TREND MICRO

Best Practices Series

Botnet Threats and Solutions

Phishing

A Trend Micro White Paper I November 2006

TABLE OF CONTENTS

TREND MICRO™

EXECUTIVE SUMMARY

In today's business and consumer computing space, a financially-motivated "ecosystem" of multiple players exists. This ecosystem—complete with its own lucrative buying and selling "microeconomy"—is fueling a rapidly growing crime wave.

Recently, malicious attacks involving tens of thousands of virus-infected PCs worldwide have targeted major organizations such as Microsoft, Google, Yahoo!, the U.S. Internal Revenue Service, and UK online betting firm Blue Square. These computers—infected via back door programs and controlled through Internet Relay Chat (IRC) commands—are covertly hijacked with software bots, applications that serve as agents to surreptitiously collect information. This mass infection transforms compromised PCs into botnets, networks of machines that serve numerous fraudulent purposes. Botnets have been responsible for identity theft, spam, phishing, pay-per-click fraud, denial-of-service (DoS) attacks, and information theft. These botnet ecosystems are not due to the actions of single creators (such as virus writers seeking notoriety), but rather, a network of players co-existing in an organized underground buying and selling "microeconomy."

As a result of phishing via botnets, businesses and consumers are adversely impacted by tremendous financial losses, identity theft, and other damages. This white paper examines the existence of and interactions within the botnet ecosystem that enables phishing—a fraudulent type of spam—and the ensuing damage. This paper also provides information on how businesses and consumers can best protect themselves against these attacks, as well as the benefits of implementing such actions.

BOTNETS AND PHISHING: THE FACTS

In today's business and consumer computing paradigm, an emerging tool for various malicious activities is the botnet. Botnets—networks of compromised machines infected with malicious programs—have been identified as a leading cause for phishing, a serious form of spam.

Bots and botnets

A bot—short for robot—is an automated software program that operates as an agent for a user or another program, or alternatively, simulates human activity. On the Internet, the most ubiquitous bots—more commonly known as spiders or Web crawlers—are legitimate programs that access Web sites and collect content for search engine databases. Bots have also been created to verify stock quotes or compare prices on shopping-based Web sites. Other bots such as knowbots and chatterbots have been used in a variety of legitimate ways.

However, bots are increasingly used for malicious purposes; these are known as IRC (Internet Relay Chat) bots. This type of bot is created when a computer virus or worm installs a backdoor program—such as a Trojan horse (a malicious program disguised as, or embedded within, legitimate software) or a drive-by downloader (which exploits Web browsers, e-mail clients, or operating system bugs to download malware without requiring any user intervention)—that leaves a PC Internet port open. The MyDoom (2004) and SoBig (2003) email worms, for example, employed this tactic. The infected machines subsequently become available for future activation.

A hacker then searches for infected PCs with open ports. Once located, the hacker installs the bot program onto their hard drives. The bot then typically connects to Internet Relay Chat to listen for commands, and the controller (a malicious third party) can unleash the effects of the bot by sending a single command to those machines.

Bots can also be formed when their creators embed malware on Web pages; creators commonly use pornography, celebrity, Web hosting, or social networking Web sites for this purpose. Users unknowingly download the malware either by clicking on links containing the code or, worse, simply by visiting a URL. The latter type of

TREND MICRO™

infection exploits specific vulnerabilities in a particular browser version—such as the Microsoft VML vulnerability in 2006—and both open users' Internet ports and expose their PCs to bot installation.

Security experts also call these bot-loaded PCs "zombies," since the hacker can wake them on command. When bots are installed on multiple PCs, this network of compromised machines—known as botnets—are commanded to perform an extensive range of activities, including spam distribution, phishing schemes, and click fraud.

An estimated one million PCs are under the control of hackers worldwide. In early 2005, German security analysts at Aachen University reported that they identified more than 100 botnets in a three-month period. These botnets ranged in size from a few hundred compromised PCs to 50,000 machines. [7]

Botnet infiltrations are often difficult to detect, and usually are not noticed until after the malicious activity has occurred. Businesses generally become aware of botnet attacks in several ways:

- End user complaints about PC, network, e-mail, or other application performance issues
- Third-party reports of attacks originating from their IP space
- Detection of excessive inbound or outbound port scanning
- Unusual traffic patterns on the network, such as increased traffic due to DoS attacks

Phishing: a serious form of spam

Increasingly, botnets are used to send spam—unsolicited, undesired bulk emails that negatively impacts consumer, business, computer, and network costs and productivity. In 2004, spam cost U.S. organizations alone more than $10 billion, including lost productivity and the additional equipment, software, and manpower needed to combat the problem. In June 2006, botnets sent an estimated 80 percent of email spam, an increase of 30 percent from 2005. [9]

Phishing is a serious and increasingly prolific form of spam, and is one of the main tactics employed in business and consumer identity theft. Phishing actually comprises two online identity thefts used together. In phishing scams, the identity of the target company—commonly a bank, online payment service, or other reputable business—is stolen first in order to steal even more identities: those of unsuspecting customers of the targeted company.

A typical phishing attack is made up of two components: an authentic-looking email and a fraudulent Web page. This form of spam frequently uses professional-looking, HTML-based emails that include company logos, colors, graphics, font styles, and other elements to successfully spoof the supposed sender. The content of the phishing email is usually designed to confuse, upset, or excite the recipient. Typical email topics include account problems, account verifications, security updates/upgrades, and new product or service offerings.

Recipients of the email are prompted to react immediately. They then click on a link provided in the email body, which actually directs them to the phishing Web page. The intent is to lure recipients into revealing sensitive information such as usernames, passwords, account IDs, ATM PINs, or credit card details.

Like the phishing email, the phishing Web page almost always possesses the look and feel of the legitimate site that it copies, often containing the same company logos, graphics, writing style, fonts, layout, and other site elements. This spoofed Web page may also include a graphical user interface (GUI) intended to lure the user into entering their bank account information, credit card number, social security number, passwords, or other sensitive information. Either the phisher, or an anonymous remote user that is sent the information, can then use the stolen information.

The growth of phishing

In October 2005, the Anti-Phishing Working Group received 15,820 unique phishing reports, compared with only 6,957 in October 2004. This industry association also discovered 4,210 phishing Web sites in October 2005, an increase from 1,142 in 2004. In addition, the group reported that more than 188 new samples of Trojan spyware were used in phishing attacks each month in the first four months of 2006, a 234 percent increase over the same period in 2005. [1]

In the United States, a Gartner survey reported that phishing attacks grew at double-digit rates in 2004. In the twelve months ending in May 2005, an estimated 73 million U.S. adult Internet users said they definitely—or believed they had—received an average of more than 50 phishing emails in the past year. [6]

Business impact from phishing

The effects caused by phishing are far-reaching, and include substantial financial losses, brand reputation damage, and identity theft. The independent research and advisory firm Financial Insights estimated that in 2004, global financial institutions experienced more than $400 million in fraud losses from phishing. U.S. businesses lose an estimated $2 billion a year as their clients become phishing victims. In the United Kingdom, losses from Web banking fraud—mostly from phishing—have nearly doubled from £12.2 million in 2004 to £23.2 million in 2005. [4]

And financial losses are not the only impact to businesses. Lost consumer data files and disclosures of unauthorized access to sensitive personal data are taking a toll on consumers' confidence in online commerce. Phishing's effects are also adversely impacting businesses in several other ways, including:

- Possible legal implications if employees are attacked on company computers
- Potential regulatory compliance issues such as HIPAA, Sarbanes-Oxley, and others if information breaches occur
- Significant decreases in employee productivity
- Impacts on IT resources, as phishing emails use storage space and reduce email system performance
- Impacts on administrators, as IT departments need to patch or repair systems, shut down applications or services, filter Transmission Control Protocol (TCP) ports 139 and 445 at the corporate gateway, apply patches or hotfixes, and instruct corporate users on email protocols

Consumer impact from phishing

Gartner also reported that the number of consumers receiving phishing attack emails increased 28 percent in the period from May 2004 to May 2005. And nearly 2.5 million online consumers lost money directly from phishing attacks: of these, approximately 1.2 million consumers lost $929 million in the previous year. In addition, one in 20 British users claimed to have lost money to phishing in 2005. [6]

In September 2003, the Identity Resource Center released the result of its survey on the impact of identity theft on its victims. The results were startling:

- Nearly 85 percent of all victims learn about their identity theft in a negative manner.
- The average time spent by victims to resolve an identity theft case is approximately 600 hours.
- While victims are discovering their identity theft sooner, the elimination of their negative credit report information takes much longer to resolve. [8, 12]

> ***The average time spent by identity theft victims to resolve their case and clear their names is 600 hours, This includes time lost from work and associated expenses.***
>
> ***— Identity Resource Center,***
> *September 2003*

The Identity Resource Center also reported that many victims suffered significant financial and emotional distress from the identity theft. In addition to credit card losses, victims incurred losses that included time lost from work, lost wages from time spent clearing their names, and costs related to travel, postage, telephone, obtaining police reports, and numerous other tasks. And some victims never regained their financial health from the identity thefts. [8, 12]

THE PHISHING ECOSYSTEM: THE KEY PLAYERS AND THEIR INTERACTIONS

The key players

The phishing "ecosystem" consists of a collection of individuals who play various roles within the phishing space, ranging from the financially-motivated botnet creators to those who actively pursue and prosecute the cybercriminals. In this ecosystem, a large industry of buying and selling—a "microeconomy"—exists within the phishing underground, involving botnet creators, perpetrators, and enablers. However, these three player groups are complex and intertwined: a single individual or multiple perpetrators can play separate or simultaneous roles.

Unlike lone virus writers who work for notoriety, botnet creators' sole purpose is to "seed" the botnet for financial gain. Typical creators have been young, technologically savvy individuals, with the most prolific located in Eastern Europe, Brazil, Morocco, and China. [10] However, botnet creation tools have become so commonplace that the level of technological knowledge and sophistication is now lower; as a result, botnet creation is becoming even more prolific—and dangerous.

Another key player in the phishing ecosystem is the botmaster or bot herder. Using an IRC channel or other underground discussion board, the botmaster instructs the botnets what to do. The botmaster may be the botnet's creator, or a separate individual whose function is to rent or lease botnets. Botmasters can also serve as auctioneers who offer botnets to the highest bidders, such as spammers and online extortionists.

The members within the phishing space retain great flexibility and creativity to consistently maintain their activities and remain one step ahead of detection. With the numerous vulnerabilities in today's software, these individuals exploit security flaws before patches are released.

Global current events also play a major role in phishing criminal planning. Researchers have learned that many of today's phishers are highly news- and current events-aware, and plan their attacks in conjunction with particular world events or disasters. For example, following natural disasters such as major hurricanes or earthquakes, phishers will prepare and implement attacks using emails and Web sites designed to solicit donations to assist affected individuals. [1]

> ***Today's phishing criminals are often highly news and current event-aware, planning and implementing their attacks in conjunction with particular events or disasters such as major hurricanes or earthquakes.***
>
> ***— The Anti-Phishing Working Group***

Security experts are also observing new trends as phishing criminals continue to evade detection. Rather than using large numbers of compromised machines for phishing attacks, today's players are leaning toward larger numbers of attacks but with smaller botnets. Detection becomes more difficult as the attacks occur from disparate locations.

Further complicating the problem is the fact that the botnet landscape is constantly changing. Once downloaded, bot creators—via the IRC or other command and control center—can activate or deactivate their bots at will, which complicates mapping the extent or makeup of the network.

Enablers of the phishing ecosystem are also as numerous as the criminals themselves. Enablers—those who unwittingly facilitate the phishers—have included major search engines, domain name registrars, hosting companies, software vendors, adware affiliate companies, or any individuals or organizations that fail to practice due diligence to prevent phishing and botnet attacks.

Enforcement

Over the past several years, law enforcement officials have successfully apprehended, prosecuted, and convicted phishers and bot herders. However, apprehending these criminals is becoming increasingly difficult as they become more professional and sophisticated in their operations.

Organizations such as the Anti-Phishing Working Group (APWG), the Federal Trade Commission, Digital Phishnet, and others have initiated collaborative enforcement programs to combat phishing and identity theft. These industry groups—many of which are global and pan-industrial in scope—focus on numerous areas, including identifying phishing Web sites, sharing best practice information, aiding criminal law enforcement, and assisting in apprehending and prosecuting those responsible for phishing and identity theft crimes. Eight of the top 10 U.S. banks belong to the APWG; its network of global research partners includes some of the world's top e-commerce associations and watchdogs.

The value of the botnet market

The trade of botnets is becoming a lucrative, high-margin industry, and is recognized as a form of organized crime. Botnet costs are low when compared to the financial losses and damages to businesses and end users. Security experts who have monitored IRC chat room exchanges report that a DoS attack allegedly costs between $500 and $1,500, while smaller botnet attacks are priced between $1 and $40 per compromised PC. [3, 11] Yet, the overall profits realized and monetary damages incurred far exceed these criminal financial outlays.

For example, Shiva Brent Sharma—arrested three times for identity theft via phishing—told investigators that he paid $60 for a program designed to harvest AOL email addresses. At age 20, Sharma had accumulated well over $150,000 in cash and merchandise. [14]

Jeanson James Ancheta—a.k.a. Resili3nt—recently used readily available software and hardware to create a botnet-for-profit consisting of at least 400,000 infected computers. Ancheta netted at least $60,000 in profits, and also provided bots for intrusion by other parties. [5]

Californian Christopher Maxwell and two unidentified co-conspirators operated multiple botnets that compromised systems at worldwide U.S. military installations, a Seattle hospital, and a California school district. Maxwell netted more than $30,000, and the entire project generated more than $100,000 in illicit installation commissions from multiple adware company affiliate schemes. Investigators reported that in two weeks, Maxwell's bots reported over two million infections of more than 629,000 unique Internet addresses, with some machines infected repeatedly. [2, 11]

German botnet researchers from the Honeynet Project recently discovered one malicious hacker who installed spyware programs on 9,700 hijacked Windows machines. The hacker—using adware from DollarRevenue.com—generated more than $430 per day. [3,11]

Paul Ferguson, a network analyst and botnet investigator for secure content and threat management company Trend Micro, explained that botnet players form a criminal enterprise that is intent on financial gains. According

to Ferguson, while the costs vary, botnets have realized revenues ranging from several hundreds of thousands to several million U.S. dollars. Criminals involved in the botnet underworld can charge $100 per day to rent 1,000 bots.

Ferguson also noted that hijacked PCs are not the only lucrative area for financial gains; members of the phishing ecosystem also deal in data. He and his colleagues learned that credit card numbers obtained through phishing have been rented out or sold to other criminal third parties with a real time price of 10 card numbers for $20. In addition, the credit card details of thousands of Britons were recently sold in Internet chat rooms. Hundreds of credit card numbers were sold in a single night of trading, with each card number fetching $1 each. [13]

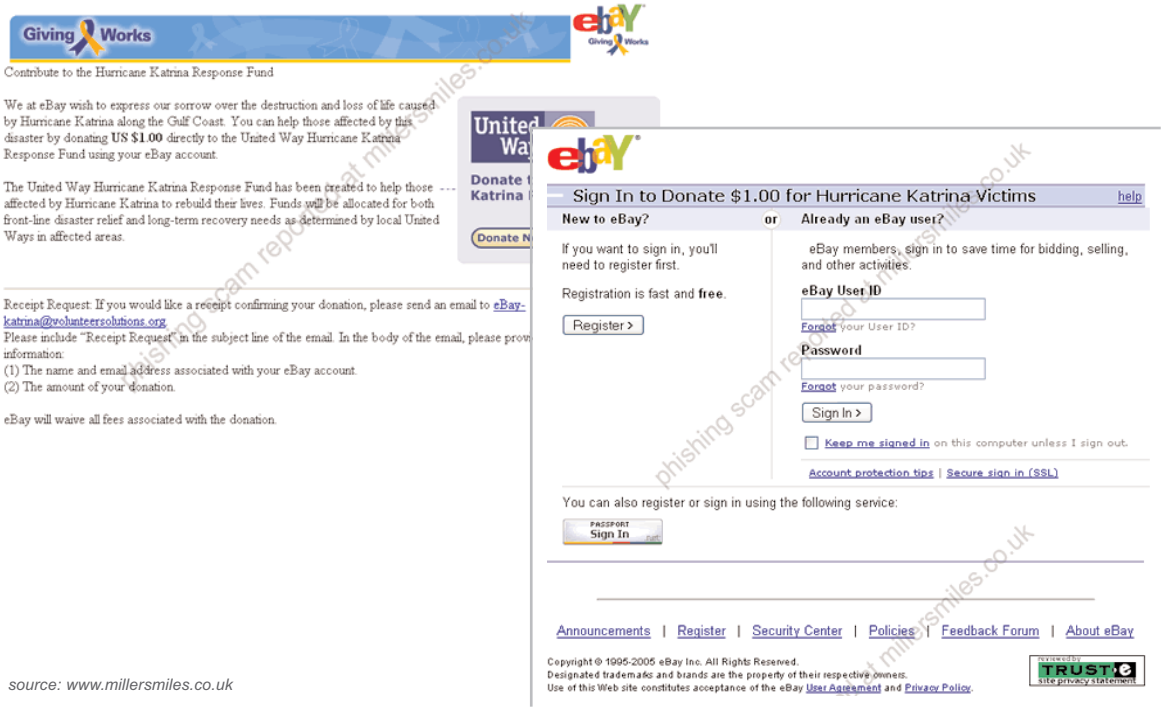
Interactions of the players

Within the phishing ecosystem, a number of interactions exist that play out in a specific manner as criminal enterprises continue to become more sophisticated and ingenious when planning their attacks. As previously discussed, researchers learned that many phishers stay abreast of current news stories and plan their attacks in conjunction with particular impending events or disasters. Such was the case during Hurricane Katrina.

During Hurricane Katrina, the APWG witnessed several phishing attacks which called upon people's willingness to assist during times of need, preying on donors who send relief funds for natural disasters. Attacks were staged against organizations such as the American Red Cross, the Salvation Army, and Hurricane Katrina Donations.[1]

Criminal groups first began registering domain names disguised as donation and victim-relief Web sites as soon as the hurricane was named. By using fraudulent emails disguised as Katrina news updates containing links directing users to the entire "news story," recipients were lured into visiting bogus Web sites hosted in the United States and Mexico. (see Figure 1 below)

Figure 1: Hurricane Katrina phishing email and bogus Web site



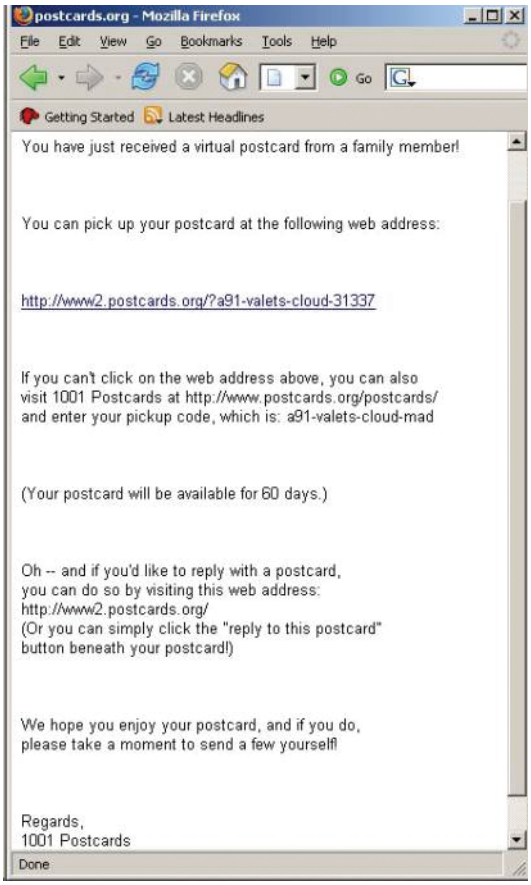
source: www.millersmiles.co.uk

TREND MICRO

However, unsuspecting visitors were lured to a Web site containing encoded JavaScript, which attempted to exploit two HTML Help vulnerabilities [14] These vulnerabilities existed in the HTML Help ActiveX control in Windows, and could allow information disclosure or remote code execution on an affected system.If successfully exploited, these vulnerabilities effected installation of a Trojan downloader on the user's machine. This Trojan subsequently began downloading a second Trojan containing backdoor functionality, providing the attackers with complete control of the PC.

Botnet and phishing researchers are constantly studying various phishing scenarios and interactions. Through their use of honeypots (a trap set to detect or counteract attempts at unauthorized use of information systems), researchers have observed very high numbers of phishing emails crafted to resemble email postcards. Victims are targeted under the premise of either sending or receiving a postcard to or from someone very familiar to them. The postcards are developed in the specific language of the particular population being targeted (i.e. Portuguese, English, Spanish, and others). By evoking a response from the victim—contact with a loved one, for example—the individual clicks on a link in the postcard to initiate the process. The link, containing a Trojan horse from a foreign server, either prompts the victim to enter personal details or downloads a malicious program. At that point, the user has already submitted personal details and has become an identity theft victim, or the PC is compromised and ready for activation within a botnet, or both. (See Figure 2 below)

Figure 2: Email postcard phishing



Source: www.Infectionvectors.com

PHISHING PROTECTION BEST PRACTICES

Businesses and consumers can protect themselves from the devastating effects of phishing due to botnet activities in two ways: educating themselves about phishing techniques and employing technology solutions that combat phishing. The following checklist is a general best practice prescription for guarding against malicious threats:

Anti-Phishing Best Practice Checklist

Best Practice	Business	Consumer
Always install, update, and maintain firewalls and intrusion detection software, including those that provide malware/spyware security	✓	✓
Use the latest Web browser version and install security patches when available	✓	✓
Practice awareness when receiving emails that request account details (financial institutions almost never request financial details in emails)	✓	✓
Never email financial or personal details	✓	✓
Only open email attachments from trusted parties	✓	✓
Never click on links in suspicious emails	✓	✓
Report suspicious emails to appropriate authorities	✓	✓
Monitor logs from firewalls, intrusion detection systems, DNS servers, and proxy servers on a daily basis for signs of infections	✓	
Monitor outbound SMTP connection attempts that do not originate from normal SMTP mail gateways	✓	
Establish rigorous password policies for clients, servers, and routers, and enforce them	✓	
Ensure that only approved devices may connect to the organization's network	✓	
Regularly read the latest news and information regarding phishing	✓	✓

TREND MICRO™

In terms of specific technologies, businesses and consumers alike should look for layered solutions that protect against both sending—that is, becoming an unwitting accomplice to propagating spam—and receiving phishing emails. From a business perspective especially, layered solutions should also offer content protection at the client side, or end points, and at the network gateway—as well as monitor network behavior. This ensures against "rogue" devices such as laptops and notebooks—which are not always under administrators' control and may not have adequate or updated threat protection installed—infecting the entire network.

The following checklist can serve as a guideline in making technology-related decisions to combat phishing:

Specific Anti-Phishing Technology Checklist

Protection Type	Protects against	
	Sending	Receiving
Client-side/endpoint	• Personal firewall • Anti-virus	• Personal firewall • Anti-virus • Anti-phishing toolbars or enabled browsers
Network behavior	• Intrusion-detection system (IDS)/ intrusion protection system (IPS) • Network content inspection	• IDS/IPS • Network content inspection
Network gateway	• Firewall • Gateway anti-virus • Gateway anti-spam	• Domain reputation measurement

Trend Micro offers numerous products and services designed to combat phishing. Consult the For More Information section below, for contact details.

Report Phishing

Businesses and consumers can file phishing reports with the following organizations:

Anti-Phishing Working Group
http://www.antiphishing.org

Digital Phishnet
http://www.digitalphishnet.org/

Federal Trade Commission
http://www.consumer.gov/idtheft/

Internet Crime Complaint Center (a joint project of the FBI and the National Collar Crime Center)
http://www.ic3.gov

Trend Micro Anti-Fraud Unit
antifraud@support.trendmicro.com

TREND MICRO™

Benefits obtained from best practice adoption

Businesses and consumers who follow these best practices can realize numerous benefits. Both groups can reduce their exposure to fraudulent emails and Web sites as well as avoid financial losses. Businesses employing these best practices can also help increase their overall customer confidence, avoid litigation, protect their brand reputations, and avoid damage to costly IT systems. Consumers can defend their personal and financial reputations that are often seriously damaged by identity theft.

SUMMARY

The existence of underground phishing ecosystems and the large financial gains through botnets have transformed phishing into worldwide organized crime. Profits for these cybercriminals—as observed through monitored chat room discussions, apprehensions, trials, and convictions— have ranged from tens of thousands to millions of dollars. Yet, businesses and consumers are greatly impacted by significant financial losses and other short- and long-term damage to overall financial health, brand, and reputation.

In order to combat phishing, business and consumers need to adopt best practices and practice awareness, educate themselves about phishing and botnets, use current security protection and protocols, and report suspicious activities. By doing so, they can reduce their exposure to fraud and identity theft, safeguard their confidential information, and help fight one of today's most serious and ongoing threats of phishing with botnets.

FOR MORE INFORMATION

Trend Micro Incorporated

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

Trend Micro Incorporated

North American Corporate Headquarters

10101 N. De Anza Blvd.

Cupertino, CA 95014

USA

Tel: 408-257-1500 or 800-228-5651

Fax: 408-257-2003

Web site: http://www.trendmicro.com

TREND MICRO™

REFERENCES

1. Anti-Phishing Working Group, http://www.antiphishing.org.

2. “Man sentenced for "botnet" attack on hospital,” The Mercury News, August 25, 2006.
http://www.mercurynews.com/mld/mercurynews/news/local/states/california/northern_california/15364273.htm

3. Biever, Celeste. “How Zombie Networks Fuel Cybercrime” New Scientist, November 3, 2004.
http://www.newscientist.com/article.ns?id=dn6616

4. CRM Today. “Financial Insights Evaluates Impact of Phishing on Retail Financial Institutions Worldwide,” CRM Today, July 15, 2004.
http://www.crm2day.com/news/crm/EplAlZlEVFjAwhYlkt.php

5. Gage, Gage and Kim S. Nash. “Security Alert: When Bots Attacks.” Baseline Magazine, April 6, 2006.
http://www.baselinemag.com/print_article2/0,1217,a=175062,00.asp

6. Gartner. “Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce,” June 23, 2005.
http://www.gartner.com/press_releases/asset_129754_11.html

7. Holz, Thurston. “On the Economics of Botnets.”
http://honeyblog.org/archives/54-On-the-Economics-of-Botnets-Part-2.html

8. Identity Theft: The Aftermath 2003, Identity Theft Resource Center, 2003.

9. Leyden, John. “Zombie PCs spew out 80% of spam,” The Register, June 4, 2004.
http://www.theregister.co.uk/2004/06/04/trojan_spam_study/

10. Leyden, John. “The illicit trade in compromised PCs,” The Register, April 30, 2004.
http://www.theregister.co.uk/2004/04/30/spam_biz/

11. Naraine, Ryan. “Money Bots: Hackers Cash in on Hijacked PCs,” eWeek.com, September 8, 2006.
http://www.eweek.com/article2/0,1759,2013924,00.asp

12. Privacy Rights Clearing House
http://www.privacyrights.org/asr/idtheftsurveys.htm

13. Richards, Jonathan. “Revealed: how credit cards are plundered on the Net,” The Times (UK) Online, April 15, 2006.
http://www.timesonline.co.uk/article/0,,2-2135422,00.html

14. Microsoft Security Bulletin MS05-001, January 11, 2005.
http://www.microsoft.com/technet/security/bulletin/MS05-001.mspx

15. Zeller, Tom. “Identity Thief Finds Easy Money Hard to Resist,” New York Times, July 4, 2006.
http://www.nytimes.com/2006/07/04/us/04identity.html?ex=1309665600&en=0c5e1099b9e02825&ei=5090&partner=rssuserland&emc=rss

TREND MICRO™
Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.
10101 N. De Anza Blvd.
Cupertino, CA 95014
USA toll free: 1+800-228-5651
phone: 1+408-257-1500
fax: 1+408-257-2003
www.trendmicro.com