Subject: - **Cyber Security Advisory – WordPress Sites Hacked with Fake Cloudflare DDoS Alerts Pushing (Advisory No. 37)**

Context. WordPress is a free and open source content management system written in PHP, supported with HTTPS and paired with My SQL and MariaDB database. Recently, it has been observed that websites developed in WordPress are being hacked to **display fake Cloudflare DDoS protection pages**. The fake pages are used to distribute malware that install **NetSupport RAT** and **RaccoonStealer password-stealing Trojan**.

2. **Malware Details**. Working mechanism of fake DDoS protection pages is as under:-

a. **DDoS protection screens** are used for protecting sites from bots, aiming to overwhelm them with garbage traffic. These screens provided with opportunity for malware campaigns where **threat actors** are hacking poorly protected WordPress sites to add a **heavily obfuscated JavaScript payload** that displays a **fake Cloudflare protection DDoS screen**.

b. On clicking button to bypass the DDoS protection screen, will download a '**security_install.iso**' file to computer, which pretends to be a tool required to **bypass the DDoS verification**. The victims are then asked to open security_install.iso, pretending to be DDOS GUARD which is security_install.exe, which is actually a **Windows shortcut** that runs a PowerShell command from **debug.txt file**.

c. Ultimately, this causes a **chain of scripts** to run that installs NetSupport RAT and scripts downloads **Raccoon Stealer 2.0** password-stealing Trojan and launches it on the device.

d. Further, the executables acquire passwords, cookies, auto-fill data and credit cards saved in the web browsers and is capable of performing file exfiltration and taking screenshots of victim's desktop.

3. **Recommendations**

a. System Administrator must check **theme files of their WordPress** sites as this is the most **common infection point**.

b. Always employ tile integrity monitoring systems to catch **JS injections** and prevent your site from being a **RAT distribution point**.

c. Internet users can protect themselves from such threats by **enabling script blocking settings** on their browser.

d. Place **2 Factor Authentication on all important logins** (such as bank/ social media accounts). Always deploy **Firewall/ Antivirus** for protection of website.