Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

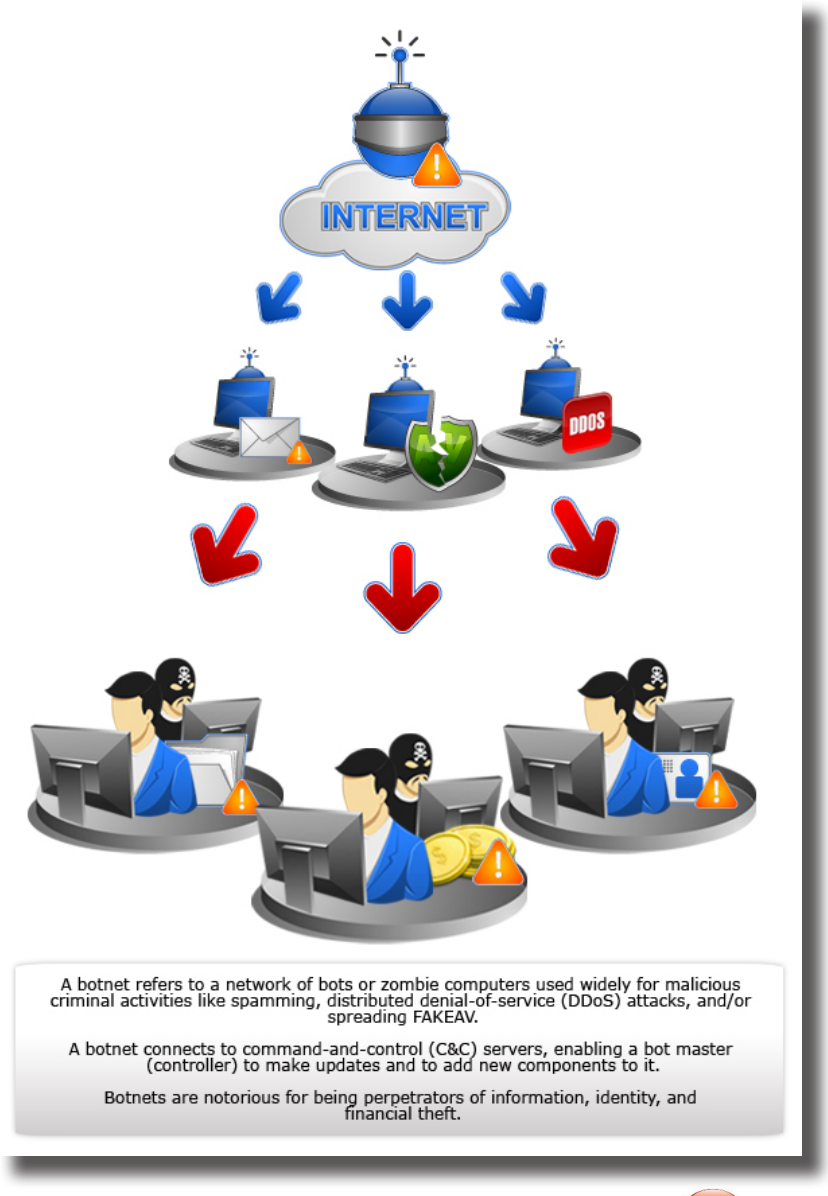
THE EVOLUTION OF BOTNETS

Botnets are considered the most prevalent and dangerous threats lurking in the Web today. The damage they cause can range from information theft and malware infection to fraud and other crimes. In this article, TrendLabs℠ examines where they first came from and how they have evolved over the past 10 years.

Botnets: Perpetrators of Crimeware

A botnet refers to a network of bots or zombie computers used widely for malicious criminal activities like spamming, distributed denial-of-service (DDoS) attacks, and/or spreading FAKEAV. A botnet connects to command-and-control (C&C) servers, enabling a bot master (controller) to make updates and to add new components to it.

A botnet refers to a network of bots or zombie computers used widely for malicious criminal activities like spamming, DDoS attacks, and/or spreading FAKEAV.



TREND MICRO

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

History of Bots

Botnets, like any other technology, are continuously evolving to stay abreast of the latest developments in the threat landscape. Botnets have always been malicious. Originally from the Internet Relay Chat (IRC) world where there were already legitimate IRC software called "bots," which were used to automate certain chat behaviors (e.g., managing chat rooms and so on), the authors of malicious bots retained the descriptor "bot" since they began life within IRC environments. These early, malicious bots did nasty things with the peculiarity that their C&C center was an IRC server and their communication method was via IRC. The very first botnets were seen in around 2001.

In 2002 and 2003, we were introduced to generic SDBOT and RBOT variants. The technology used in these early variants developed and in 2005 and 2006, these botnets began to unleash havoc in the computing world by staging DDoS attacks. DDoS attacks can temporarily knock down a particular website using hordes of compromised machines known as "bots." These also led to the proliferation of adware or programs that displayed annoying pop-up ads on infected systems.

In 2005, Microsoft released *Security Bulletin (MS05-039)* to combat a bot attack that affected many of its product users. This paved the way for what we now call "vulnerability exploitation" wherein cybercriminals exploit vulnerabilities before software developers can release patches. Cybercriminals normally compile, integrate, and pack exploit codes, which are distributed by bots.

"The trend of using botnets for cybercrime was first observed back in around 2006 when botnets evolved to become more sophisticated tools. This was when we began to see them proactively being used for spamming, pharming, information stealing, and even CAPTCHA breaking," said Trend Micro senior advanced threats researcher David Sancho.

"The trend of using botnets for cybercrime was first observed back in around 2006 when botnets evolved to become more sophisticated tools. This was when we began to see them proactively being used for spamming, pharming, information stealing, and even CAPTCHA breaking," said Trend Micro senior advanced threats researcher David Sancho.

In 2007, the emergence of the Storm botnet, hailed at the time as the "largest single source of the world's spam," ensued. Soon after, other notable botnets like Mega-D (detected by Trend Micro as TROJ_AGENT.KHA) arrived.

Botnet activities have evolved and are now geared toward making profit and enabling financial gain. No surprises there. Three of the most dangerous botnets at present are KOOBFACE, ILOMO/Clampi, and ZeuS/ZBOT, particularly with regard to information, financial, and identity theft.

Armoring Oneself Against Cybercrime Attacks

A Trend Micro study found that out of 100 million compromised IP addresses, approximately 75 percent were consumer related while the remaining 25 percent belonged to businesses. KOOBFACE alone, the "largest Web 2.0 botnet," controls and commands around 51,000 compromised machines.

TREND MICRO

Security Spotlight
April 26, 2010

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

The FBI revealed that SMBs have lost US$40 million since 2004 due to rampant online banking scams courtesy of ZBOT/ZeuS and other information-stealing malware.

Users are at great risk in terms of identity and information theft. Cybercriminals use stolen social networking and banking credentials to steal information and money from unsuspecting users. According to an article by Brian Krebs published in October 2009, the Federal Bureau of Investigation (FBI) revealed that small and medium-sized businesses (SMBs) have lost US$40 million since 2004 due to rampant online banking scams courtesy of ZBOT/ZeuS and other information-stealing malware. Also, according to the "2009 Internet Crime Report" of the Internet Crime Complaints Center (iC^3), the total monetary loss related to online fraud soared from US$265 million in 2008 to US$559.7 million in 2009.

Highlighting the risks to SMBs, another article by Krebs reported that more than US$200,000 was stolen from a Missouri-based dental practitioner in a cybercrime that took place in March 2010.

Once systems are compromised, cybercriminals use them to distribute spam, to add more bots or zombie PCs to their botnets, or for other malicious activities like click-fraud scams and data theft. Trend Micro threat research findings can also be indirectly borne out by studies published independently by other security organizations. For example, a study by ClickForensics found that 42.6 percent of click-fraud scams in the third quarter of 2009 were instigated by botnets.

Bots and botnets are embedded within cybercriminal activities and are rented out and sold in today's underground economy. Botnets have definitely become not just cybercrime catalysts but also major contributors to the growing underground economy.

Cybercrime Attacks Involving Botnets

As indicated above, attacks involving ZeuS/ZBOT are some of the most insidious and can prove very costly both for consumers and businesses alike. In a recent attack, a ZeuS/ZBOT variant targeted a number of European countries' banking systems.

ZBOT is a crimeware phenomena created using a toolkit. The ZeuS toolkit enables cybercriminals to create and customize their own remote-controlled malware. The infected machine then becomes part of criminal ZeuS botnets. ZBOT variants are information stealers specializing in robbing online banking and social networking information from victims and sending back the stolen information to a C&C server.

At the most basic level, ZeuS has always been known for engaging in criminal activities, as it signals a new wave of online criminal business enterprises wherein different organizations can cooperate with one another to perpetrate outright online theft and fraud. Trend Micro conducted a thorough analysis of ZeuS and published its findings in a recent report, "Zeus: A Persistent Criminal Enterprise."

The domains used by TSPY_ZBOT.AZX are both hosted on the same server, which is located in Serbia under a registered name. The IP address used and its registered name are both well-known for being part of FAKEAV-hosting domains and previous Canadian pharmacy spam campaigns.

TREND MICRO

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

Botnets are always on the lookout for vulnerable machines that they can compromise.

Botnets are always on the lookout for vulnerable machines that they can compromise. Users can help protect themselves from these types of attacks by keeping their systems up-to-date with the latest security patches, by using vulnerability-shielding software, and by utilizing effective free tools such as *Trend Micro Browser Guard*.

The use of powerful security technology such as Trend Micro™ Smart Protection Network™, which proactively blocks malicious email messages, access to known malicious URLs, and the download of malicious files is also highly recommended.

For more information and analyses about botnets and the way by which criminals use them for profit, visit the Research and Analysis section of *TrendWatch*.

References:

- Brian Krebs. (October 26, 2009). *Security Fix: Brian Krebs on Computer Security.* "FBI: Cybercrooks Stole US$40M from U.S. Small, Midsized Firms." http://voices.washingtonpost.com/securityfix/2009/10/fbi_cyber_gangs_stole_40mi.html (Retrieved April 2010).
- Brian Krebs. (March 30, 2010). *Krebs on Security: In-Depth Security News and Investigation.* "Online Thieves Take US$205,000 Bite Out of Missouri Dental Practice." http://krebsonsecurity.com/2010/03/online-thieves-take-205000-bite-out-of-missouri-dental-practice/ (Retrieved April 2010).
- ClickForensics.com Inc. (January 19, 2010). *ClickForensics: Traffic Quality Management.* "Industry Click-Fraud Rate at 15.3 Percent for Q4 2009: Rate Lowest in Three Years for Busy Holiday Shopping Season." http://www.clickforensics.com/newsroom/press-releases/150-industry-click-fraud-rate-q4-2009.html (Retrieved April 2010).
- iC^3. (2010). "2009 Internet Crime Report." http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf (Retrieved April 2010).
- Loucif Kharouni. (March 23, 2010). *TrendLabs Malware Blog.* "New ZBOT Variants Targeting European Banks." http://blog.trendmicro.com/new-zbot-variants-targeting-european-banks/ (Retrieved April 2010).
- Microsoft Corporation. (August 9, 2005). *Microsoft TechNet.* "Microsoft Security Bulletin MS05-039: Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)." http://www.microsoft.com/TECHNET/SECURITY/BULLETIN/MS05-039.MSPX (Retrieved April 2010).
- Trend Micro. (September 16, 2009). *TrendLabs Malware Blog.* "The Internet Infestation, How Bad Is It Really?" http://blog.trendmicro.com/the-internet-infestation-how-bad-is-it-really/ (Retrieved April 2010).
- Trend Micro Incorporated. (February 12, 2008). *Threat Encyclopedia.* "TROJ_AGENT.KHA." http://about-threats.trendmicro.com/archive/virusencyclo/default5.asp?VName=TROJ_AGENT.KHA (Retrieved April 2010).

TREND MICRO™

- Trend Micro Incorporated. (March 24, 2010). *Threat Encyclopedia.* "TSPY_ZBOT.AZX." http://about-threats.trendmicro.com/archive/grayware/ve_graywareDetails.asp?GNAME=TSPY_ZBOT.AZX (Retrieved April 2010).
- Trend Micro Threat Research Team. (March 2010). *TrendWatch.* "ZeuS: A Persistent Criminal Enterprise." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/zeusapersistentcriminalenterprise.pdf (Retrieved April 2010).
- Wikimedia Foundation Inc. (April 21, 2010). *Wikipedia.* "CAPTCHA." http://en.wikipedia.org/wiki/CAPTCHA (Retrieved April 2010).