CERT-UA warns of ongoing Distributed Denial of Service attacks targeting pro-Ukrainian websites

28th April 2022

Orpheus severity score: 59

The Computer Emergency Response Team in Ukraine (CERT-UA) published an advisory warning of ongoing Distributed Denial of Service (DDoS) attacks targeting pro-Ukrainian sites and a government web portal.

The threat actors compromised WordPress sites and injected malicious JavaScript code, known as BrownFlood, to facilitate the DDoS operations. The scripts are placed within the main website's HTML structure and are based64-encoded to circumvent detection. The malicious code runs on the website visitor's computer and directs their machine's resources to generate a large number of requests to URLs listed within the code to render the websites inaccessible. This DDoS campaign occurred without the knowledge of either the website owners or visitors.

CERT-UA is collaborating with the National Bank of Ukraine to mitigate the DDoS operations, notifying targeted site owners of the DDoS attack, and advising on how to detect and remove the malicious JavaScript code.

This DDoS campaign is highly likely to be another example of Russian state activity seeking to cause disruption within Ukraine. We previously reported on a Russian DDoS attack that caused connectivity issues for internet provider Ukrtelecom which similarly to this campaign attempted to wage disruption. We assess that these operations, along with the deployment of wiper malware, are a hallmark of Russian destabilisation attempts. In this instance, victims shared a pro-Ukrainian sentiment which strongly suggests a political motivation for the DDoS campaign and connects to a broader Russian sabotage strategy.

Threat Subcategory	Russia
Sectors	Government, Media and Entertainment, Individuals/NGO
Objective	Disruptive DDos
Target System	Website
Countries & Target	Russia, Ukraine
Target Software	HTML
Sources	https://www.bleepingcomputer.com/news/security/ukraine-targeted-by-ddos-attacks-from-compromised-wordpress-sites/ https://cert.gov.ua/article/39923