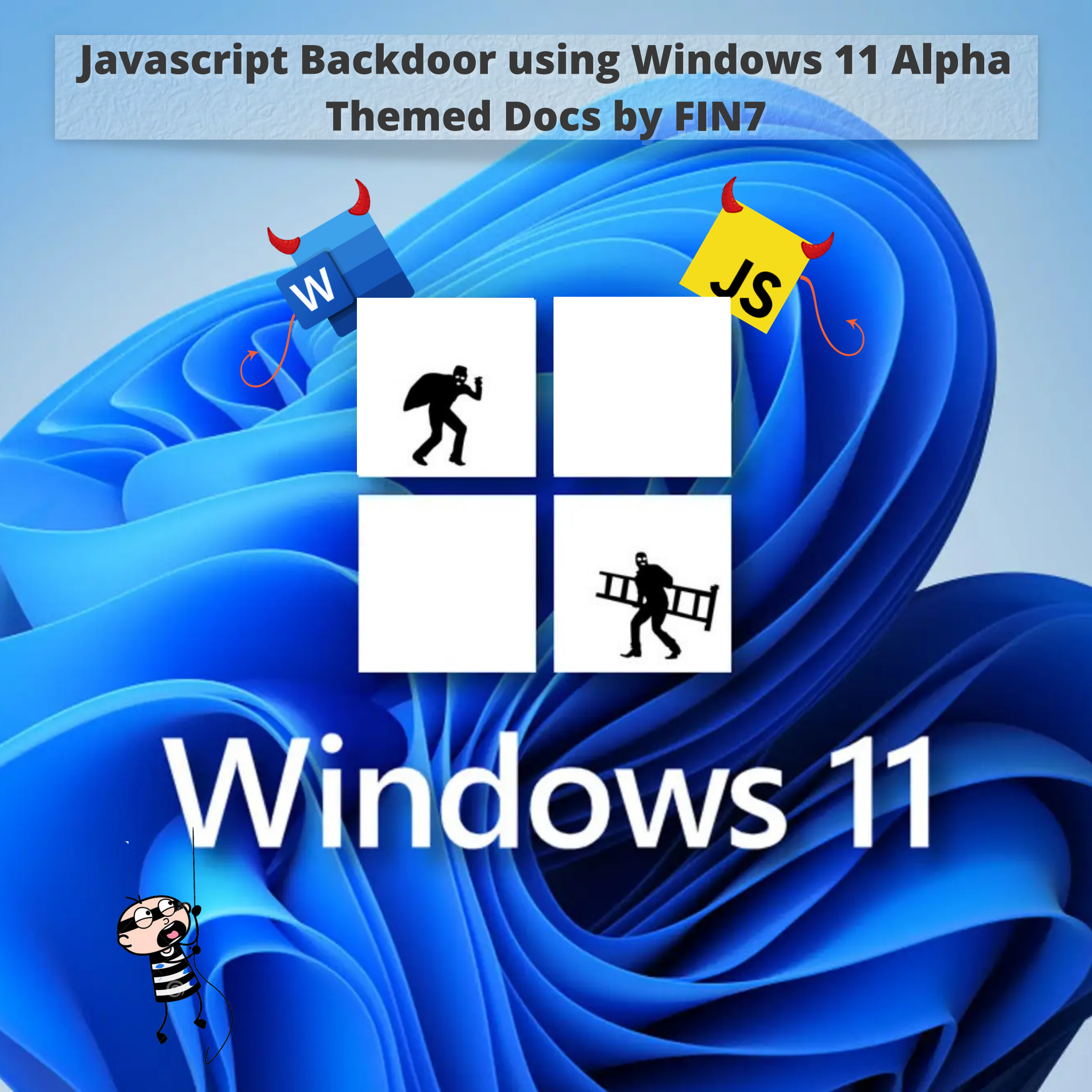
Javascript Backdoor using Windows 11 Alpha Themed Docs by FIN7



Pinned

FIN7, a financially motivated cybercrime group, has recently targeted a California-based point-of-sale service provider to steal payment-card data by delivering JavaScript backdoors using Word documents themed around the next version of Windows.

According to the researchers at Anomali, a cybersecurity company, the hacking group booby trapped the victims by leveraging six different docs, all referencing “Windows 11 Alpha” – the “Insider Preview” version of the upcoming Windows 11 operating system from Microsoft.

OWASP VITCC

Pinned

The docs which looked harmless were packed with malicious Visual Basic (VBA) macros. The infection chain began with the Microsoft Word document featuring a decoy image, telling readers that it was made with Windows 11 Alpha. The image asked users to “Enable Editing and Enable Content” to see more.

Once it was enabled, a VBA macro was executed that took encoded values from a hidden table inside the .doc file and deciphered them with an XOR key. This created a script that carried out various checks on the target.

OWASP VITCC

Pinned

If the target system had any Eastern European languages as default or if it was running in a sandboxed environment, the script would terminate. Then, it looks to see if the target is on the domain clearmind.com – the domain of the point-of-sale (PoS) service provider. If it is, then the script drops a JavaScript file called “word_data.js” into the TEMP folder which, once deobfuscated, turned out to be a JavaScript backdoor that FIN7 has been employing since 2018, researchers noted. From there, FIN7 can further penetrate a victim’s machine to steal data and perform recon for lateral movement.