PUBLISHED BY CISCO AND IRONPORT

2008 INTERNET MALWARE TRENDS

STORM AND THE FUTURE OF SOCIAL ENGINEERING

SPECIAL REPORT

IronPort is now
part of Cisco.

Quick Reference Malware Glossary

Social malware – Malware (such as Storm) which uses sophisticated social engineering techniques to make recruitment spam appealing to recipients. This malware is also highly distributed, adaptable and efficient, like many of today's legitimate applications.

Drive-by exploit – A method of using vulnerabilities in a Web browser to infect a computer with malware, without the computer user clicking on any download or other links on the site. All the user has to do is "drive by" the website – view the site without clicking on anything – to become infected.

Super Node – When a computer infected with Storm has Ports 53 and 80 open and shows it has good connectivity to the Internet, it may be promoted from Storm node to Super Node. Super Nodes take on tasks in propagating and monitoring the effectiveness of Storm that go beyond sending vast volumes of spam.

Distributed Hash Table – A new, decentralized means of discovering and sharing resources with other nodes on a network created for third-generation peer-to-peer networks. Also used with great success by Storm malware.

Fast flux – A DNS technique in which the domain name server registration for a malware website URL is deregistered and reregistered between nodes in the Storm network every few minutes. This keeps the domain name consistent for site visitors, but continually changes the IP address it is hosted from so that the site is difficult to shut down.

Money mule – Someone who launders funds through their bank or PayPal account, forwarding money on, in exchange for a "commission." Typically, this person responded to a spam message offering a job working from home. The money mule doesn't know that the funds they are transferring were fraudulently obtained from phishing emails or fake online sales. Once the defrauded individual tracks down the money mule via their bank or PayPal account, the money is gone but the mule is liable for refunding it.

> “TODAY’S MALWARE, LIKE STORM, EXISTS TO MAKE MONEY. NEW VARIANTS OF THIS
>
> socially engineered type of malware
>
> WILL BE INCREASINGLY TARGETED AND HARDER TO DETECT.”

PATRICK PETERSON,
CISCO FELLOW AND
IRONPORT DIRECTOR OF TECHNOLOGY

LEARN MORE >>

SPECIAL REPORT

Introduction

In 2007, Storm burst onto the scene and rapidly spread. A new form of malware that propagated using a combination of email and websites, it proved extraordinarily sophisticated.

Storm used social engineering techniques to make its messages highly appealing to open and click through to. It took advantage of both lightweight and advanced protocols to spread, communicate and maintain its network. It was extremely adaptable – as well as self-defending. It was built as a flexible, reusable platform. And it was designed to make money.

Estimates of the number of computers infected with Storm ranged widely, with some security researchers positing that up to 50 million computers had been infected. Cisco's IronPort® Systems estimates that, at its most destructive point in July 2007, about 1.4 million computers were simultaneously infected and active – but that Storm continued to infect and re-infect around 900,000 computers per month. Storm has since shrunk in size for a variety of reasons, such as computers being disinfected or becoming dormant until needed again, and parts of the network being separated or switched to new, different botnets.

Still, Storm and newer malware botnets that build on Storm's strengths continue to affect and threaten Internet communication. To help explain the spread of Storm and current and future threats posed by similar malware, this report offers an examination of Storm and its history.

Start of the Storm

In January 2007, a new type of malware started spreading across the Internet, widely infecting computers running Microsoft operating systems.

Storm malware was first discovered on January 17, 2007. The name "Storm" came from the header of an early Storm spam message – "230 dead as storm batters Europe" – purporting to provide news about a major windstorm, Kyril, that was passing over Europe at the time. However, because of its broad scope and capability, Storm is called different things: Storm Worm, Storm Trojan, Storm Botnet, Storm Spam Engine and Storm DDoS (Distributed Denial of Service) Network.

Storm shows several key characteristics, some new and advanced. It uses cunning social engineering techniques – such as tying spam campaigns to a current event or site of interest – as well as a blend of email and the Web to spread. It is highly coordinated, yet decentralized – and with Storm using the latest generation of peer-to-peer (P2P) technology, it cannot be disabled by simply "cutting off its head." In addition, Storm is self-propagating – once infected, computers send out massive amounts of Storm spam to keep recruiting new nodes. It is extremely adaptable and can be used for different types of attacks – including email spam, phishing, DDoS, IM attacks and blog spam. Storm is also self-defending – it has launched DoS attacks against researchers and security organizations studying it.

Because of these characteristics, Storm quickly grew to enormous proportions. By sending out millions upon millions of spam messages – as many as 30,000 to 40,000 emails per hour from each infected computer – IronPort estimates that, at its July 2007 peak, Storm infected more than one million computers and was responsible for 20 percent of spam sent out worldwide. An impressive feat – but how did this happen?

A STORM BY ANY OTHER NAME

Storm may be its most commonly known name, but different security vendors refer to this malware under various names, including:

- Nuwar
- Peacomm
- Dorf
- Zhelatin
- Small.dam
- CME-711
- Peed
- Tibs

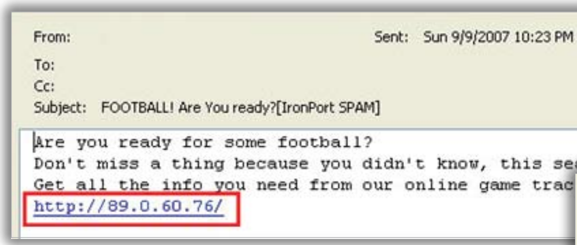
SPECIAL REPORT

Storm in Action

To achieve its remarkable results, Storm uses a sophisticated set of tools and technologies.

Social engineering strategies. In several instances, Storm spread using emails and websites that looked related to current events. For instance, spam messages were sent with news-related headers, Valentine's Day messages and holiday e-cards. Other examples included spam that apparently links to personal videos related to the recipient posted on YouTube, or points to a website that seems to offer NFL tracking tools at the beginning of football season.

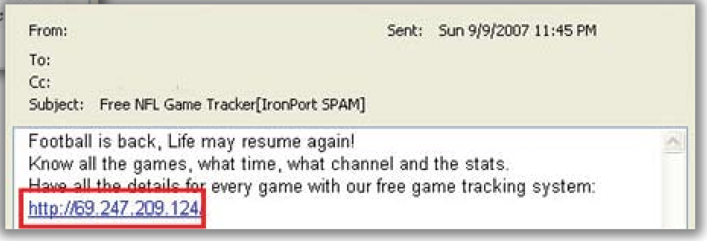
When recipients click on such links, they are offered a legitimate-looking application, which instead infects their computer with Storm when downloaded. Their computer can also be infected through a "drive-by" exploit just from viewing a compromised page with a vulnerable Web browser (such as Microsoft Internet Explorer).



From: Sent: Sun 9/9/2007 10:23 PM
To:
Cc:
Subject: FOOTBALL! Are You ready?[IronPort SPAM]

```
Are you ready for some football?
Don't miss a thing because you didn't know, this season.
Get all the info you need from our online game trac
http://89.0.60.76/
```

STORM TROJAN EMAILS – CLASSIC BLENDED THREAT



From: Sent: Sun 9/9/2007 11:45 PM
To:
Cc:
Subject: Free NFL Game Tracker[IronPort SPAM]

Football is back, Life may resume again!
Know all the games, what time, what channel and the stats.
Have all the details for every game with our free game tracking system:
http://69.247.209.124

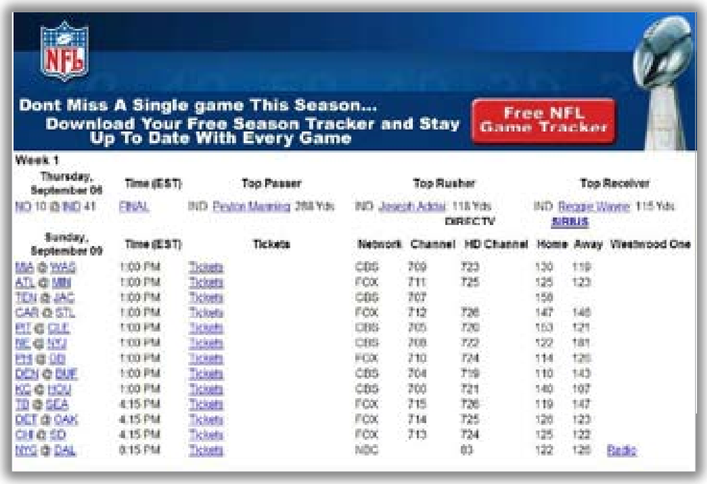
THE RECIPIENT DOES NOT KNOW WHERE THESE LINK TO

Peer-to-peer technology. Older botnets were not as effective as Storm because they used a more centralized command and control (C&C) structure or communications protocols that were relatively easy to detect and shut down. But Storm innovated by using newer open source peer-to-peer protocols, such as Overnet, to decentralize its operations.

This third generation of peer-to-peer applications employs a distributed hash table to let the different computers on a peer-to-peer network discover, store and share information about the system resources of other computers on the network. That means no longer having to depend on inefficient network flooding, a few central servers, or centralized hash table to maintain and share such information. It also eliminates the possibility of "decapitating" the network.

Efficient communications protocols. As soon as a computer is infected, Storm takes advantage of the UDP (User Datagram Protocol) – an Internet communications protocol that lets computers send short messages over any open port. This method is less reliable than TCP/IP, but good enough for Storm's first task, which is to quickly send out messages announcing its presence to other infected computers, so it can join a group of Storm-infected machines to share and compare resources.

The infected computer can then be queried about whether it has the resources to send out spam, or if certain ports are open that will let it perform more advanced Storm tasks. On an infected computer, the Storm application can also perform "health checks," such as repeatedly fetching the Google homepage to make sure the computer remains connected to the Internet and ready for spamming action, or sending out a short file every few seconds to indicate the computer is still active.



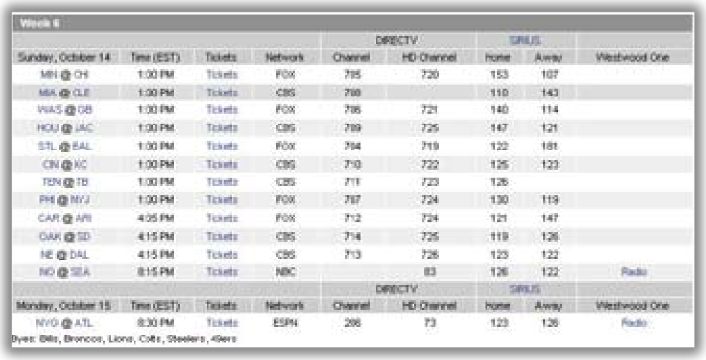
Dont Miss A Single game This Season...
Download Your Free Season Tracker and Stay
Up To Date With Every Game

Week 1

Thursday, September 06	Time (EST)	Top Passer	Top Rusher	Top Receiver
NO 10 @ IND 41	FINAL	IND Peyton Manning 288 Yds	IND Joseph Addai 118 Yds	IND Reggie Wayne 115 Yds

			DIRECTV			SIRIUS		
Sunday, September 09	Time (EST)	Tickets	Network	Channel	HD Channel	Home	Away	Westwood One
MIA @ WAS	1:00 PM	Tickets	CBS	709	723	130	119	
ATL @ MIN	1:00 PM	Tickets	FOX	711	725	125	123	
TEN @ JAC	1:00 PM	Tickets	CBS	707		158		
CAR @ STL	1:00 PM	Tickets	FOX	712	726	147	148	
PIT @ CLE	1:00 PM	Tickets	CBS	705	720	153	121	
NE @ NYJ	1:00 PM	Tickets	CBS	708	722	122	181	
PHI @ GB	1:00 PM	Tickets	FOX	710	724	114	126	
DEN @ BUF	1:00 PM	Tickets	CBS	704	719	110	143	
KC @ HOU	1:00 PM	Tickets	CBS	700	721	140	107	
TB @ SEA	4:15 PM	Tickets	FOX	715	726	119	147	
DET @ OAK	4:15 PM	Tickets	FOX	714	725	128	123	
CHI @ SD	4:15 PM	Tickets	FOX	713	724	125	122	
NYG @ DAL	8:15 PM	Tickets	NBC		83	122	126	Radio

SPOOFED NFL SITE



Week 6

				DIRECTV		SIRIUS		
Sunday, October 14	Time (EST)	Tickets	Network	Channel	HD Channel	Home	Away	Westwood One
MIN @ CHI	1:00 PM	Tickets	FOX	705	720	153	107	
MIA @ CLE	1:00 PM	Tickets	CBS	708		110	143	
WAS @ GB	1:00 PM	Tickets	FOX	706	721	140	114	
HOU @ JAC	1:00 PM	Tickets	CBS	709	725	147	121	
STL @ BAL	1:00 PM	Tickets	FOX	704	719	122	181	
CIN @ KC	1:00 PM	Tickets	CBS	710	722	125	123	
TEN @ TB	1:00 PM	Tickets	CBS	711	723	126		
PHI @ NYJ	1:00 PM	Tickets	FOX	707	724	130	119	
CAR @ ARI	4:05 PM	Tickets	FOX	712	724	121	147	
OAK @ SD	4:15 PM	Tickets	CBS	714	725	119	126	
NE @ DAL	4:15 PM	Tickets	CBS	713	726	123	122	
NO @ SEA	8:15 PM	Tickets	NBC		83	126	122	Radio
				DIRECTV		SIRIUS		
Monday, October 15	Time (EST)	Tickets	Network	Channel	HD Channel	Home	Away	Westwood One
NYG @ ATL	8:30 PM	Tickets	ESPN	206	73	123	126	Radio

Byes: Bills, Broncos, Lions, Colts, Steelers, 49ers

THE REAL NFL SITE

Effective propagation techniques. Once an infected computer announces itself to the Storm network and becomes a node (or "zombie") in the network, it receives instructions to start sending out spam. A lot of spam. IronPort found that one infected computer sent out 30,000 to 40,000 spam messages per hour. Sometimes, the infected computer would stop sending spam after a while or for a certain period of time – an effective camouflage technique that can make it more difficult to detect Storm's presence.

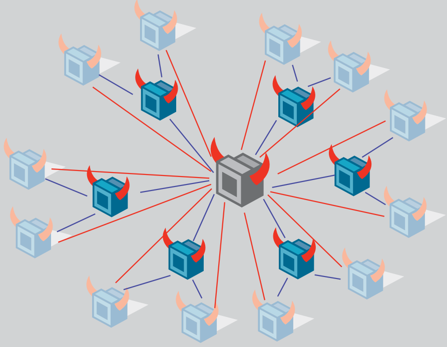
The email sent out by Storm nodes alternates between spam aimed at recruiting additional users and computers to the Storm network via social engineering and spam created to generate revenue. Both of these types of messages are designed to look legitimate and appealing.

A common use of Storm money-making spam is pharmaceutical, advertising medications for sale from (often Canadian) online pharmacies. The websites look credible and the orders are usually fulfilled – with counterfeit drugs from India or Russia. IronPort believes that many of these pharmaceutical sales are funding additional development of Storm and related malware. Other revenue-generating types of Storm email include phishing spam, spam that pushes penny stocks in "pump and dump" campaigns and spam that lures recipients into ostensible work-from-home "money mule" schemes.

Optimizing infected resources. In letting the Storm network know about their presence and capabilities, some computers identify themselves to the network as having Ports 53 and 80 open and being reliably connected to the Internet. These five percent of infected computers then go on to become Storm "Super Nodes." These computers are the Storm elite. They perform more complex tasks, such as hosting Storm recruitment and Storm

JOINING A PEER-TO-PEER BOTNET

- Bot opens a static high numbered UDP port
- Send UDP Overnet peering packets to the initial peer list
- Locate additional peers, make connections, advertise resources



STORM NODES USING PEER-TO-PEER TECHNOLOGY TO ADVERTISE THEIR RESOURCES

PEERING DATA FROM ONE INFECTION

19 February 2008 Infection Observations, 34 Hours

- Seed list contained 241 peers
- All were attempted in less than one second
- 110 were reachable (46%)
- Additional peers were located and connections attempted
- 74,465 additional peers were contacted within 34 hours
- 71,869 additional peers successful (96.5%)
- Port 19074: 973,705 flows in 34 hours
- Port 19074 was 99.875% of all flows
- UDP P2P traffic well distributed to peers
- Bootstrap file 'stale', but P2P still highly effective and distributed

pharmaceutical sales websites, assisting with DNS (Domain Name Server) resolution of these sites, helping control and assign tasks to non-elite Storm nodes, and reporting on website statistics and node health to Storm campaign creators and operators.

Constant adaptability and evolution. Storm's operators are extraordinarily sophisticated in their adaptability. Its spam campaigns (both content and type) are frequently updated to find new victims and vulnerabilities. Storm switches to different types of messages, such as current news headlines, e-card greetings, free game offers, anti-spyware tools, and more. It also varies attachment types – utilizing GIFs, PDFs, Excel files and MP3s to keep convincing recipients to click. Additionally, with Storm Super Nodes measuring the effectiveness of propagation and revenue-generating campaigns, Storm campaign creators can update or switch out less-effective campaigns for new, updated ones with more up-to-date appeal.

To make it difficult to shut down its recruitment/malware and revenue-generating websites, Storm uses a DNS technique called "fast-flux." With this method, the domain name server address for a Storm website URL is deregistered and reregistered between nodes in the network every few minutes. For the site visitor, a domain name (such as "MyCanadianPharmacy.com") stays constant, while the server the site is hosted on is switched to Storm Super Nodes all over the world – making it difficult to track and shut down.

The Storm application or malware code also morphs very frequently, keeping it difficult for anti-virus and anti-malware programs to quickly recognize all or the newest variants. Sometimes Storm goes quiet and stops sending spam from a computer, or part of a network goes dormant, also camouflaging an infection or how far it has spread. When Storm is cleaned from computers or nodes go inactive, the network quickly adapts and peers with different nodes to keep overall operations running efficiently. Finally, Storm defends itself. When it detects that computers from certain locations – such as anti-malware research organizations – are visiting infected sites too frequently, it launches DoS attacks against those locations.

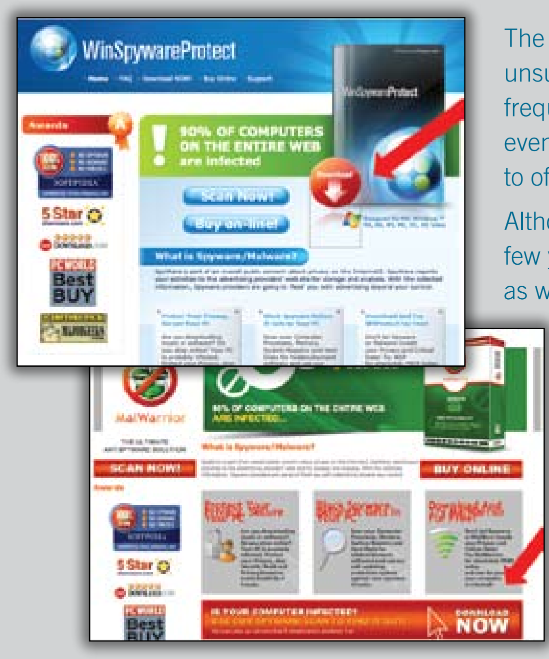
Blending attacks and blending into the background. By combining spam that is socially engineered to be appealing with websites that deliver the malware payload or generate revenue through pharmaceutical sales, Storm creates a highly-effective blended attack mechanism. Rather than trying to deliver the malware payload via an executable attachment in an email – which many consumers recognize they should avoid – the spam message instead acts as a gateway. Not obviously malicious itself, the email lures recipients to websites that will infect their computers, generate revenue for criminal organizations by selling them pharmaceuticals, or (if they respond to work-from-home money mule emails) turn them into inadvertent accessories to phishing crimes.

Meanwhile, for a computer user whose machine gets infected with Storm, most of the Storm activities their computer is performing are not noticeable. Storm is an effective parasite – it refrains from overloading a host computer with commands, instead cleverly running its own processes in parallel with the computer user's. Unless the user notices the computer is suddenly running slower than usual or their anti-virus or anti-malware program happens to detect the variant of Storm present on their computer, the user may never realize they are part of a Storm botnet.

MONEY MULES

In money mule schemes, the recipient takes a work-from-home job laundering funds through their bank or PayPal account – then forwarding the money on, in exchange for a "commission." Though the money mule doesn't know this, the funds are fraudulently obtained from phishing emails or fake online sales. Once the defrauded individual tracks down the money mule via their bank or PayPal account, the money is gone but the mule is liable for refunding it.

"ANTI"-SPYWARE SOCIAL ENGINEERING



EXAMPLES OF MALICIOUS SITES DISGUISED AS ANTI-SPYWARE SERVICES

The tactic of offering up a legitimate-looking website to unsuspecting Internet users is not new to Storm – it is frequently used by makers of Trojan software. Many such sites even disguise themselves as anti-spyware services, purporting to offer short-term trials of malware scanning software.

Although fake spyware scanners have been around for a few years, they continue to lure new victims. This is because, as with other social engineering-driven malware, they are becoming ever more sophisticated in appearance – for example, by displaying actual or slightly altered logos from legitimate companies that rate and review anti-malware software. Two such recent websites, Malwarrior.com and Winspywareprotect.com, feature logos that identify their ostensible anti-spyware scanning software as a "PC World Best Buy" and as a four-star pick from CNet's Download.com.

The number of new domain names being registered and used for fraudulent anti-spyware sites is increasing at a rapid rate, indicating that their approach continues to work.

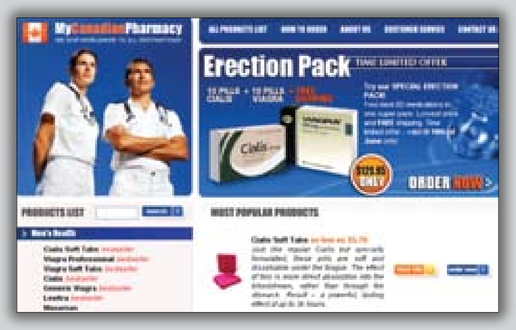
Storm's True Purpose: Revenue

From the above, we see that Storm is very well designed malware, not just a single-use application but a reusable, extensible and scalable attack platform. The creators keep working to ensure its code is updated and tasks are reassigned so the network stays active and can evade detection. The spam campaigns are frequently updated to keep victims and security companies guessing. So, who benefits from this labor?

Unlike many earlier widespread malware attacks, Storm is not designed for flash-in-the-pan glory or to bring computers and networks to a halt. Instead, Storm is deliberately architected for profit over the long term.

Part of Storm's mission is to propagate itself. But its other goal is to make money by getting people to buy pharmaceuticals from Storm-related websites, invest in Storm-promoted penny stocks, or visit phishing sites.

CANADIAN PHARMACY



- Canadian Pharmacy
  - – 1.5 billion spam messages per day
  - – Modifying content and URL domain every 15 minutes
  - – Sent from 106,000 zombies in 106 countries
- Customer Response Infrastructure
  - – 100 new domains per day
  - – 15 uniquely branded websites
  - – Use of 'zombie proxies' in HTTP path
  - – High-quality customer support
- One Criminal
  - – Shipping drugs from India and China
  - – Revenue > $150 million per year

One example, the "Canadian Pharmacy" website, which many Storm emails promote, is estimated to have sales of (US) $150 million per year. The site offers a customer service phone number that goes into voicemail and buyers do usually receive the drugs – the shipments include counterfeit pharmaceuticals from China and India, rather than brand-name ones from Canada.

The way Storm has been generating revenue for criminal counterfeit-pharmaceutical organizations and "pump and dump" stock scammers may only be the beginning.

Storm code now includes assigning an encryption key that effectively separates Storm nodes into smaller networks, whose nodes all use the same encryption key. This means Storm's creators and operators can lease or rent out these separate, smaller Storm networks to different spammers and criminal organizations.

Like booking time on a supercomputer, these organizations will be able to lease Storm time and nodes for new revenue-generating spam campaigns, DDoS attacks against corporate or government targets they select and various other purposes. Because of the effectiveness of Storm's propagation, the business model of renting out parts of the network could be exceptionally lucrative for creators of Storm and similar malware.

SOCIAL MALWARE METHODS USED FOR RECRUITMENT AND REVENUE GENERATION

Malicious "anti-spyware" sites. Sites such as antispyware911.com purport to offer a free scanner that will alert computer users to infections on their system. In reality, the user is downloading and installing malware onto their computer.

Spoofed NFL site. Active just as the 2007 fall football season started, this deceptive site, which promoted a free NFL season game tracker application, looked very much like the real NFL site. The game tracker download was in fact Storm malware.

Spurious YouTube site. Spam purporting to show a video clip posted on YouTube, in which the recipient might be featured, directed recipients to a site that showed a YouTube logo and a message implying that they should click on another link and hit "run" to see the actual video. When they do, a malware download is initiated.

Fraudulent e-cards. Sent out especially around holidays such as Valentine's Day, these messages announce that the recipient has received an e-card from someone. If the recipient clicks through to the website, they download Storm malware in the background.

Free Games, Psycho Kitty and other youth-oriented applications and sites. Especially targeted at younger demographics, these increasingly clever websites look appealing and fun in a MySpace or hip Web 2.0 way, but actually infect visitors' computers with malware.

Vulnerabilities in widely used software applications. Malware creators identify vulnerabilities in popularly downloaded, legitimate software. They take advantage of this vulnerability by inserting active code (e.g., JavaScript), which exploits the applications' flaws – automatically directing the application to retrieve malicious content from malware-laden servers.

Blog comment spam. Also know as "threat blog spam" or "thog attacks," these spam comments on legitimate blogs include links leading to sites that infect computers with malware.

Excel attachment spam. Briefly but intensely used during August of 2007, more than 1 billion spam messages that included Excel file (.xls) attachments were sent out over a six-day period. This may have been a test, which eventually failed, to see how effective Excel attachment messages were in terms of response rates and infiltrating anti-spam systems.

MP3 attachment spam. October of 2007 saw a surge in spam messages with MP3 attachments. The messages purported to be song samples from well known recording artists, but instead the audio files actually contained advertisements that pushed stocks in "pump and dump" schemes.

PDF attachment spam. Another tool for stock scams, PDF attachment spam superseded low-quality GIF spam. Many of the spam PDF attachments looked like well designed, legitimate investment newsletters.

Pharmaceutical spam. This type represents the vast majority of revenue-generating spam sent out using Storm botnets. The spam messages direct recipients to credible-looking sites offering drugs like Viagra and Cialis for sale. The sites are well designed, and include legitimate-looking information, cleverly forged logos and seals of approval, ostensibly from pharmaceutical industry watchdogs. These criminal affiliate websites usually fulfill the orders with counterfeit or inferior pharmaceuticals.

Phishing spam. Spam directing recipients to apparent financial management sites where their personal and financial information gets collected for nefarious purposes.

Money mule spam. Messages that offer recipients work-from-home jobs transferring money through their bank or PayPal accounts for a commission.

Social Malware and Beyond

Storm's presence on the Internet seems to have declined significantly since its mid-2007 peak. On one hand, widely used anti-virus and anti-malware software programs – including Microsoft's Malicious Software Removal Tool – are now able to detect and clean more variants of Storm, so many computers were cleaned. On the other hand, the creators and operators of Storm seem to be continuing to run and propagate new botnets. Possibly derived from Storm, these operate more quietly, are spread out into smaller networks and are designed to be even harder to track and disinfect.

Another disquieting trend is that malware creators are beginning to offer their products as complete solutions – including technical support, analytics and administration tools, and software updates – to increase the efficiency of the malware. MPack, which infects computers using drive-by browser exploits, is one example.

Security researchers have proposed certain countermeasures against Storm and malware like it. One proposal, submitted to the IETF (Internet Engineering Task Force), recommends limiting the number of times per day the IP address for a domain name can be changed, to stop malicious use of fast-flux DNS techniques. European researchers have also looked into creating "counter-worms" that would embed their own payload – designed to override Storm commands – into the code and spread it instead. Other ideas include trying to cut off communications between nodes by tracking the partitioning encryption keys Storm now uses.

But as with weather predictions, one key method that may prove valuable in creating countermeasures to Storm (and malware like it) is closely observing patterns.

In-depth monitoring and tracking of patterns of network traffic and types of downloads, as well of unusual activity can help identify threats more quickly. When a new, unusual pattern of activity – whether for a website or email attachment type – is compared to previously monitored patterns of activity, it

DEVELOPED BY CRIMINALS, FOR CRIMINALS?

Researchers at Cisco and IronPort found evidence of links between Storm spam email, Storm money-making as well as recruitment sites and the SpamIt/GlavMed organization. GlavMed is the affiliate program for pharmaceutical sales and the public-facing part of the organization, while SpamIt is the "spamming affiliate and fulfillment house" part of the operation. SpamIt/GlavMed is believed to have ties to the criminal "Russian Business Network." These links with Storm email and sites show that a major cybercrime organization is using, distributing and likely funding development of Storm malware.

becomes possible to assess the likelihood that the new kind of activity is either potentially malicious or instead the effect of legitimate changes.

With that pattern-based assessment, it may become possible to preventively block users on a network from visiting malicious websites, stopping the browser from retrieving the infected object and preventing nefarious iFrame redirects without a more thorough query into their provenance – even before the threat is fully developed and formally identified.

Redirects Infect Legitimate Sites

Malware writers are counting on Internet gateways' lack of pattern-assessment technologies, which can detect whether a website or Web-based application has been compromised. Emboldened with the knowledge that most administrators are only using anti-virus scanners or URL filtering at their gateway, the writers simply insert active code (e.g., JavaScript) into websites, which direct a user's browser to retrieve the malicious content from malware-laden servers.

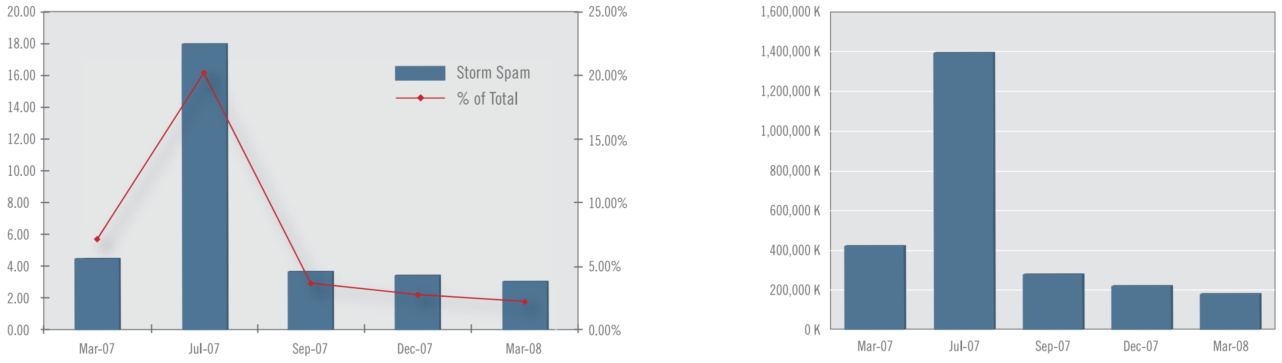
These websites can be well-known and legitimate, or botsites that were specially created to rank well in search engine results. The JavaScript tells the browsers to grab a file from another Web server hosting the actual malicious Trojan (often through an embedded iFrame), which is then installed in the background without the users' knowledge. Once installed, the Trojan can do a number of things – including stealing passwords or system data.

Employing a pattern-assessment capable Web reputation system – one which performs object scanning and has the ability to see every request made by the browsers, even after the initial HTML page is requested – is the best way to effectively protect against these types of attacks, without needing to block the entire webpage.

Combating New and Emerging Threats

The 2007 rise of Storm was a harbinger – this new kind of social malware is continuing to grow and increase in sophistication. New, widespread malware botnets which share characteristics with Storm include Srizbi, Bobax and Kraken/Kracken. IronPort is tracking these botnets and implementing protective measures against their infection mechanisms. In addition, IronPort monitors and identifies new threats designed to exploit software vulnerabilities (such as those found in application like Adobe Flash Player), as well as website redirects, Google exploits, and

STORM TIMELINE



THE NUMBER OF COMPUTERS SIMULTANEOUSLY SENDING OUT STORM-RELATED MESSAGES PEAKED IN JULY 2007, GENERATING MORE THAN 20 PERCENT OF ALL SPAM.

spam attacks that take advantage of "Out of Office" autoreplies to validate email addresses and even hijack corporate mail servers.

For most of the last thirty years, spam has been an annoyance, created by individual amateurs. Those days are over. As Storm shows, today's extremely organized, technically savvy, well funded malware efforts are comparable in scale to legitimate software vendors. Talented engineering teams have now moved to the dark side, and are a threat to every organizational network and individual with an email account and Web browser.

However, by tracking new threats as they emerge, and utilizing holistic solutions that detect not just particular variants of malware but malicious patterns in network traffic and use, administrators and security organizations can protect users and networks from becoming infected.

PREVENTING THE SPREAD

Because Storm and its successors use a blended attack – where the malware payload isn't in the email message but on a website the email points to – separate anti-spam and Web traffic monitoring systems aren't as effective at stemming the spread of such malware. For greater effectiveness, IT departments should consider solutions that can detect malicious patterns and holistically share results between the following functions:

Spam filtering. Storm sent out email with different attachment types – some of which (such as PDFs) were initially difficult for anti-spam programs to identify as spam – in different campaigns over 2007. However, Storm seems to have settled on spam that includes a short message and website link, rather than an attachment, as most effective in 2008. The anti-spam solution should block email that includes suspicious domain names and URLs as well as email with suspicious attachments.

Web reputation assessment. An anti-malware system that uses Web reputation to identify and block connections to suspicious websites, and checks every object a browser needs in order to load a webpage correctly, is crucial. As this new kind of malware may compromise trusted, legitimate websites to insert a malicious payload, an accurate Web reputation system should not merely depend on past reports of malware or the domain itself. The most effective system proactively assesses threat indicators from any URL, IP address or Web server on the Internet.

In addition, ostensible spyware scanner and fraudulent protection websites (which appear to thwart such malicious attacks, but instead deliver malware) are deceiving even sophisticated Web users with legitimate-looking language and counterfeit "endorsements" from recognized software rating companies. Systems that perform object-based checking of information and verify the source of the data, instead of relying on URL categorization, can more effectively block downloads from these sites.

Port and communications activity monitoring. A system that detects patterns and flags unexpected levels of activity on any unusual ports (such as Port 53 or 25) or using atypical communications protocols can be an excellent warning indicator.

Keeping anti-virus and anti-malware products updated. Given the speed and frequency with which Storm and its successors morph into new variants, comprehensive, reliable and very frequently (or automatically) updated anti-virus and anti-malware products are essential.

Finally, IT departments may help reduce infections by regularly reminding computer users on their network about how these new kinds of malware use social engineering and what types of email, blog comments and websites may try to infect their computers with malware payloads.

IronPort is now
part of Cisco.

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

IRONPORT SYSTEMS, now part of Cisco, 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.

DISCLAIMER: The law in this area changes rapidly and is subject to differing interpretations. It is up to the reader to review the current state of the law with a qualified attorney and other professionals before relying on it. Neither the authors nor IronPort make any guarantees or warranties regarding the outcome of the uses to which this material is put. This paper is provided with the understanding that the authors and IronPort are not engaged in rendering legal or professional services to the reader.