Contents

Executive Summary ................................................................. 3
Summary Financial Brand Findings ......................................... 3
General Phishing Trends.......................................................... 7
Social Media Phish Targets...................................................... 11
Conclusions ........................................................................ 13
Methodology & Background..................................................... 13
Glossary .............................................................................. 14
Executive Summary

In this edition of the Brandjacking Index®, we look at brand abuse trends in the financial vertical, focusing on four major financial services brands and four terms associated with the financial crisis – foreclosure, mortgage, refinance and unemployed. As the economy has worsened over the past months, we found that con artists have exploited consumers’ financial fears and uncertainties, and have rushed in to hijack well-known brands for their own profit.

There has been a profound increase – 36 percent in one quarter – in the level of phishing attacks as well as in cybersquatting. We identified more than 7,300 questionable domains that were registered using the four financial brand names. Fraudsters registered domains that combined the financial brands that we studied with our four focus terms at the rate of more than one domain per day between September 2008 and the end of our study period in April 2009. Scams continue to be complex and sophisticated to lure in unsuspecting victims; in fact, cybersquatted domains registered since September 2008 were 50 percent more likely to use the focus terms than domains registered earlier.

MarkMonitor® created the Brandjacking Index to measure how pervasive brand-based attacks are and to identify the potential threats to the world’s strongest brands. As in our previous reports, this edition of the Brandjacking Index tracked millions of emails and billions of web pages, including pages featuring online advertising, eCommerce, auctions and social networking.

Summary Financial Brand Findings

As our economy has worsened, brand abusers have sharpened their focus and created schemes to lure consumers into their trap for mortgage refinancing and phony get-rich-quick investments. Sadly, the only ones who are getting richer are the fraudsters. They are using a variety of simple yet creative techniques to misrepresent themselves.
Here are two examples of websites: the first shows you a phony mortgage refinancing site that exploits paid search listings to bring in traffic and a second site for a spam scam based on another bank brand.
Then there is this page that has so much brand abuse going on, it could be one of those find-the-hidden-picture Sunday supplement puzzles. The fraudster who created this page exploits trusted TV and newspaper media brands and has the page designed to look like an online newspaper, all with the goal of obtaining personal identity information. To add insult to injury, the page uses encryption technology to give it a greater air of legitimacy! While many of the suspicious domains that we discovered tried to extract personal information, very few went so far as this site in offering encryption; 52 percent of the domains that we identified did not encrypt any data.

Site exploiting multiple brands, including media and financial brands, takes advantage of “bailouts”

Finally, there are new efforts that make use of social media to lure victims. Here is “Jessica’s Money Blog” which on the surface looks like thousands of other legitimate blogs that participate in conversations about managing finances or running a small business. But “Jessica” is selling a “home business kit” that promises steep rewards in exchange for a small amount of effort and some personal information, including a credit card number.
Of the almost 7,400 suspicious domains that we identified, 16 percent were registered since September 2008 and 17 percent of the total used the focus terms – foreclosure, mortgage, refinance and unemployed – in the site content. When we examined the more-recently registered domains, we found evidence of opportunistic abuse. Domains registered since September 2008 were 50 percent more likely to use the focus group terms. Fraudsters registered domains that combined the financial brands that we studied with our focus terms at the rate of more than one domain per day between September 2008, and the end of our study period in April 2009.

In general, many of the suspicious domains are newly created, as you can see from our analysis of the domain registration dates in the table below:

<table>
<thead>
<tr>
<th>2007 or before</th>
<th>1H 2008</th>
<th>2H 2008</th>
<th>2009 (Jan-Apr)</th>
</tr>
</thead>
<tbody>
<tr>
<td>58%</td>
<td>13%</td>
<td>18%</td>
<td>11%</td>
</tr>
</tbody>
</table>

In terms of geography, 49 percent of the abuse domains were hosted in the United States, while six percent were hosted in the United Kingdom, four percent in Germany, and Australia and Canada tied at three percent each.

These are just a few of the sites that we have discovered that may be exploiting the financial crisis. A summary of our results is shown below for each of the four banking brands that we studied:

<table>
<thead>
<tr>
<th>Brand</th>
<th>Cybersquatting</th>
<th>eCommerce</th>
<th>False Association</th>
<th>PPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Bank Brand</td>
<td>1,149</td>
<td>130</td>
<td>334</td>
<td>131</td>
</tr>
<tr>
<td>US Bank Brand</td>
<td>998</td>
<td>115</td>
<td>280</td>
<td>303</td>
</tr>
<tr>
<td>UK Bank Brand</td>
<td>2,947</td>
<td>384</td>
<td>105</td>
<td>274</td>
</tr>
<tr>
<td>Intl. Bank Brand</td>
<td>2,276</td>
<td>332</td>
<td>838</td>
<td>266</td>
</tr>
<tr>
<td>Total</td>
<td>7,370</td>
<td>961</td>
<td>1,557</td>
<td>974</td>
</tr>
</tbody>
</table>

Number of abuses observed by brand and type of abuse

Of the almost 7,400 suspicious domains that we identified, 16 percent were registered since September 2008 and 17 percent of the total used the focus terms – foreclosure, mortgage, refinance and unemployed – in the site content. When we examined the more-recently registered domains, we found evidence of opportunistic abuse. Domains registered since September 2008 were 50 percent more likely to use the focus group terms. Fraudsters registered domains that combined the financial brands that we studied with our focus terms at the rate of more than one domain per day between September 2008, and the end of our study period in April 2009.

In general, many of the suspicious domains are newly created, as you can see from our analysis of the domain registration dates in the table below:

<table>
<thead>
<tr>
<th>2007 or before</th>
<th>1H 2008</th>
<th>2H 2008</th>
<th>2009 (Jan-Apr)</th>
</tr>
</thead>
<tbody>
<tr>
<td>58%</td>
<td>13%</td>
<td>18%</td>
<td>11%</td>
</tr>
</tbody>
</table>

In terms of geography, 49 percent of the abuse domains were hosted in the United States, while six percent were hosted in the United Kingdom, four percent in Germany, and Australia and Canada tied at three percent each.
Phishing attacks against the financial brands that we studied saw a big jump, with 10,000 attacks in Q1 2009, which was a 36 percent increase compared to Q1 2008.

### General Phishing Trends

Interestingly, when we observe phishing trends overall, we found that phish attacks against the payment services category grew more quickly than the financial services category in Q1 2009, with a 40 percent growth from the previous quarter and 285 percent annual growth.
Phishers continue to target different industries, shifting their focus from quarter to quarter as the chart below demonstrates. They sharpen their focus using standard direct marketing methods – identifying the most profitable segments and then continuously harvesting new targets within those segments.
A total of 502 organizations were phished in Q1 2009, which is a 14 percent increase compared to the last quarter of 2008, and a 24 percent annual increase – a large jump from previous observations. We also saw 93 organizations being new targets in the quarter; the vast majority of them were financial services-related businesses. This could signal that phishers will be redoubling their efforts against this segment going forward.

We also observed how phishers are adjusting their techniques targeting the retail segment. On the left is an older example of a phished retail site, using the oft-used ploy of masquerading as a trusted site, with familiar logos and credentials. On the right is a more recent example of a phish against the same brand. In this case, a phony user survey purportedly offered by a trusted retailer promises a $90 credit for its completion, once your credit card number has been given.

Evolving marketing techniques for phishers
And as legitimate sites beef up their defenses, the phishers are following right behind by using similar techniques to make their efforts seem more plausible. The first example below is a site that uses the ‘capcha’ method of typing a series of numbers to thwart subscription bots, and the second example is a Brazilian site that puts up a warning like a real credit card site. While both of these sites are aimed at the payment services vertical category, neither is legitimate.

Payment services fraudulent sites
And while the US continues to widen its lead in the hosting of phishing sites, with a ten percent increase from last quarter, Canadian hosted sites have moved up to be the second most popular host country.

Social Media Phish Targets

We continue to see that cybercriminals are targeting new communication platforms like micro-blogging, virtual worlds and social networks. Phishers are creating phishing sites to collect passwords, conduct identity theft schemes and carry out online advertising scams. Phish attacks targeting social networks have grown 241 percent from Q1 2008 to Q1 2009 and have grown 1,500-fold since we first started tracking the category in 2007.
Phishers have also expanded their reach to web infrastructure sites such as domain registrars and hosting services. Economic reasons for exploiting these sites include redirecting traffic, holding a domain portfolio ransom or hosting further phish scams or pirated content.

Registrars

Hosting

Phishing attacks target web infrastructure
Conclusions

Brand abuse is increasing, but more important than the sheer volume is the increased sophistication and the opportunistic nature of brandjackers, who are quick to take advantage of current events and popular concerns. Brandjackers continue to exploit the confusion over the financial markets that began in the last quarter of 2008 to prey upon vulnerable consumers. Wielding a wide variety of techniques from more established abuses like spam, cybersquatting and phishing, brandjackers are also taking advantage of newer avenues like blogs and social media sites to find their victims.

Methodology and Background

The Brandjacking Index is produced by MarkMonitor and explores numerical trends and statistics about online brand abuse. It contains anecdotal information about the business and technical methods used by brandjackers, along with analysis and discussion of the business and social implications of brand abuse.

The cornerstone of the Brandjacking Index is the volume of public data analyzed by MarkMonitor using the company’s proprietary algorithms. MarkMonitor searches approximately 134 million public domain records, billions of web pages and spam emails and up to 16 million unique suspect phishing emails on a daily basis in order to identify brand abuse. These records come from various public domain data sources, along with Internet feeds from leading international Internet Service Providers (ISPs), email providers and other alliance partners. None of this data contains proprietary customer information.
Glossary

**Brandjacking** – To hijack a brand to deceive or divert attention; often used in abusive or fraudulent activities devised for gain at the expense of the goodwill, brand equity and customer trust of actual brand owners.

**Cybersquatting** – The practice of abusing trademarks within the domain name system.

**Domain Kiting** – The process whereby domains are registered and dropped within the five-day ICANN grace period, and then registered again for another five days. Kiting a domain lets the registrant gain the benefit of ownership without ever paying for the domain.

**eCommerce Content** – Websites containing a specified brand that appears in visible text, hidden text, meta tags or title in conjunction with other site content that indicates online sales are being transacted on the site.

**False Association** – The practice of using a specified brand or trademark in web content to imply a relationship with a company or brand where none exists.

**Offensive Content** – Websites containing a specified brand that appears in visible text, hidden text, meta tags or title in conjunction with pornographic, online gaming or hate content.

**PPC** *(Pay-Per-Click)* – Paid placement advertising appearing on web pages. Operators of websites hosting PPC advertising derive revenue from ads that are clicked, hence the name PPC.

**Phishing** – Criminal use of email to divert traffic to websites in order to fraudulently acquire usernames, passwords, credit card details and other personal information. The email and websites used in these operations employ “social engineering” techniques to trick users into believing they are interacting with a business or organization that they trust.

**Rock Phishing** – A method of phishing first implemented by the ‘rock’ phish gang that utilizes multiple layers of redundant infrastructure to increase the difficulty of shutting down the attack. Other phishers are now using these tactics as well.

**SEO Manipulation** – The use of brands, slogans or trademarks located in visible text, hidden text, meta tags and title in order to manipulate search engine rankings so that the brandjacker’s site can gain a more favorable search engine placement.

**Traffic Diversion** – Hijacking a brand to drive traffic to a competitive or illicit site in order to generate revenue at the expense of the rightful brand owner.
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 patented 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.

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