Technology in Society 32 (2010) 183–196

Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

An overview of social engineering malware: Trends, tactics, and implications

Sherly Abraham [a,*], InduShobha Chengalur-Smith [b]

[a] College of Computing & Information, State University of New York, Albany, NY 12222, USA
[b] BA 311, School of Business, State University of New York, Albany, NY 12222, USA

Keywords:
Backdoors
Botnets
E-mail
Fast flux
Hijacking
Information security
Internet
Key loggers
Malware
Rootkits
SMTP engine
Social engineering
Social software
Whaling

A B S T R A C T

Social engineering continues to be an increasing attack vector for the propagation of malicious programs. For this article, we collected data on malware incidents and highlighted the prevalence and longevity of social engineering malware. We developed a framework that shows the steps social engineering malware executes to be successful. To explain its pervasiveness and persistence, we discuss some common avenues through which such attacks occur. The attack vector is a combination of psychological and technical ploys, which includes luring a computer user to execute the malware, and combating any existing technical countermeasures. We describe some of the prevalent psychological ploys and technical countermeasures used by social engineering malware. We show how the techniques used by purveyors of such malware have evolved to circumvent existing countermeasures. The implications of our analyses lead us to emphasize (1) the importance for organizations to plan a comprehensive information security program, and (2) the shared social responsibility required to combat social engineering malware.

1. Introduction

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return of investments and business opportunities [1]. Identifying and classifying threats to information systems is vital to building defensive mechanisms [2–4]. As organizations become vigilant about protecting their networks by investing in better security technologies, attackers have focused their attention on exploiting the weakest link in security – end users. Human error is often a major cause of problems in technological implementations, and people are generally considered the weakest link in an information security program [5].

A major threat to organizational information security is the rising number of incidents caused by social engineering attacks. Social engineering is defined as the use of social disguises, cultural ploys, and psychological tricks to get computer users to assist hackers in their illegal intrusion or use of computer systems and networks [6]. Social engineering is one of the strongest weapons in the armory of hackers and malicious code writers, as it is much easier to trick someone into giving his or her password for a system than to spend the effort to hack in [7]. Despite the continued effort of organizations to improve user awareness about information security, social engineering malware has been successful in spreading across the Internet and infecting numerous computers. By 2007 social engineering techniques became the number-one method used by insiders to commit e-crimes [8], but unsuspecting users remain the predominant conduit for the authors of malicious code. Given this susceptibility to social engineering techniques, our primary research objective is to identify and describe social engineering malware trends and tactics.

For social engineering malware to be successful, it needs to be activated by the end user and run on the system

* Corresponding author. Tel.: +1 518 437 3812; fax: 518 437 3810.
E-mail address: abrahamsherly@gmail.com (S. Abraham).

0160-791X/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.techsoc.2010.07.001

without interruption. But if the malware can be prevented from reaching users it will not be successful. Identifying attack strategies is vital to developing countermeasures that can be incorporated into preventive mechanisms like e-mail filtering and end-user security training. Information on the behavior of the malware during propagation helps in the creation of early warning systems [9]. Even if the malware bypasses the prevention stage and is executed by a user, if it can be detected on the machine and blocked from performing its harmful routine, the effects of the malware can be alleviated.

When computer malware is activated, it makes various changes in the computer by opening backdoors that enable it to spread to other machines. It also executes defensive strategies in order to remain undetected. Identification of such defensive strategies is helpful in discovering malware in its early stages on end-user machines, and blocking it from being executed completely and propagating further. Identifying it also aids in the development of heuristics analysis – a method of malware scanning that evaluates patterns of behavior to discover anomalies [10]. Security researchers use this data to build behavioral models of malware, and end users can receive alerts notifying them of unusual behavior on their machines.

In order to provide guidelines for strengthening an organization's defenses against social engineering malware, we gathered data on such malware and analyzed their characteristics. The analysis allowed us to identify the strategies employed, both psychological and technical. This paper provides empirical evidence of the growing reach of social engineering malware. The following section describes our data collection process and summarizes trends in social engineering malware incidents. Next we present a framework for the propagation of social engineering malware and discuss some common avenues of attack. This discussion is followed by an analysis of the psychological tactics used by the malware as well as descriptions of some of the technical features that are designed to help the malware counter existing security precautions. The paper concludes with a discussion of the implications of our findings as well as recommendations to mitigate the threat posed by social engineering malware.

2. Trends in social engineering malware

"Malware" is a general term used for viruses, worms, trojan horses, etc. [11]. In order to succeed, social engineering malware uses technological countermeasures and psychological ploys. The malware is delivered through various channels, and the malware has continually evolved as the technology to thwart it has also evolved. Likewise, the psychological tactics used by hackers are also continuously updated.

Rather than rely on anecdotal information, we sought to explore the reach of social engineering malware empirically. We drew from multiple data sources to develop a dataset of social engineering malware incidents and their characteristics. Our primary data source is an online journal, *Virus Bulletin*, which provides independent advice on developments in viruses and anti-virus products. This journal also serves as a repository of reported malware incidents worldwide. These incidents are first verified by the journal and then compiled to create a list of monthly incidents. Based on this data, *Virus Bulletin* publishes an annual list of the top malware. The list for 2009 is shown in Table 1.

By examining the descriptions of these malware, we discovered that all of them relied on social engineering to be activated and were spread mainly via e-mail. Additional information about these malware, available from Symantec's Search Threat database, showed that malware discovered several years ago remain at the top of the 2009 malware prevalence tables (see the last column in Table 1). Thus, social engineering malware can be characterized by its pervasiveness and persistence – two aspects that clearly pose a challenge to organizations and users.

We also wanted to track the prevalence of social engineering malware over the years. Using data from *Virus Bulletin*'s monthly reports going back to 2000, we identified malware that relied on social engineering. We noted that some have multiple variants, i.e., strains of the malware that are created by borrowing code and altering it slightly. The variants are generally denoted by a letter or letters following the virus family name; for example, Netsky.A, Netsky.B, and so on [12]. Rather than treating each variant as an independent malware, we grouped the different strains into a single malware family. Following this process we identified 56 malware families and documented the monthly number of incidents reported by that malware.

The reported number of security incidents using social engineering malware from 2000 to 2007 shows a definite upward trend (see Fig. 1). We fit an exponential trend model to this data, and it resulted in an R-square of 92%. The analysis shows that social engineering malware is growing explosively and will continue to pose a substantial security hazard.

In order to investigate the behavior and characteristics of the malware in our dataset, we performed keyword searches on each malware using the information available from malware dictionaries, encyclopedia, and blog postings of the major anti-virus vendors such as Symantec, Sophos, and Trend Micron. By combining information on malware prevalence reports available from these sources, we created a comprehensive description of malware incidents. This process resulted in detailed information about the behavior and technical characteristics of the malware. In certain cases, we used listed aliases for the malware names to

Table 1
Top Malware, 2009.

Position	Name of Malware	Date of Discovery
1	Netsky	February 16, 2004
2	Mytob	April 1, 2005
3	Bagle	January 18, 2004
4	Agent	May 19, 2008
5	Bifrose/Pakes	July 21, 2005
6	Small	August 21, 2008
7	Mywife/Nyxem	September 21, 2005
8	Mydoom	January 26, 2004
9	Zafi	September 14, 2004
10	LovGate	March 27, 2003

Source: *Virus Bulletin* (as of September 15, 2009).

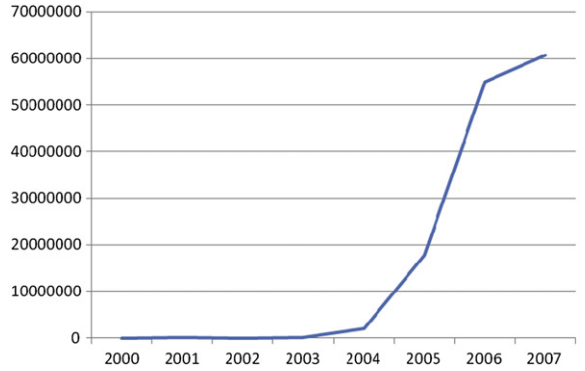


Fig. 1. Reported security incidents that used social engineering techniques.

match the data across websites. For instance, the Troj/Dorf worm listed by Sophos has multiple aliases, and Symantec refers to it as Trojan.Peacomm. By searching for all possible alias names for each malware listed, we resolved any duplications or omissions.

Our analysis of the malware behavior showed some commonalities in steps malware takes to be successfully activated. Using technical details for our sample of malware, we created a master list of actions that malware undertakes to carry out its tasks. The malware's actions generally fell into four categories: (1) persuade a user to activate it, (2) subvert protective technologies, (3) accomplish its mission, and finally (4) propagate. Fig. 2 provides a framework that describes the steps that a social engineering malware undertakes in order to infiltrate a system successfully.

It should be noted that not all social engineering malware sequentially follow the steps outlined in Fig. 2, but the figure does provide a general framework describing the steps that lead to a successful infection by a social engineering malware. The malware utilizes a number of avenues, such as websites, social software, e-mail, etc. to infect user machines. These approaches are combined with tactics that entice and trick users into opening an e-mail attachment or clicking on a web link. This action by the user leads to the execution and activation of the malware on the computer system. At this point the malware is fully activated and proceeds to carry out a number of tasks, such as altering security settings, opening backdoors, downloading files, etc. The actions vary depending on the specific malware. In most cases, the malware also propagates further by e-mailing itself to addresses on the infected users' contact list.

We now elaborate on the various steps the malware undertakes, particularly focusing on the different attack avenues, the tactics deployed, and the actions that are taken by the malware in order to combat existing security measures and continue to propagate.

3. Common infiltration channels

Social engineering malware proliferates through a variety of channels, including e-mail, social software, websites, portable storage devices, and mobile devices. Below we discuss some of the common infiltration channels.

3.1. E-mail

E-mail is the most popular medium used by attackers to deceive users, causing them to violate information security policies inadvertently. The Radicati technology market research group estimates that there were 1.2 billion e-mail users in 2007, and this number is expected to rise to 1.6 billion by 2011 [13]. E-mail worms are malicious programs that, upon execution on a machine, exploit the users' e-mail capabilities to further propagate the worm. The first use of e-mail to propagate malicious code can be traced back to 1987 and the Christmas Tree trojan horse [14]. End users received an e-mail message with an attachment that drew a graphical Christmas tree when executed. Upon execution, the worm sent a copy of itself to everyone on the user's address list. The worm was successful enough to bring down IBM's network worldwide [15].

A prevalent trend in social engineering malware is phishing, where users are led to believe they are interacting with a trusted site or entity and are tricked into providing sensitive information. The complexity of phishing attacks

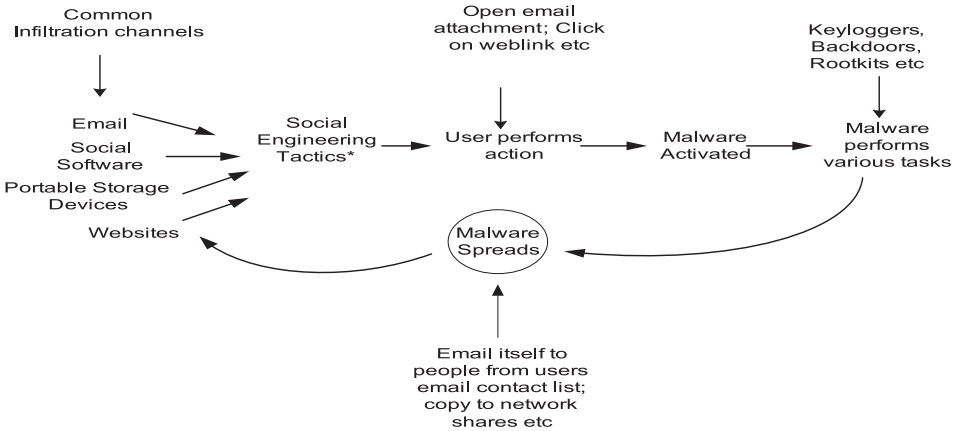


Fig. 2. Steps taken by malware to infiltrate a system.

has drastically increased over the years as more people have moved toward Internet banking and buying. Phishing attacks are initiated primarily via e-mails that direct users to fraudulent websites, which in turn collect credentials such as bank account numbers, social security numbers and the like from end users [16]. The e-mail messages appear to originate from a trusted source, such as a bank or government agency. The verbiage and language used in the e-mail are devised to appear professional and elegant, so many users never question the identity of the sender. However, a closer look at the e-mail address might reveal that the sender's e-mail address is different.

3.2. Websites

Websites are increasingly used to launch malware on user computers. Google tracks websites with potential malware, and the number of such websites has increased by around 190,0000 since 2008 (see Google's Safe Browsing malware list). Vulnerable websites are hacked into and malicious code installed, which redirects visitors to fake websites that closely resemble legitimate websites. Such camouflage attack techniques involve manipulating the appearance, content, and/or images on websites to lure users to carry out actions such as clicking on a link or opening an e-mail attachment. Malware have been known to query popular news sites like CNN to fetch current news and send e-mail messages with keywords from news and sports events with malware attached [17]. Even popular search engine websites are vulnerable, as exemplified by results of searches on the 2009 solar eclipse, which redirected users to malware-infiltrated websites [18].

Another camouflage strategy includes manipulating words in web addresses. Here legitimate websites are altered by flipping a character, and the difference might not be easily recognized. For example, instead of a legitimate website *icecream.com* users are provided with the address *iceccream.com*. Another example is replacing the letter "o" with the number "0" and changing the font so that the web address mimics the address of a legitimate website. As users become more aware of and suspicious of e-mail attachments and links, cyber criminals manipulate search engine optimization results to peddle malware using fake anti-virus software.

Drive-by-Pharming is an emerging attack concept that infects user machines by asking users to simply view the attackers' malicious code, which could be placed on a web page or embedded in an e-mail [19]. The malicious code alters the address settings on the user's home broadband router, which then gives the attacker control over the home user's Internet connection. This provides attackers with personally identifiable information and credit card information by redirecting users to fake websites.

3.3. Social software

Attack tactics using social software as a medium is on the rise. Social software includes various loosely connected applications that enable individuals to communicate with one another and track discussions across the Web as they occur [20]. The emergence of Web 2.0 is characterized by a broad array of social software, including instant messaging, social networking websites, blogs, Wikipedia, etc. These have caused a significant increase in the number of users involved in social software, and opened doors to new opportunities for knowledge exchange and socializing. Malware authors see this population as potential targets encased in social networks, and so have extended their umbrella of attacks to these venues. As people increasingly share and release personal information on social networking sites, they become rich sources of information for identity theft. Major social networking sites such as Facebook and Twitter are targets of denial-of-service attacks that disrupt or slow services. For instance, some Twitter users who were tricked into clicking on a link in a tweet were directed to a rogue site that attempted to download malware [21]. The availability of personal information on social networking sites, such as MySpace and LinkedIn, increases the vulnerability of the victims and the success rate of phishing [22]. Not surprisingly, the number of new phishing sites has significantly increased [23], with Twitter users being the most recent victims [24].

File-sharing websites are now increasingly used by Internet users to facilitate sharing large files, pictures, and videos with family and friends. Malware authors often rename malware-infected files to resemble music or video files in order to lure people to download and install the malware. A variant of the Koobface worm spread through Facebook, with users receiving messages from their friends including a picture of their friend extracted from Facebook [25]. The message had an embedded web link pointing to a spoofed web page, and the user was prompted to install a flash update resulting in the Koobface variant being installed on the user machine. Another malware, Worm SD_BOT, spread rapidly through instant messaging services by sending messages from infected friends of the social network users [26]. Once users click on malware-infected zip files, the worm opens backdoors, connects with other Internet relay chat (IRC) sites, and downloads other malware. Blog pages are also being heavily exploited to launch malware attacks. Popular and trusted blogging websites are hacked into with fake blog posts that include web links with malware.

3.4. Portable storage drives

Portage storage drives, such as CD-ROMs and USB flash drives, are being used to introduce social engineering malware on end-user computers. The use of portable storage media to spread malware is not a new avenue; it can be traced back to the use of floppy drives. W32/Hakaglan and Conficker are examples of malware that spread through portable flash drives.

4. Tactics

4.1. Psychological ploys

Social engineering works by manipulating emotions such as fear, curiosity, excitement, empathy, and greed or through the exploitation of cognitive biases [27]. Despite

up-to-date technical security protection, it only takes one gullible user to circumvent security controls. As mentioned earlier, persuading a user to activate malware is the first step in social engineering attacks. Some persuasive tactics that beguile users are described below.

4.1.1. Curiosity, empathy, and excitement

Intriguing and curiosity-exploiting subject lines are used by malware authors to capture the attention of users and lure them to open malicious e-mail attachments or web links. The Storm worm, discovered in January 2007, is a good example of an e-mail worm that caused major havoc worldwide [28]. The worm took its toll during a devastating winter storm in Europe when thousands of users interested in obtaining information on the storm were tricked into opening the e-mail attachment and infecting their computers. To bypass the users' e-mail filters, instead of an e-mail attachment users were given a compromised web link that resulted in a trojan being installed on their computer. Timely techniques are used to exploit search results related to major events and seasons. For instance, following the 2008 presidential elections, malware authors deceived numerous users into opening attachments that purported to include President Obama's acceptance speech.

Social engineering takes advantage of people's abiding interest in celebrities. For example, a mass mailing with an attachment named AnnaKournikova.jpg.vbs contained a worm that would e-mail itself to contacts from the users Outlook address book [29]. The devastation that resulted from this virus was felt worldwide in 2001. MacAfee ranks the names of riskiest celebrities to search for on the Internet; in 2009 Bradd Pitt was succeeded by Jessica Biel as the most dangerous celebrity to search for on the Internet. The ranking indicates the likelihood of people getting infected with malware by searching for information on the celebrity. Twitter and Facebook accounts of famous celebrities have been hacked into to create fake posts to video clips or websites that result in malware being installed on the computers of friends or followers of the celebrity.

4.1.2. Fear

A recent application of social engineering is the emergence of scareware, where the intent is to frighten users through the use of fake pop-up warnings of disk corruption, fraud alerts, etc. As the number of malware attacks has increased over the years, organizations and service providers try to educate users to be vigilant about installing security patches and anti-virus software. This has increased user awareness to the need for security, and promotes the idea that the Internet is not a safe place to surf. To exploit this belief, users are presented with fake pop-ups telling them their machine is infected with a virus and needs to be cleaned or patched. The pop-up directs users to click on a malicious link or executable program. Users are prompted to click on the offered software solution which, at the very least, results in the purchase of unnecessary software, and at worst could result in malware being installed on their machine [30].

Another extension of this strategy, known as Ransomware, is a malware that encrypts documents (Word, PDF, Excel) on a user's computer, then charges a license fee for a program that will decrypt the files. In another type, a trojan arrives as e-mail attachments containing messages about critical updates for Microsoft Outlook [31]. A cunning feature of this e-mail is the existence of legitimate web links for information on Contact Us, Privacy Statement, Trademarks, and Terms of Use – except that the location of the update to be downloaded is not legitimate. Users who do not pay careful attention click on the link and unknowingly install the trojan on their machines.

4.1.3. Greed

Malware authors are tuned in to people's weakness for free things. A lot of Internet users are deceived into opening e-mail attachments or websites with the false hope of receiving something free. While browsing a website, users may be presented with pop-ups offering free screen savers, movie tickets, or coupons with clickable links that result in malware being installed on their computers. Free offers are often released during major holidays, such as free greeting cards and screens savers that are seasonal. In December 2008, Panda Labs discovered a worm that sent users' e-mails with the subject line "Merry Christmas" and free coupons to McDonalds. Opening them resulted in malware that infected the user's computer. Fig. 3 shows a screen shot of an e-mail received at a U.S. university, which tells users of their eligibility for a tax refund. This e-mail was sent during the tax filing season, so it is likely that many end users were deceived into following the web link and compromising their personal information.

4.2. Targeted attacks

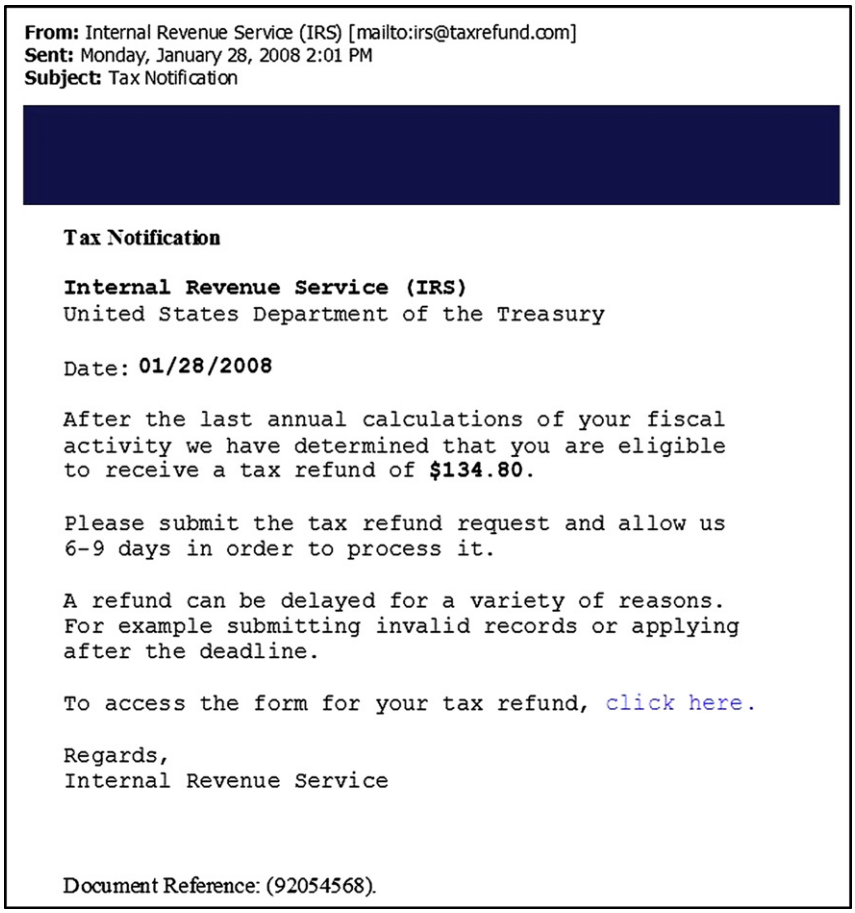
Attackers are now increasing the sophistication of their attack strategies by researching their target base and devising tactics that are tailored to certain user groups. The attackers invest time and resources to gather personality traits and other information about groups of individuals, then devise e-mails and websites that deceive the target groups. Some examples of user groups targeted by social engineering attackers are described below.

4.2.1. College students

Social engineering malware targets college students with e-mail messages that offer scholarships, student loans, free books, etc. Attackers harvest e-mail addresses from college directories, chat rooms, and networking sites or guess e-mail addresses based on first and last names, and send out e-mails that appear to come from legitimate and trust worthy sources.

4.2.2. Corporate executives

"Whaling" is an emerging type of targeted social engineering attack technique aimed at executives – i.e., the "big whales" in corporations. Attackers utilize publicly available information from company websites to send e-mail messages camouflaged to appear that they have originated from the Better Business Bureau alerting them of a complaint against the corporation that needs to be immediately addressed [32]. The e-mail contains malicious e-mail attachments or web links that lure executives to click, which then installs malware.


From: Internal Revenue Service (IRS) [mailto:irs@taxrefund.com]
Sent: Monday, January 28, 2008 2:01 PM
Subject: Tax Notification

Tax Notification

Internal Revenue Service (IRS)
United States Department of the Treasury

Date: 01/28/2008

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of $134.80.

Please submit the tax refund request and allow us 6-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, click here.

Regards,
Internal Revenue Service

Document Reference: (92054568).

Fig. 3. Example of a timely technique.

4.2.3. Countries, religious groups, and sects

Attackers have moved their bases to geographical regions across the globe that have less stringent laws governing the mass mailings referred to as "spam." By infecting computers in these countries, attackers can use machines there to send out spam and malware to millions of machines worldwide. Due to a lack of detection and remedy tools, the computers remain infected for long periods of time and are used to spread malware. Embassies and government organizations in countries such as India, South Korea, and Malta have been targeted with social engineering malware [33]. Recently several Tibetan computers in the office of the Dalai Lama were infiltrated with malware. The hacker network Ghostnet has been identified as the root of these targeted attacks of government systems [33]. The fundamental attack vector in spreading the Ghostnet network is social engineering. E-mails that appear legitimate and relevant are sent to the target groups with a trojan known as *Ghost Rat* as an attachment. Once installed by the user, the trojan takes full control of the computer, monitoring, downloading and even operating video and audio devices attached to the computer to capture conversations and relay them to the hacker network [34].

4.3. Technical tactics

By analyzing the technical descriptions compiled from our malware sample, we identified two major activities that malware perform once they are activated: (1) they combat existing protection mechanisms, and (2) they continue to execute by opening backdoors and/or installing key loggers. Given that activities vary from malware to malware, this is not a comprehensive list, but the discussion below provides a general understanding of technical countermeasures that such malware are designed to thwart.

4.3.1. Combating existing protection mechanisms

Whitman [2] is one of the first authors to bring Sun Tzu's theory of "knowing the enemy" into the context of information security. Several research studies use game theory to describe and model the interactions between organizations and attackers (e.g., [35]). Akin to an arms race, the security community constantly plays catch-up with malicious code authors who continually evolve their malware to combat existing protection mechanisms. Anti-virus products are one of the most widely used security tools. The annual CSI/FBI survey [36] reports that 97% of organizations have deployed anti-virus software, which works by

looking for signatures of known threats. However, if the signature file of a malware has not yet been discovered, anti-virus software cannot detect or subdue it.

To avoid being detected by spam filters, attackers now send out malware-infested e-mail messages with images instead of text in the body of the e-mail message. The images are included as clickable links that lead to malware that infects the machine. Similarly, to circumvent highly secure and monitored networks, some social engineering malware avoid sending e-mails to certain domain names. For example, MyDoom.AE is a social engineering malware that reaches inboxes as an attachment but avoids sending e-mails to certain strings. Some of the strings include gov, syma, mil, usenet, unix, tanford.e, utgers.ed, and webmaster [12]. An analysis of the strings shows that they are e-mail domains of government agencies, educational organizations, and anti-virus vendors. By avoiding these domains, the malware hopes to remain undetected longer.

DNS (Domain Name Server) addresses include characters (e.g., www.education.edu) so humans can more easily remember them; however, these DNS addresses are actually translated further to IP addresses for computers to relay the messages. Hence if an IP address is entered in the address space of a browser, the computer will complete the communication. Users are sometimes presented with IP addresses as clickable links that hide the real domain address of a fraudulent website. The examples below describe the interactions between attack strategies and protective technologies.

```
U:\>ipconfig/displaydns

    Record Name . . . . . :
    www.rroyalcasino.com
 Record Type . . . . . : 1
 Time To Live . . . . : 172
 Data Length . . . . . : 4
 Section . . . . . : Answer
 A (Host) Record . . . : 97.90.158.85

    Record Name . . . . . :
    www.rroyalcasino.com
 Record Type . . . . . : 1
 Time To Live . . . . : 172
 Data Length . . . . . : 4
 Section . . . . . : Answer
 A (Host) Record . . . : 12.219.119.34


    Record Name . . . . . :
    www.rroyalcasino.com
 Record Type . . . . . : 1
 Time To Live . . . . : 172
 Data Length . . . . . : 4
 Section . . . . . : Answer
 A (Host) Record . . . : 24.9.9.34
```

Fig. 4. Output of displaydns command highlighting the fast flux technique.

4.3.2. Fast-Flux

One technique used to prevent malicious e-mail messages and web links from being viewed by end users is to block the IP address of the e-mail and website domains [6]. This technique, known as blacklisting, is used in an organization to prevent traffic from malicious domains from reaching the organization's network.

In order to combat this protection mechanism, attackers use a technique known as *fast flux*. This technique rapidly modifies the IP addresses of the domains names involved in malicious activities making it difficult to detect [37]. Consequently, it poses a challenge for preventive technologies that rely on blocking IP addresses. The Storm worm is one of the first e-mail worms to utilize fast flux. To improve response times to domain name queries, the DNS stores IP addresses in its local cache. The time-to-live (TTL) value determines how long the corresponding record is cached on the server. If the TTL value is very low the domain name will be refreshed very often. Fast flux changes the IP address of the domain name rapidly by making the TTL very low (e.g., 180 s). Thus, each time the DNS record for the domain is refreshed, a new IP address is obtained.

During a six-month period in 2007 alone, there were over 40,000 domains with more than 150,000 fast flux IP addresses [38]. Fig. 4 shows a partial screen shot of a DNS name resolution for the fast flux domain name rroyalcasino.com, a blacklisted domain. We used the Windows command Ipconfig/displaydns to display the contents of the DNS resolver cache after pinging the domain www.rroyalcasino.com. There were 12 different IP addresses for the domain, and the TTL value was only 172 s. We ran the command at different time intervals and obtained 19 different IP addresses for the domain. This attack strategy serves as an excellent example of the constant evolution of malicious activities to combat preventive mechanisms.

4.3.3. Deactivating security tools

Social engineering malware have also succeeded in disabling anti-virus software applications and blocking attempts to go to Microsoft's website for patches. MyDoom.B exhibited the characteristic of null routing the DNS entries on the local machine to security websites. On a Windows machine the hostnames to IP address mappings are stored in a folder called the Hosts file. This file is loaded into the memory of the computer during startup. The Hosts file also blocks access to malicious websites as, prior to connecting to a website, the file is verified to resolve the hostname to the IP address. Malware counteract this mechanism by including null entries to hostnames of anti-virus vendors and Microsoft websites. Some malware overwrite the local machine's Hosts file that is used for DNS resolutions. Fig. 5 provides a screen shot from an analysis of the modified hosts file on a MyDoom.B infected computer [39]. A close look at the list shows that the addresses belong to anti-virus vendors and Windows updates. If the anti-virus application is disabled, it is difficult to detect the existence of malware on the machine. This defensive strategy helps the malware live for a longer period on user computers.

The modified hosts file is provided below:

```
127.0.0.1   localhost localhost.localdomain local lo
0.0.0.0     0.0.0.0
0.0.0.0     engine.awaps.net awaps.net www.awaps.net ad.doubleclick.net
0.0.0.0     spd.atdmt.com atdmt.com click.atdmt.com clicks.atdmt.com
0.0.0.0     media.fastclick.net fastclick.net www.fastclick.net ad.fastclick.net
0.0.0.0     ads.fastclick.net banner.fastclick.net banners.fastclick.net
0.0.0.0     www.sophos.com sophos.com ftp.sophos.com f-secure.com www.f-secure.com
0.0.0.0     ftp.f-secure.com securityresponse.symantec.com
0.0.0.0     www.symantec.com symantec.com service1.symantec.com
0.0.0.0     liveupdate.symantec.com update.symantec.com updates.symantec.com
0.0.0.0     support.microsoft.com downloads.microsoft.com
0.0.0.0     download.microsoft.com windowsupdate.microsoft.com
0.0.0.0     office.microsoft.com msdn.microsoft.com go.microsoft.com
0.0.0.0     nai.com www.nai.com vil.nai.com secure.nai.com www.networkassociates.com
0.0.0.0     networkassociates.com avp.ru www.avp.ru www.kaspersky.ru
0.0.0.0     www.viruslist.ru viruslist.ru avp.ch www.avp.ch www.avp.com
0.0.0.0     avp.com us.mcafee.com mcafee.com www.mcafee.com dispatch.mcafee.com
0.0.0.0     download.mcafee.com mast.mcafee.com www.trendmicro.com
0.0.0.0     www3.ca.com ca.com www.ca.com www.my-etrust.com
0.0.0.0     my-etrust.com ar.atwola.com phx.corporate-ir.net

0.0.0.0 www.microsoft.com
```

Fig. 5. Disabling protection mechanisms [39].

4.3.4. Own SMTP engine

SMTP (Simple Mail Transfer Protocol) is the standard for sending e-mail messages across the Internet. The protocol works by sending requests to a remote server by using queries and responses. The message uses a relay server that delivers the message to the destination e-mail server. An e-mail server that is an open relay, transfers e-mail messages from destinations outside of its domain. One of SMTP's biggest security challenges is that it does authenticate the sender of the message. In our analysis, there were several cases where the malware harvested e-mail addresses from victims' address books and sent fake e-mails from users' e-mail accounts. This crafty strategy deceives the receiver into thinking that the e-mail is being sent from a trusted source. This is known as e-mail "spoofing," and is defined as forgery of the e-mail header, which makes the e-mail message appear to have been received from a different source than the actual source [40].

In the past malware utilized organizations' e-mail servers to relay e-mail messages (e.g., Hybris, Haiku worm, etc.). However, as organizations have become proactive in reducing e-mail spoofing and blocking e-mail servers from being open relay agents, malware authors now use their own SMTP engines to propagate across the Internet. Upon activation by the end user, the malware installs the necessary SMTP program files on the user's machine thereby turning it into an e-mail server. This strategy enables the malware to propagate even if the organization's e-mail server prevents address spoofing or open relay agents. Several open source e-mail server programs are available that can be used by the malware authors without any cost. The e-mail worm Netsky.C is one among numerous social engineering malware that uses its own SMTP engine to propagate. The worm verifies the domain name of the target e-mail addresses and obtains the SMTP server's IP address for that domain from the local DNS server. MyDoom goes one step further by using the backup SMTP server addresses instead of the primary server IP addresses [41]. Once the IP address of the target domain name is obtained, the worm uses its own SMTP engine to send the e-mail. Some researchers [42] recommend monitoring DNS patterns and examining traffic on the SMTP port in the infected machine to detect malware that use their own SMTP engines to propagate. However, such detective methods are still in their infancy and are not widely used by organizations.

4.3.5. Self-defending

Malware now strike back at those who try to stop them. Storm worm is one of the first worms known for striking back by creating distributed denial-of-service attacks at machines trying to probe its command-and-control servers. Storm worm-infected machines form massive bot networks can be used to launch denial-of-service attacks at targeted machines and even paralyze the machine for weeks [43]. A botnet is a network of malicious bots – programs that perform user-centric tasks automatically without any interaction from a user – that illegally control computing resources. Botnets generally have a central command-and-control location. Extensive methods to combat botnets are still being developed, but one way to stop botnets is by detecting the command-and-control point of the botnet. This centralized property of botnets is helpful for security professionals, as they identify a single point of failure for the botnet [44]. The bot network of the storm worm is unique in that it is a decentralized

command-and-control network. This means the root of the bot cannot be detected and eliminated. Some have estimated the massive Storm bot network to comprise one million to fifty million computers [43]. Recent social engineering malware are designed to add computers to bot networks that are then used by malware authors to send out e-mail spam, launch denial-of-service attacks, and provide false information from illegally controlled sources [44]. The owner of a bot network can sell parts of the bot network to criminals enabling them to launch denial-of-service attacks against organizations and to send out spam.

5. Malware actions

Once the malware has breached a system's defenses, it is ready to complete its mission. Based on our sample of malware, the next steps executed are often some combination of installing key loggers, and/or opening backdoors. We describe each of these below.

5.1. Key loggers

Some of the social engineering malware we analyzed resulted in key loggers being installed on a user's computer. Key loggers are malicious programs that capture keystroke information, and in most cases relay the information to outside sources. For example, W32.HLLW.Fizzer@mm is a mass mailing malware that installs a key logger on the infected machine. The malware attempts to spread by e-mailing itself to addresses on the user's contact list and through file-sharing programs. The logs on all the keystrokes are saved to an encrypted file on the user's computer. The malware connects to various IRC servers and waits for commands to execute functions and transfer files. The dangerous aspect of key loggers is the potential to obtain credit card numbers, social security numbers, and other personal information from users' keystrokes. Key loggers are easy programs to create, and there are numerous pre-build key loggers available for users to download.

5.2. Backdoors

Many of the social engineering malware we analyzed open backdoors on computers. A backdoor is the malware author's hacking tool of choice, as it allows remote connections to the system [41]. Generally a backdoor opens network ports (TCP/UPD) and waits for remote connections from the attacker on the open port, providing access to the system. Several malware come with built-in backdoors. Depending on the motive of the malware authors, various backdoors are installed on an infected computer. Dumaru.Y is an e-mail worm that, upon execution, installs several backdoors and data-stealing components. The worm also attempts to steal personal data and keystroke information, which is then e-mailed to predefined e-mail addresses. Mydoom.A is another example of an e-mail worm that opens backdoors by opening TCP ports that permit attackers to connect to the system and use its network resources. The backdoor also can download and execute files on the computer. Furnell and Ward [45] call every backdoor an asset that the attacker acquires in the form of a compromised system.

5.3. Rootkits

Rootkits are a group of programs designed to remain obscure and undetectable in computers that have administrative access to a larger system. The malware (e.g., Bagel worm) then searches the computers' directories and files for stored passwords. In many cases Rootkits are used to control and monitor the system for website visits, including bank transactions.

5.4. Hijacking

Malware can hijack an active session between a user and an e-commerce or banking site. The hijacked session steals the role and authentication of the established legitimate source and obtains sensitive information and even redirects or alters active transactions.

Alternatively, browser hijackers alter the default web address in the browser, redirecting web page visits to fraudulent websites or displaying pop-ups and stealing confidential information.

6. Implications

The observed trends and tactics used by social engineering malware show that organizations need to adopt a multi-pronged approach to combating social engineering malware rather than pursuing purely technical solutions. Organizations have made great strides in implementing effective security technologies and processes, but there is a gap in integrating these efforts with people [46]. Technology and security policies alone cannot protect organizational assets from cyber attacks. Technology is only useful if adopted and accepted by people in the organization [47]. People play a major role in shaping the effectiveness of information security policies in an organization. Below we identify areas that assist organizations in mitigating the human risks posed by social engineering malware.

6.1. Increase awareness of information security

Among user, the lack of awareness about security policies and best practices has been identified by several security scholars as a major cause of failure [47–49]. Although many organizations provide information security awareness training, it is generally provided when an employee starts working at the organization or is a one-time effort. The evolving landscape of social engineering tactics, as described here, shows that training processes need to be updated regularly in order to remain current with the changing environment. This calls for ongoing information security training for all levels of an organization. Information security portals in the form of websites or knowledge bases should be available where employees can obtain information on the latest threats, fixes, and security patches. Employees should be aware of the existence of these information security resources. It is imperative that

tutorials and/or knowledge bases be accessible and interesting to users. Resources containing language filled with technical jargon should be avoided so all users can understand the information.

As discussed earlier, malicious code authors employ timely techniques during major holidays and events. Therefore, notifications should be sent to employees during these times to remind users of the possibility that they may receive e-mails or pop-ups that in fact direct them to malware. Users should be provided with examples of e-mails and pop-ups so they become alert to the types of attacks. Depending on the number of employees, an organization can choose between various channels to relay information to users, such as computer-based training, in-person training, videos, etc. Rather than simply making such awareness programs available to employees, organizations should require employees to attend and prove proficiency in the programs. Organizations can measure the level of awareness among employees by surveys, security tests, etc., and measure the level of security proficiency among employees. Managers need to be trained to promote an information security culture within their supervising units. Essentially, organizations need a comprehensive, ongoing information security program that caters to employees at all levels in the organization, and that can be evaluated for success.

6.2. Monitor home use

Organizations should train employees to continue following information security best practices beyond the physical realm of the organization. A relatively neglected area in organizational security is security of employees' residential computers. The changing work environment that now demands anytime, anywhere communication causes employees to access e-mail constantly from various locations and devices. Given the growth of the telecommuting workforce, the protection of residential networks is vital to the continued protection of organizational networks. In a study of corporate and government organizations, only half of them reported having developed guidelines for telecommuting [50]. Also about 50% of respondents indicated that telecommuting employees occasionally used their personally owned computers for work purposes. A study of remote workers found that people working from home tend to be less conscious of information security practices [51]. Additionally, the home computer might be used by other family members who are not trained in information security best practices.

Even though home users may get security training at work, they need to take some initiative to ascertain that their home computers are secure. Organizations employ staff to ensure that their networks are protected and provide employees with machines that have updated anti-virus and security technologies. However, employees themselves have to purchase the necessary security technologies for their home computers and keep them updated. If the employee uses a home computer that is unlikely to be actively monitored for malicious software, it can remain compromised for long periods of time. It only takes a handful of compromised residential computers to disable an organization's networks with distributed denial-of-service attacks.

Many wireless routers, especially in homes, use default settings that prioritize ease of setup over security, thereby increasing the risk of Internet fraud [52]. Organizations can help improve employee home computer security by providing information security tools such as anti-virus and firewalls at a discounted rate to employees for their home computers. Organizations can extend the services of their IT staff to off-sites and during non-business hours in order to ensure that their employees' home computers are protected. Essentially organizations need to be proactive and expand their security safety net to include employee home computers as well.

6.3. Manage personal use of work computers

Personal use of computers at work is another neglected area of information security policies. The increased use of social software blurs the line between personal and professional exchange of information. Employers now rely on information posted on social websites for recommendations and hiring purposes. Organizations increasingly turn to social websites like Facebook and Twitter to promote information exchange among employees. Paradoxically, a large number of social engineering attacks are engineered using social software. Hence it is critical for organizations to consider how to mitigate the risks involved when employees utilize the organization's computers for personal purposes.

Employees who access personal e-mail accounts from, and download files to, work computers increase the risks to organizational security. The level of authority and authentication credentials of employees can make it easier for hackers to gain access as well as risk the organization's network security. It is critical for organizations to have policies that manage personal use of work computers. However, in today's information environment, totally restricting employee access to the Internet could be counterproductive. Instead, organizations could provide dedicated workstations in lounges for employees to access the Internet for personal use. These machines could be configured on a different network with restricted access to organizational resources. They would help mitigate the risks associated with employees using work computer for their personal use as well as give employees alternative avenues for accessing personal information.

6.4. Motivate users to follow secure practices

As pointed out earlier, it is important to provide ongoing training for employees, to educate them about the evolving landscape of attack strategies. Although awareness is necessary for involving end users in security efforts, it does not guarantee compliance with information security policies. It is equally important to motivate users to incorporate a security culture. As security is a secondary goal of end users [53], they are not always motivated to behave in a secure manner [54,55]. Motivation is an antecedent to end user behavior, and a number of studies have identified the need to focus on motivating users to behave in a secure

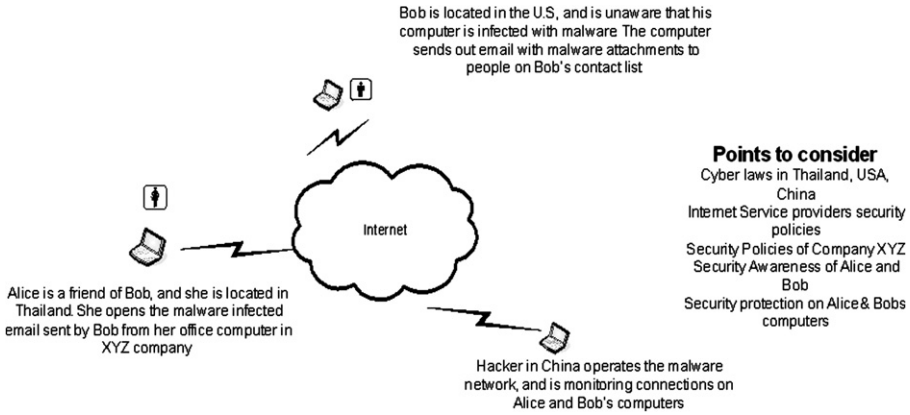


Fig. 6. Social responsibility in combating malware.

manner [53,54,47,48]. Information security needs to be embedded into the culture of the organization. Incentive programs that recognize and reward employees for keeping their computers virus-free can create a positive buzz around information security. Employees need to understand the importance of information security, and incorporate a security culture not just inside the organization but outside as well, to foster an information security culture from home and during personal use of the organization's resources.

7. Social responsibility in combating social engineering malware

Fig. 6 captures the interactions between end users, governments, and other organizations, and highlights the fact that combating social engineering malware calls for shared social responsibility. The figure shows a scenario where a user located in the US unintentionally sends an e-mail message embedded with malware to a friend in Thailand. From the spatial boundaries and policy implications, we can see that the responsibility to combat malware spans a wide array of entities, from organizations, governments, Internet service providers, international bodies, and end users. We further investigate the role of these entities and the challenges they confront in combating malware attacks.

Even if organizations become more proactive about creating policies for protecting against social engineering attacks, it is important to have laws in place that are enforceable. It is impossible to implement a single law that pertains to mitigating the risk of social engineering malware or computer crimes because the landscape of attacks spans the realms of websites, e-mail, international areas, software compliance, etc. Hence we find a myriad of laws in place that aid in reducing the risk of social engineering computer crimes. Table 2 lists some of the laws in the United States that aim to improve information security.

The mere existence of laws does not produce viable results unless they are enforced and verified for compliance. It is important to ensure that penalties are sanctioned for failure to comply with laws. A major challenge for governments is enforcing and ensuring compliance of cyber-crime laws.

Unlike organizations that have a responsibility to protect the users of their network, ISPs (Internet Service Providers) are not held responsible for monitoring their networks for malicious activities. Information security laws like Sarbanes–Oxley and the Federal Information Security Management Act specifically target organizations. The Trusted Internet Connection (TIC) Initiative issued in November 2007 is a start in streamlining ISP security, but it focuses on Internet access points for federal agencies. There are currently no specific laws governing security standards for ISPs that provide services to home users. It is equally

Table 2
Information security laws in the US.

Law	Enacted	Information security protection
Family Educational Rights and Privacy Act	1974	Protects privacy of student educational records
Health Insurance Portability & Accounting Act	1996	Security and privacy of health data
Gramm–Leach–Bliley Act	1999	Imposes security policies for financial institutions
Electronic Signatures in Global and National Commerce Act	2000	Security requirements for businesses using electronic transactions
USA PATRIOT Act	2001	Increases law enforcement agency's ability to conduct searches
Sarbanes–Oxley	2002	Security standards for public corporations
Federal Information Security Management Act	2002	Requires federal agencies to adhere to security standards
CAN-SPAM	2003	Security rules for commercial e-mail
Security Breach Notification Laws	Since 2002	Requires disclosure in the event of security breaches of personally identifiable information

important to develop security standards to protect networks including homes and small businesses. Majority of botnets are believed to be operating from residential computers. Such malicious activities can be stopped if ISPs take a lead in detecting anomalous activities. A number of ISPs offer security solutions to their customers for an additional fee, but the major challenge for ISPs is to integrate cost-effective services with embedded security services.

We recognize that it is not feasible for ISPs to ensure that every user in the network has up-to-date anti-virus software and security protections. End users also share the responsibility to ensure that they have appropriate protection mechanisms that facilitate safe Internet surfing. A simple analogy is the seatbelt law that protect drivers from accidents. Most countries have some form of seatbelt legislation requiring manufacturers to fit their vehicles with seatbelts and their occupants to wear the belts while driving. If the Internet is considered to be an information highway, and the computer the motor vehicle being driven, manufacturers should include anti-virus and security protection mechanisms with any computer sold. Analogously, if end users are the drivers, they should be required to use protective mechanisms while using the Internet. End users need to be mindful of ensuring that their ignorance does not cause loss of data or service for other users.

The Internet is not limited by geographical boundaries, and it requires the participation of international bodies to foster the cooperation of all countries in tracking and eliminating social engineering crime networks. A major challenge in tracking such crime lies in overcoming the barriers of language, culture, and laws across countries. Cross-national information sharing among international government entities is challenging, and it is important to set security standards that enable safe and active monitoring of cyber crime. Table 3 lists some of the international organizations fighting computer crime and their initiatives.

An important area that calls for international attention is the abuse of Internet domain name service. Stricter laws need to be enforced when selecting domain name services. Attackers have increasingly tricked users by registering domain name services that appear to be similar to organizations or banks. The allocation of domain name services needs to be monitored and requests for domain names tracked, especially for those that are typographically close to existing and established domain names. ICANN (Internet Corporation for Assigned Names and Numbers) is working to streamline the process of approving domain name sellers. With more than 500 domain name registrants in the market, and the existence of third-party domain name registrants, the process to authenticate domain name registrants is enormously complicated. Authentication needs to be strictly verified and monitored to prevent phony domain name registrations. A major challenge for ICANN includes identifying the registrants and tracking international domain name sellers. Table 4 summarizes some of the challenges we identified in combating social engineering malware.

Table 3
Initiatives by international standard-setting bodies.

International bodies	Outreaches
ISO (International Organization for Standardization)	Develops security standards
NIST (National Institute of Standards and Technology)	Develops supportive documentations, standards, recommendations, evaluate security policies
Internet Society	Provides leadership in Internet related standards, education and policy
ITU (International Telecommunications Union)	Facilitates cooperation internationally to strengthen cyber security
Information Security Forum	Independent non-profit organization that provides guidance in information security
FBI (Federal Bureau of Investigation)	Enforce laws and investigate cyber crimes

Table 4
Challenges in combating social engineering malware.

Motivating end users toward information security practices
Enforcement and compliance of information security laws
Implementing security standards for Internet service providers
Cultural and language barriers in fighting international crimes
Information sharing across boundaries
Abuse of domain names service

8. Conclusion

Even as computer systems continue to become more secure through better software development and testing, they are just as easily subverted by hackers using social engineering techniques [56]. We determined that social engineering malware is both pervasive and persistent. As presented here, our analysis of attack strategies shows that social engineering attacks are evolving and becoming more complex and sophisticated. The relative lethargy of users toward security practices, coupled with the aggressiveness of spammers and hackers, is a dangerous combination. In the early days of hacking, one had to be an expert and technically savvy in order launch and create malware. Today custom-built malware kits are commercially available that can be used to test potential networks and machines to launch attacks [12].

Technology and security policies alone cannot protect organizational assets from cyber attacks; they are useful only if adopted and accepted by people in the organization [47]. Although this has long been recognized, our analysis leads us to urge organizations to expand their efforts to encourage and cater to safe home computer use as well. Culnan et al. [57] advocate security awareness training programs to reduce risks stemming from unsecured home computers and mobile devices used in unsecured networks away from the office. However, the efficacy of such training programs may be limited due to the fact that malicious code authors are now utilizing highly sophisticated attack strategies that make it difficult for end users to distinguish between legitimate and non-legitimate e-mail messages and websites. We emphasize the need for organizations to provide ongoing training at all levels, and for such training to be tested and evaluated for success.

We recognize that organizations alone cannot mitigate the risks of social engineering malware, and that responsibility spans governments, ISPs, end users, and international bodies. The collective effort of these entities in overcoming current and future challenges is needed in order to mitigate the crimes perpetrated using social engineering malware.

References

[1] International Standards Organization (ISO). ISO/IEC 17799 information technology security techniques: code of practice for information security management. Geneva: ISO; 2005.
[2] Whitman M. Enemy at the gate: threats to information security. Communications of the ACM 2003;46:91–5.
[3] Stacey TR, Helsley RE, Baston JV. Identifying information security threats. Information Systems Security 1996;5:50–9.
[4] Loch KD, Carr HH, Warkentin ME. Threats to information systems: today's reality, yesterday's understanding. MIS Quarterly 1992;16:173–86.
[5] Solms RV, Solms BV. From policies to culture. Computers & Security 2004;23:275–9.
[6] Erbschloe M. Trojans, worms, and spyware: a computer security professional's guide to malicious code. Butterworth-Heinemann; 2004.
[7] Mitnick KD, Simon WL. The art of deception: controlling the human element of security. Wiley & Sons; 2002.
[8] CERT. E-crime watch survey. Available from: <http://www.cert.org/>; 2007.
[9] Wagner A, Dübendorfer T, Plattner T, Hiestand R. Experiences with worm propagation simulations. In: Proceedings of the 2003 ACM Workshop on Rapid Malcode. Washington, DC; 2003.
[10] Sanok D. An analysis of how antivirus methodologies are utilized in protecting computers from malicious code. In: Proceedings of the 2nd Annual Conference on Information Security Curriculum Development. Kennesaw, GA; 2005.
[11] Siponen M, Oinas-Kukkonen H. A review of information security issues and respective research Contributions. Database for Advances in Information Systems 2007;38:60–81.
[12] Symantec. Security response: Symantec. Available from: <http://www.symantec.com/security_response/>; 2008.
[13] Brownlow M. E-mail and website statistics. E-mail Marketing Reports; May 3, 2008.
[14] Kienzle D, Elder M. Recent worms: a survey and trends. In: Proceedings of the 2003 ACM Workshop on Rapid Malcode. Washington, DC; 2003.
[15] National Institute of Standards and Technology (NIST). History of worms. Available from: <http://csrc.nist.gov/publications/nistir/threats/subsubsection3_3_2_1.html>; 1994.
[16] Jakobbson M, Myers S. Phishing and countermeasures: understanding the increasing problem of electronic identity theft. Wiley-Interscience; 2006.
[17] Tiauzon S. TrendLabs malware blog. Available from: <http://blog.trendmicro.com/nu-war-tactics/>; 2006.
[18] De la Paz R. TrendLabs malware blogs. Available from: <http://blog.trendmicro.com/solar-eclipse-2009-in-america-leads-to-fakeav>; 2009.
[19] Ramzan R. Drive-by-pharming in the wild. Symantec. Available from: <https://forums.symantec.com/t5/Emerging/Drive-by-Pharming-in-the-Wild/bap/305989;jsessionid=A89BA88385E764FD3EACA223FD0346F6#A94>; 2008.
[20] Tepper M. The rise of social software. netWorker 2003;7:19–23.
[21] Narain R. Rogue advertisement pushes scareware to NYTimes.com readers. Threat Post: Kaspersky Lab Security News Service; 2009.
[22] Jagatic T, Johnson N, Jakobsson M, Menczer F. Social phishing. Communications of the ACM 2007;50:94–100.
[23] Dang H. The origins of social engineering. McAfee Security Journal; 2008. Fall.
[24] Krebs B. Phishers now twittering their scams. Washington Post January 2009;5.
[25] Fergusen R. TrendLabs malware blog. Available from: <http://blog.trendmicro.com/new-variant-of-koobface-worm-spreading-on-facebook/>; 2009.
[26] Pimentel J. TrendLabs malware blog. Available from: <http://blog.trendmicro.com/worm-sdbot-variant-spreading-through-msn-instant-messenger/%23ixzz0PsFb6PTN>; 2007.
[27] Raman K. Ask and you will receive. McAfee Security Journal Fall 2008;2008:9–12.
[28] Kanich C, Kreibich C, Levchenko K, et al. Proceedings of the 15th ACM Conference on Computer and Communications Security," Alexandria, Virginia, 2008.
[29] Chien E. Symantec threats and risks. Available from: <http://www.symantec.com/security_response/writeup.jsp?docid=2001-021219-1830-99>; 2007.
[30] Sharek D, Swofford C, Wogalter M. Failure to recognize fake Internet popup warning messages. Human Factors and Ergonomics Society 52nd Annual Meeting, New York; 2008.
[31] Gallego A. TrendLabs malware blogs. Available from: <http://blog.trendmicro.com/critical-update-leads-to-critical-info-theft/>; 2009.
[32] Garretson C. Whaling: latest e-mail scam targets executives. Available from: <http://www.networkworld.com/news/2007/111407-whaling.html>; 2007.
[33] BBC News. Major cyber spy network uncovered. Available from: <http://news.bbc.co.uk/2/hi/7970471.stm>; 2009.
[34] Tracking GhostNet: investigating a cyber espionage network. Information warfare monitor. Available from: <http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network>; 2009.
[35] Wang J, Chaudhury A, Rao R. A value-at-risk approach to information security investment. Information Systems Research 2008;19:106–20.
[36] Computer Security Institute (CSI). Computer crime and security survey. Available from: <http://www.gocsi.com/forms/csi_survey.jhtml;jsessionid=XIAUBOB54ND50QSNDLPCKH0CJUNN2JVN>; 2008.
[37] Internet Corporation for Assigned Names and Numbers (ICANN). SSAC advisory on fast flux hosting and DNS. Available from: <www.icann.org/committees/security/sac025.pdf>; 2008.
[38] HoneynetProject. Honeynet project. Available from: <http://www.dts.ca.gov/security_awareness_fair/DTS_Security_Awareness_Fair_Presenter_Patrick_McCarty.ppt>; 2007.
[39] Hines ES. MyDoom.B worm analysis. Applied Watch Technologies, <https://isc.sans.org/presentations/MyDoom_B_Analysis.pdf>; 2004 [accessed 02.11.07].
[40] Kruck GP, Kruck SE. Spoofing: a look at an evolving threat. Journal of Computer Information Systems; 2006 Fall:95–100.
[41] Szor P. The art of computer virus research and defense. Addison-Wesley Professional; 2005.
[42] Wong C, Bielski S, Mccune J, Wang C. A study of mass-mailing worms. Paper presented at the 2004 ACM workshop on rapid malcode. Washington, DC; 2004.
[43] Larkin E. Storm worm's virulence may change tactics. Available from: <http://www.networkworld.com/news/2007/080207-black-hat-storm-worms-virulence.html>; 2007.
[44] Julian BG, Vikram S. Peer-to-peer botnets: overview and case study. In: Proceedings of the first conference of the first workshop on hot topics in understanding botnets. Cambridge, MA: USENIX Association; 2007.
[45] Furnell S, Ward J. Malware comes of age: the arrival of the true computer parasite. Network Security; 2004:11–5.
[46] Andress A. Surviving security: how to integrate people, process and technology. Lincoln, NE: CRC Press; 2005.
[47] Siponen M. A conceptual foundation for organizational IS security awareness. Information Management & Computer Security 2000;8:31–4.
[48] Puhakainen P. A design theory for information security awareness. Unpublished dissertation, University of Oulu: Oulu, Finland; 2006.
[49] Thomson ME, Solms RV. Information security awareness: educating our users effectively. Information Management & Computer Security 1998;6:167–73.
[50] Telecommuting poses security risk. NetworkWorld 2008:24.
[51] Cisco. Understanding remote worker security. Available from: <http://www.cisco.com/web/CA/pdf/Understanding_Remote_Worker_Security_A_survey_of_User_Awareness_vs_Behaviour.pdf>; 2006.
[52] Tsow A, Jakobsson M, Yang L, Wetzel S. Warkitting: the drive-by subversion of wireless home routers. Journal of Digital Forensic Practice 2006;1:179–92.
[53] Good N, Krekelbert A. Usability and privacy: a study of Kazaa P2P sharing. O'Reilly Media; 2005.
[54] Adams A, Sasse A. Users are not the enemy: why users compromise security mechanisms and how to take remedial measures. O'Reilly Media; 2005.
[55] Stanton J, Stam K, Mastrangelo P, Jolton J. Analysis of end user security behavior. Computers & Security 2005;24:124–33.

[56] Kashyap R. The changing face of vulnerabilities. McAfee Security Journal; 2008 Fall:31–3.
[57] Culnan M, Fosman ER, Ray AW. Why IT executives should help employees secure their home computer. MIS Quarterly Executive 2008;7:49–56.

Sherly Abraham is a PhD student at the College of Computing & Information, State University of New York, Albany. She has a Masters degree in Telecommunications from SUNY Institute of Technology, Utica, NY, and a Bachelors degree in Computer Engineering from Assumption University, Bangkok, Thailand. Her research interests include information security, software patents, and telecommunication policies. She has presented her research at various conferences and her work has been published in *Computer Law and Security Review*.

InduShobha Chengalur-Smith is Chair of the Information Technology Management Department at the School of Business, State University of New York, Albany. She received her PhD from Virginia Tech, Blacksburg, VA. Prior to joining academia, she worked in the private and public sectors. Her research interests are in open source software, technology adoption and implementation, information quality, and security. She serves on the editorial boards of several journals, and her research has been published in journals such as *Information Systems Research*, *Communications of the ACM*, and multiple issues of *IEEE Transactions*.