webnames
CORPORATE

The Growing Threat of Domain Hijacking (and How to Protect Against It)

Domain hijacking seems like a foreign concept to most but it is a very real threat. While it doesn't gain as much attention as spam or malware, hijacking is equally as disruptive to businesses and organizations. In most cases, these disruptions are temporary but they can produce lingering fallout on brands.

Whenever domain hijacking occurs, hackers can gain full control over a domain name, including its DNS settings. This may result in one or all of the following scenarios:

1. "Listen" in on all traffic to and from a particular domain name, including communications via email.
2. Redirect traffic to a page with malicious content.
3. Theft of domain name(s) by initiating a registrar and/or registrant transfer.

Domain Hijacking Cases

Domain hijackers typically target the domain names of reputable brands in order to steal the domain name or to intercept sensitive corporate data. In some cases, hijacking incidents are motivated by something as small as acquiring a rare Twitter handle to larger scale political affairs.

In 2005, the luxury brand Coach became a target of the UGNazi hacking group. Many counterfeit versions of Coach's products are regularly found in China and the brand's support of SOPA (Stop Online Privacy Act) made it a target for hackers. During the attack, users were redirected to a page managed by the UGNazi group. Luckily, Coach's corporate emails were not intercepted, nor were visitors sent to a phishing site.

In 2013, both the New York Times and Washington Post websites were compromised by the Syrian Electronic Army (SEA). In these incidents, hackers succeeded in altering each company's DNS settings. While both companies were able to recover control of their respective domain names, the incident clearly disrupted operations and affected their reputation for online security.

In 2014, the SEA targeted high-profile domain names once more. This time, they took aim at Facebook's domain, modifying their WHOIS listing information. Fortunately for Facebook, the change was merely cosmetic. Due to a security lock applied to its domain name, the attackers were not able to modify their DNS settings.

While a few of the examples above show the disruptive nature of domain hijacking, the Facebook incident stands out due to the resliency the company displayed during the attack.

Domain Hijacking Prevention

Domain hijacking is undoubtedly disruptive and potentially damaging for companies, but it is also preventable by utilizing the appropriate security measures.

Use Domain Privacy to Protect Administrator Details

Applying domain privacy uses proxy contact information on the WHOIS public records. This minimizes threats which originate from scraping WHOIS information. Through the proxy contact information, hijackers only see generic registrar contact information. Any attempt to utilize this information to log into an account will automatically fail and be rejected.

Webnames customers automatically receive Domain Privacy on ALL domain names within your portfolio. This immediately adds a layer of security and prevents hackers from scraping WHOIS data to access your account.

Utilize Domain Locking Mechanisms

Various corporate registrars, including Webnames, offer the ability to implement security locks for a portfolio or a single domain name.

At the domain name level, registrar lock and registry lock, which is more secure, effectively adds multiple layers of security to each domain name. Depending on the security level of the mechanism, the locks applied are:

- **Registrar Lock:**clientUpdateProhibited and clientTransferProhibited
- **Registry Lock:** serverDeleteProhibited, serverTransferProhibited and serverUpdateProhibited

Businesses that choose to utilize a form of domain lock harden their accounts by adding a human verification system at the registrar and/or registry level. Modifications to the DNS settings of a domain name are required to be scheduled in advance, pending verification. Even if an account has been compromised, the locks prevent unscheduled changes to a domain name's DNS settings and provides administrators time to react and resolve the breach.

Update and Install Security Patches

While IP professionals and brand managers have no control over an organization's security, they need to work with IT and security professionals to ensure that internal systems utilize the latest security patches.

In a report by Wired UK on the Panama Papers, it found that Mossack Fonseca's systems were riddled with security flaws. Despite managing large accounts, the company's systems were severely outdated, including the obsolete SSL v2 protocol.

While domain names are typically managed externally, unpatched systems allow hackers to take advantage of known exploits to compromise accounts, usernames, passwords and confidential information. Hackers can then use the obtained information to access the account associated with the domain name or portfolio.

Raise Awareness within the Organization

The strongest infrastructure in the world is only as strong as its weakest link and for businesses, your employees are part of that infrastructure. While hackers may not directly attack your servers, employess are just as vulnerable to attacks; usually in the form of phishing attempts. While domain names are typically managed through a registrar, all it takes is one employee to take the bait and unknowingly grant access to a portfolio.

The most apparent phishing emails are easy to spot - misspelled words, an unfamiliar domain name, bad grammar, etc. - but what about those that look legitimate, even after intense scrutiny?

This makes implementing an effective education program even more important. As part of the education program, corporations should do the following:

- Educate employees on how to identify phishing attempts. The most complex attacks can spoof even a legitimate sender's address and mask emails, making them appear legitimate.
- Raise awareness about opening attachments and unverified documents embedded in emails.
- Educate employees on how to identify URLs embedded in emails. Attackers often use a similar domain name to give them the appearance of being legitimate. Make srue the URL matches the sender's domain name.

Furthermore, companies should consider implementing two-factor authentication whenever possible; as well as enforcing password complexity and password expiration policies.

Conclusion

While the threat of domain hijacking continues to rise each year, prevention is far more cost-effective than recovery from a security breach. Despite the numerous attack vectors available to hackers, deploying the right security tools, updating internal systems and educating employees will allow companies to effectively defend against hijacking attempts.

For companies seeking a robust security mechanism to prevent threats like domain hijacking, Webnames offers a comprehensive suite of tools to harden your domain names - from private registration (offered for free to all clients) to registry locks.

For more information, visit **https://corporate.webnames.ca** or contact us at **1-866-470-6820**.