Mphasis
The Next Applied

Mphasis SOC – Information Security News
Date & Time Issued: 21-06-2024, 23:00 IST

Title

Hackers Exploit Legitimate Websites to Deliver BadSpace Windows Backdoor

Summary

- Hackers abuse high-ranking infected websites to leverage their established credibility and large user base to spread malware, launch phishing attacks, or redirect traffic to malicious sites.
- While exploiting such trusted infected platforms they can now reach out to larger audiences, increase the efficiency of their attacks, and escape from being caught for a longer period of time through this way.
- Cybersecurity analysts at GData Software recently identified that BadSpace malware has been actively attacking users by leveraging high-ranking infected websites.
- The backdoor uses a hardcoded RC4 key for encrypting C2 communication, which differs for each sample.
- A researcher has created an IDA Python script based on the OALabs Revil decryption script to decode strings and APIs in IDA.

Severity

Medium

Attack Vectors

- Collaborative research identified a multi-stage attack chain involving an infected website, a command and control (C2) server, sometimes a fake browser update, and a JScript downloader to deploy the backdoor.
- BadSpace is delivered via infected websites that set a cookie to track first-time visitors.
- It constructs a URL with device information and sends a GET request, overwriting the original webpage with a malicious payload unless an error occurs.
- Infected sites tend to be WordPress sites that inject malicious code into JavaScript libraries or index pages.
- Acquired JScript files drop and run BadSpace, sometimes using extension spoofing like ".pdf.js".
- The C2 domains used are associated with the SocGholish threat actor known for using fake updates and JS files.
- This attack shares similarities with SocGholish's delivery methods for backdoors. The JScript file has three functions and an array of strings that utilize obfuscation techniques.
- Most variables are left undeclared to make things a bit more complicated.
- The third function, which is also obfuscated using the JavaScript Compressor, builds a PowerShell downloader that downloads and runs BadSpace backdoor silently in rundll32.exe after 10 seconds.

Indicator of Compromise

INDICATOR TYPE	INDICATORS
File Hash	• 2b4d7ed8d12d34cbf5d57811ce32f9072845f5274a2934221dd53421c7b8762b • f3fed82131853a35ebb0060cb364c89f42f55e357099289ca22f7af651ee2c48 • 255cc818a2e11d7485c1e6cc1722b72c1429b899304881cf36c95ae65af2e566 • c64cb9e0740c17b2561eed963a4d9cf452e84f462d5004ddbd0e0c021a8fdabc • 9786569f7c5e5183f98986b78b8e6d7afcad78329c9e61fb881d3d0960bc6a15 • c7fc0661c1dabd6efd61eaf6c11f724c573bb70510e1345911bdb68197e598e7 • 2a311dd5902d8c6654f2b50f3656201f4ceb98c829678834edaeae5c50c316f5 • 0da87bff1a95de9fc7467b9894a8d8e0486dfd868c2c7305e83951babacde642 • 6a195e6111c9a4b8c874d51937b53cd5b4b78efc32f7bb255012d05087586d8f • 2a5a12cc4ef2f0f527cc072243aa27d3e95e48402ef674e92c6709dc03a0836a • 2a4451ef47b1f4b971539fb6916f7954f80a6735cf75333fa9d19b169c31de2e • 9bc4c44b24f4ba71a1c7f5dd1c8135544218235ae58efa81898e55515938da6a • 475edfbb2b03182ef7c42c1bc2cc4179b3060d882827029a6e67c045a0c1149b • 676cbcaa74ee8e43abaf0a2767c7559a8f4a7c6720ecc5ae53101a16a3219b9a • 770cafb3fe795c2f13eb44f0a6073b8fe4fb3ee08240b3243c747444592d85ff • 84519a45da0535087202b576391d1952a4cc81213f0e470db65f1817b65ee9d7 • a5f16fa960fe0461e2009bd748bc9057ef5cd31f05f48b12cfd7790fa741a24e • a725883bd1c39e48ab60b2c26b5692f7334a3e4544927057a9ffbdabfeedf432 • ad2333e1403e3d8f5d9bd89d7178e85523fa7445e0a05b57fd9bc35547ec0d98 • ba4c8be6a1eb92d79df396eea8658b778f4bc0f010da48e1d26e3fc55d83e9c7 • b6ac7f6e3b03acd364123a07b2122d943c4111ac4786bb188d94eae0e5b22c02 • bb74c6fc0323956dd140988372c412f8b32735fb0ed1ad416e367d29c06af9cc • c437e5caa4f644024014d40e62a5436c59046efc76c666ea3f83ab61df615314

	Domain	• uhsee[.]com • kongtuke[.]com
	IP	• 80.66.88[.]146 • 185.49.69[.]41

Recommendations	• Block all threat indicators at your respective controls. • Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls. • Never trust or open links and attachments received from unknown sources/senders. • Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway. **NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.**
References	• https://cybersecuritynews[.]com/badspace-malware-high-ranking-sites/ • https://thehackernews[.]com/2024/06/hackers-exploit-legitimate-websites-to.html