A Storm (Worm) Is Brewing

Brad Smith

Last year marked a turning point in malicious software's evolution that has caused serious concern among security experts. Skilled hackers have designed a sophisticated type of malware that blends multiple techniques, hides and changes its code, and employs tricks to entice users to implement and spread it.

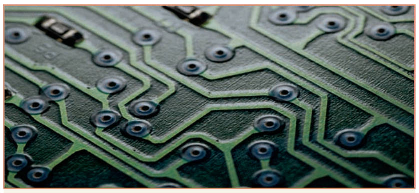
The malware is generally called the Storm worm, although it is also known by names such as Nuwar, Peacomm, Tibs, and Zhelatin. Security vendors believe the malware has been around since August 2006. However, it began gaining widespread attention on 19 January 2007, when it launched a series of attacks that generated an estimated 20 times the normal spam volume.

The Storm worm has created a massive network of remotely operated zombie computers that the person or people who control the malware have used to launch spam and distributed denial-of-service (DDoS) attacks.

A key to Storm's success has been its controllers' clever and creative use of social engineering to entice unsuspecting victims to open e-mail attachments or connect to harmful websites.

In addition, the controllers regularly change the malware's code and delivery mechanism.

Bruce Schneier, chief technology officer of security vendor and consultancy BT Counterpane, said the Storm worm is probably the wave of the future and is particularly dangerous because of its complex design and aggregation of existing malware tools.



Despite its name, the malware is not just a worm but also includes Trojans, botnets, rootkits, encryption, and peer-to-peer networking, noted Joe Stewart, researcher for SecureWorks, a managed-security service provider.

"This is top-quality, state-of-the-art malware," said David Perry, director of global education for security vendor Trend Micro.

INSIDE THE STORM WORM

The Storm worm has been definitively linked to several large waves of spam attacks in April, May, July, and August 2007, as Figure 1 shows. It is probably responsible for several others, according to security experts.

The malware's controllers have also used their zombie network to launch DDoS attacks on antispam and antivirus organizations, such as the Spamhaus Project (www.spamhaus.org), that have tried to stop their activities.

Storm targets PCs running Windows 2000, XP, and Server 2003, and security experts expect it also will target Vista.

Most experts think Storm's controllers are based in Russia or Eastern Europe. Much of the traffic from the botnet's controllers appears to come from that area, based on IP addresses traced to server farms there, noted Stewart.

The hosting servers also apparently use text written in Russian for communications, he added.

Show me the money

"The Storm worm is crimeware," noted Symantec director of security response Kevin Haley. "It's about making money in the underground economy."

For example, it has launched spam as part of "pump and dump" schemes, which promote low-value stocks that hackers have purchased. The promotion drives up the stocks' price so that the hackers can sell them for a profit.

Some evidence indicates that Storm's owners have divided the botnet into pieces they can rent to spammers, SecureWorks' Stewart said. In one case, he noted, it appears part of the Storm botnet was used to send out spam for a Canadian pharmaceutical outlet.

Social engineering

For Storm to spread, victims must voluntarily open e-mail attachments or click on links to infected websites. To convince people to open attachments, Storm-related messages use attractive subject lines about a fake or real news event, easy ways to make money, inexpensive products, or communications from a friend or family member.

The subject lines, which sometimes are grammatically incorrect, have read, for example, "230 dead as storm batters Europe," "A killer at 11, he's free at 21 and kill again!," "British Muslims Genocide," "Naked teens attack home director," "Re: Your text," "Russian missile shot down USA satellite," and "US Secretary of State

Published by the IEEE Computer Society

Condoleezza Rice has kicked German Chancellor Angela Merkel."

The person in command of the computer that controls the botnet generates the subject lines and sends them to the bots to use with the e-mail they send.

Storm worm elements

Trend Micro senior researcher Jaime Yaneza said the Storm worm infects computers with multiple payloads that contain several key elements.

The payload includes software that handles the forwarding of spam and the replacement of the core botnet code to disguise the malware's presence.

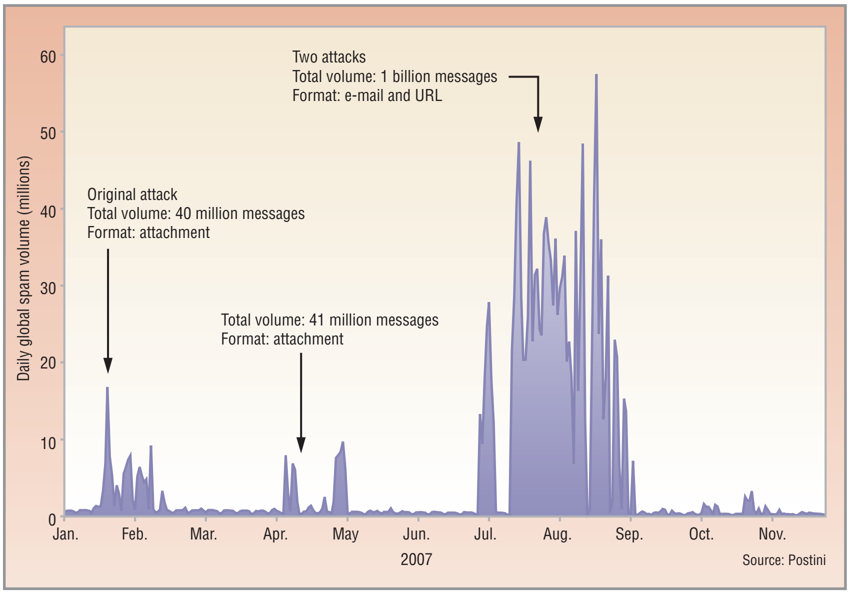
It also contains a worm that enables Storm to replicate and spread by sending copies of itself over a network and then infiltrating victims' systems by exploiting Web browser and other system vulnerabilities.

Storm also includes a Trojan horse that, once loaded on the infected bot, creates a backdoor that the malware's authors can use to issue attack commands. The Trojan—which appears to be a legitimate file such as a video clip of a news event—also carries a rootkit, which masks the malware. The rootkits add to or replace part of the kernel code, which makes them difficult for security software to detect.

The rootkit also removes evidence of Storm by replacing binaries that list a system's files and processes with a version that doesn't reveal the malicious code. It also intercepts API calls that provide a list of running processes and removes the ones related to Storm. And it deletes entire files or utilities that could indicate the malware's presence.

In addition, the rootkit can modify the code of legitimate existing drivers in the Windows registry so that they launch Storm every time Windows starts.

Storm's owners can divide the core botnet into subnetworks to, for example, rent to different groups of spammers. The owners can configure each of these subnetworks differently.



Source: Postini

Figure 1. The Storm worm, which its controllers unleashed last year to distribute large amounts of unsolicited e-mail, caused huge spikes in global spam volumes during its major 2007 attacks.

Communications

The malware uses peer-to-peer networking—via the Overnet protocol, designed for decentralized networks such as Storm's botnet—and Internet Relay Chat to feed new code to the zombies.

Storm's human controllers typically use the ICQ instant-messaging platform—a favorite of Russian hackers—to send messages to each other or associates, perhaps to set up a spam attack or discuss new strategies, according to Stewart.

The infection process

Storm can spread via either opened e-mail attachments or visits to infected websites.

Its e-mail messages generally include no text but carry a link to an executable attachment—titled "Read More.exe," "FullClip.exe," "Full Story.exe," "FullVideo.exe," or "Video.exe"—that, if clicked on, downloads software that turns the victim's computer into a zombie.

The messages also sometimes link to infected websites. If unsuspecting users visit an infected site and click on an embedded hyperlink, they can download the Trojan.

Storm can infect webpages with a malicious iFrame (inline frame) that includes a piece of HTML code that, when clicked on, downloads the malware.

Once Storm infects a computer, it can take several additional actions. For example, the malware can upload keylogging software that reads a victim's keystrokes to capture information such as credit card numbers or passwords.

Botnets

According to BT Counterpane's Schneier, estimates of the Storm botnet's size frequently range from 1 million to 50 million computers.

Microsoft says there were probably about 500,000 Storm zombies as of September 2007, based on information from its Malicious Software Removal Tool installed on Windows-based PCs.

Storm worm was so big, it generated 20 million spam messages—20 times the normal volume—during an attack that occurred between 19 and 23 January 2007, noted Adam Swidler, product marketing manager for security vendor Postini.

During a six-week attack the following July and August, Storm worm generated 1 billion spam messages, including about 60 million in one day.

Security experts speculate that Storm worm was responsible for a massive DDoS attack against the Estonian government's cyberinfrastructure in May 2007.

Self-preservation

Storm's authors have changed the malware's delivery mechanism regularly and have used several other sophisticated techniques to make recognition by security products difficult.

Multiple delivery approaches. One of Storm's gambits has been to use spam that includes PDF attachments or electronic greeting cards—such as those distributed this past Christmas and New Year's holidays—with links that actually take users to infected websites. It has also worked via infected audio-file attachments and links in instant messages.

In addition, Storm spam has contained an attractive invitation and a supposed link to a YouTube video. The link actually takes users to a Storm distribution site with the YouTube logo and tells them to click on another link, which uploads malware onto their computer.

Decentralization. Unlike many botnets, Storm uses multiple zombies, rather than a single, central server, for command and control. There is thus no single computer that security experts can target to stop the malware's activities.

Using few bots at a time. Schneier said a small fraction of Storm's zombies spread the malware and an even smaller fraction act as command-and-control servers, while the rest wait for orders.

"By allowing only a small number of hosts to propagate the virus and act as command-and-control servers, Storm is resilient," he explained. Even if security experts shut down the active bots, he noted, the network remains largely intact and other zombies can take over.

Encryption. According to Trend Micro's Yaneza, Storm uses 40-bit encryption to prevent antivirus software from accurately reading its code and identifying it as malware. The system also takes each of its bots out of service for long periods, making them harder to detect.

Code replacement. Commands sent by Storm's controllers replace the malware's core code up to 10 times per hour, making identification by security software difficult, said Yaneza.

Fast fluxing. Storm also makes itself harder to detect via *fast fluxing*, which hides websites that can infect visitors behind an ever-changing network of compromised hosts acting as proxies. The compromised computers' public domain-name records change constantly, in some cases every few minutes. This makes it difficult to track their activities and shut them down.

To combat the Storm worm, security experts recommend basic computer hygiene by individuals and organizations. This includes exercising care when opening e-mail attachments, using intrusion- and rootkit-detection systems, and employing techniques such as the blocking of peer-to-peer communications.

Nonetheless, keeping up with Storm's many changes presents a challenge to security vendors, so the malware promises to continue causing problems.

For the time being, eliminating malware like Storm is going to be difficult because people will continue to open unsafe e-mail attachments, according to computing pioneer and Carnegie Mellon University professor David Farber.

Ultimately, he said, eliminating such malware will require authenticated e-mail because currently, there is no way of knowing whether a message has come from a trusted source or includes a malicious attachment.

In fact, he added, "I think we're going to have to redesign the protocols of the Internet anyway, and when we do that, we will have to pay attention to security."

"We designed the network with very little attention to security," Farber noted. "It wasn't a problem then." ■

Brad Smith is a freelance technology writer based in Castle Rock, Colorado. Contact him at pbradsmith@gmail.com.

Editor: Lee Garber, ***Computer***, l.garber@computer.org