Terror Spam and Phishing

Tomer Ben-Ari, The Interdisciplinary Center Herzliya, Israel; E-mail: ben-ari.tomer@idc.ac.il
Ron Rymon, The Interdisciplinary Center Herzliya, Israel; E-mail: ben-ari.tomer@idc.ac.il

ABSTRACT

We claim that mail Spam and Phishing can become an operational tool in the hands of terrorists, to perform more than just simple recruiting and fund raising activities. We show that by using spam methods terrorists can reach the heart of society, and succeed in getting some of its fringes to act on their behalf. This "outsourcing" of terrorist activity to own members of the attacked society may adversely affect law enforcement ability to use profiling in the war against terror. We describe a system that combines standard spamming techniques with standard and adapted security mechanisms, and which provides the functionality needed to target, recruit, and operate terrorist cells and opportunistic accomplices.

1. INTRODUCTION

If you are like most Internet users, your mailbox has been routinely flooded with "spam". Spam are email messages that try to tempt the recipient into buying something, and spammers typically send millions of identical unsolicited messages in order to get only a few buyers – altogether it estimated that spammers send 12 billion messages daily, or more than half of all email messages[Spam Filter Review, 2004].

Whereas today, spam is used primarily by commercial companies who want to increase their sales, we are already seeing cyber criminals who start using spam-based "phishing".

Phishing is a form of criminal activity using social engineering mainly to access private and secret information. Phishing today is mainly being used to extract secret codes and other information for fraudulent financial transactions [Phishing report 2004]. According to a recent survey, 43% of US adults have been targeted by phishing attempts [First Data *Phishing Survey, 2005]*.

This Article reveals a new possible method that terrorists can easly take advantage of when carrying out there terror activities, and exposes the absence of current technology from tackling such terrorists activity

The article will show how terrorists can use spam and phishing methods not only to recruit members and raise funds, but also to influence other people to carry out attacks on their behalf. We will also show that through the use of spam terror, terrorists can create fear and terrorize the public, even without taking any action.

Clearly, however, the most dangerous prospect is that terror spam can be used to draft agnostic individuals and units, from within the inner parts of the attacked society, who will commit terror attacks on behalf of, and under the guidance of terrorists. When the enemy could be almost anyone and anywhere, law enforcement will find it very difficult to use profiling techniques in its war against terror.

2. CURRENT USE OF CYBER MEDIA BY TERRORIST GROUPS

The Internet today contains endless information, tools and opportunities. Terrorist use the Internet today to satisfy their own needs. Much has been said about terrorists seeking to enlarge their power and capabilities taking advantage this important tool. Listed down are some of the main ways in which terrorists are using the Internet today.

- Mass-Communication Tool.
- Planning and coordination of terror attacks.
- Intelligence gathering.
- Fund raising.
- Recruitment.
- Psychological Warfare.
- Cyber Attacks.
- Providing Instructions to Potential Attackers.

Is Spam the Next Ultimate Tool in the Hands of Terrorists?

In this article, we claim that spam may become the important tool in the war against terrorism. Clearly spam can serve as a useful tool to spread terrorist's messages and knowledge, and to raise funds for terrorist's organizations. More interestingly, we claim that Spam can also serve as a tool for terrorists to influence individuals to act on their behalf or at least serving their purpose.

3. SPAM AND SPAMMING METHODS

The Spam Phenomenon

Spam refers to one or more **unsolicited** messages, sent or posted as part of a larger collection of messages, all having **substantially identical content**. It usually manifests itself as an email campaign that targets millions of email accounts around the world, in an unsolicited fashion *[Monkeys]*. Experts estimate as many as 12 billion spam messages daily, making for over 75% of all email traffic *[Spam Filter Review, 2004*

Spam proved itself as an easy way to reach a large audience, and an effective sales tool that works well despite the low apriority success rate of each individual email message.

Phishing

Whereas most spam is commercially motivated, "phishing" is a relatively new form of spam that is probably closest to the terror spam that we introduce next. Phishing is spam, used by fraudsters to get access to the passwords and other private or financial information of unsuspecting users. *[Drake, Jonathan & Eugene 2004]*

4. TERROR SPAM

We believe that spam can become attractive to terrorist groups, not merely as a tool to spread their messages, but also to raise funds and recruiting members. More importantly, we speculate that spam can be used by terrorists to influence non-members to carry out attacks that coincide with the terrorist's goals and plans, and to coordinate activities of a dispersed heterogeneously motivated network of activists. Whereas today, it is commonly assumed that some Islamic terrorist organizations will only recruit staunch believers to carry out attacks (especially suicide attacks), we believe that in the future they may use "outsourcing" techniques, and will find the right justification to doing so. The trigger may be lack of resources, or the clear logistical and operationally benefits of "outsourced" activity, but in any event this may result in higher quality attacks.

The main features that make terror spam and phishing attractive to terrorists are:

1. Anonymity and difficulty of tracing;
2. Low cost to reach a large audience and hence the ability to engage a large number of (low probability) initiatives;
3. Leverage in reaching new and otherwise inaccessible audiences
4. Ability to recruit operatives from within the attacked society
5. Ability to spread fear, even without any action being taken

Usage

Terrorists can clearly use spam as a means to achieve there goals. Especially by focusing on direct needs to carry out attacks such as:

- Communications.
- Funding.
- Recruitment.
- Influencing individuals on taking extreme actions.

5. HOW TERROR SPAM MAY WORK

In this section, we describe how terror spam may work. We start by reviewing potential target audiences for terror spam, and the chances of response/success. We then discuss various technical modifications to traditional spam, which may be required to facilitate terror spam.

Target Audiences

In this section, we present terror as a "product" to be spammed. Like any other product, the terror spammer needs to consider the target audience(s), so that the campaign reaches the intended recipients, and so that the campaign is structured to appeal to the respective audiences. While it is true that the direct cost of spamming is very low, terror spammers may still want to avoid indiscriminant campaigns. First, spamming indiscriminately requires more resources, and will also reduce the time-to-block time frame, i.e., the time it would take law authorities to stop the spam and to block the next step of making contact with a collaborating receiver. Second, and more importantly, it may be important for terror spammers to craft different messages that will appeal to specific audiences.

We consider the following groups as primary targets for terror spammers:

- **Affinity religious, ethnic, and national groups**.
- **Sympathizers.**
- **Disadvantaged and disgruntled groups**.
- **Teens**.

Terrorists group can benefit from almost any outcome such a spam campaign will bring.

By throwing spam campaign terrorists will be able to achieve physical damage in some cases and advertisement that can lead to public panic in other cases, in both cases terror organization will benefit.

A spam campaign can be used to coordinate an attack among a number of people

This type of coordination can be achieved due to the high level of control that the technology environment provides i.e. giving guide to many people that are located in distance places. Exact orders can be given to all executers telling them precisely what to do in a specific time period or place, additional guidelines can be given via SMS. More over a special secured forum or chat room can be opened and enable the attackers to exchange information between themselves.

If at the same day a number of American symbols such as restaurants, entertainment chains etc…will be attacked the media effect will be very large.

The spam campaign can simply empower "Traditional" cyber terror actions

By encouraging users to DDOS web sites email addresses and other web based services of governments and private companies such as banks, e-com web site etc…and by that disrupt public services.

In some cases the potential users will prefer not to take an active role in terror actions but will be willing to volunteer critical information. Security leaks of critical infrastructure, governmental offices and public places can give a meaningful added value to the terror organizations. Terrorists can tempt users to "help" by offering money to any sensitive information that will be delivered to them.

In Some cases the spread of fear and instability is far more damaging then the physical act of terror itself.

If up until now we thought that a terrorist must come from a certain part of the world or alternative believe in certain things at this point we will have a problem of defining a terrorists due to the fact that it can be the next door neighbor that doesn't believe in anything suspicious and revenge is the only thing that guides him.

6. TECHNICAL IMPLEMENTATION OF TERROR SPAM CAMPAIGN

We propose an implementation blueprint for a Terror Spam System (TSS) that uses available spam technology, and simple modifications thereof that provide the additional security services that terrorists may need.

System Overview

The TSS is designed to enable terrorists to initially contact a wide target audience, and to then continue to communicate with respondents safely until and after the terror act is actually committed.

In the initial phase, the TSS enables the terrorist groups to reach as many potential agents (prospects) as possible. Some prospects may share the terrorist's motivations, whereas others may simply want to leverage the terrorist's capabilities and resources in order to achieve their own goals (which may partially coincide with the sponsoring terrorists). In this phase, the TSS provides some mechanisms that would reduce the risk of detection, and others that would help segregate communication channels.

Once the first responses are received, The TSS provides additional security mechanisms, and various controls on the communication with different prospects, including mechanisms designed to segregate communication channels, and to reduce the risks posed by informants and ingenuine respondents, as well as the risk of exposure of genuine respondents.

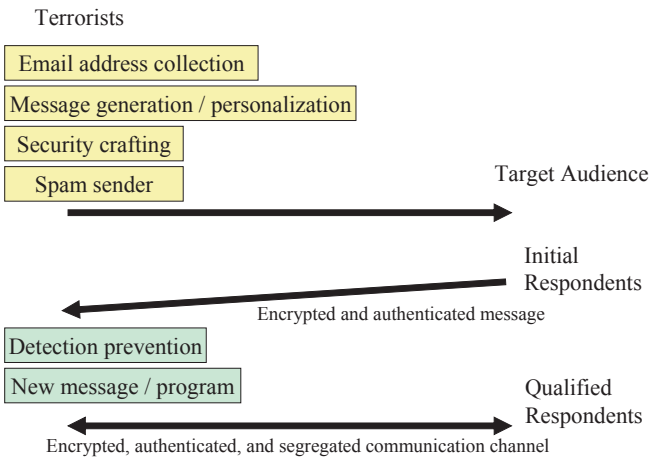
Figure 1 shows an overview of the TSS system and the flow of information and processing.

Just like in a marketing spam campaign, the goal of the first phase is to mass mail to prospective "agents". The first step in this phase is to acquire lists of email addresses of potential prospects, based on a specified set of target audience criteria. This is done by the "**Email address collection**" component.

Next, the TSS "**Message generation and personalization**" component shall construct/design a message (or select one from a number of pre-designed alternatives) to match each of the targeted prospects. The goal here is to personalize a message that is likely to draw the attention and response of targets. Thus, different messages can be mapped to different target audiences.

Subsequently, each message shall be enhanced with security mechanisms using the "**Security crafting**" component. For example, we propose that messages contain a script, and recipients are requested to reply through this script rather than by clicking "Reply" and using the regular SMTP reply. This script may, for example, encrypt the reply using a public-key scheme. The security mechanisms shall make it more difficult for the ISP to record and track the response, and shall make it difficult for an eavedropper to interpret the actual message. The script may also collect some information about the recipient's machine, using spyware-like technologies. This information, together with the message unique ID, and a time

Figure 1. Overview of TSS system



stamp indicating when the message was sent, may later be used to authenticate the respondent and to detect possible "mischief". Finally, different batches of outgoing messages shall be designed to respond to different email addresses (collection points), for segregation reasons.

The next step is of course to send the messages, using the "**Spam Sender**" component. This component will use standard spamming techniques to distribute the email messages to the target addresses. As an example, to avoid detection, the Spam Sender may distribute the messages into several batches which will be sent through several mail servers and at different times.

This completes the first phase of mass mailing.

The expectation is that a small fraction of recipients will respond to the initial email campaign. The secured script that is embedded in the message will use the identifier, time stamp, and the unique public-key that is provided for this message to encrypt this communication. The reply will be sent to one of several receiving email addresses, per the above mentioned segregation policies. The receiving program will then use the "**Detection prevention**" component to review the responses for authenticity and for various tell-tales of possible risks. Replies in which there is a mismatch between the unique identifier and the address to which the original message was sent, and the address from which the response was received will be ignored. It is also possible to ignore responses that are not received within a certain time window from their time stamp, as ones that may have been tampered with, e.g., the received may have contacted law enforcement authorities. (of course this may result in some loss of genuine respondents). Filtered messages will be sent to human operators, who will then use a separate communication channel with each respondent.

In the beginning of this "second level communication", the prospect would be provided with software components that would enable the implementation of additional security mechanisms, e.g.

- confidentiality – through encryption using public and/or symmetric key schemes for the communications, as well as for communication traces and data stored locally on the prospect computer
- authentication – using cryptographic means, and also physical and OS identification of the prospect computer
- segregation – using a unique channel and communication address for each prospect
- detection avoidance – by frequent changing email addresses and other "meeting locations"
- detection of mischief – through a spyware component that would monitor the activities of the prospect, and his/her other communications

Description of Specific System Components

In this section, we provide a more granular description and discussion of each of the TSS components.

1. Email addresses collection
   The role of this component (which will likely be implemented as a set of specific systems and procedures) is to acquire email lists according to the characterization of the target audience. Spammers are implementing similar systems, which use a variety of automatic and manual methods, e.g.,
   - extracting email addresses from mailing lists, directories, chat rooms, and discussion forums
   - automated harvesting of email addresses from web pages, who-is contact lists, etc.;
   - guessing email addresses for a specific domain, e.g., as a combination of first and last name;
   - using social engineering methods to obtain email addresses and other personal information;
   - legitimate purchase, and/or bribing for, and/or breaking into consumer databases
2. **Message generation/personalization**
   Mail messages should attract prospects to open and read, and if possible entice prospects to respond/act. In general, messages should be short and to the point. As indicated, the message shall also collect necessary information and initiate second-level contact.
   A possible implementation may start with a number of pre-composed message templates in several languages that will support localization, and then select and fill out the template that best fits each targeted recipient. A matching function shall be constructed to maximize the match between the features of the message and those of the prospective recipient. Dynamically adapting matching functions may be programmed to learn from past response rates.
3. Security crafting
   This component adds a security response script to each message. The script shall support automated encryption of the response, and targeting of the response directly to one of the collection centers. The script shall also verify that response does not exceed the valid time window. In addition, the script shall collect and send back some identifiers from the user's machine like the user and machine names, MAC, and IP address. The script may also collect more subtle information such as email correspondence, browsing information, bookmarks, etc, and may even install a spyware component (or even a trojan) that will continue monitoring the activity on the machine.
4. Spam Sender
   The spam sender is fed with a list of email addresses and the message templates that were selected for each. Before sending, the spam sender attaches a time stamp to each message, to start its validity window. The main challenge of the spam sender is to avoid its detection and the blocking of its messages. Spammers have specialized in this, and use methods such as:
   - use many and frequently changing IP addresses, as well as use of spoofed addresses;
   - use third-party outgoing mail relays that were left open
   - sending smaller batches from each outgoing mail server;
   - adapt the templates messages to a form that would be less detectable by filtering programs (this shall probably be done in the messages database itself, rather than in the sender, but we bring it here because it is one of the ways to avoid detection)
   - use HTML messages with Java script-encrypted frame tags that launch the body text only at the email client
   - use web beacons, and deceptive opt-out links to verify which addresses are active (again, this shall probably be fed back into the email addresses database)
   - use Trojans on some of the recipients to send more messages from *their* machines
5. Detection prevention
   The role of the receiver is to detect responses from law enforcement and other impersonators. Responses that are not well encrypted with the originally provided keys (in the script) will be rejected. Several rules in the detection prevention component shall seek suspicious information in the machine-specific data returned from script. This data shall also be stored and compared to future communication with same prospect. In case of serious suspicion, the receiver may abandon the entire communication associated with this email collection center, assuming it was compromised.

7. SOME RECOMMENDATIONS

In order to prevent and/or minimize terrorist's success in achieving their goals by using spam we'll suggest a few actions that could be taken.

1. Create a "Terror Spam Tracing Center" that will monitor all terror transportation.
   This center will gather data from all ISP's and publish domains, ISP', IP's etc…of mails that are suspected to be from terror organizations and publish them to all ISP's. The ISP's will be obliged to block all mails from the terrorists list.
2. Send a follow up email to every address that receives a "spam-terror" email saying that you just received an email from a terror organization, please delete it, Indicating that cooperating with terror organizations is a felony, letting the recipient understand that is actions are being watched and he's will be better off if he stops the contact with terrorist organization.
3. Create a unit that will detect and follow the traces of terror spam, in order to reach the perpetrators. Detectives in this unit shall respond to terror spam, and shall create contact where possible (under cover of course) with the relevant cells, with the goal of gathering intelligence and making arrests
4. Shut down servers that were used to send terror spam using either legal or semi-legal means depending on the location of those servers.
5. Some thought should be taken in order to protect the mobile phone industry from SMS terror Spam.

8. CONCLUSION

There is evidence today that religions terror organizations are linking with other terror organization in order to join forces against common enemies. For example Al Qaeda and far right groups such as neo-nazis and skinheads in Europe, these links are suspected to be both on the financial and action carrying levels. If terror organization will decide to further extend there links to individuals whom not necessarily believe in their organization ideology but are willing to take actions that might serve it than Spam email might serve as a perfect tool to achieve those links. By using this simple tool we showed how terror organizations can easily cause more violent incidents and increase the terror level world wide. Spam can reach civilians inside a target population that want to harm their own population provides a perfect communication tool. The spam will allow individuals to contribute both silently and actively to terror organizations dependent on each individual's preference. We showed that spam is hard to stop and detect, although the industry is taking more meaningful and aggressive approaches verse spam still spam is difficult to detect and many spam emails reach the users mailbox at the end of the day. By using spam terror organization will spread the knowledge of creating dangerous weapons, as technology is getting better and better the task of creating explosives is getting to be unbelievably simple in a way that teenagers can easily build explosives and activate them, Moreover spam can help coordinate between people who do not interact directly and by that increase the level of the terror actions and the public insecurity and fear. Finally we showed a few actions that can be taken in order to fight the phenomena of spam terror.

REFERENCES

1) [France2002] France, Mike "Commentary: Needed Now: Laws to can spam Business Week September 26, 2002 http://www.businessweek.com/magazine/content/02_40/b3802104.htm
2) [Weimann 2004] Weimann, Gabriel "How Modern Terrorists use uses the internet" 2004
3) [Wanger 2004] Thomas, Wanger: "Internet Emerges As Potent Terrorist Tool" September 24, 2004 http://federalnewsradio.com/index.php?nid=84&sid=138527
4) [SearchSecurity 2004] SearchSecurity.com Definitions - distributed denial-of-service attack http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci557336,00.html
5)[Prichard & MacDonald, 2004] Prichard, Janet and MacDonald, Laurie: "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks" 2004
6) [Wikipedia] Wikipedia: "Spam Definition" http://en.wikipedia.org/wiki/Spam_(e-mail)
7) [Leung 2003] Leung, Andrew: "Spam The Current State" August 8, 2003
8) [Monkeys] Monkeys, Spam Defined " http://www.monkeys.com/spam-defined/definition.shtml"
9) [Spam Filter Review 2004] Spam Filter Review : Spam Statistics http://spam-filter-review.toptenreviews.com/spam-statistics.html
10) [Vatis 2004] Vatis, Michael : "Cyber Attacks: Protecting America's Security Against Digital Threats" June 2004
11) [Lewis 2002] Lewis, James: "Accessing the risk of cyber-terrorism cyber war and other cyber threats" December 2002
12) [Denning, 2000] Denning, Dorothy: "Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of representatives http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html May 23, 2000
13) [Erica, 2004] Erica, Bozzi "Expectations of social behavior and cognitive dissonance among college freshman as influenced by mass media"http://www.anselm.edu/internet/psych/sr2003/bozzi/webpage.htm 2004
14) [Phishing report, 2004] Anti fishing working group "Phishing attack trend report 2004"
15) [Prashanth, 2003] Prashanth , Srikanthan "An overview of spam handling techniques" 2003
16) [Drake, Jonathan & Eugene 1004] "Christine E. Drake, Jonathan J. Oliver, and Eugene J. Koontz Anatomy of fishing email"
17) [ASTA, 2004] "Anti-Spam Technical Alliance Publishes Industry Recommendations to Help Stop Spam"
18) [AOL Spam Lawsuit] "AOL signs on to anti-spam lawsuit" 2004 http://www.bizjournals.com/washington/stories/2004/03/08/daily21.html
19) [Microsoft Spam Lawsuit] Microsoft spam lawsuits http://informationweek.com/story/showArticle.jhtml?articleID=54201964
20) [EL Qaeda 2004] "How El Qaeda uses the internet" 2004
21) [Garfinkel, 2003] Simson L. Garfinkel "Enabling Email Confidentiality through the use of Opportunistic Encryption" 2003
22) [Adabi, Glew, Horne & Pinkas, 2002] Matrin Adabi, Neal Glew, Bill Horne & Benny Pinkas"Certified Email with a Light Onlinerusted Third Party:Design and Implementation" 2002
23) [First Data Phishing Survey, 2005]. Survey: 43 Percent of Adults Get 'Phished'. http://news.yahoo.com/s/ap/20050512/ap_on_hi_te/phishing_survey
24) [Hinnen] Todd M. Hinnen "The cyber-front in the war on terrorism: curbing terrorist use of the internet"
25) [Timothy L] Timothy L. "Al Qaeda and the Internet:The Danger of "Cyber-planning"