


## Mphasis SOC – Information Security News

### Date & Time Issued: 06-JUL-2024, 19:00 IST

<b>Title</b>	<b>Exploiting_Microsoft_SmartScreen_vulnerability</b>	
<b>Summary</b>	<ul style="list-style-type: none"> <li>• Cyble Research and Intelligence Labs (CRIL) recently came across an active campaign exploiting the Microsoft SmartScreen vulnerability (CVE-2024-21412).</li> <li>• The ongoing campaign targets multiple regions, including Spain, the US, and Australia.</li> <li>• It employs lures related to healthcare insurance schemes, transportation notices, and tax-related communications to deceive individuals and organizations into downloading malicious payloads onto their machines.</li> <li>• The infection starts with a spam email containing a link that redirects users to a WebDAV share using a search protocol, deceiving them into executing a malicious internet shortcut file, exploiting CVE-2024-21412.</li> <li>• The threat actors (TAs) conducted a multi-stage attack utilizing legitimate tools such as forfiles.exe, PowerShell, mshta, and other trusted files to circumvent security measures.</li> <li>• The attack chain utilizes DLL sideloading and IDATLoader to inject the final payload into explorer.exe.</li> <li>• This campaign delivers Lumma and Meduza Stealer as its final payloads.</li> </ul>	
<b>Severity</b>	Medium 	
<b>Attack Vectors</b>	<ul style="list-style-type: none"> <li>• The Zero Day Initiative (ZDI) uncovered a sophisticated DarkGate campaign in mid-January 2024, exploiting CVE-2024-21412 through fake software installers.</li> <li>• On February 13, 2024, Microsoft patched this Microsoft Defender SmartScreen vulnerability, which involved internet shortcuts. Later, the APT group known as Water Hydra has been leveraging CVE-2024-21412 in a targeted campaign against financial market traders, bypassing SmartScreen to deploy the DarkMe remote access trojan (RAT).</li> <li>• The initial infection starts with a spam email that appears to come from a trusted source. The email is crafted to entice the recipient into clicking a link, which tricks the user into viewing an internet shortcut file hosted on a remote WebDAV share. When the user double-clicks the internet shortcut file, it exploits CVE-2024-21212 and executes another LNK file hosted on the same WebDAV share, initiating the infection process.</li> <li>• This attack employs a multifaceted approach, utilizing various script files, including PowerShell and JavaScript, to deliver the final payload. This multi-stage process ultimately culminates in the deployment of malicious payloads like Lumma and Meduza Stealer, both of which focus on collecting sensitive information from the victim's machine.</li> <li>• The threat actor targets a wide array of individuals and organizations across various regions and sectors. Based on the lure documents observed in this campaign, the threat actor targets Spanish taxpayers, transportation companies with emails purportedly from the US Department of Transportation, and individuals in Australia by mimicking official Medicare enrollment forms, as shown in the images below.</li> </ul>	
<b>Indicator of Compromise</b>	INDICATOR TYPE	INDICATORS
	File Hash	<ul style="list-style-type: none"> <li>• 473abb2c272295473e5556ec7dec06f2018c0a67f208d8ab33de1fb6d40895f5</li> <li>• 81e89754ae2324c684fce71acafc30f8085870be947e7a76971b4fec1b24b5d1</li> <li>• 7ee31fa89e9e68f20004bdc31f8f05a95861b6c678bfa3b57f09dfad9ef5290</li> <li>• 6481462f15ad4213f83a3d28304f14496bae1feb8580056959a657d0ee8981db</li> <li>• 4eccb7813cee8c8039424aebf69f4269d4a6c2c72d81a001254bcdce80034555</li> <li>• 2460e7590e09af09ced6f75c001a9066c18629d956edbe8041f08cd21b7528b2</li> <li>• aceee450c55d61671c2d3d154b5f77e7f99688b6da8a8f3256a4bae2cdb76a4c</li> <li>• 268a0de2468726a106fd92563a846e764f2ba313e37b5fc0cf76171b0a363f6f</li> <li>• 58e2b766dec37cc5fcfb63bc16d69627cd87e7e46f0b9f48899889479f12611e</li> </ul>

<b>Recommendations</b>	<ul style="list-style-type: none"><li>• Block all threat indicators at your respective controls.</li><li>• Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.</li><li>• Never trust or open links and attachments received from unknown sources/senders.</li><li>• Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway.</li></ul> <p><b>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.</b></p>
<b>References</b>	<ul style="list-style-type: none"><li>• <a href="https://cyble.com/blog/increase-in-the-exploitation-of-microsoft-smartscreen-vulnerability-cve-2024-21412/">https://cyble.com/blog/increase-in-the-exploitation-of-microsoft-smartscreen-vulnerability-cve-2024-21412/</a></li></ul>
<p>The information contained in this message is proprietary. It is for Mphasis and its customers only. Copyright © 2024. All rights reserved by Mphasis.</p>	