Marketing Vulnerabilities in an Age of Online Commerce

Robert S. Owen
Texas A&M University, Texarkana, USA

INTRODUCTION

This article provides an overview of strategic and tactical threats to the marketing efforts of businesses engaged in online marketing activities. Marketing-related assets that are vulnerable to attack include networking and hardware resources, human resources, information resources, promotion resources, and brand equity and customer good will. Vulnerable areas that an organization should protect include its core network and computing infrastructure, its internal social infrastructure, domain name registrations related to its branding, and branding exploits on external social networks. Although hacks of networking and hardware resources are of concern, the focus of this article is on encouraging marketing managers and strategists to consider a wider variety of external and internal threats.

BACKGROUND

While the Internet has provided new opportunities for businesses and marketing, it has also created new vulnerabilities to attack. An organization's existing brand name can be taken hostage or destroyed via the online activities of third parties; opportunities to penetrate an online market with a new brand name can be diminished or eliminated by the actions of external third parties. Customer good will can be destroyed by the online activities of competitors or disgruntled customers. Technical, financial, and human resources can be diluted or consumed by the online activities of third parties. Confidential internal information can be compromised by employees who use e-mail and social networking Web sites for nonmission or personal uses.

This article attempts to outline such emerging strategic and tactical threats to online marketing efforts. While technical support people tend to focus on threats to hardware and networks, little guidance exists for marketing managers who should be interested in a wider variety of issues that can affect an organization's products, promotion, distribution, and costs (which affect pricing). "Scholarly" discussion on the subject is almost nonexistent, so this article attempts to compile, categorize, and discuss the sorts of issues that are starting to emerge in the popular press.

STRATEGIES AND TACTICS FOR ATTACK

The following are emerging strategies and tactics that have been enabled by online activities.

Fishing for Information

There are three basic ways to gain access to information within an organization: through exploits of the networking infrastructure, through exploits of the human social network, and through human mistakes. Networking exploits to obtain internal information could include system scans and probes, account and root compromises, packet sniffing, and malicious programming (cf. NIAC, 2004). A survey of 700 organizations by the Computer Security Institute and the U.S. Federal Bureau of Investigation found that unauthorized access amounted to $31.2 million in annual losses, and theft of proprietary information amounted to $30.9 million (Gordon, Loeg, Lucyshyn, & Richardson, 2005).

Attempts to fish for information do not have to be aimed directly at scanning and probing a networking system from the outside environment. A remote access Trojan is a hidden piece of malicious software that is attached to another seemingly innocent software application, such as a cute electronic greeting card or a more serious looking Excel spreadsheet (Vamosi, 2004). When these executable applications (greeting card, screen saver, spreadsheet, etc.) are opened, the Trojan is silently released to begin, say, covertly scanning files or logging keystrokes to be silently sent to another organization. These can be injected into an organization's computer if an employee opens an infected e-mail message or if an employee brings work that was infected on an online home computer. Once inside the organization, the Trojan can attach itself to internal applications that are exchanged, such as when employees exchange internal e-mail with executable attachments.

Microsoft employees, for example, reportedly received an infected e-mail which released a Trojan inside the Microsft organization; this in turn disguised itself as the Notepad text editor and sent information to a remote computer in Asia, with stolen passwords then used to gain access to the source code of Microsoft products (Thurrott, 2001). Attempts to

fish for information can be targeted to individual high-level executives, not just the organization as a whole. For example, an individual who opens an Excel spreadsheet attached to an e-mail message could unknowingly be installing a malicious program that now scans that person's files for information that is sent back to the criminal hacker (cf. Miller, 2003).

Information can be released through the mistakes or ignorance of employees. Members of the British Computer Society were sent a customer satisfaction survey that mistakenly contained the e-mail addresses of all recipients in the "to" field, allowing recipients to see the addresses of all other members (Oates, 2007). Information can also be obtained through simple employee ignorance. For example, employee names and e-mail addresses can be harvested through the use of chain e-mail (also known as a chain letter). Chain e-mail relies on social engineering, whereby one employee receives an e-mail message, for example, describing a cute lost puppy looking for a good home, and feels compelled to forward it to others within and outside of the organization. As each recipient forwards the seemingly harmless message to several others, a name and address list can be accumulated in each forward. This list can then be harvested when the chain letter eventually makes its way back out of the organization to the perpetrator; this allows a competitive intelligence researcher to find out who is employed by the organization, to find out who are partners or affiliates with the organization, or to find out who are the less-careful employees who are more likely to open e-mail of malicious intent. One of the more well-known incidents is the "Richard Douche Free CD" chain letter, in which the perpetrator offered a free CD to anyone who forwarded it to others with a CC to the perpetrator (Hoaxbusters, undated a).

Another way to harvest e-mail addresses is to send a message that contains a single unseen one pixel image tag. If the e-mail is received and opened, the hidden link accesses an external server and a record that this is a live e-mail address is made. The sender merely needs to guess at e-mail addresses and to use a subject line that is either motivating (social engineering) or appears to be official business in order to get a recipient to open it. The simple method of implementing this tactic is described by Voicenet Communications (undated). Organizations can use e-mail clients that block images, but this in turn creates problems for marketers (e.g., suppliers and other business partners) who send e-mail with legitimate product images (cf. Popov & McDonald, 2004).

Disruption and Consumption of Network and Hardware Resources

Disruption and consumption of networking and computing resources can temporarily inhibit an organization from conducting online commerce (cf. CERT, undated). Gordon et al. (2005) reported that annual business financial loss due to virus attacks were $42.8 million for 700 survey respondents, while denial of service (DOS) attacks were costing $7.3 million. Costs associated with attacks include not only the cost of defence, but also include the cost of lost business. After launching World Series online-only ticket sales, the Colorado Rockies baseball team received a malicious attack of 8.5 million hits. With their online resources swamped, they were forced to stop sales after only two hours and 500 tickets sold (Sports Illustrated, 2007).

In addition to shutting down an organization's Web site server, an organization's e-mail server could be swamped or crashed, temporarily disrupting communications with customers, suppliers, business partners, and employees. A former employee was convicted after crashing the server of a UK-based insurance company by swamping it with five million e-mail messages (BBC News, 2006). More difficult to trace, forged e-mails that contain hundreds of nonexistent recipient addresses in the "copy to" fields can cause some e-mail servers to then forward duplicate messages with huge attachments to those hundreds of e-mail addresses. Even if the recipient name is nonexistent, the server receiving those e-mails can be swamped to the point of crashing. Researchers tested the mail servers of all Fortune 500 companies and found that 30% could be used to make this kind of attack (Knight, 2004).

Disruption and Consumption of Human Resources

British mobile phone retailer Phones 4U started a ban on the use of e-mail on the belief that this would save each employee 3 hours per day. The company moved to communicating via phone and its internal intranet (Thomas, 2003). Deliberately flooding an organization with bogus e-mail messages can consume substantial amounts of recipient time as well as computing resources. Deliberately flooding an organization with electronic greeting cards, chain e-mail, and other such tactics that rely on social engineering can cause employees to waste time with activities that are not related to work. These could cause the organization to quit trusting e-mail or even to quit using e-mail communications altogether; if e-mail attacks are spoofed (faked) to appear to be from a particular business partner, an unscrupulous competitor might be able to cause the receiving organization to block incoming communications from that competitor.

Disruption of Promotion Strategies

These attacks are used to consume a competitor's promotion budget, to discourage a competitor from investing in online promotion activities, or to trick an organization into believing that its online marketing tactics are working better than actual performance. Traffic aggregation is the use of