White Paper

Six Steps to Securing Your Domains

Abstract

We all know that hackers and cybercriminals attack websites directly, skillfully and frequently. Now, with growing frequency, a new breed of politically-motivated hackers known as “hacktivists” have turned to another attack vector—hijacking domain credentials. Attacks against domain name registration accounts and the hijacking of domain name system (DNS) records are profoundly disruptive and dangerous to business as they result in a redirected website, making visitors unable to access the site that they expect. 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.

Domain name attacks have grown in frequency as hackers have discovered that many domain registries and registrars are 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 domain attacks 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 to investigate more elevated locking mechanisms for mission-critical domains.

MarkMonitor®
PART OF THOMSON REUTERS

Contents

Introduction and History

In the digital world, your customers and partners naturally rely on your website to interact with you. As a result, your domain names are high-value business-critical assets, as important to your organization as any tangible asset, trademark or other intellectual property. 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?

Your domains are high-value business critical assets as important to your organization as any tangible asset, trademark or other intellectual property.

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 gain access to update nameservers or even transfer domains, it can "result in the loss or disruption of Internet presence, loss of communications (email, Internet voice, streaming media or collaboration applications), reputational or even direct financial harm,"[1] says ICANN's Security and Stability Advisory Committee (SSAC), which authored a white paper on Protecting Domain Name Registration Accounts in November 2010.

Having learned that many registries and registrars are vulnerable to social engineering schemes, as well as SQL injection attacks, hackers and hacktivists are actively targeting the domain industry. In the last year alone, there have been close to 20 registry and registrar breaches.

The Risks You Face

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 redirected to another website—are the same.

Registrar Breaches

Registrars need to harden their configuration and management portals and back-end environments. In 2011, a European-based registrar was attacked by hackers using a relatively simple technique—a SQL injection—that allowed them to modify the nameserver settings on several domains.[2] In a separate case, an

1 ICANN SSAC: "SAC 044, A Registrant's Guide to Protecting Domain Name Registration Accounts" November 2010

2 "Turkish Hackers Strike Websites with DNS Hack", September 5, 2011 http://www.pcworld.com/article/239501/turkish_hackers_strike_websites_with_dns_hack.html

attack on another registrar led to several domains being hijacked by hacktivists and the sites being redirected.[3] By modifying the nameservers of their victims' domains, the hackers were able to redirect visitors to other sites that promoted a political message.

Registrars 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. Even worse still is a scenario where a breached domain is 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.

Phishing and Other Social Engineering Attacks

Beyond system hardening, registrars need to evaluate the weakness of their human links. Some have been 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 they can proceed with their work. In many cases, a user ID and password combination is all an attacker needs to gain control of an entire domain name portfolio. Domain administrators, too, can be tricked by phishing.

In one recent example, a registrars' sales partner was duped into providing log-in credentials to several of their partner accounts. The information provided by the sales partner, in response to a targeted phishing attack, gave the hackers the opportunity to update Whois and nameserver records of several high-profile websites and redirect them to politically motivated websites.[4] Not only did the attack result in a leading media organization's website being unavailable for several hours, it also disrupted their email communication.

Domain Name Hijacking

In a more targeted type of attack, a scammer may make a fraudulent email request for the actual 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 domains are not only pointing somewhere malevolent, but are no longer under their ownership. In one example from 2012, a bookmarking and annotation site lost control of its address when their domain was illegally transferred out of their account and into another domain registrar's account. As a result of the attack, five million customers could not access the site for over 50 hours.[5]

---

3 Cybercrime: Hacktivists Turn To DNS Hijacking, January 26, 2012. http://cyberwarzone.com/cyberwarfare/cybercrime-hacktivists-turn-dns-hijacking

4 "New York Times outage traced to phishing email to Melbourne IT partner", August 27, 2013 http://www.latimes.com/business/technology/la-fi-tn-melbourne-it-discovers-breach-that-took-down-nytimescom-20130827,0,7651273.story

5 Social Annotation Site Diigo.com Recovering After Domain Hijacking Nightmare", October 2012 http://techcrunch.com/2012/10/27/social-annotation-site-diigo-com-recovering-after-domain-hijacking-nightmare/

Collection of Credential Information by Malware

Another type of attack involves the targeted deployment of malware, such as keyloggers. In this type of attack, domain administrators are tricked into clicking on a website link, or opening an attachment in an email. 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, and 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 domains. There is simply too much at risk—business continuity depends upon properly functioning URLs and sites. While the goal is to withstand attacks as well as to mitigate damage 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. Such a situation could be catastrophic to business if a mission-critical domain 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.

Steps You Can Take to Mitigate Risks

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. Partnering with a corporate-only registrar that is committed to supporting new gTLDs and ccTLDs globally is key.

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.

Business continuity depends on properly functioning URLs and sites.

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 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"

Generic domain locking can still be exploited by an attacker who updates nameservers and redirects 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 for .com, .net and several ccTLD 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. Most likely, you will find this level of sophistication with a registrar that deals exclusively with corporate clients. Such a registrar will also have specialized security features for preventing, detecting and responding to attacks against any domains, including:

- Verifying portal account access via two-factor authentication
- 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 function as part of the security ecosystem, with strong relationships with other registrars, top ISPs, security organizations, browser partners, major software developers and standards groups that will keep it well-informed as new threats emerge. Speed matters—these relationships will enable your registrar to *quickly* rectify any security breaches that do occur. Seek out a registrar 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 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 issues can be remediated quickly.

Conclusion: Domain Hijacking Is Now Front Page News. Do You Want Your Domain to Be Next?

In the digital 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 other intellectual property. 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?

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 these critical assets—your domains, your business—in the digital world.

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

About MarkMonitor

MarkMonitor®, the world leader in enterprise brand protection and a Thomson Reuters Intellectual Property & Science business, provides advanced technology and expertise that protects the revenues and reputations of the world's leading brands. In the digital world, brands face new risks due to the Web's anonymity, global reach and shifting consumption patterns for digital content, goods and services. Customers choose MarkMonitor for its unique combination of industry-leading expertise, advanced technology and extensive industry relationships to preserve their marketing investments, revenues and customer trust.

To learn more about MarkMonitor and our Domain Management services, please visit **1-800-745-9229**.

Boise | San Francisco | Washington D.C. | London

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) 207 433 4000
www.markmonitor.com

MarkMonitor®
PART OF THOMSON REUTERS