Anti-Phishing Working Group

The Relationship of Phishing and Domain Tasting

A report and analysis by the APWG DNS Policy Working Group

Contributors:

Greg Aaron, Afilias
Dmitri Alperovitch, Secure Computing
Laura Mather, MarkMonitor

September 14, 2007

Preamble and Summary

The Anti-Phishing Working Group (APWG) is the global pan-industrial and law enforcement association focused on eliminating fraud and identity theft that result from phishing, pharming and e-mail spoofing of all types. The APWG's Domain Name System Policy Working Group (DNSPWG) focuses on policy-related issues associated with the Domain Name System (DNS) to examine abuses of the DNS that may require remediation. DNSPWG analysts examined the consequences of 'domain tasting' – the practice of opportunistically registering domain names to determine their traffic-generating potential and dropping those with less-than-promising prospects – on the larger Internet community and asked whether or not phishers use "tasted" domain names to perpetrate their crimes. APWG analysts found domain name tasting to be antithetical to the phishers' enterprise model and therefore no relationship exists at this time between phishing and domain name tasting, though the large increase in domain name registrations requires a commensurate increase in resources by the anti-phishing entities to monitor for new phishing attacks.

Background

All ICANN accredited generic top-level domains (gTLDs: .com, .net, .org, .info, .biz) and some country-code top-level domains (ccTLDs) have a five-day Add Grace Period. A registrar may delete a new registration within this period to receive a refund. Such cancelled names are returned to the pool of available names in the registry. The Add Grace Period was invented to give registrars a way to deal with registration mistakes, registrant fraud, and credit card charge-backs.

Domain tasting is a practice in which a registrant takes advantage of the Add Grace Period to test whether a domain name can be profitably monetized. The most common monetization practice is to place pay-per-click advertising on the newly-registered domain name and measure how much revenue and traffic the domain name generates in the first days of the registration. If the taster determines that the domain name will not make a profit over the course of a year, the taster cancels the domain name before the end of the Add Grace Period and receives a refund for the registration. Domain names that are deemed profitable are retained in the taster's portfolio. These are often domain names that were previously used by other parties and have since been cancelled. Such domain names enjoy residual traffic from search engines and hyperlinks across the Web. Other examples of profitable domain names include misspellings and misstypes of other popular Web sites or product names; these garner type-in traffic as Web users make spelling and typing errors in their browsers.

It is generally perceived that the great majority of domain name tasting is performed by a small number of registrars who exist specifically to amass and maintain tasting portfolios. Typically, these registrars do not offer registration services to the public. In an observed example, one tasting registrar created 1.8 million domain names in one gTLD over a three-month period, and cancelled all but 10,000 of those names within the Add Grace Period.

This study considers the possible relationship between domain name tasting and phishing. Currently, domain name tasting is an allowable activity (possible cases of intellectual property infringement notwithstanding). Phishing is illegal in most jurisdictions. It would be surprising for an ICANN-accredited registrar to knowingly engage in phishing, since such criminal activity would endanger its accreditation and reputation.

This report gives details of the findings of several studies that evaluated how much domain name tasting is performed by phishers. First, the results of the analyses are detailed including a description of the methodology used in each analysis. Second, data that are still needed is described. Finally, APWG's analysts make a statement about the way domain name tasting affects the fight against phishing, even if the phishers are not using domain name tasting practices themselves.

Findings

Independently, members of the APWG Domain Name System Policy Working Group conducted two different studies to determine whether or not domain name tasting occurs in instances of phishing. The studies approached the problem employing two different methodologies and correlative data sets, but arrived at the same conclusions.

Phishing Domains used by Tasters

The first study analyzed a list of 793 unique domain names that had been used for phishing during the first half of 2007. (These were second-level domains, not the URLs on those domains used for phishing pages.) The study determined whether these phishing domain names had been cancelled during the Add Grace Period, and which registrars had registered them.

Here are the findings from that study:

1. Some 78% of domain names reviewed in this study that had been used for phishing had never been cancelled in the Add Grace Period, and were present in the registry at the time of the study. This is contrary to the behavior typical of tasters, who keep a tiny percentage of the names they taste and return the vast majority for refund of registration fees.
2. Six of the phishing domain names used in this study was ever registered at any point by the suspected tasting registrars. Those domain names that were registered by suspected tasting registrars are likely unrelated to the phishing activity on those domain names. It appears that a taster often registered and rejected a name before a phisher subsequently registered it, or a taster registered a name after a phisher had used it.
3. Less than 20% of the phishing domain names reviewed in this study was cancelled within the five-day Add Grace Period. Note that:
    A. This takes into account only the last create-and-cancel cycle for each domain name. Some of these domains names were deleted more than once. In some cases a domain name may have been used for phishing and deleted, and then tasted and deleted within the grace period.
    B. We do not know who ordered the cancellations of these domain names, or the rationale for their cancellation. Some or all may have been tasted and then deleted by domain name tasters. Some or all may have been deleted by the phishers who were finished with them. Some or all may have been

deleted by the registrars because they received reports that these domain names were being used for phishing. Some or all may have been deleted by the registrars because the domain names were purchased using fraudulent accounts or the registrars encountered credit card charge-backs.

In conclusion, the data in this study revealed no correlation between domain names used in phishing attacks and domain names registered for tasting that were returned during the Add Grace Period.

Tasted Domains used for Phishing

In the second study, APWG analysts took the opposite approach and examined all tasted domain names for a large gTLD over a one week period and identified the domain names that were used in phishing attacks from this sample. We classified approximately three million domain names as very likely being subject to a tasting routine during this period. We then compared the domain names classified as tasted against the list of domain names that were known to be used for phishing campaigns. Of the approximately three million domain names that were tasted in this time frame, less than 10 domain names were identified as being used for phishing. Upon further examination, it appears that the cancellation of these 10 domain names was not initiated by the registrants of the domain names themselves, as it would be in the case of tasting. Instead, it appears that the registrar removed them from its system, likely because the registrar was notified that the domain names were being used for fraudulent purposes.

Again, this study showed that there are very few cases of possible domain name tasting performed by phishers and the cases that do exist have possible explanations that are not related to tasting.

Other Implications of Tasting

Despite the above conclusions that phishers do not take advantage of domain name tasting with the domain names they use to host their phishing sites, domain name tasting does affect the anti-phishing community in other ways. Several companies monitor new domain name registrations to identify domain names that may be used for phishing. These companies look for keywords in the domain names themselves that are similar to the brands that are targeted by phishers, additional indicators in WHOIS records, and other identifiers that may signify that the domain name might be used for fraudulent purposes. Years ago, when domain name tasting was much less prevalent than it is today, there were approximately 50,000 new domain names registered a day. With the increase in domain name tasting over the last year or so, there are often between two and three million new domain name registrations per day.

Many organizations monitor domain names to protect their brands as well as any trade and service marks they hold. Several third party providers monitor domain names to identify domain names that are likely candidates for use in phishing attacks. At two million domain name registrations per day, tasting has expanded the pool of potential infringers by a factor of 40. This dramatically increases the cost of monitoring.

Therefore, while the evidence suggests that phishers do not use domain name tasting in their exploits, the anti-phishing community is bearing more burdens in the pursuit of phishers because of the increase in cost of early identification of domain names that may eventually be used to in a phishing attack.

Conclusions

Domain name registration is inexpensive, with the cost of a retail registration being only $6.00 to $10.00. The cost of a legitimately purchased domain name is the least of a phisher's concerns. Moreover, since the phishers' business is to steal financial instruments, they often have a supply of stolen credit card numbers that they can use to illegitimately register domain names. Simply put, phishers have no incentive to practice domain name tasting. In fact, the notion of deleting a domain name that might continue to serve as a phishing site beyond the Add Grace Period because it has eluded detection is entirely contrary to the phishing business model.

While these studies demonstrate that tasting is not used by phishers, APWG does note that tasting affects anti-phishing efforts. Members of the anti-phishing community have had to increase their infrastructure to account for the larger number of potential phish sites that are being registered by tasters, and this impedes anti-phishing efforts and increases the cost of detecting and mitigating the fraudulent behavior.

Contributors' Contact Data
Greg Aaron, Afilias: gaaron@afilias.info
Dmitri Alperovitch, Secure Computing: dmitri_alperovitch@securecomputing.com
Laura Mather, MarkMonitor: lmather@markmonitor.com