

In the last year, several of the world's most recognizable brands fell victim to domain name hijacking including: The U.S. Marines, The New York Times, Twitter, Google and the Huffington Post. Any organization with significant traffic, brand, intellectual property or a valuable domain name should consider themselves a Target of Opportunity for domain name hijacking.

Overview

Domain hijacking, or domain theft, occurs when domain names are stolen from their legitimate owners.

Compromised domain names can create significant financial, legal, operational and reputational damage to affected companies.

Domains are hijacked when unauthorized users steal the domain owner's credentials and access the domain's administrative control panel to point the domain to another domain name server and therefore to another Webserver. Ultimately whatever content appears on the Webserver will appear when a domain name is entered into the browser.

It is important to note that cyber criminals are able to hijack a domain name without the need to access the target Webserver or the need to bypass firewalls or other security measures. Domain hijacking circumvents all these defenses.

There is no typical profile to identify potential domain name hijackers. Analysis of reported domain hijackings indicates that they are just as likely to be perpetrated by disgruntled employees or customers/contractors as they are a vendor, a competitor, a company, or an organization looking to make a political statement or cause general mischief.

Unfortunately, utilizing a simple username/password combination has proven insufficient for enterprises at risk for domain name hijacking. Attackers leverage a range of techniques to steal domain name credentials including: hacking emails, brute force attack, keystroke logging, improper password management and social engineering. Ultimately domain names must be treated as critical business assets supporting the company's communications and transaction systems.

How WebLock Works

Weblock is designed to significantly reduce the changes of domain name hijackings by deploying the following:

- Locking down your domain name at the Registry and/or Registrar.
- Employing a multi-factor authentication process before any changes can be made to your domain name(s).
- Alerting you to any requests to changes to your domain configuration settings – usually an early warning sign for an attack on your business.

Key Features:

1. Multi-layer Architecture

WebLock uses a system of different types of locks on the same asset, greatly reducing the potential of a complete hijack.

2. Distributed Systems and Processes

WebLock ensures that critical information is protected, prohibiting the keys and processes used to unlock, transfer, delete or redirect your domains from being housed in one single system or with one group of individuals. Portions of the credentials, keys and authentication processes are distributed among different groups and systems.

3. Isolated Systems and Processes

As an additional layer of security, parts of the system and processes are isolated and completely disconnected from one another. Keys are only held by your authorized personnel and our selected personnel and systems. This prevents inadvertent sharing of information which in turn prevents social engineering.

4. Encryption

Weblock uses the highest level of encryption to protect not only authorized domain credentials, but also the processes and systems supporting the product.

5. Multi-factor Authentication

WebLock uses a mix of online and offline authentication methods to ensure that unauthorized persons with stolen credentials are unable to gain administrative control. Even if someone should get through to your domain control panel, if the account has not been unlocked, the transactions for transfer, delete or redirect will not execute.

How do I enroll in WebLock?

Secure your domain names today by contacting your personal Corporate Services team member to set up an appointment. You can reach our Corporate Services team at 509.329.5457 Monday through Friday, 9am – 7pm EST.

Learn More

Please visit <http://weblock.web.com/weblock-whitepaper.pdf> for a more detailed primer on Domain Hijacking.

About Network Solutions

Network Solutions, a [Web.com](#) company, is here for one reason: to help businesses compete and succeed online.

Network Solutions is a global domain registrar and further meets the needs of businesses anywhere along their lifecycle.

With over 3 million customers and 30 years of experience, we know what businesses need to succeed on the web. We provide subscription-based solutions including website design and management, search engine optimization, online marketing campaigns, local sales leads, social media, mobile products, eCommerce solutions, call center services and domain security solutions.