Mphasis SOC – Information Security News
Date & Time Issued: 22-06-2024, 18:30 IST

Title	**Hackers Use Weaponized Lnk File to Deploy AutoIt Malware.**
Summary	• Hackers have been found utilizing weaponized LNK files to deploy a strain of AutoIt malware, raising alarms across the cybersecurity community.
Severity	Medium
Attack Vectors	• The infection chain begins with a seemingly innocuous LNK file, which, upon closer inspection, reveals a malicious command disguised as an image file. This command is designed to download and execute an HTA file using PowerShell from a remote server. • To function, the HTA file must contain readable script code. After searching for the term “script,” JavaScript code was found and beautified. This code contained a string of ASCII characters in decimal format, which appeared to be encoded. Researchers could automatically deobfuscate the code using the Chrome console, revealing a custom encoding process. • The malware’s code was further encrypted with the AES algorithm. Decrypting this layer unveiled Layer 2 PowerShell commands. To reach the final layer, Layer 3, the encrypted string in the Maf function, considered the main function, had to be decrypted using PowerShell. • The payload, solaris.exe, was downloaded from the remote server and inspected with Detect it Easy, revealing an embedded ZIP file. After extraction, the first file, named United, contained obfuscated CMD commands. A custom script was written to parse these commands, making them readable and revealing their functions, which included process checks, file operations, and pinging the local host.

Indicator of Compromise	INDICATOR TYPE	INDICATORS
	File Hash	• 848164d084384c49937f99d5b894253e • 3d89cbe9713713fc038093637a602b29 • 21a3a0d9aaae768fb4104c053db5ba98 • 848164d084384c49937f99d5b894253e • 80376f01128e490f9d69dc67c724104f • 5d9e35b2d9e36e9ba926fd73260feabc • 8ab6a7b4be9af49dc2af1589644d1380 • 8e6f4ac729932bc4ca1528848ac18f1b • c05ecddfe47cf14835932fba0cc1d3e1 • 848164d084384c49937f99d5b894253e • 1a189425d72fd5d2cb9045ffdfcb7c31 • 7e012cfad9fc2540936792e39cfeb683 • 6cef3ef2026901b5a99b1e19e3c01839 • 034a0c0440743b5596be0c6fe4f6c4e5
	Domains	• mw-solaris[.]com
	IP	• 91[.92.251].35

Recommendations	• Block all threat indicators at your respective controls. • Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls. • Be cautious when downloading and installing software, especially from untrusted sources. • Regularly update your security software and keep your operating system patched. • Educate users about the risks associated with downloading and running MSI files from unknown origins. **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://gbhackers.com/hackers-use-weaponized/ • https://gbhackers.com/weaponizing-windows-phishing/#google_vignette