The New World of eCrime: Targeted Brand Attacks and How to Combat Them

Abstract

Nothing is more valuable to a business than its reputation. That is why brand attacks, which leverage a company's valuable brand for nefarious purposes, must be battled on every possible front. Brand attacks are the new form of eCrime, and they're being launched with new and rapidly evolving exploits, including phishing and—most recently—malware. Fighting today's most dangerous targeted brand attacks requires a multi-pronged approach combining proactive prevention, fast detection, and forceful resolution.

Brand attacks strike at a company's reputation, eroding customer trust and confidence, and causing damage that can be difficult and expensive to repair. Therefore, security professionals must be concerned about brand attacks and reputational risk, and address them with a holistic approach to online brand protection, monitoring channels they may not have previously considered. Companies who ignore this risk do so at their peril. Once their brands are tarnished, many find it difficult to restore brand integrity and conduct business online effectively. With almost half a million instances of brand abuse being measured each week against a small number of leading brands, according to the MarkMonitor Brandjacking Index®, there is no time to avoid the issue.

In this paper, we discuss how brand attacks, and malware attacks in particular, have evolved and proliferated, becoming another one of the many varied and sophisticated types of eCrime that any security professional should be ready to confront. We outline the most effective strategies for those experts to pursue as they guard against reputational risk and diminished customer trust.

MarkMonitor®

Contents

Introduction and History

eCrime is evolving. Earlier generations of malware, for example, such as viruses, worms, and Trojan horses were sent anonymously and often appeared in users' email boxes as easily avoided junk mail. Early malware writers had more in common with vandals than with international crime syndicates. With attacks like these, the bad guys appeared as either nameless or fictitious to the recipient, so when damage was done, there was no one to blame but themself for clicking on a sketchy attachment.

In a September 2008 article in SC Magazine, Michael Barrett, CISO at PayPal, characterized the new type of cybercriminal who is "constantly deploying new, creative methods to attack and steal money from Internet users." Barrett wrote:

> …security technology failures go through a predictable sequence: initial discovery by security professionals, followed by wide scale abuse by teenage vandals and, finally, appropriation by criminal enterprises. Now that the teenage vandals have largely dropped away, we are left with professionally executed attacks motivated solely by money…in less than five years, eCrime has changed from an anomaly into an industry.

Phishing changed everything and brought with it the danger of targeted brand attacks. By soliciting confidential identity information under the guise of a well-crafted but counterfeit communication and/or website bearing the name, logo, style, and even a credible URL of a bank, financial institution, or other organization, ecriminals were suddenly far more effective. At the same time, through the use of a brand in the attack, users now had someone to blame. How could the bank let this happen? How could its brand be stolen and misused in this way? How could it ever be trusted again?

While generic email blasts remain popular, they're also being supplanted by targeted, brand-based solicitations. They're not just doing damage to users. They are doing damage to the brands which they are posing as in order to do their dirty work. As if they didn't already have enough of a technical advantage, ecriminals gain a further leg up by exploiting their victims' confidence in trusted brands; and now this form of social engineering ties together various attack vectors—or blended abuse—to increase their potency.

Today, there are all sorts of phishing techniques, and although MarkMonitor® research on global brands shows that 14 companies were the targets of 90 percent of all phishing—and that 12 of that 14 are banks, financial institutions, and eCommerce sites—it is not just financial institutions who find themselves falling victim. New organizations are being subjected to attacks—according to the research, 945 companies were targeted by phishing in 2008, and of these, 444

> "In less than five years, eCrime has changed from an anomaly into an industry."
> — Michael Barrett, CISO, PayPal

were new targets. Even more intimidating, phishing techniques are quickly being adapted to new technologies.

Similar to the evolution of phishing, malware is evolving: While it has been a threat for a long time, a new breed is emerging. In fact, malware has become "the new" brand attack culprit, arriving alongside targeted, brand-based solicitations, and ultimately costing corporations not just the price of vigilance and defense but also the indirect but huge cost of damage to brand integrity—which can be very difficult to repair once tarnished.

Various Types of Brand Attacks

Classic Phishing is an attempt to gather anything from usernames and passwords to personal information and credit card details by fabricating a legitimate-looking inquiry from a trusted brand that leads users to a phony website set up to collect the data.

Vishing, which is also called VoIP phishing, moves phishing to the phone. Instead of asking users to visit a website, this technique directs them to make a phone call to a toll-free number and follow commands to punch in their confidential information. In this case, the initial contact may come via email or via phone.

SMiShing, or SMS phishing, is the text message version of phishing. Users receive a legitimate-looking text message that tricks them into clicking on a link, which then installs a Trojan on the mobile device. Because SMiShing is the newest phishing technique and mobile phones have relatively few standard security tools, it is proving to be an increasingly widespread and annoying mode of attack.

Malware is the general term covering any type of software that is deployed to cause damage to devices or to collect confidential data from users.

419 Scams are the sometimes comical but still serious email solicitations that invite recipients to participate in huge payouts of frozen or misdirected bank accounts if only they'll provide enough information (and perhaps a fee) to get the paperwork going. Named after the section of the Nigerian criminal code that defines them, 419 scams have traditionally originated in Africa but may sometimes carry the names and brands of international banks and financial institutions to add the look of legitimacy.

Blended Abuse combines multiple techniques. For example, cybersquatting on domain names and bringing in ad revenue from misleading ads positioned on the pages (pay-per-click abuse) or using the pages to launch phishing and/or malware attacks. By combining the social engineering aspects of phishing with a browser-based exploit to download and install malware, fraudsters are able to leverage many different tools in their attacks.

The effectiveness of online brandjacking can't be denied. What better way to steal a user's online banking user name and password than to show up bearing the mark of a familiar and trusted brand? And because ecriminals can quickly and easily set up (or compromise) websites, they can not only attract users to them but also make them effortless to find via search engine optimization tricks that bring even more potential victims to their digital doorsteps. As reported in Ernst & Young's *2008 Global Information Security Survey*, high-profile incidents that people hear about in

media reports serve as a reminder of how vulnerable a company's brand can be[1]. The damage caused by online brand attacks is prevalent and has both direct and indirect costs. The same survey noted that "A positive brand can take years to build, but can be severely damaged by a single incident."

Warning: New Channels Are Being Used for Attacks

It is vital to realize that today, eCrime is changing from being a battle at the user's desktop, where antivirus and security software can be effective in repelling attacks, to being a battle in the cloud, where web-based brandjacking via phishing and malware is proliferating with a new level of sophistication and through new distribution channels. That is why companies need to expand their traditional view of the channels they monitor to an ever-wider scope.

Instead of emailing executable files to users who may be equipped with the software necessary to stop malware from infecting their machines, the new bait is either a legitimate-looking link in an email message that takes them to an equally legitimate-looking site, or, increasingly, an exploited but otherwise trusted site. In some cases, the new bait is a phony site that the user finds through a typical web search. eCriminals now have multiple channels that are both more effective and easier to scale to deploy their malware.

In fact, it has been estimated that approximately 9 percent of all suspicious websites serve malware. In a 2007 study, researchers analyzed several billion URLs, of which they conducted a deeper analysis of 4.5 million; they determined that 400,000 of the URLs launched drive-by downloads of malware. (Incidentally, another 700,000 URLs may also have been malicious.)[2]

The arsenal of weapons and channels available to scammers, and the methods by which they can be deployed have never been more plentiful. Here are examples of the exploits potential fraudsters deploy and the channels they use.

Brand Attack via the Email Channel

- **A Fraudulent Email Blast**: They send out millions of emails with a subject line indicating that the message is from an institution such as a bank. The body of the text includes the bank's logo and verbiage that has been lifted from the bank's real website. The message directs the user to a fraudulent website where account numbers, PINs, and other personal information are requested.

eCriminals now have multiple channels that are both more effective and easier to scale to deploy their malware.

[1] E&Y 2008 Global Information Security Survey: "Moving Beyond Compliance" http://www.ey.com/Global/assets.nsf/International/TSRS_Global_Information_Security_Survey_2008/$file/TSRS_Global_Information_Security_Survey_2008.pdf

[2] Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, and Nagendra Modadugu: "The Ghost in the Browser Analysis of Web-based Malware", May 2007.

- **An Email Blast with Malware**: They attach automatically-downloading software to an enticing message from a trusted brand. Once the attachment is opened and activated, the malware is stealthily installed.

- **A 419 Email Attack**: They convince users to send their personal information in response to a compelling offer from a popular brand.

- **An Email Blast with a Phone Solicitation**: Using vishing techniques, they entice users to call a phone number where their personal information will be requested.

Brand Attack via the Web Channel

- **A Phony Website**: They simply register domain names similar to those of a company (BrandnameUS.com, Brandname-USA.com, Brandnameeonline.com) and wait for users to arrive. This can also take the form of typosquatting, where the domain name is close enough to the legitimate domain name that a user might arrive there through a typing error (brndname.com). These phony websites can be used to steal user's credentials and/or plant malware on a user's computer.

- **An Infected Website**: They set up a malicious site to attract users to it simply by using search engine optimization (SEO) tricks such as meta-tagging of the brand's name (or any collection of popular search terms for that matter) and posting keyword-rich text to make the malicious site rise to the top of search engine results. By the time a user clicks on the search result and arrives at the site, the damage is already done. The user's computer may now be a zombie in a botnet.

- **Paid Search**: They buy sponsored search result positions which lead to their malicious websites.

- **Social Networking**: A scammer who hijacks a social network account can abuse the "friends" list to direct users to malicious sites. In another tactic, an attacker can pose as the "official" profile for a company or brand in social networks, making "friends" with whoever wants to connect. Counting on the fact that the convivial environment of social networks will catch users with their guards down, he can easily mine for personal information or attempt to send malware in the guise of a fun social networking "application."

- **Blogs**: They comment on popular posts including links to their malicious websites.

- **Drive-by Downloads**: They dump malware onto users' computers without requiring any proactive action, such as downloading an attachment, on the part of the users. It's a very different kind of threat from the traditional Trojan horses and worms we're familiar with. You simply visit such a page, and it installs adware, spyware, dialers, rogue anti-spyware, or any combination of them with no interaction by the user. What could be more damaging than having your brand name on a site that turns out to be an invisible attacker?

- **A Fake Download Site**: They build and maintain an enticing "free software site" at which the free software is actually malware.

Brand Attack via the Phone Channel

- They send automated phone calls with voice prompts asking users to submit their personal information (vishing).

- They send email requesting users to call a phone number where they are prompted to provide personal information.

- They send SMS messages to cell phones phishing for personal information (SMiShing).

Any Combination of the Above

It is possible that existing security measures may protect a brand from attack through a single vector, but once the game is elevated through the use of blended abuse then protection becomes much more difficult. By combining different attack strategies, scammers increase their chances of success. They might try a mix of cybersquatting, phony search advertising, and malware; or email, plus a phony website, plus an invitation to become a social networking "friend." The malware itself can include keylogging components or URL redirectors. The well-known Storm botnet actually combines a worm, a Trojan horse, a bot, and a spam agent all blended into one and then uses multiple attack vectors including DNS, Web, peer-to-peer, and more. The idea is to exploit the inability of conventional network protection to provide a unified defense; when one avenue is protected, the attack just moves to another. The possibilities, sad to say, are endless.

Anyone who has looked into Internet security in even the most casual way knows that due to its very nature, malware can be devastating. Unlike old school viruses that often visibly touted their own damage, malware is most often a silent threat, taking up residence and doing its dirty work of keylogging, redirecting, or "zombiefication" for as long as it possibly can. While savvy users can potentially spot a classic email phishing attempt, brandjacking effectively conceals the malware attack behind a veneer of trust, and therefore they have no idea that malware is now present on their systems. Even worse, recent malware has displayed the ability to evolve after it has been installed. There's no telling the extent of future damage.

What Are the Most Effective Defenses?

Given that likely fraudsters have so many tools and so many ways to attack, it is obvious that a holistic approach is required to protect a brand—an approach that doesn't depend solely on users and client-side technologies to take care of themselves. Blended brand abuse requires a blended response. Traditional antivirus and security software coupled with thorough user education is a start, but ultimately it is up to the owners of a brand to take responsibility for protecting users online in a proactive way. What can you do to fight back against potential revenue loss, reputational risk, and diminished customer trust and confidence that impact the bottom line of your online business transactions?

By combining different attack strategies, scammers increase their chances of success.

Prevent Brand Attacks

The philosophy of "a stitch in time saves nine" makes an excellent guideline for most proactive and preventive measures. It is vital to use constant automated monitoring to detect the registration of potentially malicious domain names before an attack can be launched. Companies should employ a domain management strategy, monitoring zone files for new registration of domain names, looking for similarities to their own legitimate URLs, and then monitoring the bogus sites once they come online. Some best practices:

- Establish an early warning system. It's vital to monitor new domain registrations for those likely to be used in a brand attack.

- Track previous offenders. Monitor those who have abused domains in the past because they are likely to abuse them again.

- Monitor web server logs. Keep an eye out for suspicious referral links.

- Monitor DNS records. Changes to entries may be indicative of pharming attacks.

- Follow domain management best practices. Register core trademarks and similar domain names in order to prevent cybersquatting and malicious domain registrations.

Taking these steps ensures that more attacks are prevented; reduces the costs associated with responding to attacks, customer service, and fraud losses; makes your organization a less attractive target; and preserves your investment in your online channel and your brand's reputation.

Detect Brand Attacks

Constant monitoring of online activity relating to the brand and products will also be effective in detecting attacks as soon as they occur, not days or weeks later when the damage has already been done. Because phishing and malware attacks have extended into the cloud, any solution of this type must also include cloud-based detection. Some best practices:

- Monitor and analyze a wide range of intelligence sources, including spam feeds from the top email providers and ISPs, honeypots, and desktop sensors, plus antivirus vendor partners and other industry feeds.

- Monitor blogs and blog comment fields, message boards, wikis, and product review sites. It's not enough to merely monitor the content of the site—monitoring meta tags and paid search links for mentions of your brand are equally important.

- Monitor customer abuse inboxes.

Taking these steps ensures mitigation of your losses if a brand attack does occur.

Respond to Brand Attacks

Companies should also work with a brand protection services provider that can help with monitoring forensics, shut down attacks effectively and efficiently, provide instant communication about any threat to the brand owner as well as communication to customers to warn them of any fraudulent use of the brand, and undertake credential recovery for anything which has been lost. Such a partner should also be in close contact with providers of desktop security software so they can update their signatures quickly. Some best practices:

- Achieve shutdowns by leveraging 24x7 security operations with a broad technical shutdown network. Make sure your partner has established relationships with ISPs, domain registries, and web hosting providers.

- Use dilution when appropriate. Render stolen credentials useless and prevent access to the harmful site.

- Protect consumers via a fraudcasting network. Join a network of ISPs, browsers, email providers, and security vendors. Once an alert goes out, you can block emails that contain confirmed fraudulent URLs, implement blocking in web browsers, or use web content filtering systems for protection.

The faster your response is, the less damage your brand will suffer.

Conclusion

eCrime attacks damage the reputations and brands of companies who are targeted by such malfeasance. Although primarily technical in nature, these attacks have evolved such that they are no longer simply a question of corporate information security to be handled by the IT department, but are a pressing concern for C-level executives and anyone involved with marketing or brand equity.

Fighting brand attacks requires an approach combining proactive prevention, fast detection, and forceful resolution. Companies must learn to monitor channels they have not considered before. Yes, it's vital to protect your infrastructure and your data, but the bottom line is that nothing is more important to protect than customers and your company's good name. An effective security campaign should leverage all resources at your disposal in order to holistically protect company, partner, and customer data, and above all to preserve the trust customers have in your brand. Any successful security strategy must extend beyond the data, the desktop, the network; successful security strategies must extend into the cloud. The ability to prevent, detect, and respond to online brand attacks may be the only way to preserve consumer confidence not only in your own brand, but in eCommerce itself.

About MarkMonitor

MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks. With end-to-end solutions that address the growing threats of online fraud, brand abuse and unauthorized channels, MarkMonitor enables a secure Internet for businesses and their customers. The company's exclusive access to data combined with its real-time prevention, detection and response capabilities provide wide-ranging protection to the ever-changing online risks faced by brands today.

More than half the Fortune 100 trust MarkMonitor to protect their brands online. **See what we can do for you.**

MarkMonitor, Inc.
U.S.   (800) 745.9229
Europe   +44 (0) 207.840.1300
www.markmonitor.com

Boise | San Francisco | Washington D.C. | New York | London | Toronto | Frankfurt

MarkMonitor®