Sucuri Blog

blog.sucuri.net/2020/11/hackers-love-expired-domains.html

Luke Leal November 26, 2020

Sometimes, website owners no longer want to own a domain name and they allow it to expire without attempting to renew it.

This happens all the time and is totally normal, but it's important to remember that attackers regularly monitor domain expirations and may target certain domains that meet specific criteria.

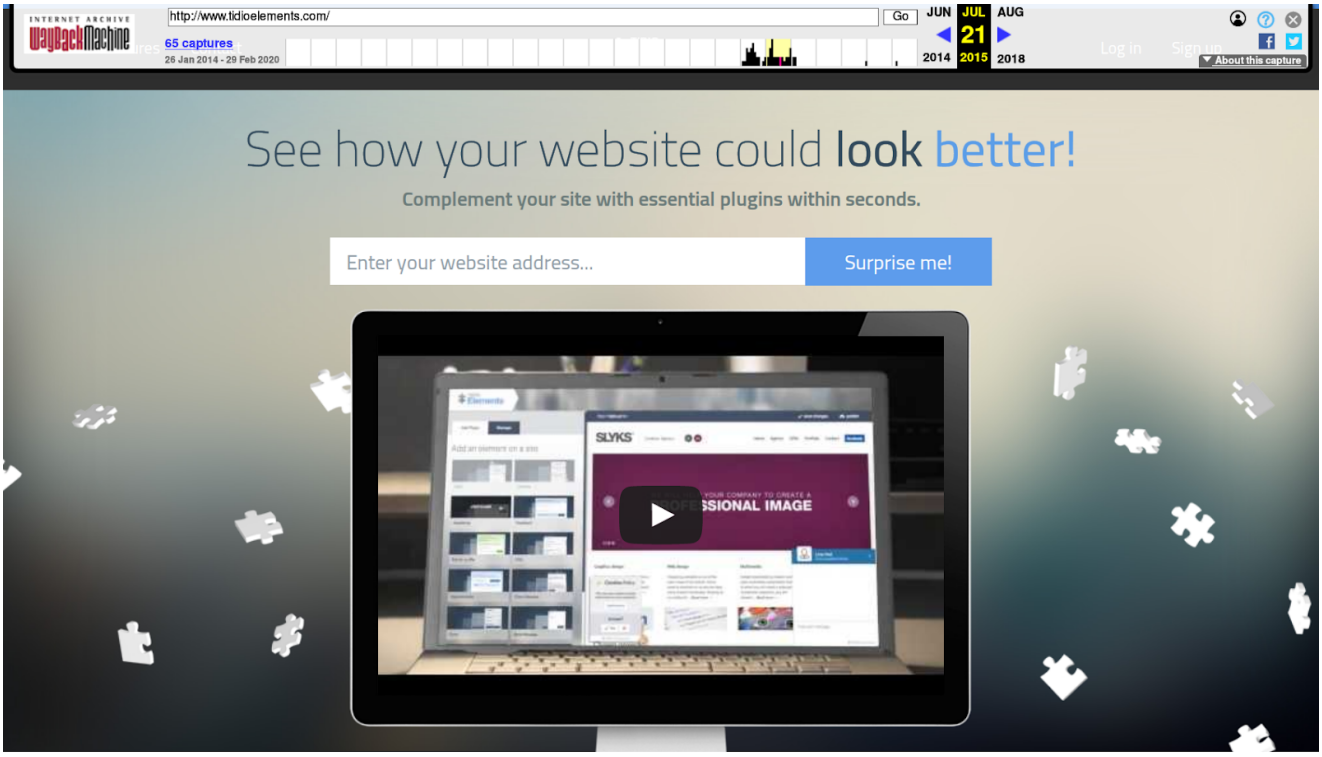
Vendor domains can be an easy backdoor

A vendor (supplier) domain is defined as a website that is used to host and load third party Javascript resources — for example, something like a live chat widget or also advertisements. This also includes domains used to load Javascript sources for specific WordPress plugins.

For whatever reason, a vendor may allow their domain's registration to expire, which means it can become available for an attacker (or anyone else) to register it.

Attackers typically perform reconnaissance to ascertain whether or not a domain is valuable to them. For example, if the expired domain is used within a plugin to load a Javascript resource, then it would make it a perfect target.

We recently found this exact scenario with the now defunct WordPress plugin **visual-website-editor** and its domain **tidioelements[.]com**, which was kindly reported to us by a website owner that encountered suspicious activity while using it.



The landing page for tidioelements[.]com in 2015, back when it was still an active plugin website.The attacker's strategy relies on the fact that some websites might still have the plugin installed and activated, and continue to load resources from the expired domain. Once the attacker has registered the domain, they can then "assume" control by replacing any legitimate Javascript resources with something malicious.

The plugin won't know that the domain has expired or that the Javascript resource is now loading from an attacker's server — the only information it has is the URL to the Javascript resource, which it tries to include wherever the plugin is loaded.

```
public function jsRedirectCodeRescure(){

    echo "<script data-type='tidioelements' type='text/javascript'>
if(typeof tidioElementsEditedElements=='undefined'){
var s = document.createElement('script');
s.type = 'text/javascript';
s.src = 'https://tidioelements.com/redirect/".get_option('tidio-visual-public-key
    ').".js';
document.getElementsByTagName('head')[0].appendChild(s);
}</script>";

}
```

The project was abandoned and is no longer available for download in the WordPress repository. Nevertheless, attackers were able to take advantage of the expired domain to load arbitrary content, which highlights the importance of keeping all software updated and removing any old plugins that aren't actively used in your environment. Another important tip to harden your website is to only use resources from official and reputable sources.