Domain management – the best attack against hackers

Charlie Abrahams says protection and policing of domain names is key in today's digital era

www.worldcommercereview.com

In the digital world, all consumers rely on domain names to find, interact and transact with companies online. Domains are one of the most high-value, business-critical assets, and are as important to a company as any other type of tangible asset, trademark or intellectual property. In recent years domain hijacking has become front page news and it would certainly send shudders down the spines of any company executive if they were to consider the fallout of their entire portfolio of domain names, or even one mission-critical URL, being rendered useless for a relatively short period of time.

It is no secret that hackers and cybercriminals attack websites directly, skilfully and frequently. Attacks against domain name registration accounts and the hijacking of domain name system (DNS) records are profoundly disruptive and dangerous to the target business. The implications of a redirected website means visitors are unable to access the expected site, so it is perhaps unsurprising that these security breaches have a real impact on both corporate reputation and customer trust, and can also hurt an organisation's bottom line quickly and painfully.

Today, most businesses with an online presence are defined by their domain names and it is critical to guard these valuable corporate assets with round-the-clock protection. In the modern domain environment, brand owners should continuously refine their domain management strategies in order to stay impactful and help the constantly evolving brand abuse.

There are several fundamental steps that need to be considered for effective domain management, from ensuring pre-emptive security measures are in place, such as two-factor authentication and IP access restrictions, locking domains at both the registrar and registry level, and selecting a hardened and experienced registrar to prevent or react quickly to any attacks.

A risky business

The methods of how hackers and scammers launch domain name system attacks may vary, however, the risk to consumer confidence which effects both a brand and the bottom line, remains the same. One possible method is registrar breaches and it is crucial that registrars harden their configuration and management portals and back-end environments. Relatively simple techniques are sometimes used by attackers, such as SQL injections, which allow them to modify the nameserver settings on several domains. Registrars should always be prepared—and scanning—for intrusions.

A site going down is not even a worse-case scenario. The consequences could be even more serious if a site is hijacked and there is bogus information presented or if a breached domain is used in a man-in-the-middle attack. This is where 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 completely unaware of the malfeasance.

Phishing and other social engineering attacks

Beyond system hardening, registrars also need to evaluate the weakness of their human links. There have been cases where some have been victimised by simple social engineering tricks, such as a hacker looking up the registrar for a site, calling the registrar's technical support line, claiming to be a new contact and asking for the password so

> *In today's digital era, businesses can no longer focus simply on the cost of acquiring domain names, protection and policing is key*

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 can also be tricked by phishing.

Domain name hijacking

There is also the possibility of more targeted types of attacks, for example, a scammer may make a fraudulent email request for the actual transfer of a domain name to which they have 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, these requests could 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.

gTLDs

The domain name space has changed beyond recognition in recent years and the introduction of more than nine hundred new gTLD registries has seen many businesses review their current domain portfolios and plan for the implications of the expanded namespace. The addition of so many new TLDs has prompted organisations to cast a critical eye over the defensive portions of their domain portfolios, deciding which existing domain names are no longer necessary. Prudent steps included keeping those domain names with a high likelihood of squatting or those that would incur high recovery costs if circumstances changed.

The expansion of the domain name space means that organisations can now take a new and proactive approach to managing domains. Previously, they may have tried to register every variation, typosquat, and misspelling, whereas in this new environment that would obviously prove to be cost prohibitive. There is now more of a shift towards policing a brand by monitoring domain registrations and taking action where it makes sense. Blocking domains, where available, will allow companies to opt out of traditional registration while providing protection from squatters.

The gTLD revolution provides an ideal opportunity for organisations to review their domain management policies whilst underlining the importance of protecting domains in a continuously changing landscape.

Prevent and protect

The risks to domain names are clear, but what can organisations do to protect their domain names as effectively and robustly as possible? At MarkMonitor, we have developed five basic steps advising companies on the best approach to managing their domain portfolios.

1. Implementing and enforce policies

As business needs continue to change and evolve, companies should have clearly defined internal domain guidelines in place. Internal policies that address what, when and where domains should be registered, who is allowed to request registrations, and budget limitations. The criteria needs to be defined for those domains to let expire or sell, and work with stakeholders to determine where domains should point.

2. Align domain management strategies with policing and enforcement programmes

Companies continue to face tough registration and renewal decisions. Now is the time for businesses to ensure their domain registration and renewal strategies align with their policing and enforcement programs. Strategies should consist of registrations to support online objectives and a strategic monitoring program that allows them to quickly identify and address abusive registrations when they occur.

3. Secure and protect critical assets

Cybercriminals are using increasingly advanced techniques to target companies' critical assets. Domains require around-the-clock protection to maintain business continuity, brand reputation and customer trust. Organisations can partner with registrars that offers multi-level security and pre-emptive security measures to provide the necessary peace of mind, including locking domains at the registry level, two-factor authentication, and IP access restrictions, as well as consistent use of strong internal security controls.

4. Maximise the value of your domain portfolio

The expansion of the domain environment does not necessarily mean increasing domain budgets. Companies can maximise the value of their existing portfolio through portfolio rightsizing and domain utilisation. A portfolio should be reviewed at least once a year to identify registration gaps, out-of-policy registrations, underutilised domains and legacy domains that may be unnecessarily eating into the business-wide budget.

5. Stay informed and get involved

Staying up-to-date with the latest and greatest happenings in the domain industry is an increasingly complex challenge. Companies can get involved by joining trade or industry associations like INTA or ICANN. Alternatively, businesses can stay informed by partnering with a corporate-only domain registrar who advocates for brand owner's rights and is committed to ongoing customer education.

In today's digital era, businesses can no longer focus simply on the cost of acquiring domain names, protection and policing is key. The landscape is continuously evolving and by following these fundamental steps every organisation can ensure they have the most effective domain portfolio in place. ■

Charlie Abrahams is Senior Vice President, Worldwide Sales at MarkMonitor®