


## Mphasis SOC – Information Security News

### Date & Time Issued: 04-JUL-2024, 14:30 IST

<b>Title</b>	<b>New Orcinius Trojan Uses VBA Stomping to Mask Infection</b>	
<b>Summary</b>	<ul style="list-style-type: none"> <li>• This multi-stage trojan utilizes Dropbox and Google Docs to update and deliver payloads.</li> <li>• It uses the VBA stomping technique, removing the VBA source code in a Microsoft Office document, leaving only compiled p-code.</li> <li>• It contains an obfuscated VBA macro that hooks into Windows to monitor running windows and keystrokes and creates persistence using registry keys.</li> </ul>	
<b>Severity</b>	Medium 	
<b>Attack Vectors</b>	<ul style="list-style-type: none"> <li>• This is a multi-stage trojan that is using Dropbox and Google Docs to download second-stage payloads and stay updated.</li> <li>• The initial infection method is an Excel spreadsheet, in this case, "CALENDARIO AZZORTI.xls".</li> <li>• The file appears to be an Italian calendar with three worksheets that discuss billing cycles in various cities.</li> <li>• The file has a VBA macro that has been modified with a technique called 'VBA stomping', where the original source code is destroyed, leaving only compiled p-code.</li> <li>• This means that viewing the macro within the document will show either nothing or a harmless version of the code that will run when opening (and closing) the file.</li> <li>• On runtime, the file will run the macro and perform the following actions:</li> <li>• Check registry keys and write a new key to hide warnings.</li> <li>• "HKCU\Software\Microsoft\Office\Excel\Security\VBAWarnings"</li> <li>• "HKCU\Software\Microsoft\Office\Word\Security\VBAWarnings"</li> <li>• Enumerate windows currently running using EnumThreadWindows</li> <li>• Set up persistence by writing a key to HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems</li> <li>• Reach out to both encoded URLs and attempt to download using WScript.Shell</li> <li>• Use SetWindowsHookEx to monitor keyboard input.</li> <li>• Create a few randomized timers for activation and download attempts.</li> </ul>	
<b>Indicator of Compromise</b>	INDICATOR TYPE	INDICATORS
	File Hash	<ul style="list-style-type: none"> <li>• 28dd92363338b539aee00df283e20666ad1bdee90d78c6376f615a0b9481f97</li> </ul>
	Url	<ul style="list-style-type: none"> <li>• www-env.dropbox-dns[.]com</li> <li>• hxxps://docs.google[.]com/uc?id=0BxsMXGfPIZfSVzUyaHFYvkQxeFk&amp;export=download</li> <li>• hxxps://www.dropbox.com/s/zhp1b06imehwylq/Synaptics.rar?dl=1</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://blog.sonicwall.com/en-us/2024/06/new-orcinius-trojan-uses-vba-stomping-to-mask-infection/?&amp;web_view=true">https://blog.sonicwall.com/en-us/2024/06/new-orcinius-trojan-uses-vba-stomping-to-mask-infection/?&amp;web_view=true</a></li></ul>
<p>The information contained in this message is proprietary. It is for Mphasis and its customers only. Copyright © 2023. All rights reserved by Mphasis.</p>	