Neutrino

Archived: 2026-04-05 12:46:26 UTC

Short bio

The Neutrino exploit kit is a malicious tool kit, which can be used by attackers who are not experts on computer security. Threat actors can have zero coding experience and still use exploit kits like Neutrino to conduct their illegal activity.

History

Exploit kits, sometimes referred to as exploit packs, are toolkits that automate the exploitation of client-side vulnerabilities, often targeting browsers and applications that a website can invoke through the browser. Known exploit targets have been vulnerabilities in Adobe Reader, Java Runtime Environment, and Adobe Flash Player.

Neutrino began targeting CVE-2012-1723, CVE-2013-0431, and, CVE-2013-0422, all exploiting vulnerabilities in the Java Runtime Environment (JRE) component. It was marketed as a simple-to-use kit with a nicely user friendly control panel.

Common infection method

Neutrino toolkit compromises systems by targeting various vendor vulnerabilities on the victim's machine.

Campaigns targeting WordPress have been observed using dynamic iframe injection. The goal of the campaign was to fully compromise the site, which included adding a webshell (Remote Access Tool (RAT) or backdoor), harvesting credentials, and finally injecting an iframe that loads a Neutrino landing page. The iframe is injected into the compromised site immediately after the BODY tag, which resembles recent Angler samples. Threat actors want to re-direct victims to their payload, which includes ransomware.

Associated families

Exploit kits/packs and ransomware.

Remediation

Malwarebytes Anti-Exploit stops Neutrino EK while Malwarebytes Anti-Malware already detects known dropped binaries, such as Andromeda/Gamarue malware. Keep your system patched and keep your applications updated.

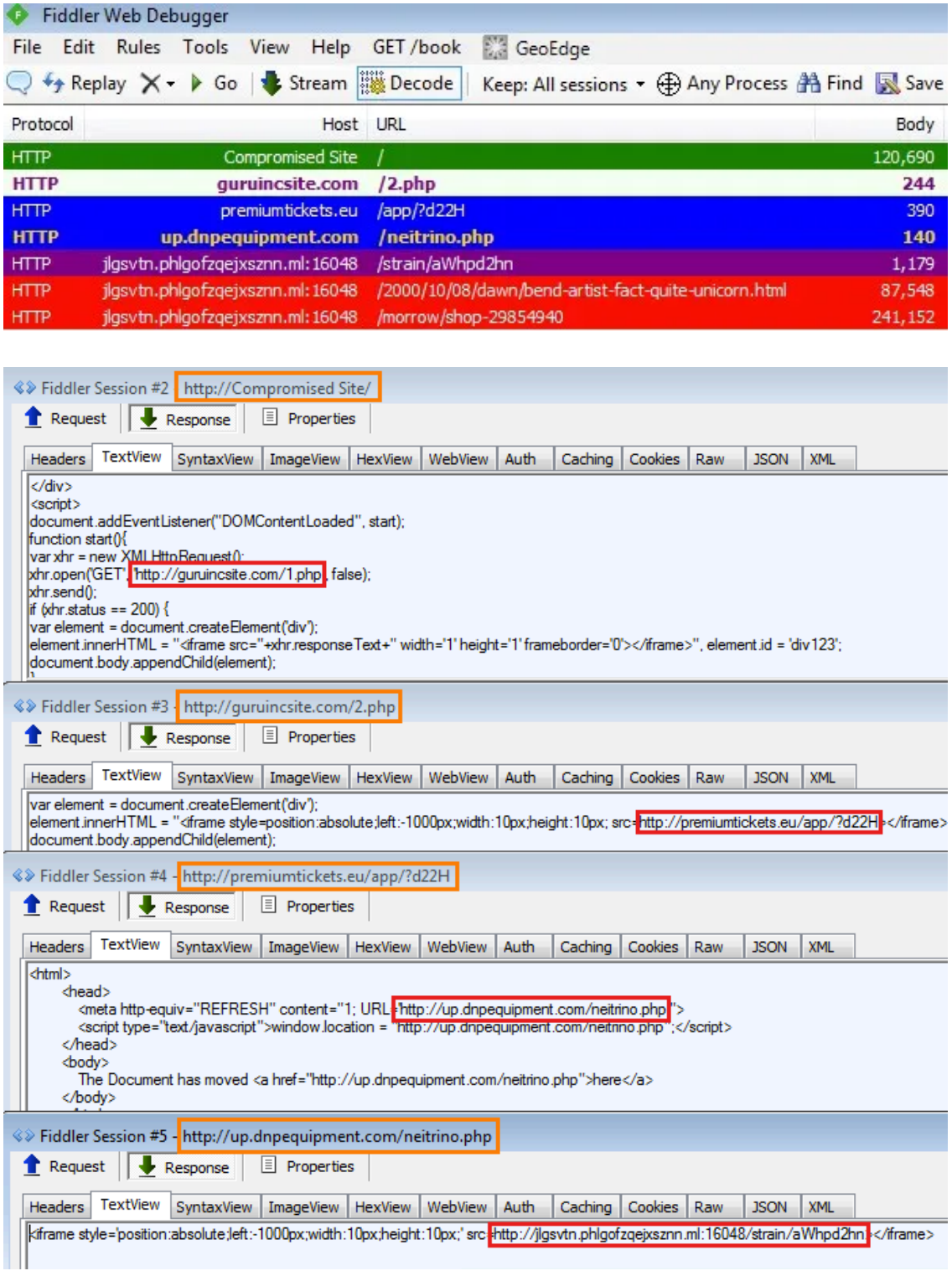
Aftermath

Successful exploitation of a victim's system varies but can lead to an encrypted executable download. The binary is decrypted and begins beaconing immediately, which can lead to CryptoWall.

Avoidance

It is best to practice good security by keeping systems patched and programs updated. Furthermore, ensure you have antivirus, anti-exploit, anti-malware protection. For even more protection, it is good to have a dedicated firewall.

Screenshots



Source: https://blog.malwarebytes.com/threats/neutrino/