

## Secure Your Domains. Secure Your Business.

### Abstract

We all know that hackers and eCriminals attack websites directly, skillfully — and frequently. Now, as site administrators have grown more skilled at protecting themselves, hackers have turned to a new attack vector: hijacking site addresses. Attacks against domain name registration accounts and the hijacking of domain name system records are profoundly disruptive and dangerous to business. Such security breaches can not only have a real impact on corporate reputation and customer trust, but can also hurt an organization's bottom line quickly and painfully. Your company's domain names enable customers to interact and transact with you online and, as a result, are a valuable corporate asset that needs round-the-clock protection.

Site-address attacks — a relatively new phenomenon — emerged as hackers discovered that many domain registries and registrars were relatively soft targets. Targeting registries and registrars with the aim of pointing the domains to a different location — “changing the signpost,” so to speak — is becoming more prevalent and is a danger that must be addressed by a solid domain security strategy. According to the Internet Corporation for Names and Numbers (ICANN), corporations large and small have suffered such attacks, so every organization needs to take action and “harden” the security of their domain name portfolio.

In this paper, we discuss these new types of domain attacks, including DNS attacks and those against the domain registration and management portal, and describe the damage they inflict. We suggest strategies for avoiding these attacks by putting a plan in place to ensure your domains are secure not only at the registrar level, but at the registry level as well. It's vital to ensure that domains are 'locked' to prevent unauthorized transfer — and investigate more elevated locking mechanisms for mission critical domains. Selecting the right partner to ensure your domains remain safe is critical.

## Contents

Introduction and History .....	3
What You Must Guard Against .....	4
Registrar Breaches .....	4
Phishing and Other Social Engineering Attacks .....	5
Domain Name Hijacking .....	5
Collection of Credential Information by Malware .....	5
What You Should Do to Protect Your Domains .....	5
What Steps Can You Take to Make Sure Such Problems Don't Occur? .....	6
Consolidate Your Portfolio of Domains .....	6
Ensure Your Registrar Is Secure .....	6
Set Your Domain Names as "Locked" .....	6
Work with a Hardened Registrar .....	7
Ensure Your Registrar Has Solid and Extensive Industry Relationships .....	7
Monitor Critical Domains .....	7
Conclusion .....	8

## Introduction and History

In today's connected world, your customers and partners naturally rely on your domain names to interact with you online. As a result, your domains are high-value business-critical assets, as important to your organization as any tangible asset, trademark, or intellectual property. They are how your customers find you, after all. Why aren't such vital assets better protected from hackers by domain name registries and registrars? And why is it that so many corporations focus simply on the cost of acquiring domain names and not on the vital task of securing them? The two entities managing the domain name system, registries and registrars, differ mainly by who their customers are. A *registry* provides direct services to registrars and consists mainly of a database containing DNS information (domain name, name server names and IP addresses) along with the name of the registrar that registered the name and basic transaction data. A *registrar* provides direct services to domain name registrants. Registrars process domain name registrations for Internet end-users and send the necessary DNS information to a registry for entry into their centralized registry database. The registrar database contains customer information in addition to the DNS information contained in the registry database.

When hackers or scammers accomplish unauthorized modification of DNS configuration information, it can "severely disrupt business operations and can cause financial and reputational harm," says ICANN's Security and Stability Advisory Committee (SSAC), which authored a white paper on DNS attacks in June 2009.

For years, hackers focused mainly on getting their hands on web content. Now however, they're targeting the domain name infrastructure, having learned that many registries and registrars are not hardened. This weakness stems in part from the common practice of operating highly automated, retail domain registration services designed to serve a high volume of customers quickly and inexpensively, with little human intervention. In fact, many notable domain name attacks can be traced back to situations in which large enterprises entrusted their domain names to a registration service that was equipped to primarily handle simple retail domain name registrations.

"The most recently studied attacks... include a worrisome twist," the report continues: "Whereas some attacks remain malicious and motivated by needs for notoriety or political advocacy, others are criminally motivated, where the purpose of the attack is to acquire resources (domain names or name servers) to support attack infrastructures including botnets and fast flux attack networks."<sup>1</sup> According to research by the Anti-Phishing Working Group (APWG), the second half of 2008 saw close to 57,000 domain-based phishing attacks on close to 25,000 hijacked domain names, up 20 percent over the first half of 2008.<sup>2</sup> This is why it is so important for companies to proactively secure their domains.

<sup>1</sup> ICANN SSAC: "SAC 40: Measures to Protect Domain Registration Services against Exploitation or Misuse," June 2009.

<sup>2</sup> APWG "Global Phishing Survey: Trends and Domain Name Use 2H2008," May 2009 [http://www.antiphishing.org/reports/APWG\\_GlobalPhishingSurvey2H2008.pdf](http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf)

Your domains are high-value business critical assets. They are how your customers find you.

The problem is serious enough to garner the attention of ICANN's SSAC:

We've been doing a study... on protecting high-value domains. The stimulus for this study was multiple incidents involving weaknesses at registrars. That is, there were hijackings or comparable kinds of problems with visible well-known names that were either — where the problems were not solely due to the way that the registrant (that is, the domain holder) conducted themselves, or were wholly or substantially complicated by the processes and procedures at the registrars.<sup>3</sup>

## What You Must Guard Against

How are hackers and scammers launching domain name system attacks? The methods vary, but the risks to consumer confidence in your brand and your bottom line — when your site suddenly becomes unavailable or begins serving up bogus information — are the same.

### Registrar Breaches

At a minimum, registrars need to harden their configuration and management portals and back-end environments. Recently, a New Zealand-based registrar called DomainZ was attacked by hackers using a relatively simple technique — a SQL injection — that gave them access to the account database. This led them to a password retrieval page where they collected account profiles of many of the registrar's customers, including some very large corporate clients.<sup>4</sup> By modifying the DNS configuration records of many of their victims' domains, the hackers were able to redirect visitors to other sites that either attacked the brands or promoted political messages. While the vandalism was short-lived, real damage was done to the reputation of DomainZ clients as they scrambled to find a fix and explain the embarrassment to their visitors.

It is clear from the DomainZ example that registrars need to harden their configuration and management portals and back-end environments. They should always be prepared (and scanning) for intrusions. While a site going down is bad, it can be worse for a site to be hijacked and present bogus information, which in turn can erode customer trust in the real brand and product. This method can also be used in a “man in the middle” attack, in which hackers redirect a domain to a malicious web server and capture user IDs and passwords while forwarding traffic to and from the real site, leaving the victims unaware of the malfeasance.

<sup>3</sup> Transcript of SSAC Open Meeting, Mexico City, February, 25, 2009.  
<http://mex.icann.org/files/meetings/mexico2009/transcript-ssac-open-meeting-02mar09-en.txt>

<sup>4</sup> “High Profile New Zealand Sites Registered At Domainz.net Defaced Through DNS Hijack,” April 21, 2009.  
<http://cyberinsecure.com/high-profile-new-zealand-sites-registered-at-domainznet-defaced-through-dns-hijack/>

## Phishing and Other Social Engineering Attacks

Beyond system hardening, registrars need to evaluate how weak their human links are. Some are certainly lax enough to be easily victimized by simple social engineering tricks, such as a hacker looking up the registrar for a site, calling the registrar's tech support line, claiming to be a new technical contact, and asking for the passwords so she can proceed with her work. In many cases, a user ID and password is all an attacker needs to gain control of an entire domain name portfolio. Domain administrators, too, can be tricked by phishing.

In one notable example of the above, customers of Network Solutions were sent an email asking for their IDs and passwords. It is believed that one respondent was an employee of CheckFree, whose information gave the phishers the opportunity to redirect CheckFree's customers to a rogue server located in the Ukraine for 5 dangerous hours.<sup>5</sup>

## Domain Name Hijacking

In a more targeted type of attack, a scammer may make a fraudulent email request for the transfer of a domain name to which he has no right. Such a transfer can be denied, but typically denial hinges entirely on knowledgeable human intervention. In the more automated systems of some consumer-focused domain registrars, such requests can slip through, leaving the rightful domain name owner to find its URLs are pointing somewhere malevolent. In one famous 2005 example, Panix.com lost control of its addresses over a long holiday weekend in such an attack. As a result of the attack, all of Panix.com's email services bounced, calling into question their reputation as a reliable ISP and email service provider.<sup>6</sup>

## Collection of Credential Information by Malware

The most recent development in domain name attacks is the targeted deployment of malware, such as keyloggers sent to corporate domain name administrators. These keyloggers track logins and passwords for corporate domain name management portals. With this credential information, scammers can unlock and hijack domains, update name servers, or even change DNS settings — any of which could result in site downtime, or the proliferation of more malware to unsuspecting website visitors.

## What You Should Do to Protect Your Domains

Every corporation needs to have a strategy in place for securing its portfolio of

Business continuity depends on properly functioning URLs and sites.

<sup>5</sup> "Network Solutions Phishing Attack Preceded CheckFree Domain Takeover," Computerworld, December 4, 2008. [http://www.computerworld.com/s/article/9122722/Network\\_Solutions\\_phishing\\_attack\\_preceded\\_CheckFree\\_domain\\_takeover](http://www.computerworld.com/s/article/9122722/Network_Solutions_phishing_attack_preceded_CheckFree_domain_takeover)

<sup>6</sup> "Panix.com Hijacking Causes Panic," Internetnews.com, January 18, 2005. <http://www.internetnews.com/security/article.php/3460871>

domains. There is simply too much at risk — business continuity depends upon properly functioning URLs and sites. While the goal is to avoid attacks altogether, sound procedures and experienced partners must be in place to mitigate damage — quickly.

One of the most daunting problems facing anyone responding to a DNS attack is time. For example, once a problem is discovered and addressed, it can take anywhere from 20 minutes to 72 hours for all of the servers in the DNS system to be re-updated with the correct information. If the “Time to Live” (TTL) setting is set to update only every three days, for example, an updated and corrected DNS record won’t be pushed to caching servers until that time has passed. Such a situation could be catastrophic to business if a mission-critical domain, such as a retailer’s eCommerce site, is compromised. Because of these potential time-delays and their impact on your business, it is essential that you insist on a registrar who is experienced and has strong security protocols in place — including a hardened portal. This type of registrar will minimize the likelihood of attacks. If an attack does occur, they will be in the best position to help you mitigate damage, and ensure your domains are back online quickly and efficiently.

## What Steps Can You Take to Make Sure Such Problems Don’t Occur?

### Consolidate Your Portfolio of Domains

Know which domains you own, and make sure you have a global, centralized view of all your domain names across all offices and locations. Maintaining careful records and keeping track of your entire domain portfolio is half of the battle.

### Ensure Your Registrar Is Secure

Ensure that your registrar employs a “hardened” portal — one that employs constant checks for security and code vulnerabilities the same way the web security team does for your websites. The registrar must have a track record of being able to stay on top of new exploits, and of researching and understanding new vulnerabilities. In addition, the registrar must be able to demonstrate use of strong internal security controls and best practices.

### Set Your Domain Names as “Locked”

In response to the threat of domain name hijacking, ensure that your organization’s domains are “locked,” making them unavailable for transfer. All domains should be created, configured, and then locked.

### Implement “Registrar Locking”

There is also an elevated locking mechanism, sometimes referred to as a “registrar

lock” or a “super lock,” that essentially freezes all domain configurations until the registrar unlocks them only upon completion of a customer-specified security protocol. Companies control the level of complexity associated with their specific protocol and domains are made available for updating through the portal only when these security protocols are accurately completed. This extra level of security should be applied to your most mission-critical domains such as transactional sites, email systems, intranets, and site-supporting applications.

### Demand “Registry Locking”

It is true that generic domain locking can still be exploited by an attacker who updates name servers, thereby redirecting customers to illegitimate websites without transferring actual control of the domain from one registrar to another. To combat this, another step is “registry locking,” or “premium locking,” which makes the domain unavailable for any updates at all. This method of locking is currently available only for .com and .net registrations.

### Work with a Hardened Registrar

A hardened registrar will be familiar with all the potential attack strategies outlined above, including social engineering techniques, and will be able to guard against them. This is also most-likely a registrar that deals with corporate clients only. It will also have specialized security features for preventing, detecting, and responding to attacks against any domains, including:

- Restricting access to a portal via IP address
- Sending notifications on any name changes
- Avoiding automated emails as a primary means of communication
- Keeping activity logs to track all domain name updates
- Maintaining strong password management to force password changes
- Offering multiple levels of access

### Ensure Your Registrar Has Solid and Extensive Industry Relationships

Make sure your registrar is well established and experienced. It should also have relationships with other registrars, top ISPs, security organizations, browser partners, major software developers, and standards groups that will keep it in the loop as new threats emerge. Speed matters — these relationships will enable your registrar to *quickly* rectify any security breaches that do occur. Seek out a partner that offers both guidance and deep experience in security as well as domain management.

### Monitor Critical Domains

Domains that are vital to ongoing operations should be continually monitored for

Seek out a partner that offers deep experience in security as well as domain management.

unauthorized DNS updates, changes to website content and DNS cache poisoning. While there are foolproof methods for locking down .com and .net domains at the registry, other domains may still be at risk. Continual monitoring of core sites is recommended, so that any identified issues can be quickly remediated.

## Conclusion

In today's connected world, your customers and partners naturally rely on your domain names to find and interact with you online. As a result, your domains are high-value business-critical assets, as important to your organization as any tangible asset, trademark, or intellectual property. When Panix.com lost control of its domains, the trouble lasted for 48 hours. An attack on Hushmail.com redirected its users for just 6 hours, but some customers were affected for up to 72 hours. In some cases, domains have taken years to recover.<sup>7</sup> Think for a moment about what would happen to your organization if your entire portfolio of domain names, or even one mission-critical URL, was rendered useless for thirty minutes, an hour, or even days. What would the impact be? Pondering that threat should be more than enough to motivate you to take all the necessary steps to make sure your domains are secured and that access to them is controlled in a strictly monitored and professional way.

It is vital to execute a plan which secures your domains at both the registry and registrar level. All domains should be locked, with the highest locking-levels applied to mission-critical domains. Finally, it is essential to select a hardened and experienced registrar, who will prevent attacks from occurring in the first place, and who is equipped to quickly and effectively react to any attacks which might occur. Vigilance is mandatory when it comes to securing your most critical assets – your domains, your business — online.

<sup>7</sup> ICANN: "Domain Name Hijacking: Incidents, Threats, Risks, and Remedial Actions," July 2005. <http://www.icann.org/en/announcements/hijacking-report-12jul05.pdf>

## 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.

To learn more about the MarkMonitor Brand Protection Platform, Domain Management, and Domain Advisory Services, please visit [www.markmonitor.com](http://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](http://www.markmonitor.com)