The Botnet Chronicles
A Journey to Infamy

Trend Micro, Incorporated

Rik Ferguson
Senior Security Advisor

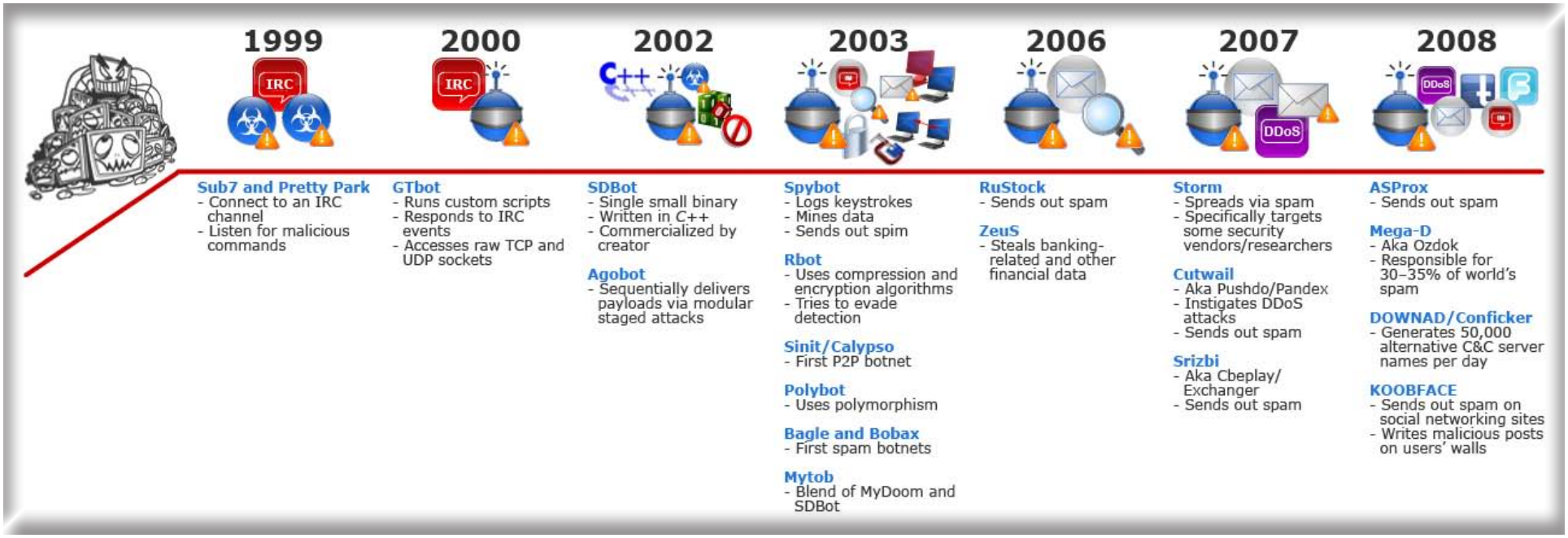
A Trend Micro White Paper | November 2010

CONTENTS

TREND MICRO

The Botnet Chronicles
A Journey to Infamy

The botnet time line below shows a rundown of the botnets discussed in this white paper. Clicking each botnet's name in blue will bring you to the page where it is described in more detail. To go back to the time line below from each page, click the ▲ at the end of the section.



Sub7 and Pretty Park
- Connect to an IRC channel
- Listen for malicious commands

GTbot
- Runs custom scripts
- Responds to IRC events
- Accesses raw TCP and UDP sockets

SDBot
- Single small binary
- Written in C++
- Commercialized by creator

Agobot
- Sequentially delivers payloads via modular staged attacks

Spybot
- Logs keystrokes
- Mines data
- Sends out spim

Rbot
- Uses compression and encryption algorithms
- Tries to evade detection

Sinit/Calypso
- First P2P botnet

Polybot
- Uses polymorphism

Bagle and Bobax
- First spam botnets

Mytob
- Blend of MyDoom and SDBot

RuStock
- Sends out spam

ZeuS
- Steals banking-related and other financial data

Storm
- Spreads via spam
- Specifically targets some security vendors/researchers

Cutwail
- Aka Pushdo/Pandex
- Instigates DDoS attacks
- Sends out spam

Srizbi
- Aka Cbeplay/ Exchanger
- Sends out spam

ASProx
- Sends out spam

Mega-D
- Aka Ozdok
- Responsible for 30–35% of world's spam

DOWNAD/Conficker
- Generates 50,000 alternative C&C server names per day

KOOBFACE
- Sends out spam on social networking sites
- Writes malicious posts on users' walls

A PRELUDE TO EVOLUTION

Botnets are considered one of the most prevalent and dangerous threats lurking on the Web today. The damage they cause can range from information theft and malware infection to fraud and other crimes.

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

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

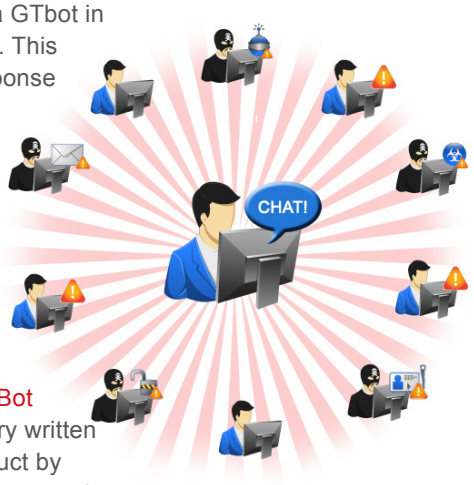
This white paper examines where the first botnets came from and how they have evolved over the past 10 years to become some of the biggest cybercrime perpetrators on the Web at present.

THE BOTNET SAGA BEGINS

Two contenders vie for being the malware that started the botnet ball rolling—Sub7, a Trojan, and Pretty Park, a worm. These malware introduced the concept of connecting to an Internet Relay Chat (IRC) channel to listen for malicious commands. They first surfaced in 1999, which has since then led to constant botnet innovation.

mIRC is a popular IRC client used by millions of people and by thousands of organizations to communicate, share, play, and work with one another on IRC networks around the world.

Several notable points exist along the botnet evolution time line, the first of which was the emergence of the Global Threat bot aka GTbot in 2000. GTbot was based on the *mIRC* client. This means that it can run custom scripts in response to IRC events and, more importantly, that it has access to raw TCP and UDP sockets. This makes it perfect for rudimentary denial-of-service (DoS) attacks, with some even going as far as scanning for Sub7-infected hosts and updating them to become GTbots.



2002 saw a couple of further developments in botnet technology with the release of SDBot and Agobot. SDBot was a single small binary written in *C++*. Its creator commercialized his product by making the source code widely available. As a result, many subsequent bots include codes or ideas taken from SDBot.

In the same year, Agobot broke new ground with the introduction of a modular staged attack whose payloads were sequentially delivered. The initial attack installed a backdoor program, the second attempted to disable antivirus software, and the third blocked access to security vendors' websites—all painfully familiar techniques to anyone that has suffered from a malware infection in the recent past.

Early botnets aimed to remotely control infected systems and to steal confidential information. The move toward modularization and open sourcing led to the huge increase in number of variants and to the expansion of botnets' functionality. Malware authors gradually introduced encryption for ransomware, HTTP and SOCKS proxies that allowed them to use their victims for onward connection, and FTP servers to store illegal content.

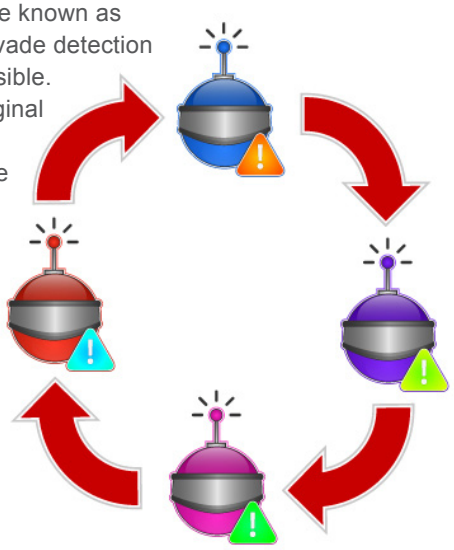
In 2003, SDBot transformed into Spybot with the introduction of new functions such as key logging, data mining, and sending out spammed instant messages aka spim.

In the same year, Rbot also rose to introduce the use of the SOCKS proxy. It also had DDoS functionality and made use of data-stealing tools. Rbot was also the first family of bots that used compression and encryption algorithms to try to evade detection.

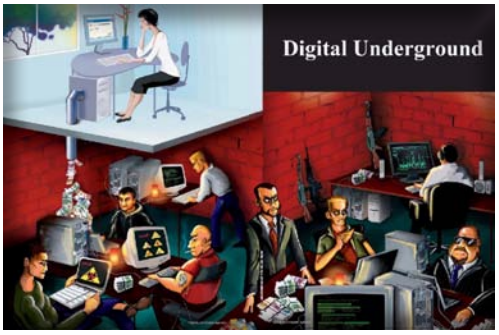
2003 also saw the first manifestation of a peer-to-peer (P2P) botnet that went by the name of Sinit or Calypso. Later on, Agobot modules were also developed to incorporate this P2P functionality.

Polymorphism allows a botnet to change its appearance as often as possible to try to evade detection.

The following year, another Agobot derivative known as Polybot introduced polymorphism to try to evade detection by changing its appearance as often as possible. Botnets steadily migrated away from the original IRC C&C channel, as this port was seldom opened due to firewall restrictions and as the protocol is easily identified in network traffic. Instead, bots began to communicate over HTTP, ICMP, and Secure Sockets Layer (SSL), often using custom protocols. They also continued adopting and refining their P2P communication capability, as was demonstrated five years later by a now infamous botnet that went by the name Conficker aka DOWNAD.



THE BIRTH OF ORGANIZED CRIME



At around 2003, criminal interest in the possibilities afforded by botnets began to become apparent. At the start of the decade, spamming was still largely a "work-from-home" occupation with large volumes of spam sent from dedicated server farms, open relays, or compromised servers. This changed for good, however, with the entry of Bagle, Bobax, and Mytob.

Bagle and Bobax were the first spam botnets while Mytob malware variants were essentially a blend of an older mass-mailing worm, MyDoom, and SDBot. This combination enabled cybercriminals to build large botnets and to widen their spamming activities to reach more victims' PCs. It also gave them agility and flexibility and, more importantly, helped them avoid legal enforcement activities that companies were aggressively pursuing.

From then on, many famous botnets rose and fell, led by probably the oldest cybercriminal spam botnets, Bagle and Bobax, in 2004. Bobax was eventually badly hurt by the McColo takedown in 2008, which may have even finally caused its disappearance.

At around 2003, criminal interest in the possibilities afforded by botnets began to become apparent.

RuStock dates back to 2006 along with the now infamous ZeuS crimeware family. RuStock was another spam botnet while ZeuS was a data-stealing tool.

Since then, ZeuS has probably become the most widely used data-stealing tool on the Web. ZeuS' creator has been regularly updating, beta testing, and releasing new versions of the toolkit by adding or improving its various functions. As new versions are offered for sale at very high prices, older versions are being distributed free of charge. These older versions, however, are oftentimes backdoored by cybercriminals, thereby making the novice thieves their victims, too. The proliferation of freely available cybercrime tools has lowered cost barriers and has encouraged more wannabe gangsters to take up cybercrime.

ZeuS is, however, not the only tool out there. There are several others that often compete with one another. These are usually designed with the nonexpert user in mind and so feature simple point-and-click interfaces to manage infected systems.

2007 saw the birth of the infamous Storm botnet along with the Cutwail and Srizbi botnets. The following year, ASProx appeared on the scene. Keep in mind, however, that the aforementioned botnets are just a few of the thousands of botnets out there.

At present, the Shadowserver Foundation tracks almost 6,000 unique C&C servers. Even this figure, however, does not encompass all of the existing botnets.

At any one time, Trend Micro tracks tens of millions of infected PCs that are being used to send out spam. This figure, however, does not include all of the other infected PCs that are being used for the purposes of stealing information, of launching DDoS attacks, or of instigating any other cybercrime.

THE SECURITY WAR RAGES ON

Several successful coordinated takedowns targeting cybercrime service providers that host many of the C&C infrastructure have been conducted so far. The action against Intercage/Atrivo, for instance, in 2008, almost destroyed the Mega-D botnet. Within weeks, however, it reappeared with a vengeance.

McColo had its fingers in a number of cybercrime pies and, among other activities, was hosting C&C servers for Srizbi, the revived Mega-D, RuStock, ASProx, Bobax, Gheg, and Cutwail botnets. As such, when McColo was taken off the Web in November 2008, a global drop in the number of spam of almost 80 percent became immediately apparent.

History has shown that there is too much money at stake for cybercriminals to simply walk away.

Unfortunately, however, by January 2009, the number of spam returned to its previous level. Earlier that June, the Federal Trade Commission (FTC) closed down the ISP, 3FN Service, as it was found to host some Cutwail C&C servers. It was taken down but went back in business a few days after. History has, after all, shown that there is too much money at stake for cybercriminals to simply walk away.

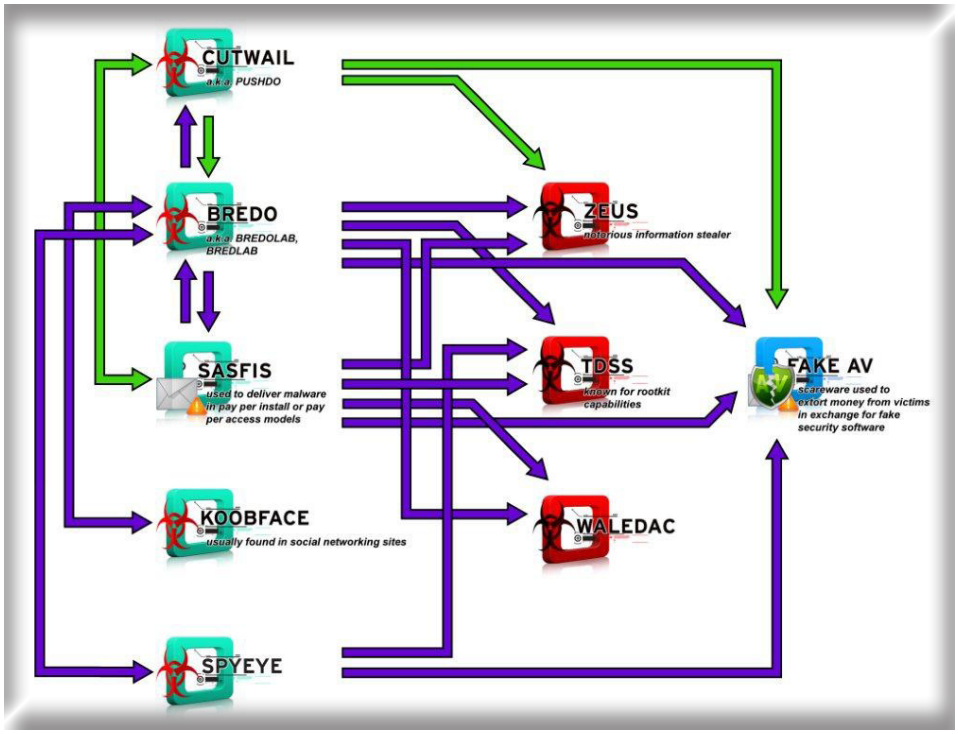
The concerted action that both public and private organizations are taking against botnets means that cybercrime innovation never stops. As new technologies emerge, cybercriminals continuously look for ways to adopt or abuse them, whether to facilitate profit generation, to increase their botnets' scalability and flexibility, or to provide a more effective camouflage for their malicious creations.

Initially, C&C IP addresses were hard coded into each bot, which made identification and eventual disruption by security researchers simple. However, the bad guys learn from their failure every time. Cutwail, for example, included the concept of backing up connections. Each Cutwail bot is capable of cryptographically generating alternative host names for its C&C servers on a daily basis. The cybercriminals, of course, know which host names will be generated on a given day and simply need to bring that alternative command channel into operation.

Similar techniques were used by the cybercriminals behind Conficker, which was capable of generating 50,000 alternative names every day. The security industry had to attempt to block access to all of them while their criminal counterparts only had to get it right once. It is worth remembering that around 6 million machines still remain infected by Conficker even after almost two years since it first reared its ugly head.

In addition to spam, DoS attacks, information theft, blackmail, and extortion, botnets have also evolved to become highly efficient malicious software distribution networks used by cybercriminals.

In addition to spam, DoS attacks, information theft, blackmail, and extortion, botnets have also evolved to become highly efficient malicious software distribution networks used by cybercriminals. In fact, fellow cybercriminals pay for access to compromised systems by the thousands to deliver even more malware to already-infected computers. Spam bots can also deliver secondary data-stealing malware such as rogue antivirus software and ransomware, which have become perennial favorites to maximize the revenue potential of each individual infected system. In fact, many cybercriminals make money by simply renting out access to their botnets rather than by engaging in their own spam, DDoS, or information theft campaigns.



LOST IN THE WHITE NOISE

Since the second half of 2007, cybercriminals have been abusing the user-generated content aspect of Web 2.0. Blogs and Really Simple Syndication (RSS) feeds were the first alternative C&C channels that cybercriminals identified. They posted commands on a public blog for bots to retrieve through an RSS feed. Likewise, outputs from infected systems were posted on an entirely separate and legitimate public blog for later retrieval by the C&C server, again via RSS feeds.

As Web 2.0 services grew in number and gained a certain level of acceptance among enterprises, cybercrime innovation also continued. Compromised servers in *Amazon Elastic Compute Cloud (EC2),* for example, have been used to host configuration files for the ZeuS bot. *Twitter* has been used as a landing page in several spam campaigns in an attempt to overcome URL filtering in email messages. *Twitter, Facebook, Pastebin, Google Groups,* and *Google App Engine* have also been used as surrogate C&C infrastructure. These public forums have been configured to issue obfuscated commands to globally distributed botnets. The said commands contained more URLs that a bot then accesses to download commands or components.

Moving forward, more botnets will take advantage of more effective P2P communication, update, and management channels.

The attraction to these sites and services lies in the fact that they offer public, open, scalable, highly available, and relatively anonymous means of maintaining a C&C infrastructure, which further reduces chances of detection by traditional antivirus technologies.

While network content inspection solutions can reasonably be expected to identify compromised endpoints that communicate with known bad sites or over suspicious or unwanted channels such as IRC, it has been historically safe to assume that a PC making a standard HTTP GET request over port 80 to a content provider such as *Facebook, Google,* or *Twitter,* even several times a day, is entirely normal. However, as botnet owners and cybercriminal outfits seek to further dissipate their C&C infrastructure and to blend into the general white noise on the Internet, that is no longer the case.

Of course, we can fully expect cybercriminals to continue their unceasing innovation. Moving forward, more botnets will take advantage of more effective P2P communication, update, and management channels. Communication between bots or between a bot and its controller will become more effectively encrypted, perhaps through the adoption of public key infrastructure (PKI). The C&C functionality will be more effectively dissipated using cloud services as well as P2P and other covert channels though compromised legitimate services. Spamming capabilities will further be enhanced. Pernicious botnets such as KOOBFACE already use social networking services for propagation by sending out messages and by writing malicious posts on users' walls. We can thus fully expect to see the addition of social network spamming capabilities to bot agents in the very near future.

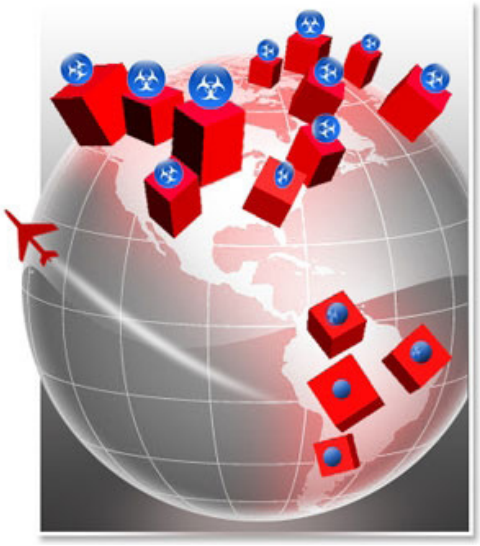
WHERE DO WE GO FROM HERE?

So what can we do? Is all hope lost?

Not entirely. The battles continue in a war that must be waged on several fronts.

Governments and international organizations such as the European Union (EU), the Organisation for Economic Cooperation and Development (OECD), and the United Nations (UN) need to strongly focus on globally harmonizing cybercriminal laws to enable more effective prosecution. Law enforcement agencies need to formalize multilateral agreements to tackle crimes that are truly transnational in nature.

ISPs and domain registrars also have a key role to play. ISPs should inform and assist customers they believe to have been compromised—a trend that appears to be on the rise. They should terminate services provided to customers they believe to be malicious. Domain registrars should demand more effective forms of traceable identification upon registration and should suspend services provided to bad actors as soon as credible suspicion is raised.



The security industry is already drawing valuable lessons from the levels of cooperation achieved among prior rivals in the fight against Conficker. Hopefully, this effective cooperation will continue and deepen.

The security industry should take past successes to heart but should not rely on past technology alone. Innovation is key to keeping up with and to hopefully surpassing every technique the bad guys continuously come up with.

Initiatives must be financed on a national level to more effectively educate and inform citizens of the dangers cybercrimes pose and to encourage safer computing practices.

Finally, the security industry must not rest on its laurels. It should take past successes to heart but should not rely on past technology alone. Innovation is key to keeping up with and to hopefully surpassing every technique the bad guys continuously come up with.

TREND MICRO

REFERENCES

- Dancho Danchev. (October 7, 2008). *ZDNet.* "Atrivo/Intercage's Disconnection Briefly Disrupts Spam Levels." http://www.zdnet.com/blog/security/atrivointercages-disconnection-briefly-disrupts-spam-levels/2006 (Retrieved October 2010).

- Det Caraig. (November 16, 2009). *TrendWatch.* "ASProx Botnet, Reactivated." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/secspot_46_111609_ASProx_botnet_reactivated2.pdf (Retrieved October 2010).

- Federal Trade Commission. (June 4, 2009). *Federal Trade Commission.* "FTC Shuts Down Notorious Rogue ISP, 3FN Service Specializes in Hosting Spam-Spewing Botnets, Phishing Websites, Child Pornography, and Other Illegal, Malicious Web Content." http://www.ftc.gov/opa/2009/06/3fn.shtm (Retrieved October 2010).

- Jonell Baltazar. (May 2010). *TrendWatch.* "Web 2.0 Botnet Evolution." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/web_2_0_botnet_evolution_-_koobface_revisited__may_2010_.pdf (Retrieved October 2010).

- mIRC Co. Ltd. (1995–2010). *mIRC.* http://www.mirc.com/ (Retrieved October 2010).

- Trend Micro Incorporated. (1989–2009). *Threat Encyclopedia.* "ZeuS and Its Continuing Drive Toward Stealing Online Data." http://threatinfo.trendmicro.com/vinfo/web_attacks/ZeuS_and_its_Continuing_Drive_Towards_Stealing_Online_Data.html (Retrieved October 2010).

- TrendLabs. (April 26, 2010). *TrendWatch.* "The Evolution of Botnets." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_evolution_of_botnets__april_26__2010_.pdf (Retrieved October 2010).

- Trend Micro Incorporated. (February 27, 2005). *Threat Encyclopedia.* "WORM_MYTOB.A." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYTOB.A (Retrieved October 2010).

- Trend Micro Incorporated. (March 24, 2004). *Threat Encyclopedia.* "WORM_RBOT.A." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_RBOT.A (Retrieved October 2010).

- Trend Micro Incorporated. (October 18, 2003). *Threat Encyclopedia.* "BKDR_SINIT.A." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=BKDR_SINIT.A (Retrieved October 2010).

- Trend Micro Incorporated. (July 17, 2003). *Threat Encyclopedia.* "WORM_AGOBOT.GEN." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?vname=WORM_AGOBOT.GEN (Retrieved October 2010).

- Trend Micro Incorporated. (June 24, 2003). *Threat Encyclopedia.* "WORM_SPYBOT.A." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SPYBOT.A (Retrieved October 2010).

- Trend Micro Incorporated. (March 9, 2000). *Threat Encyclopedia.* "WORM_PRETTYPARK." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_PRETTYPARK (Retrieved October 2010).
- Wikimedia Foundation Inc. (October 9, 2010). *Wikipedia.* "Internet Relay Chat." http://en.wikipedia.org/wiki/Internet_Relay_Chat (Retrieved October 2010).
- Wikimedia Foundation Inc. (October 5, 2010). *Wikipedia.* "Conficker." http://en.wikipedia.org/wiki/Conficker (Retrieved October 2010).
- Wikimedia Foundation Inc. (September 22, 2010). *Wikipedia.* "Cutwail Botnet." http://en.wikipedia.org/wiki/Cutwail (Retrieved October 2010).
- Wikimedia Foundation Inc. (September 8, 2010). *Wikipedia.* "Sub7." http://en.wikipedia.org/wiki/Sub7 (Retrieved October 2010).
- Wikimedia Foundation Inc. (September 1, 2010). *Wikipedia.* "Bagle (Computer Worm)." http://en.wikipedia.org/wiki/Bagle_%28computer_worm%29 (Retrieved October 2010).
- Wikimedia Foundation Inc. (September 1, 2010). *Wikipedia.* "MyDoom." http://en.wikipedia.org/wiki/Mydoom (Retrieved October 2010).
- Wikimedia Foundation Inc. (August 30, 2010). *Wikipedia.* "RuStock Botnet." http://en.wikipedia.org/wiki/Rustock (Retrieved October 2010).
- Wikimedia Foundation Inc. (August 6, 2010). *Wikipedia.* "Storm Botnet." http://en.wikipedia.org/wiki/Storm_botnet (Retrieved October 2010).
- Wikimedia Foundation Inc. (August 4, 2010). *Wikipedia.* "Mega-D Botnet." http://en.wikipedia.org/wiki/Mega-D_botnet (Retrieved October 2010).
- Wikimedia Foundation Inc. (July 7, 2010). *Wikipedia.* "McColo." http://en.wikipedia.org/wiki/McColo (Retrieved October 2010).
- Wikimedia Foundation Inc. (May 23, 2010). *Wikipedia.* "Srizbi Botnet." http://en.wikipedia.org/wiki/Srizbi_Botnet (Retrieved October 2010).

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003

www.trendmicro.com