The Darkgate Menace: Leveraging Autohotkey & Attempt to Evade Smartscreen

Date: 01st May 2024 | Severity: High

Summary

McAfee Labs has recently uncovered a novel infection chain associated with DarkGate malware. This chain commences with an HTML-based entry point and progresses to exploit the AutoHotkey utility in its subsequent stages. DarkGate, a Remote Access Trojan (RAT) developed using Borland Delphi, has been marketed as a Malware-as-a-Service (MaaS).

This malicious software boasts an array of functionalities, such as process injection, file download and execution, data theft, shell command execution, keylogging capabilities, among others. DarkGate notably circumvented Microsoft Defender SmartScreen, prompting Microsoft to subsequently release a patch to address this vulnerability.

DarkGate was observed being distributed in phishing email campaigns, in which a Windows Defender SmartScreen vulnerability (CVE-2024-21412) was leveraged to bypass security checks and automatically install malicious software installers.

Attack Vectors

- CVE-2023-36025 is a vulnerability impacting Microsoft Windows Defender SmartScreen. This flaw arises from the absence of proper checks and corresponding prompts related to Internet Shortcut (.url) files. Cyber adversaries exploit this vulnerability by creating malicious .url files capable of downloading and executing harmful scripts, effectively evading the warning and inspection mechanisms of Windows Defender SmartScreen. This year, same way, CVE-2024-21412 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412) was identified and patched. This vulnerability is about “Internet Shortcut Files Security Feature Bypass Vulnerability”.
- McAfee Labs has identified two distinct initial vectors carrying identical DarkGate shellcode and payload. The first vector originates from an HTML file, while the second begins with an XLS file.
- The infection chain initiates with a phishing HTML page masquerading as a Word document. Users are prompted to open the document in “Cloud View” creating a deceptive lure for unwitting individuals to interact with malicious content.
- The vulnerability CVE-2023-36025 (https://nvd.nist.gov/vuln/detail/CVE-2023-36025) pertains to Microsoft Windows Defender SmartScreen failing to issue a security prompt prior to executing a .url file from an untrusted source. Attackers exploit this by constructing a Windows shortcut (.url) file that sidesteps the SmartScreen protection prompt. This evasion is achieved by incorporating a script file as a component of the malicious payload delivery mechanism. Although Microsoft has released a patch https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025 to address this vulnerability, it remains exploitable in unpatched versions of Windows.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 196bb36f7d63c845afd40c5c17ce061e320d110f28ebe8c7c998b9e6b3fe1005 • 038db3b838d0cd437fa530c001c9913a1320d1d7ac0fd3b35d974a806735c907 • 897b0d0e64cf87ac7086241c86f757f3c94d6826f949a1f0fec9c40892c0cecb • dd7a8b55e4b7dc032ea6d6aed6153bec9b5b68b45369e877bb66ba21acc81455 • 6ed1b68de55791a6534ea96e721ff6a5662f2aefff471929d23638f854a80031 • 1a960526c132a5293e1e02b49f43df1383bf37a0bbadd7ba7c106375c418dad4 • 2e34908f60502ead6ad08af1554c305b88741d09e36b2c24d85fd9bac4a11d2f
IP Address	• 5.252.177[.]207 • 103.124.106[.]237 • 170.130.55[.]130 • 45.89.53[.]187

Recommendation

- Verify Sender Information
- Think Before Clicking Links and Warnings
- Check for Spelling and Grammar Errors
- Be Cautious with Email Content
- Verify Unusual Requests
- Use Email Spam Filters
- Check for Secure HTTP Connections
- Delete Suspicious Emails
- Keep Windows and Security Software Up to date

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.

Reference Link

- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/the-darkgate-menace-leveraging-autohotkey-attempt-to-evade-smartscreen/