

<b>NCA-240522-03</b>	<b>ADVISORY ON FAKE WINDOWS 11 UPGRADE TO DISTRIBUTE VIDAR MALWARE</b>
<b>Overview</b>	
<p>Hackers are tricking users with fraudulent domains, masquerading as Microsoft's Windows 11 download portal in attempt to make users deploy trojanized installation files which infect systems with the Vidar information stealer malware. This malware, primarily, steals sensitive data and spies on victims.</p>	
<b>Impact</b>	
<p>When a victim accidentally installs the downloaded file, it sets up a remote command and control server to retrieve data from the system. The malware locates and steals a victim's sensitive information, including online account credentials, browser history, and financial information, before deleting itself from the system.</p>	
<b>Preventive Measures</b>	
<ul style="list-style-type: none"><li>• Avoid cracked and free version software's and sites.</li><li>• Download software's only from vendor websites.</li><li>• Install legit and updated versions of Anti-virus and Anti-malware software.</li></ul>	

For further enquiries, please contact CERRT.NG through the following channels:

**E-mail:** [cerrt@nitda.gov.ng](mailto:cerrt@nitda.gov.ng)

**Phone:** +2348178774580

**Web:** [www.cerrt.ng](http://www.cerrt.ng)