

## E-scammers trashing reputations

Through tactics like cyber-squatting and phishing, online criminals are hurting the reputations of legitimate businesses as they ply their trade

PHISHERS, CYBER-SQUATTERS, AND OTHER online fraudsters continued their assault on well-known corporate brands over the last 12 months, increasing the burden on the companies being targeted and further frustrating consumers.

According to MarkMonitor's annual "brand-jacking" report — which attempts to gauge the level of damage being extracted on corporate reputations by online scammers via schemes like phishing — problems only intensified last year for businesses in defending their public images online.

Among the biggest shifts from the findings of the company's previous report was a dramatic spike in 2007 in the prevalence of cyber-squatting, or the practice of occupying a URL that either contains or is constructed to appear similar to the name of an established corporate brand for the sake of deceiving users or carrying out some form of fraud. MarkMonitor, which bases its results on investigations of public records, including URL registration applications filed with Internet Corporation for Assigned Names and Numbers (ICANN), estimates that cyber-squatting rose by 33 percent in 2007 compared to the previous year.

The research firm said that it observed some 382,248 instances of cyber-squatting during the fourth quarter of 2007 alone with a particularly noticeable increase in the use of brand names and trademarks utilized to drive traffic to illegitimate, unauthorized, or offensive Web sites through popular search engines.

MarkMonitor experts said that the renewed growth in cyber-squatting, which had become less prevalent than brand attacks carried out using phishing schemes over the last several years, is likely tied to the large number of people trying to make money through online advertising scams.

While people could make money through buying generic URL names and building sites that pointed to advertisements using legitimate means in the past, the increase in operating expenses driven by the price of attractive domains names is pushing wider brand abuse, experts said.

"With well-known terms going for six to seven

figures in legitimate domain auctions, people trying to make money by driving traffic to online advertising find themselves struggling because all the most recognized dictionary words and phrases are already gone," said Frederick Felman, chief marketing officer at MarkMonitor. "As a result, some of these people who are trying to make money are resorting back to exploiting brand names to do that."

Another increasingly common tactic emerging among cyber-squatters is the use of combinations of popular brands in URL names, the report said, such as a site recently observed by MarkMonitor at "GucciFendi.com" which adds a pair of well-known fashion brands together for the sake of drawing eyeballs. The site was not authorized by either Gucci or Fendi but could show up in Web searches for either company.

### Phishing still a favorite tactic

Phishing schemes also remain extremely popular in 2007. MarkMonitor said that it tracked attacks aimed at 412 different organizations during the fourth quarter of last year, an increase of 38 percent from the previous quarter and a 37 percent gain over 2006.

The report also finds that 122 of the organizations phished during the fourth quarter were being victimized for the first time. The company said that phishing scams aimed at retailers increased a staggering 533 percent over the course of 2007 with campaigns targeting retail and auction brands accounting for 50 percent of the attacks during the fourth quarter.

Interestingly, after years of hammering on financial services companies' brands, phishers appear to have moved their focus away from the market, at least slightly. The research company said that phishing attacks against financial services providers decreased by 20 percent during Q4 2007 and fell by 10 percent for the entire year.

In addition to changing the companies that they're targeting, phishers have also continued to refine both their technological and social engineering techniques, according to the report. The use of schemes aimed at people posting to social networking sites is one manifestation of the new methods for roping users in, MarkMonitor said,

with attackers using the information posted on such forums to play on the level of familiarity fostered among users of the sites and launch more targeted phishing campaigns.

On the technical end, phishers have begun launching a greater number of attacks that integrate VoIP components in an effort to trick people into calling phone numbers to share their personal data as well as a larger variety of scams delivered via text message to handhelds.

"We're seeing a lot of interesting marketing techniques from the phishers, which shows how business savvy many of them have become; on the back end it's clear that people are moving cash around by recruiting mules and the like, it's all very professional," Felman said. "And there is a lot of really whacky stuff going on with the techniques we see with hard core blended abuse that combines voice capabilities, phishing, and malware."

Despite all the dour news, MarkMonitor said there are some signs of light around brand protection online.

Aggressive legal action carried out by some of the companies whose brands have been repeatedly tarnished by the activity as well as increasing scrutiny of new domain registrations by ICANN have helped improve some aspects of the issue, said Felman.

Prosecution on the part of financial services companies may have also helped contribute to the lower overall volume of attacks in that sector, the expert maintains.

"To fight this activity, companies need to marshal their resources, their legal and marketing teams, and operational research, to hammer at brand-jackers until they move on to more fertile fields and undefended brands," Felman said. "People are finally admitting this is a big problem that hits at their bottom line; it's very interesting to see the difference between firms who approach the problem passively and those who are more aggressive; you can do a lot to help yourself."

— Matt Hines

MarkMonitor®