

As Seen In



Monday, March 17, 2008

Botnet scams are exploding

By Byron Acohido and Jon Swartz, USA TODAY

SEATTLE — Two days after actor Heath Ledger died, e-mails began moving across the Internet purportedly carrying a link to a detailed police report divulging “the real reason” behind the actor’s death. Ledger had been summarily drafted into the service of a botnet.

Bots are compromised computers controlled by profit-minded crooks. Those e-mails were spread by a network of thousands of bots, called a botnet. Anyone who clicked on the link got instantly absorbed into the fast-spreading Mega-D botnet, says security firm Marshal. Mega-D enriches its operators, mainly by distributing spam for male-enhancement pills.

Largely unnoticed by the public, botnets have come to inundate the Internet. On a typical day, 40% of the 800 million computers connected to the Internet are bots engaged in distributing e-mail spam, stealing sensitive data typed at banking and shopping websites, bombarding websites as part of extortionist denial-of-service attacks, and spreading fresh infections, says Rick Wesson, CEO of Support Intelligence, a San Francisco-based company that tracks and sells threat data.

“It’s like a disease you can’t even feel,” Wesson says. “The mechanisms we use to protect our networks simply are not working.”

The botnet problem shows no sign of easing. Security firm Damballa pinpointed 7.3 million unique instances of bots carrying out nefarious activities on an average day in January — an astronomical leap from a daily average of 333,000 in August 2006. That included botnet-delivered spam, which accounted for 91% of all e-mails in early March, up from 64% last June, says e-mail management firm Cloudmark.

The upshot of this deluge is profound, if not immediately obvious, says Adam O’Donnell, Cloudmark’s director of emerging technology. Telecoms and Internet service providers must absorb the cost of carrying botnet traffic; they can be expected to pass that expense onto companies and consumers, he says. Meanwhile, tens of millions of botnetted computer users are experiencing degraded performance with no clue why.

“Newer machines feel old, so people end up buying new machines more often than they have to,” O’Donnell says.

Beyond that, cybercrime gangs are stockpiling enough stolen data to fuel identity theft scams for years to come. Meanwhile, law enforcement is negligible, and security protections for consumers and businesses remain, at best, patchwork and haphazardly deployed, says Somesh Jha, computer science professor at the University of Wisconsin-Madison. “The botnet landscape is shifting, and the worst hasn’t happened yet,” says Jha, who is also chief scientist at security software firm NovaShield.

A perfected Storm

Exhibit No. 1 showcasing botnets’ criminal potential: the mega botnet Storm.

At first, the e-mail that began circulating on Jan. 19, 2007, appeared to security researchers to be a garden variety e-mail virus. It carried a tainted link to a news story about a deadly storm. In fact, the gang that released the e-mail had spent months preparing a strategy for amassing a sprawling, impenetrable botnet designed to self-replicate.

Fourteen months later, Storm remains entrenched as the largest, most active botnet clogging the Internet. Security experts credit Storm’s operators with breakthroughs now being widely emulated by copycat botnet operators.

Storm was first to make wide use of peer-to-peer, or P2P, communications — the technology that allows one computer to share files with any other computer across the Internet. Bots in a botnet typically receive instructions from a central PC, called the command-and-control server. Authorities are getting better at discovering and shutting down such central servers.

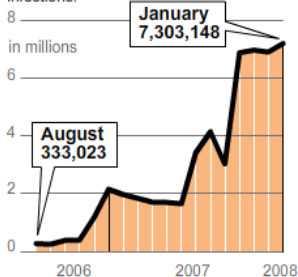
■ CYBERCRIME PAYS

The escalating number of botnets have helped feed a surge in various forms of online fraud.

- Botnet deluge
- Virus rate
- E-mail spam
- Phishing attacks

Botnet deluge

The average daily number of unique botnet communiqués to accept instructions from a controller, deliver spam, conduct phishing campaigns, click on ads to earn ad revenue, carry out denial-of-service attacks, steal data, scan for vulnerable computers, and spread infections.



Sources: Damballa, MessageLabs
By Julie Snider and Bob Laird, USA TODAY

So Storm's operators perfected a way to use P2P communications to issue commands from a rotating subset of PCs inside the botnet. As extra protection, Storm became the first botnet to encrypt its instructions.

"They've built a very resilient infrastructure," says Dmitri Alperovitch, principal researcher at Secure Computing. "If one command server gets shut down, it moves to the next."

Meanwhile, Storm rewrote the book on the psychological ploys — known as social engineering — that lure victims into clicking on tainted attachments or Web links. Storm e-mails arrived with irresistible links to holiday-themed greeting cards, Beyoncé Knowles and Kelly Clarkson music videos, even an NFL game-tracking tool. Storm peaked last July, infecting an estimated 1.7 million PCs, according to Symantec.

Anti-virus firms began to block Storm e-mail, and Microsoft (MSFT) helped clean up Windows PCs infected by Storm. But Storm's operators proved adept at dodging the latest anti-virus filters. Subscribing to the idea that the best defense is an aggressive offense, they also began attacking any researcher who tried to isolate any of their bots. Outsiders detected trying to establish contact with a Storm bot are inundated by an avalanche of nuisance requests launched from the wider botnet.

"Storm has a self-defense mechanism," Alperovitch says. "Any time someone probes the botnet too much, it reacts automatically and starts a denial-of-service attack against that researcher."

Tool of choice

The result: Storm endures as the king of botnets with several hundred thousand infected PCs doing its bidding on any given day. Yet Storm is really a one-trick pony. It generates cash mainly by spewing spam urging recipients to buy shares in obscure companies, the linchpin to an array of scams spinning off the artificial inflation of the share price.

Another tier of smaller, multipurpose botnets spring from widely available tool kits that make it easy for anyone to infect computers, assemble a basic botnet and embark on a criminal career. Dozens of crime rings, for instance, have cropped up to run phishing scams that lure victims into clicking on fake Web pages where they get tricked into divulging passwords and other sensitive data.

Botnets distribute phishing spam, host phishing Web pages and store phished data. Since 2005, phishers have used botnets to take aim at more than 1,750 companies and government agencies, mainly financial institutions, including 106 fresh targets in the fourth quarter of 2007, according to a survey by security data firm Cyveillance.

Phishing expeditions are just one of many uses of botnets. Some botnets crawl the Internet looking for Web pages that can be corrupted with pop-up ads selling fake anti-spyware; some implant programs on popular Web pages to harvest any sensitive personal data typed there by visitors; some repeatedly click on online advertisements to earn fraudulent "click through" revenue.

"Botnets have become the tool of choice for bad guys," says Rick Howard, director of intelligence at VeriSign iDefense. "You take over a box (PC), put it in your botnet and forevermore you own that box and can do whatever you like with it."

One particularly invasive collection of botnets, known as Zbot, is controlled by Russian crime groups going by the online designations UPLEVEL, CAR Group and Glamorous Team. Zbot's operators late last year got away with swiping millions from banks in four nations, says Don Jackson, a senior researcher at SecureWorks who has been monitoring Zbot.

"We know that the amount stolen in December, which affected banks in the USA, U.K., Italy and Spain, was just over \$6 million," Jackson says. "This is based on sources within the banks and law enforcement that work with us."

The scammers enticed bank customers to click on a link purportedly to download an updated digital certificate, the equivalent of a digital ID card. Instead, Zbot installed a program that positioned it to come along for the ride the next time the user successfully accessed the account.

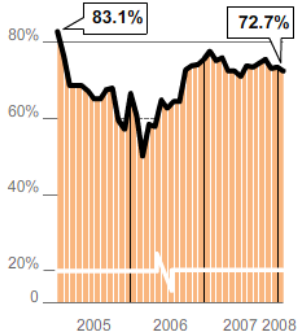
■ CYBERCRIME PAYS

The escalating number of botnets have helped feed a surge in various forms of online fraud.

- Botnet deluge
- Virus rate
- E-mail spam
- Phishing attacks

E-mail spam

In February, 73% of e-mails contained spam. Monthly percentage of global e-mail containing spam:



Sources: Damballa, MessageLabs
By Julie Snider and Bob Laird, USA TODAY

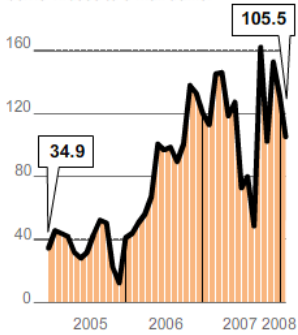
■ CYBERCRIME PAYS

The escalating number of botnets have helped feed a surge in various forms of online fraud.

- Botnet deluge
- Virus rate
- E-mail spam
- Phishing attacks

Virus rate

Monthly ratio of virus to e-mail, as 1 in: In February, one in 106 e-mails contained a virus. Monthly global ratio of e-mail-borne viruses to e-mail traffic:



Sources: Damballa, MessageLabs

By Julie Snider and Bob Laird, USA TODAY

Zbot then automatically executed cash transfers to other accounts controlled by its operators — while the victim did his or her online banking.

“This scheme is extremely clever and quite ironic considering that digital certificates are provided by financial institutions to protect online bank users from fraud,” Jackson says.

Deeper footholds

Zbot notwithstanding, organized crime groups have only scratched the surface of the criminal capabilities of botnets. Meanwhile, law enforcement agencies globally remain hamstrung by a lack of technical expertise, manpower and political resolve to put a dent in the botnet scourge, says Paul Ferguson, senior threat researcher at anti-virus firm Trend Micro.

Numerous indicators portend botnets are destined to increasingly corrupt consumer online transactions and range deeper into corporate and government networks, security experts say.

Some criminals on the cutting edge, for instance, are using data harvested by botnets to send e-mail to specific executives at certain government agencies and large corporations. Carefully crafted to look like they come from a colleague or business contact, the e-mails include a corrupted Microsoft Office file.

Once opened, the tainted file cloaks itself and installs a tool that monitors incoming and outgoing traffic, collecting clues on ways to drill deeper inside the organization’s internal network. Such a foothold can give a botnet operator access to more firepower and improved cover, says Paul Royal, principal researcher at Damballa. “If I can get on a workplace computer, I have a lot more bandwidth and reliability with which to perpetuate illegal activities,” he says. “And the person whose workstation is infected may not even notice.”

Achido reported from Seattle, Swartz from San Francisco.

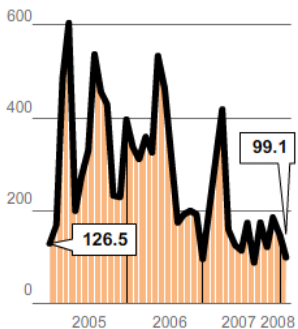
■ CYBERCRIME PAYS

The escalating number of botnets have helped feed a surge in various forms of online fraud.

- Botnet deluge
- Virus rate
- E-mail spam
- Phishing attacks

Phishing attacks

In February, one in 99 e-mails contained some form of phishing attack. Monthly global ratio of phishing to e-mail:



Sources: Damballa, MessageLabs

By Julie Snider and Bob Laird, USA TODAY