

**Phishanomics: The Economics of Phishing, the
iframe attack and the Brand ROI of Security
Spending**

NT OBJECTives, Inc.
White Paper
Authored by Matthew Cohen

Phishanomics: The Economics of Phishing, the iframe attack and the Brand ROI of Security Spending

This paper will argue that the iframe attack (popularized by the Bank of India hack) has fundamentally altered the way that security professionals must defend less important websites. By allowing phishers to leverage a company's brand to steal from users, the iframe attack has made an entirely new class of formerly unimportant sites into material security concerns.

Iframe Attack

While a full analysis of the iframe attack is beyond the scope of this paper, a summary will be useful.

At the Bank of India, an iframe was embedded in the home page. A phisher would create the same iframe by embedding JavaScript code either in an E-Mail or a forum posting (a compelling video about of the attack, with a wonderfully dry English play by play, can be seen at <http://youtube.com/watch?v=aWV8d2rWf8E>). The site would launch an invisible iframe that would access a website that would launch a series of attacks against the user in the background. Each attack page launches websites that launch additional attacks against the user as well as additional websites (all in invisible iframes). Hackers can purchase toolkits to trivially create these websites (e.g. n404, Web Attacker, Mpack or Icepack).

The end result is that the website launches a series of attacks against the user and if the user it not fully patched, he will be completely compromised with a combination of keystroke loggers, root kits, etc..

Phishanomics 101

Although it may seem repulsive to think of it this way, phishers are driven by the same profit motive that drives legal businesses. Some analysis of this will prove useful in considering the impact of the iframe attack.

A phisher's profit from a traditional phishing campaign can be expressed as follows:

$$\Pi = EM \cdot P \cdot S \cdot E - EMc$$

Where

EM = number of E-Mails

P = Participation rate (the percentage of recipients who are members of the site)

S = Success rate for each recipient that has an account with the targeted site

E = Earnings per successful phishing attack

c = Cost per E-Mail

Two interesting points can be raised with respect to the iframe attack

- 1) The participation rate is effectively increased to close to 100% or more. Because the iframe attack is not used to directly gather information from the vulnerable

Phishanomics: The Economics of Phishing, the iframe attack and the Brand ROI of Security Spending

- site, but rather as a vector to monitor subsequent activity, or subvert the target for later use, the phisher can leverage any user so long as they are not completely patched. Potentially, a phisher could install a keystroke logger and steal a social security number from one site, a credit card from another and a bank account from a third.
- 2) The participation rate explains why certain sites are most common for phishers. The greater the membership, the higher P and the more profitable each phish will be. Unfortunately (for the phishers), the popular sites are used as targets so often that people should learn to ignore them. The sites become phished out (does anyone even read eBay E-Mails any more?). This decreases the overall level of profitable phishing. With the new iframe attack, this is not the case. Any site with a decent brand can be used to phish, even those with absolutely no customer data. Unfortunately, we are about to enter a new golden age of phishing.

Traditional ROI of Security Spending

While a complete analysis of security ROI is beyond the scope of this paper, a small review will be in order to make further points.

Traditional security ROI are fairly straightforward to model theoretically and extremely difficult to calculate in practice.

In theory, enterprises should be willing to spend up to the amount of expected damage from a hack times the percentage decrease in the likelihood of an attack from security spending. Basically, if my expected hacking cost for a site in a year is \$100,000 and I can spend \$50,000 to reduce that by 50%, I am breaking even on my security investment. If I spend less, I can have a positive ROI.

Cost of hacking is simply defined as

$$C = L \cdot S$$

Where

L is the likelihood of an attack and

S is the cost of a successful attack

The cost of successful hacks depends on a number of factors and the type of attack.

- 1) Defacements: there are two aspects of defacement attacks
 - a. Branding – replacing normal Acme company branding with “Our Company sucks – you’ve been owned” is certainly embarrassing, particularly if it receives press coverage.
 - b. Loss of service – if a site functionality is destroyed, there will certainly be revenue loss for the time it takes to fix the site.
- 2) Customer Data Theft: there are several aspects to these attacks as well
 - a. Branding – informing your customers that their credit card that you stored has been stolen by a hacker has an obvious negative impact on your brand.

NT OBJECTIVES, Inc.

- 3 -

www.ntobjectives.com

Phishanomics: The Economics of Phishing, the iframe attack and the Brand ROI of Security Spending

- b. Fines – VISA and MasterCard have been fining companies for data theft.
- c. Litigation – consumer have been suing companies for data loss.

Based on the above analysis, companies have traditionally allocated resources to security for websites by evaluating varying factors specific to the websites:

- 1) Revenue – sites that generate revenue have a greater cost of successful attack in the event of a loss of service. Technically, companies should focus on gross profit instead of revenues but this is a minor point.
- 2) Customer data – obviously, sites that have customer data are susceptible to customer data theft losses while those that do not are not.

The implication here is that sites that collect customer data and/or earn revenue are going to get significant investments in security while those that do not will get relatively little. If a minor web site is defaced, the potential impact on the Acme Company brand is limited.

The iframe attack – a Brave New World for Phishers, a Nightmare for Security Teams

Cross Site Scripting has always been the Rodney Dangerfield of web attacks – it simply got no respect. I think that this is largely due to the fact that highly sophisticated security personnel could not believe that anyone would be so stupid as to be a victim. Over time the community has started to see the serious threat and difficulty in solving these attack vectors. Now with the advent of iframe attack, Cross Site Scripting has become a huge concern.

Let us tell the story of Acme Antarctica, a small fictional site built for use by the Emperor Penguins of Antarctica. After its creation, it was discovered that penguins do not use the Internet and it remained unused.

Enter Phinneas Phisher, an enterprising young hacker. He realizes that the Acme Antarctica site is vulnerable to cross site scripting. He creates a clever phishing E-Mail offering free entry to a lottery with a \$1,000,000 grand prize with a link (with embedded cross site scripting attack) to Antarctica.acme.com. He blasts it out to 10 million E-Mail addresses and leverages the iframe attack to install keystroke loggers and root kits on thousands of computers.

Given the global recognition of and respect for the Acme brand, 10,000 people sign up. Phinneas collects 10,000 credit cards, 5,000 bank accounts, 2,000 social security numbers, 200 other assorted accounts and sells the lot of them for \$500,000. He also signs up 40,000 computers for his zombie network. Not a bad day at the office.

One of the banks investigates and discovers the Antarctica.acme.com URL, embedded with the iframe attack in the browser history. “I lost my life savings because of Acme” graces the front page of the paper next day. I am no lawyer but it would seem that an argument could be made that Acme is liable for these losses.

Phishanomics: The Economics of Phishing, the iframe attack and the Brand ROI of Security Spending

The point is, of course, that a site that previously justified no security investment because it collected no data and garnered no revenue, now has almost an equivalent potential to cause brand damage (and potentially litigation) as a large site.

As security teams plan their budgets, this new world must impact their calculations. Although I will not suggest that security teams ever report to marketing departments, the argument can be made that some of their budgets should come from marketing. This can be seen in a similar vein as spending money to prevent misuse of a company's logo.

Conclusion: The Death of Triage

The playful Antarctica.acme.com story is just one example of potential social engineering that hackers can use to get unsuspecting users to click on a link. As familiarity with the iframe attack grows in the hacker community, phishers will no doubt come up with new and more clever techniques.

The potential for exploit by iframe attack is something that needs to be carefully considered by security teams and marketing departments. Large numbers of websites that formerly received little or no attention or security investment must now be secured against cross site scripting with the same diligence that has been paid at larger sites.

About the Author

Matthew Cohen is the Chief Operating Officer of NT OBJECTives, Inc. Mr. Cohen brings extensive experience in the investment banking industry and executive management to NTO, where he manages the organization's operations and finances. Previous to NTO, Matthew was CFO of publicly traded TTR Technologies. Prior to TTR, Mr. Cohen was the founding CFO at APB Online, Inc., where he raised \$27 million in three private placements and built a financial infrastructure to support a 140 person company. Matthew has held positions at The Blackstone Group, Rothschild, Inc., and Kidder, Peabody & Co.; where he worked on restructurings, capital financings, and mergers and acquisitions. In one of these restructurings, New Dartmouth Bank, the investor group acquired 3 insolvent banks from the FDIC, invested \$40 million to re-capitalize them and after an operating restructuring, sold the bank for \$160 million two and a half years later. He holds a degree in economics from Princeton University.