow) throughout 2007. Storm's architecture means it will be measured by its longevity rather than overall destructive power or noisy headline grabbing infection techniques.

Looking ahead, the malware-as-platform design that Storm has so successfully demonstrated will no doubt be copied, improved and refined in the coming years.

> “Malware is a serious issue that must be addressed **alongside viruses, worms, spam and other threats,** but one that many organizations focus on less than they should.”

—OSTERMAN RESEARCH

Malware Trends

For many years, virus and Trojan infections spread predominately through email. As the threat grew, most organizations deployed multiple layers of generic virus defense: multi-vendor best-of-breed scanning engines running on clients, groupware and gateways; zero-day virus outbreak protection; and restrictions on malicious attachment types flowing into an organization.

The infection landscape is now changing. In 2007 we saw a significant growth in the number of virus outbreaks that started as text-only email message that simply contained a link to an attackers' webpage. Once a user clicked on that link, malware payloads would be delivered through known Web browser exploits while the user saw some seemingly innocuous advertising or banal humor.

Compromising Users Where They Feel "Safe"

Even more threatening is the compromise of legitimate sites by attackers that piggyback on the user's trust of a known domain to deliver malware payloads while the user thinks they are on a perfectly safe site. First generation URL filtering techniques do not provide adequate protection from this type of threat – companies should rely on Web reputation systems to detect and block embedded threats.

While most spam URLs point to Web servers with extremely low reputations that can be blocked by advanced multi-protocol reputation systems, the overwhelming majority of sites visited by users over the course of a day have comparably good reputation scores.

ISN'T MALWARE JUST A VIRUS?

"Malware" is a term used to describe specific threats that are downloaded from webpages without a user's knowledge. While similar to viruses (in that malware can infect a users computer and cause system damage or loss of sensitive information), malware is a unique threat – which, at times, cannot be detected by traditional anti-virus scanners.

So, while many users think they are protected from malware because they are running one or two anti-virus engines on their desktop computer, the truth is that often they are not. Many companies are beginning to deploy special malware scanning engines at several points in their network to help protect sensitive corporate data.

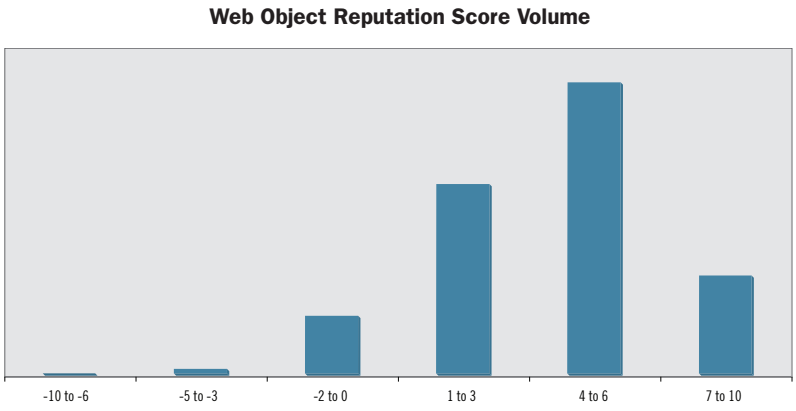
While spam can be a way to drive users to specific infection traps, attackers also have an incentive to spread their malware by compromising high-traffic legitimate websites and attempting to infect as many systems as possible that are merely "driving by."

A Google study released in May 2007 analyzed the presence of malware across all pages indexed by the Google search crawler. It was reported that one in ten webpages are infected with malicious code, and that 70 percent of Web-based infections were found on "legitimate" websites (those with a neutral to positive reputation).

In January 2007, during the run-up to the Super Bowl, the websites of the Miami Dolphins and of Dolphin Stadium was compromised and attackers subtly altered the HTML pages to infect user's PCs during normal Web browsing. This was a well-chosen target for the attackers, as the Super Bowl is the most-watched sporting event on U.S. television. Attackers are picking their targets to guarantee as many exposures as possible.

Later in the year, the website for the Bank of India was similarly hacked, distributing the password-stealing MPack Trojan through an HTML IFrame compromise.

These "malframe" compromises are becoming more common on legitimate sites, as the crime syndicates behind these organized attacks have realized the return on investment from distributing reusable Trojan software far and wide. Recently it



USER BROWSING ACTIVITY BY REPUTATION SCORE

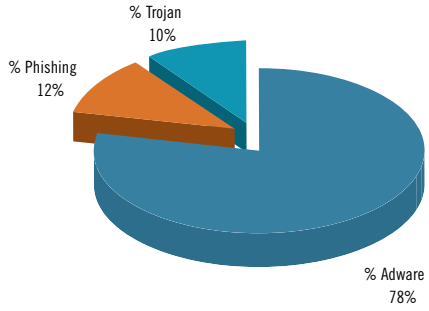
IN AUGUST, THE BANK OF INDIA WEBSITE WAS HACKED – FOR DAYS, IT DISTRIBUTED THE PASSWORD-STEALING MPACK TROJAN THROUGH AN HTML IFRAME COMPROMISE

has been discovered that the Bank of India attack was financed and organized by a well-known cyber criminal group euphemistically known as the "Russian Business Network." This organization is said to be based in St. Petersburg, have protective political connections, and provides network and computing resources for malware distribution, child pornography and phishing.

Malware Infiltrates the Web

The figure at right shows the malware categories found by scanning Web objects retrieved from pages that were not outright blocked because of their low reputation history (such as those found in the URLs of spam messages), and shows that it is possible and even common for well-known and trusted sites to contain malicious content that must scanned for and blocked.

Malware Categories Detected In Scanned Objects



MALWARE CATEGORIES FOUND BY SCANNING WEB OBJECTS RETRIEVED FROM PAGES THAT WERE NOT BLOCKED OUTRIGHT

Spam, viruses, phishing, Trojans and malware have all blended together, with one attack being used to propagate the platform to deliver another attack that launches a coordinated email and Web campaign designed to defraud and compromise the security of all Internet users. Just as no organization today would consider running their email systems without multiple layers of defense, the Web threat must be similarly secured, with categorization of URLs – based on historic reputation, in-depth scanning of Web objects with multiple anti-malware engines, and constant vigilance against internal infections that may come from unprotected networks such as home offices and public wi-fi access.

A Google study, released in May 2007, analyzed the presence of malware across all pages indexed by the Google search crawler. It was reported that one in ten webpages are infected with malicious code, and that 70 percent of Web-based infections were found on "legitimate" websites (those with a neutral to positive reputation).

A LOOK BEHIND THE CURTAIN AT MALWARE PRODUCTION, SALE AND DISTRIBUTION.

MPack Attack Analysis

MALWARE INSIDE THE FIREWALL

In 2007, attackers repeatedly compromised legitimate websites to distribute malicious code. Many of these attacks used a new malware kit called MPack. Like Storm, MPack uses a two-stage attack to infect computer users.

MPACK SUMMARY:

- PHP-based malware kit
- Sold by Dream Coders Team
- Includes one year of support, fresh exploits and add-on modules
- Designed specifically for Web-based attack
- Deployed using an IFrame attack injected into legitimate websites
- Maintains infection and attack statistics

> ***"Do you feel sorry for the people whose machines are infected by an attack?"***
>
> ***"Well, I feel that we are just a factory producing ammunition."***
>
> ***Robert Lemos – DCT, MPack Developer***
> *in an interview with Security Focus*
> *July 20, 2007*

TROJANS FOR HIRE

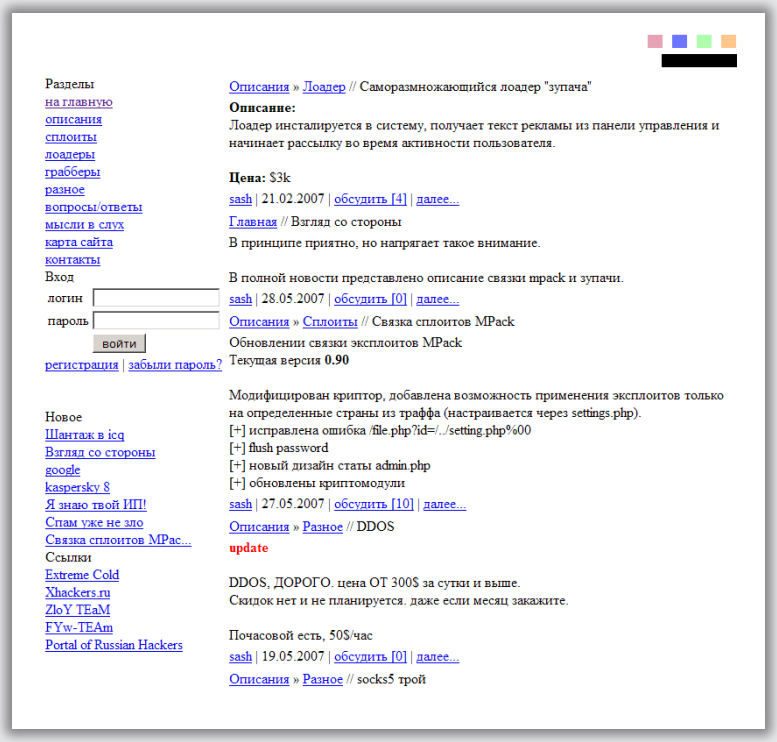
MPack is a PHP-based malware kit that is commercially designed, updated, supported and sold. $500 to $1000 buys the base system. For a period of one year, the Dream Coders Team (DCT) will supply fresh exploits and support the MPack tool. Add-on modules ranging from $50 to $300 can be purchased for the most recent vulnerabilities – the more serious the vulnerability and the more systems that can be compromised, the higher the cost.

Selling malware or exploits isn't new, but providing service and support does set a precedent. MPack and the Dream Coders Team have created a market, providing up-sell add-ons and offering on-going support for the malicious products they sell.

MAINTAINING ATTACK STATS

MPack "customers" purchase the MPack kit, but in order to carry out actual infections, they must load the exploit pack on victim computers. Unpatched computers hit by drive-by exploits are the simplest targets.

An MPack attack is meant to hit a large number of systems with little to no oversight by the attacker. To monitor infection rates, the MPack toolkit provides an administrative interface. The interface records statistics on the number of systems viewing each infected page and the number of successful exploits. It breaks down infection rates into geographic areas and monitors which exploits are most successful. These statistics and metrics allow the MPack customer to measure the attack's effectiveness and demonstrably measure their return on investment. The MPack design and frequency of these types of attacks indicate that both are likely to grow.



MPACK DISTRIBUTORS PROVIDE UP-SELL ADD-ONS AND OFFER ON-GOING SUPPORT FOR THEIR MALICIOUS PRODUCTS

MPack v0.90 stats

Attacked hosts (total - uniq)	
IE XP ALL	20295 - 18373
QuickTime	5316 - 4595
Win2000	625 - 559
Firefox	2363 - 2312
Opera7	75 - 54

Traffic (total - uniq)	
Total traff	25294 - 22723
Exploited	12128 - 4043
Loads count	-
Loader's response	0% - 0%
Efficiency 0% - 0%	

Browser stats (total)

Modules state	
Statistic type	MySQL-based
User blocking	ON
Country blocking	OFF

Country	Traff	Loads	Efficiency
IL - Israel	10826 42.8%	0 0%	0%
US - United states	4577 18.1%	0 0%	0%
RU - Russian federation	2956 11.7%	0 0%	0%
XX - Unknown country	1483 5.9%	0 0%	0%
ES - Spain	920 3.6%	0 0%	0%
CA - Canada	483 1.9%	0 0%	0%
DE - Germany	425 1.7%	0 0%	0%
TR - Turkey	421 1.7%	0 0%	0%
GB - United kingdom	314 1.2%	0 0%	0%
UA - Ukraine	257 1%	0 0%	0%
A2 - Satellite provider	237 0.9%	0 0%	0%
FI - Finland	177 0.7%	0 0%	0%
MX - Mexico	160 0.6%	0 0%	0%
FR - France	104 0.4%	0 0%	0%
NL - Netherlands	96 0.4%	0 0%	0%
IN - India	92 0.4%	0 0%	0%

TO MONITOR INFECTION RATES, THE MPACK TOOLKIT PROVIDES AN ADMINISTRATIVE INTERFACE

DISTRIBUTION TECHNIQUES

Just prior to the Super Bowl, the website of the Miami Dolphins was compromised, delivering a malicious payload to anyone viewing the site. Rather than being an unplanned, opportunistic attack, the compromise of the Dolphin's site was obviously timed to inflict the most damage on the largest number of systems.

In June there was a similar incident; attackers hit more than 10,000 websites, mostly based in Italy. These sites had an illicit "IFrame" element added to the page which went undetected by the original site's authors. As end-users viewed the infected webpages, the IFrame (without user intervention) delivered a set of drive-by exploits, compromising the target system. The exploits included keyloggers and Trojan-downloaders – small bits of code that can be used to load other malware on the system.

WEB USAGE LEADS TO CORPORATE DATA LOSS

First generation URL filters that attempt to categorize sites and block risky websites or behavior cannot provide effective protection when even the trusted sites are hijacked and become malicious. For companies this change in tactics means even employees who engage in "Safe Browsing" and avoid questionable websites represent risk.

Many of the MPack attacks infected systems with "phone-home" malware – which attempts to steal data from the infected system and post it to a central location. Many corporate firewalls are not designed to monitor or block data transfers initiated from within the corporate network – especially if they are cloaked to look like normal user activity.

Even previous best practices of scanning incoming email streams for virus content and keeping desktop anti-virus software up-to-date is not enough. Because the MPack exploits come over HTTP from what are assumed to be safe sites, the email channel is not involved.

IFRAME OR iFRAME?

Many of the Web-based browser attacks these days make use of the <iframe> HTML tag. IFrame is a useful feature that enables numerous Web 2.0 sites to dynamically construct webpages for users.

Unfortunately the <iframe> tag can also be used by attackers to insert a malicious payload into an existing website without changing the actual appearance of the page.

IFrame attacks have come to be one of the most common threats on the Internet, usually used to distribute Trojan software like MPack. Organizations must ensure they have secured their Web traffic as well as their email traffic to defend against these new multi-phase threats.

With professional malware developers providing new exploits to surreptitious criminal networks in order to exploit a user's trust, we see a worrisome shift in the threat network where the economics of labor have been divided to allow each participant to focus on what they are best at, and further advance the sophistication and damage posed by malware attacks such as MPack and Storm.

Conclusion

The theme for malware in 2007 is increased sophistication. Attackers are still engaged in the traditional types of attacks: spam, malware and data theft. However, these attacks became more sophisticated and refined. Attackers moved away from the single-shot, specifically designed attack and moved into reusable platforms that can cycle, synchronize and distribute dynamic attacks. Spam is increasingly used as a benign gateway into corporate networks, using social engineering techniques that cause the end-user to draw malware into the network.

Malware is no longer a single-step infection. New attacks are multi-phase – supported, distributed and managed by a well-defined infrastructure.

Spam Still Pays

2007 was the year of spam attachments. Spammers conducted trials of more than 20 different file attachment types to determine which had the best success rates. Rapid onset spam attacks became commonplace, with outbreaks spiking in volume very quickly and anti-spam companies scrambling to adapt. This left little reaction time, and many customers found themselves reevaluating anti-spam products that could not adapt.

Many of the most malicious attacks start as a seemingly innocuous spam message with nothing more than a few words of text and a single URL. These messages often slip past traditional spam engines that are looking for keywords, or for graphics touting the latest stock spam. When they land in the recipient's inbox they have made it to the most sensitive part of the corporate network. All

PREDICTIONS FOR 2008

2008 will be the year of social malware. Modern malware borrows attributes from the social networks of Web 2.0 – it is collaborative, adaptive and intelligent. Corporations are under increasing pressure to ensure the integrity of their sensitive information. The sophisticated peer-to-peer networks (like Storm) that malware writers are building to harvest this data are becoming harder to detect and stop. To combat this threat, companies need to deploy comprehensive security systems.

Spam volumes will continue to grow without limit. The underlying economics support this and it has profound implications for the anti-spam industry. As spam volumes grow, spam filters must increase their catch rates. The escalating investment required to accomplish this will drive consolidation of the anti-spam industry, as only a small number of vendors will have the resources to stay ahead of spam.

The use of blended attack techniques will continue. This means that organizations must think holistically about their approach to security. Point solutions for email and Web will not be as effective as a comprehensive system that analyzes email and Web traffic and sharesinformation between the two. This is the best defense to protect against blended threats.

it takes is one errant click of the mouse and the payload is downloaded – providing full access to the user's computer, and possibly the internal network.

Malware Platforms

Storm and MPack dominated much of the Internet security news in 2007, but not just because of their size and scope. They both introduced new, more sophisticated techniques that demonstrate the refinement of malicious software. Malware creators are spending more time and resources developing an actual platform that is designed to last and be reused. Delivery methods are also changing, moving toward blended attacks that combine both email and Web services.

Attacks are now originating from directly inside the "protected" corporate network. Many administrators believe they have secured their infrastructures and that spam is nothing more than an irritant. The truth: spam is being used as a gateway, designed to lure users to dangerous sites. To respond, companies must deploy the most advanced email security systems to stop inbound threats, enforce strong classification and scanning of all user-initiated Web traffic and monitor closely for possible internal malware infections.

A higher frequency of attacks is also being seen – timed to coincide with popular events and major news stories in an attempt to make the message seem more legitimate. These attacks are designed to maximize the spread of malicious content by piggy-backing on strong public interest in sports, political activities, or natural disasters.

Recommendations

The multi-phase, multi-protocol nature of these new attacks renders some previous security best practices obsolete. Legacy anti-spam gateways can no longer keep up with the diversity and sheer amount of spam being sent. Traditional Web proxies (used for caching and acceptable-use enforcement for Web browsing) are insufficient when it comes to protecting users against many of the new threats being delivered through HTTP.

Secure Web Traffic

Even if a company has deployed a URL filtering solution to control and report on individual Web usage behavior, these databases are insufficient when it comes to preventing malware downloads into its network. A URL filter's security category maintains a list of webpages where malware has been seen in the past, but does not actually scan Web objects for new infections in real-time. Relying on a reactive security list for malware protection is akin to using only a legacy DNL blacklist in email to protect against spam: totally insufficient. As malware distributors are getting better at inserting their malicious payload into compromised "legitimate" sites, the URL filtering protection becomes even more useless, as the longer-term reputation of (for example) Yahoo as a search engine will trump an occasional user-generated malware package from keeping people from going there.

Deploy Preventive Protection For Email

With malicious Trojans like *Feebs* and Storm evolving faster, the "traditional" protocols for virus distribution (email) still need advanced protection. Spam volumes are increasing which calls for scalable, multi-core spam defenses to keep pace with the attacks. Reputation systems that can block incoming attacks at the connection level – without the need to examine the message body – reduce the burden on both the anti-spam gateway and the overall network traffic. Deploying zero-day defenses that can detect and quarantine possible viral attachments before traditional virus signatures have been published is imperative for complete network detection.

Protect Against Corporate Data Loss

Some of the worst Trojans aim to scan users' hard drive and send the important information (passwords, corporate documents, financial information) back to their command-and-control centers for use by the criminal gangs financing the development of these programs. Data loss can occur without a Trojan infection however. 2007 has already seen nearly 350 publicly reported data loss incidents involving sensitive personal information, most of which happened

accidentally through employee error. While defending against outside threats coming into the network to steal important information is critical, scanning outgoing communications for possible policy violations is also extremeley important to any organization that deals with any kind of sensitive personal or customer information.

Prevent "Phone-home" Activity

Scanning ingress and egress traffic is the first step to protection, but security personnel must also be vigilant against the risk of laptops and other systems being compromised while on public networks outside of the corporate security blanket. For this reason, it is important to scan for and block malicious "phone home" activity from malware-infected computers that may be trying to retrieve new attack commands or upload sensitive data back to their operators.

Track Important Communications

With the increase in threats, defenses are going to get tighter. It is an unfortunate fact of life: as spam becomes more and more legitimate-looking, poor spam engines are going to start (or continue) losing legitimate email messages. Because of this, and the sizable volume of mail that most recipients are dealing with on a day-to-day basis, it is important to offer users the ability to have a higher level of visibility and control on their messages than traditional email provides. New technologies are available that give real-time tracking of email messages similar to what we are used to with physical package shipping. For email to maintain its usefulness as a cheap and fast way to foster communication around the Internet, we must take added care that messages of high importance are treated as such and given a different class of service.

IronPort Systems, Inc.
950 Elm Avenue, San Bruno, California 94066 **tel** 650.989.6500
fax 650.989.6543 **email** info@ironport.com **web** www.ironport.com

IRONPORT SYSTEMS, a Cisco business unit, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase®, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use — providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

 P/N 451-0309-1 12/07