White Paper

Rock Phishing: The Threat and Recommended Countermeasures

Abstract

Phishing, an online scam in which people are tricked into divulging sensitive personal and account information, is a serious threat both to consumers and institutions doing business on the Web.

Statistics show a continued increase in phishing attacks. Not only that, but these scams are becoming more and more elaborate and therefore more difficult to defeat. In particular, one group known as the Rock Phish Gang has developed a methodology that makes their attacks virtually untraceable. Ironically, their success relies on many of the information technology best practices that legitimate companies use to ensure business continuity.

In this paper, we discuss the history of the Rock Phish Gang as well as their attack methodology and how it has evolved. We also review the actions that businesses can take to prevent and defeat an attack by the Rock Phish Gang including an analysis of how MarkMonitor is uniquely positioned to prevent and defend against rock phishing attacks.

MarkMonitor®

Contents

Introduction and History

Phishing: A Growing Concern

Phishing scams lure people to fraudulent web sites, mostly by authentic-looking emails, and ask them to divulge personal information such as their user names, passwords, account numbers, addresses, personal identification numbers (PINs), and so on. The phisher, or modern con artist, then uses this information to appropriate the victim's identity and withdraw money from his or her bank account, run fraudulent online auctions, apply for credit cards, obtain loans, launder money, and engage in a variety of illegal online activities. While these schemes are focused on individual consumers, the institutions that phishers are impersonating are also victims: their brand and hard-earned reputation is impugned. Banks are the most common targets of phishing attacks, but more and more, such attacks are being carried out against auction sites, payment sites, social networking sites, online brokerages, gambling web sites, and online merchants.

More and more, phishing attacks are being carried out against auction sites, payment sites, social networking sites, online brokerages, gambling web sites, and online merchants.

This form of fraud has become an unfortunate and thriving economic reality. Online phishing can be traced back as far as 1996[1] and has escalated swiftly: the number of unique phishing web sites detected by the Anti-Phishing Working Group rose to 55,643 in April 2007, a massive jump from March's 20,871[2]. Similarly, PhishTank (a collaborative clearinghouse for data and information about phishing) received 53,263 submissions of suspected phishing sites in May 2007, of which 43,789 were verified.[3] A more accurate measurement of phishers' activities is the number of corporate brands attacked. According to the MarkMonitor Brandjacking Index™, a quarterly report that measures the effect of online threats to brands, the number of brands phished each month reached an all-time high of 229 in March 2007.

Phishing is a serious threat not only to consumers and companies but also to the general perception of the Internet's suitability for business transactions. A recent poll of 2,120 American adults conducted by the *Wall Street Journal* and Harris Interactive confirmed online businesses' worst fears: 30 percent of those polled said they limit online transactions, and 24 percent limit online banking transactions.[4]

[1] Next Generation Security Software Ltd., (2004, April 22) "The Phishing Guide: Understanding and Preventing Phishing Attacks," [online] available http://www.ngssoftware.com/papers/NISR-WP-Phishing.pdf.

[2] Anti-Phishing Working Group. (2007, May 23). APWG Phishing Trends Activity Report for April 2007. [online], available http://www.antiphishing.org/reports/apwg_report_april_2007.pdf.

[3] PhishTank. (2007, June 1). Stats: May 2007. [online], available http://www.phishtank.com/stats/2007/05/.

[4] "Harris Poll: Taking Steps Against Identity Fraud," The Journal Report Online, May 15, 2006. Poll of 2,120 American adults.

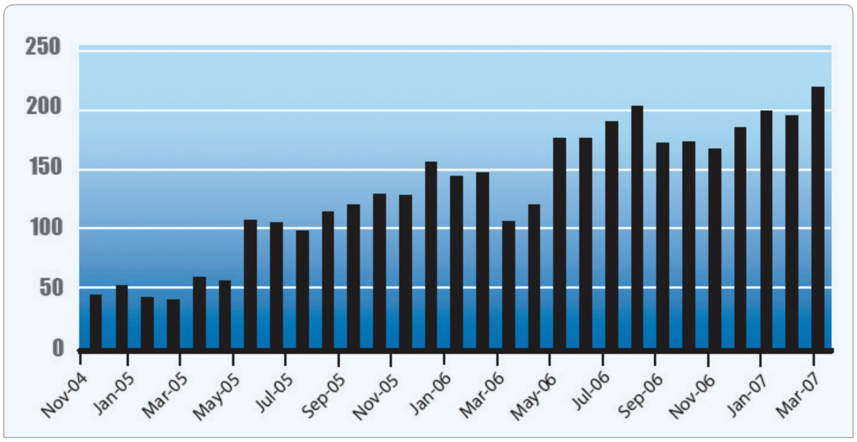


Figure 1. Companies targeted by phishers. Source: April 2007 MarkMonitor Brandjacking Index™

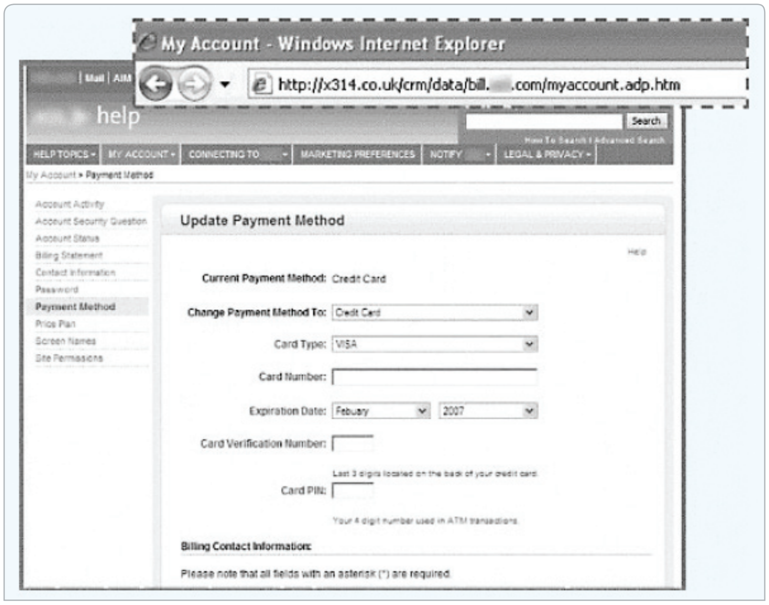
Of particular cause for alarm is the growing threat presented by the Rock Phish Gang, a formidable twist on the standard phishing scheme that has garnered tremendous amounts of money for its perpetrators. They are clearly not an average group of thieves, but rather a sophisticated international crime syndicate that has a talented IT staff. By exploiting high-availability practices to achieve system redundancy and horizontal scaling, and relying on a geographically dispersed system, the Rock Phish Gang has developed a methodology that makes them very difficult to defeat using standard anti-phishing measures. Ironically, their success relies on many of the information technology best practices that legitimate companies use to ensure business continuity.

The Typical Phish

In a typical phishing attack, the perpetrator sends out enormous amounts of spam (unsolicited commercial email) including links to fraudulent web sites that are under the control of the attackers. This means that the first step of a successful phishing attack is to evade recipients’ spam filters. Anyone with an email account has been inundated by spam in recent years, and phishers rely on the fact that as spam filters analyze billions of emails a day, dangerous ones can slip by. The phishing email must look legitimate enough that the victim believes it is a genuine communication from a legitimate business. In addition, the phishing email has to entice the victim to act on it (and hand over personal information), perhaps by reporting a fake transaction that needs to be cancelled or requesting account maintenance. Thus, phishing is not purely a technology problem: it is a combination of social engineering and technology prowess. Though phishers rely on technology to carry out their attacks, consumers must take the bait and then voluntarily provide sensitive information for attacks to succeed.

When a victim is persuaded to act by a phishing email, he connects to a fake web site by clicking on a link in the email. A web browser window opens and takes him either directly or through a series of redirects to the spoofed (fraudulent) web site. Once the victim arrives at the web site, he is presented with a web page that looks like a legitimate company page; usually these pages contain mock corporate logos, privacy policies, and links to report fraud. The victim then fills in his personal information, which is transmitted to the attackers or stored in a text file on the server. Typically, the attacker sells the information to other criminals who then engage in fraudulent transactions.

The fake web site is normally hosted on a compromised web server, one which has been exploited by the phishing attacker for this purpose. The attacker may also use rapidly provisioned free web space, such as that provided by a social networking site, which is usually untraceable; although that is becoming less common. The URL pointing to the fake web site usually contains some wording that impersonates the organization being attacked. For example, if the attacker has compromised the server at http://www.site.com, he may then send victims to http://www.site.com/bankname.com where "bankname" represents the institution being impersonated. This fools naive users, who quickly scan the URL for "bankname" and when they see it, decide that the link is legitimate.



http://x314.co.uk/crm/data/bill.[redacted].com/myaccount.adp.htm

Update Payment Method

Current Payment Method: Credit Card

Change Payment Method To: Credit Card

Card Type: VISA

Card Number:

Expiration Date: Febuary 2007

Card Verification Number:

Last 3 digits located on the back of your credit card.

Card PIN:

Your 4 digit number used in ATM transactions.

Billing Contact Information:

Please note that all fields with an asterisk (*) are required.

Figure 2. Example of a phisher site

There are a number of variations on this theme. Phishers may use the IP address of the server to further confuse victims. They may also go so far as to register fake domain names, which are typically a variation of the legitimate institution's domain name, such as securesite.com, and then create a sub-domain that typically includes a variation of the legitimate institution's domain name, such as: http://www.bankname.securesite.com.

The Rock Phish Gang

In late 2004, a notorious group of phishers arose, which was suspected to be working out of Eastern Europe. They were referred to as the Rock Phish Gang, because early versions of their attacks contained the word "rock" (and later just the letter "r") in the URL: for instance, http://www.bankname.securesite.com/rock/123/signin.html. Although they no longer use this naming convention, the Rock Phish Gang is still very active, possibly accounting for over $100 million in damages to date.[5] They have targeted national and regional banks throughout the USA, Europe, and Latin America. Recently, they have broadened their scope to include online brokerages, information services, treasury management companies, and even social networking sites.

As of June 2007, the Rock Phish Gang has employed several techniques that make them more difficult to defeat than other phishers. In an elaborate, multi-tiered scheme, they use the stolen credentials of their victims to register multiple domain names at multiple registrars. These domain names are usually short and meaningless, such as "342egt.info". The gang then hosts their own authoritative

[5] McMillan, R. (2006, December 12). 'Rock Phish' blamed for surge in phishing. InfoWorld, available http://www.infoworld.com/article/06/12/12/HNrockphish_1.html

DNS servers using wildcard "A" records to provide name-to-IP service for each of the fraudulently registered domain names. The IP addresses used (and there may be upwards of 100 at a time) point to multiple compromised PCs. These PCs are part of a botnet, which act as proxy connections to a handful of servers that host phish pages of up to 20 fake web sites at a time.

Challenges Presented by Rock Phishing

The difficulty of preventing this technique is that each layer of the phisher's infrastructure (DNS, proxy server, back-end server) contains redundancies and variations. The advantage to phishers of implementing a distributed architecture is that attacks can continue unfettered when any one element of the system is shut down: a traditional phishing site can be defeated by removing the hosting web site or domain, but Rock Phish sites share hosts and domains; if one is removed, the site automatically switches to another.

It is extremely difficult to track Rock Phish attacks all the way through to the back-end server. The rapid cycling through domain names and IP addresses makes them appear to be always on the move and leaves much of the international security community in a quandary; the Rock Phish Gang seems to be able to bring up countless combinations of multiple tiers in their attacks. This matrix of sites provides a robust system with many levels of failover. If a domain server is taken down, then name-to-IP services failover to another domain server. If a proxy server running on a compromised host is taken down, then the proxy services failover to another compromised host. Although they will typically only be using 10 to 20 such hosts at a time, the Rock Phish Gang is known to be in control of a multitude of compromised web servers, which are commissioned as needed.

To defeat site-blacklisting techniques such as those employed by PhishTank, Google, and many other anti-spam and anti-phishing services, the Rock Phish Gang uses large numbers of slightly varied URLs to draw victims to their fraudulent web site, such as these:

http://welcome23.bank.com.cbibsweb168st.342egt.info/confirm/submit.do/

http://welcome24.bank.com.cbibsweb59121j.342egt.info/confirm/submit.do/

http://welcome22.bank.com.cbibsweb146121k.342egt.info/confirm/submit.do/

http://welcome24.bank.com.cbibsweb574721a.342egt.info/confirm/submit.do/

MarkMonitor has seen as many as 5,000 unique URLs targeting a single organization within a one-month period.[6] This high number indicates that approximately 50 percent of all active phishing URLs during a given period can be attributed to the Rock Phish Gang. As long as a single URL can still be resolved to a single IP address the attack is still fully functioning and dangerously harvesting

[6] MarkMonitor Security Operations Center

information. Many combinations of URLs, domains, DNS servers, compromised hosts providing proxy services, and back-end servers can exist.

The Rock Phish Gang has evolved—now, the initial spam email they send to their victims is likely to contain random text followed by a GIF image containing the actual phishing message. Spam filters currently lack an effective means to analyze this GIF image and thus are ineffective. Many analysts estimate that between one third and one half of all phishing email can be traced back to the Rock Phish Gang.

Unfortunately, the successful sophisticated techniques employed by the Rock Phish Gang have motivated other phishers to emulate their methods. These copycats use similar tactics, such as registering bogus domains and using large numbers of variations of URLs. These attacks are much more difficult to defeat and represent an increased threat to consumers and institutions doing business on the Web.

It is difficult, if not impossible to distinguish between the Rock Phish Gang's attack on a bank and a copycat's attack on an online payment service, as shown by the URLs each used:

URLs Used on a Bank

http://session-05856.bankname.com.kitrt.cn/corporate/onlineservices/TreasuryMgmt/

http://session-101101156.bankname.com.dllet.bz/corporate/onlineservices/TreasuryMgmt/

http://session-101101186.bankname.com.dllet.bz/corporate/onlineservices/TreasuryMgmt/

URLs Used on a Online Payment Service

http://www.onlinepaymentservicename.com.156254.oagty79a.com/cmd-confirm/login.php

http://www.onlinepaymentservicename.com.177461.aaasjpa0.com/cmd-confirm/login.php

http://www.onlinepaymentservicename.com.306716.oagty79a.com/cmd-confirm/login.php

Countermeasures

How can legitimate institutions combat phishing—especially, the treacherous rock phishing? Just as successful phishers have turned to a distributed, multi-tiered system of attacks, so must institutions and consumers rely on a distributed, multi-tiered and layered defense in order to protect themselves. There is no silver bullet solution to defeat phishing; instead, a variety of technical and social techniques must be employed.

User Education

One key element of the war on phishing, and of information security in general, is consumer education. After all, if potential victims could be convinced to inspect email headers, to verify URLS, and not to reveal their personal and financial information to phishers, then the problem would just go away. However, education is not a sufficient answer in itself; con men have been running the same scams via Internet, telephone, and postal mail for ages. Yet many consumers are eager to learn how to protect themselves from online fraud. Savvy ones will learn if they are taught how to protect themselves. User education can be an inexpensive yet high-profile way to decrease fraud while convincing customers that their trust is important to a business.

Email Authentication

An important technical countermeasure to phishing is for businesses to implement an email authentication technology like SenderID or Domain Keys Identified Mail (DKIM) on their email systems. Since no authentication is supported by Simple Mail Transfer Protocol (SMTP), the dominant standard for email transmission, it is very easy for attackers to send spoofed email messages that appear to have originated from a legitimate domain. Designed to combat this, DKIM is an email authentication system that can verify the domain of an email sender and the message integrity. SenderID is an extension to SMTP that allows email servers to identify and reject forged addresses based on entries in DNS records.

In essence, using DKIM and SenderID discourages phishing because they make it difficult for a spammer's email server to masquerade as a legitimate email server, such as that of a bank or other financial institution. Since DKIM and SenderID are complementary technologies, it is ideal for businesses to implement both if possible.

Consumer Reporting

Phishing threatens every company and consumer who uses the Internet, and because of this, many users are eager to help by reporting suspected hoaxes. This is often the most successful method of identifying phishing sites. Potentially targeted companies should make it easy for consumers to report phishing and other methods of Internet scams: every company should have a link on its home page to a web form where anyone can easily report suspected fraud. In addition, every company should have a publicized email account that allows users to easily forward possible phish emails.

Anti-phishing Solution Deployment

Institutions must be proactive in order to defend their brand, reputation and customers from the threat of phishing. There are many components to an anti-phishing solution, including preventing the establishment of cousin or mock domains, detection and analysis of attacks, and technical and physical shutdown of phishing sites. Some solutions try to prevent phishing from occurring by authenticating and filtering email. Others filter web content through consumer products such as browser toolbars. Most anti-phishing solutions rely on an Internet data center that collects, analyzes, and responds to threats. Many rely on consumers to report phishing email and phishing web sites, and then target those email and web servers for shutdown. Anti-phishing solutions must offer this full range of services in order to defeat a phishing attack in a timely manner.

MarkMonitor is Uniquely Capable to Combat Rock Phishing

A multi-tiered security approach protects online consumers with several lines of defense that prevent them from reaching phishing sites. MarkMonitor is uniquely positioned to respond to Rock Phish attacks and can help companies develop appropriate solutions based on their risk profiles. MarkMonitor maintains a dedicated team focused on Rock Phish attacks, and leveraging the relationships built in eight years as an ICANN-accredited registrar, can also coordinate international activities on behalf of multi-targeted organizations to maximize the effectiveness of countermeasures. For example, a regional bank in the United States was attacked by the Rock Phish Gang in early 2007. The attack spammed consumers with phishing emails that contained 15,645 unique URLs, which made URL blacklisting ineffective. In seven weeks (approximately two domains every hour), MarkMonitor was able to shut down the 565 domains that comprised the URLs and effectively end the attack.

MarkMonitor's Proven Countermeasures Include:

1. **Rapid shut down of Rock Phish sites**
   Attacking phishers at a domain level prevents access to multiple fraudulent hosts using pooled IP addresses. As an ICANN-accredited registrar since 1999, MarkMonitor has a large, well entrenched worldwide network of domain registrars who know the company and have worked with it. By leveraging these relationships, and in combination with it's deep understanding of the industry, MarkMonitor is able to report fraudulent domains, have the domain registration revoked, and have corresponding entries removed from the DNS system, all within a timely manner in order that the phishing attack can be defeated before a large number of consumers are duped.

2. **The MarkMonitor Fraud Broadcasting Network™**
   MarkMonitor maintains a world-class Security Operations Center (SOC) that continuously broadcasts fraud intelligence to the major ISPs, web browsers, toolbars, and spam filtering tools to block users from accessing phishing sites. The SOC administers 24/7 threat research and analysis of more than 16 million unique suspicious URLS and emails daily, detecting and verifying 15,000 phish attacks around the world each month. Customer abuse inboxes are also closely monitored, and fraudulent sites are blacklisted and reported to ISPs so that phishing emails can be blocked.

   MarkMonitor also offers Trust Guard™, a small client-side application that has been licensed by major ISPs for use in their anti-phishing browser plug-ins. With Trust Guard installed on their computers, hundreds of thousands of users act as a phish site detection network, transparently reporting suspicious sites to MarkMonitor. Trust Guard combines a block list with real-time heuristics to protect consumers.

3. **Dilution™**

   By submitting false user credentials—fake names, account numbers, and other personal information—to phishing sites, MarkMonitor can make it very difficult for phishers to know what they've really stolen. Real credentials are lost in a sea of false ones, so the phisher must find the proverbial needle in a haystack to make his attack a success.

4. **Phish Tagging**

   MarkMonitor also offers phish tagging, which allows banks and other financial institutions to understand how phishers access financial data and money once they have a user's password and user name. Banks set up a fake customer account and pass the username and password to MarkMonitor. MarkMonitor then uses the username and password on a known phishing site. The bank can then observe what the phisher does using the fake credentials.

MarkMonitor is uniquely positioned to prevent and defend against phishing attacks and has a proven methodology that can address the threat presented by the Rock Phish gang.

Conclusion

Phishing is a serious threat to consumer confidence and weakens trust in e-commerce. Online fraud scams continue to grow by fifteen percent per quarter, targeting financial institutions of all sizes as well as other types of businesses. Even worse, these scams are becoming more and more elaborate and therefore more difficult to defeat. The Rock Phish Gang has developed an insidious multi-tiered methodology with several failover layers. They exploit the domain registration and DNS system, compromise web servers, and ultimately lead victims down a virtually untraceable path. The social and technical issues presented by the Rock Phish gang must be addressed so that financial institutions and e-commerce companies can combat these scams and avoid erosion of customer trust.

MarkMonitor is uniquely positioned to prevent and defend against phishing attacks and has developed a proven social and technical methodology, beginning with domain protection and running all the way through to web-site shutdown, that can address the more complex and sophisticated threat presented by the Rock Phish gang.

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