Who Is Fighting Phishing
An Overview of the Phishing Lifecycle and the Entities Involved

White Paper
Who Is Fighting Phishing

An Overview of the Phishing Lifecycle and the Entities Involved

Contents

Introduction 3

The Phishing Lifecycle – Shutdown Should Begin Within Minutes of An Attack 3

Access to WHOIS Information is Critical 6

Summary 6

Appendix: The Brandjacking Index - Phishing Examples 7

Real Phishing Threat Increases 8

Phishers Cast a Wider Net 9

Phishers Target More Financials 10

Global Phish Hosting 11
Introduction

Online fraud scams continue to grow by 15% per quarter, targeting financial institutions of all sizes as well as e-commerce venues.\(^1\) Phishing scams are growing in sophistication and often occur in sudden rashes over a several month period, unexpectedly hitting both large and small businesses. While the direct cost to financial and e-commerce industries is significant—Gartner estimates that cumulative financial losses stemming from phishing attacks rose to more than $2.8 billion in 2006\(^2\)—the impact on consumer confidence in conducting financial transactions online is more worrisome. According to a 2006 poll conducted by the Wall Street Journal and Harris Interactive, 24% of consumers limit their online banking transactions due to these growing fraudulent schemes.\(^3\)

The most effective way to protect consumers from phishing attacks is to quickly detect the attack, use domain name WHOIS information to identify the owner of the site and the organization providing domain name service for the phishing site, and to work with the registrar or registry to shut down the phishing site—all within minutes of the attack’s launch. As preeminent phish site detection and shut-down specialists, MarkMonitor’s security analysts have extensive knowledge and understanding of the lifecycle of phish attacks and the best methodologies for mitigating those attacks. Our security analysts have developed many contacts at Internet Service Providers, registrars, and registries so that they can get phish sites shut down in the most efficient way possible.

In this white paper, we address the lifecycle of a phishing attack and how different entities—including third-party take down services and law enforcement—are involved in the process of disabling phishing sites. We also explain how critical it is for brand owners and third parties to have immediate access to data like domain WHOIS to prevent identity theft from phishing. Last, we provide an overview of current phishing trends and top threats.

The Phishing Lifecycle - Shutdown Should Begin Within Minutes of An Attack

According to the Anti-Phishing Working Group, phishing is a form of online identity theft that employs both social engineering and technical subterfuge to steal consumers’ personal identity data and financial account credentials. Social-engineering schemes use ‘spoofed’ emails to lead consumers to counterfeit web sites designed to trick recipients into divulging financial data such as account usernames and passwords.

When determining the best ways to respond to phishing, it is important to understand all of the actors in a phishing attack and the role played by each. You may be surprised to learn that law enforcement usually does not get involved in a phishing incident until weeks after the phish attack has been launched. Instead, brand owners or third-party entities like MarkMonitor are tasked with detecting phish sites and getting them shut down. The detection and shutdown process begins extremely quickly, usually within a few minutes of the attack being launched. Therefore, it is critical that the investigation and response to a phish attack, including the use of domain WHOIS information, be as efficient as possible.

---

1 Source: MarkMonitor AntiPhishing Security Operations
2 Statistic from Gartner, Inc. cited in “Phishing Attacks Leapfrog Despite Attempts to Stop Them,” by Avivah Litan, November 1, 2006
The most important aspect of the timeline of a phishing attack is the amount of activity that happens within the first few hours of the attack. After the phishing site has been set up and the phishing email has gone out, the brand owner or a third-party entity like MarkMonitor needs to identify and shutdown the phishing site as quickly as possible. Minutes are critical in this scenario since consumers tend to respond fairly quickly to phishing emails and the only way to guarantee the safety of a consumer’s information is to make sure the phish site is not accessible by taking it down.

Once the site is identified, an investigation is launched by either the brand owner or the third-party anti-phishing solution provider. This investigation uses details about the site including WHOIS information, the domain registrar, the ISP hosting the site, etc. to determine who to contact about getting the site shut down.

The phish site shutdown process is then initiated and involves the following steps:

**Step 1**
Investigate the site to determine:

- Domain owner
- ISP hosting the site
- Registrar that registered the domain name
- Which brand is being targeted

---

**Figure 1** above gives an overview of a phishing attack and indicates the timeframe of involvement for each of the entities associated with the attack. The various entities include: the phisher, the consumer, the brand owner or a third-party contracted by the brand owner to address phishing, the registrar/registry, and law enforcement.

The statistic from Gartner, Inc. cited in “Phishing Attacks Leapfrog Despite Attempts to Stop Them,” by Avivah Litan, November 1, 2006 is: **4**
Step 2
Use information in the domain WHOIS record to determine whether the domain owner is a legitimate party (whose web site has been hacked to host the phish site) or a phisher (who has registered the site specifically for hosting the phish site).

- In the case that the web site has been hacked, contact the legitimate owner to explain the problem and work with them to regain control of their systems and remove the phish site. If the legitimate owner is not responsive (within an hour or two), contact the ISP about the problem.
- In the case that the domain was registered to perpetrate phishing, contact the ISP to get the site disabled and contact the registrar to remove the domain from the DNS.
  - ISPs are the most responsive to these types of contacts
  - Unfortunately, if an ISP takes down a phish site, but the registrar does not disable the domain, the phisher can put the domain up on a new ISP and the battle starts over

Step 3
Gather forensic evidence about the site including:
- Archives of web pages, scripts, and images
- Copies of any malicious code hosted on the site
- Various technical information about the web server hosting the phish site
- Information about the network which hosts the phish site
- WHOIS information about the domain name used for the phish site

Step 4
After the site has been taken down, monitor the URL in case it is brought back up on another ISP or web server.

Again, it is critical to get the phish site shut down as quickly as possible to minimize the theft of consumer credentials. In most cases, MarkMonitor gets sites shut down within 90 minutes of detection. On rare occasions, registrars and ISPs are not cooperative and it takes longer to get phishing sites shut down. This lack of cooperation is usually either due to the registrar or ISP not being aware of the impact of phishing or the registrar or ISP not having appropriate policies and processes in place to rapidly disable phish sites and domain names.

It can take the phisher anywhere from 1 to 90 days to use the information that the phishing site stole. According to Gartner, the average loss for a phishing victim in 2006 was $1,244.\(^5\) Law enforcement usually gets involved with phishing investigations once many consumers have been identified and linked to a specific site. Since law enforcement must prioritize their work, it often takes weeks or months to identify a significant number of individuals impacted by a unique phishing site.

\(^5\) Statistic from Gartner, Inc. cited in “Phishing Attacks Leapfrog Despite Attempts to Stop Them,” by Avivah Litan, November 1, 2006
Access to WHOIS Information is Critical

In order to shut down a phishing site, WHOIS information and other forensic details are required by either the brand owner or third party anti-phishing solution provider within minutes to hours of the phish site going live. Law enforcement also needs this information, but they often don’t access the information until days or weeks following the attack.

There are several ways in which WHOIS information is used to identify the individuals hosting a phishing site. If the computer hosting the site has been hacked, information about the domain owner can be used to contact the domain owner and notify him or her that there is a security problem. This is often the most efficient way to mitigate phish sites that are hosted on hacked computers.

If the phisher registered a new domain to host the phish site, the phisher will often use fake credentials in the WHOIS record. Surprisingly, even these fake credentials are often informative. Since registrars are now more careful about verifying financial information, phishers often use stolen identities to register their phish sites and this will sometimes make it possible to find multiple domains registered by the same phisher or prove that a domain is going to be used for phishing due to its association with other phishing domains.

For example, let’s say that BankABC has identified a domain registered to phish their customers: bankabc-update.com, and that the email address of the registrant for bankabc-update.com is joe@phisher.com. When BankABC investigates, they find three other domains registered with the email address joe@phisher.com: bankabc-accountalert.com, bankabc-login.com, and bank123-update.com. Identifying these other domains serves two purposes. First, it is evidence for the ISPs and registrar that all of these domains are fraudulent and should be disabled. Second, BankABC has now found two other domains that would likely have been used for phishing in the future and have protected their customers from these domains before the email campaign was sent.

Summary

- Law enforcement does not typically request phishing site shutdowns
- WHOIS information plays a key role in investigating and shutting down phish sites and it is critical that brand owners and third party takedown services are able to access domain WHOIS information in real time
- The timeframe of phish site investigation and shut down is hours—more money is stolen and more consumers are impacted the longer phishing sites are available for access
- Anti-phishing service organizations like MarkMonitor depend upon the cooperation from registries, registrars, and ISPs to shutdown phishing sites

Timing is of the essence during a phishing attack and access to WHOIS is the critical tool that anti-phishing organizations and law enforcement need to identify the people responsible for an attack. The MarkMonitor Brandjacking Index gives an overview of current trends in phishing and provides examples of the different tactics phishers employ.
Appendix: The Brandjacking Index

Brands open enormous new prospects yet face new and evolving risks as they move online. Criminals, profiteers and opportunists take advantage of the global reach of the Internet and the anonymity it affords in order to hijack strong brands for their own profit. These ‘brandjackers’ have learned the rules of online marketing and are exploiting those rules to their advantage and at the expense of true brand owners. As a result, brand owners face threats to their reputations, customer relationships, and, ultimately, their revenues.

In order to shed light on the brandjacking phenomenon, MarkMonitor created the Brandjacking Index™, a quarterly report that measures the effect of online threats to brands.

The following is an overview of the phishing portion of the first quarterly Brandjacking Index published by MarkMonitor.

Summary Findings

- The phishing threat continues to increase with a 104% jump in annual attacks in Q1-07. Phishers actively avoid browser-based consumer protection technology evidenced by the more than 300,000 unique URLs used in phishing attacks.
- Phishers cast a wider net; in March ’07, 229 companies were targeted. Of that number, 158 companies were phished for the first time.
- Phishers target more Financial Services companies. Financial Services companies made up 41% of all attacks in Q1-07. This represents a jump from 29% in Q1-06. Evidence suggests phishers prey on customer confusion during mergers and security system upgrades.
Real Phishing Threat Increases

- 104% jump in annual attacks is due to adaptive phishing techniques (Q1’07)
- Phishers have adapted their techniques in response to consumer adoption of phish-blocking browsers
- Since Sept-05, there have been roughly 300,000 phish URLs discovered

Example:

- Browser security upgrades in IE and Firefox prevent users from visiting known phishing URLs
- Phishers are now using one time and unique URL’s to defeat simplistic browser blocking techniques

Impact:

- The recent sharp increase in phish attacks is directly related to the use of unique URLs, which may warrant a review of the industry definition of “phish attack”
- Phishers avoid simplistic browser-based consumer protection
- Change in phishing behavior validates the impact current blocking strategies have had on phishers
Phishers Cast a Wider Net

- 229 companies targeted in March ‘07
- In Q1-07, 158 organizations were phished for the first time
- Phishers reduce required resources to execute phish through technology

Example:

- The figure to the right shows a phish site that was part of a mail campaign requesting customers to update their billing information
- The phish URL contains the trademarked brand name, but is not an authentic domain owned by the brand owner

Impact:

- Phishers will continue to scale their operations via botnets and phish kits to expand their reach to new brands
- Botnets and phish kits help phishers sharpen their attack
- Phishers are using “Direct Marketing” methodologies to experiment against more brands and evaluate efficiency of phishing expeditions

Companies Targeted by Phishing

Impact:

- Phishers will continue to scale their operations via botnets and phish kits to expand their reach to new brands
- Botnets and phish kits help phishers sharpen their attack
- Phishers are using “Direct Marketing” methodologies to experiment against more brands and evaluate efficiency of phishing expeditions
Phishers Target More Financials

- 41% of all Phish attacks target Financials in Q1-07 vs. 29% in Q1-06
- Financials unseat auctions as leading targets
- High yields for online banking credentials

Impact:

- High “street” value of online banking credentials drive economic success of financial attacks
- Phishers continue to prey upon customer confusion during mergers and upgrades to more secure authentication systems
Global Phish Hosting

- US continues to lead overall in Q1-07
- Republic of Korea is a distant second overall, but growing
- High quarterly growth from Russia, Taiwan, Italy, Korea
- Russia moved into the top 5 in Q1-07

<table>
<thead>
<tr>
<th>Phishing Hosting by Country</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Top 5 phish hosting countries Q1-07</strong></td>
</tr>
<tr>
<td>United State, 35%</td>
</tr>
<tr>
<td>Korea, Republic of, 12%</td>
</tr>
<tr>
<td>Russian Federation, 7%</td>
</tr>
<tr>
<td>China, 4%</td>
</tr>
<tr>
<td>Taiwan, 4%</td>
</tr>
<tr>
<td><strong>Other Countries, 30%</strong></td>
</tr>
<tr>
<td><strong>Top 5 phish hosting countries growth Q1-07</strong></td>
</tr>
<tr>
<td>Russian Federation</td>
</tr>
<tr>
<td>Taiwan</td>
</tr>
<tr>
<td>Italy</td>
</tr>
<tr>
<td>Korea, Rep of</td>
</tr>
<tr>
<td>Bulgaria</td>
</tr>
</tbody>
</table>
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.

For more information, please visit www.markmonitor.com.