

Forum:[Hack Forums](#)

Thread: [Legacy Windows Tool MSHTA Fuels Surge in Silent Malware Attacks](#)

MadScientist - May 27, 2026, 10:40 am

MSHTA (Microsoft HTML Application) has been a part of Windows since 1999 and the release of Win98 SE and Internet Explorer 5.0. It has remained part of Windows throughout, including the latest current releases. It also continues to run with the Edge browser through the IE mode. The purpose is to conform to Microsoft's policy of prioritizing backward compatibility.

Over the years, legitimate use of MSHTA has declined. Abuse, however, has grown. MSHTA is increasingly used by bad actors as a Living-off-the-Land binary (LOLBIN) to silently deliver a growing range of malware – ranging from commodity stealers and loaders to advanced and persistent malware such as PurpleFox.

Since the start of this year, Bitdefender has detected a dramatic rise in MSHTA-related activity. The firm believes this reflects increased threat actor use rather than renewed administrative adoption. MSHTA

MSHTA is designed to execute HTML application (HTA) files, which are programs written in HTML, VBScript or JavaScript. An HTA file loaded from an offsite server can be manipulated to run VBScript in memory. The local server would only see the activity of a trusted and MS-signed binary, not what is happening in memory. Because of that trust and the continued legitimate use, it would be difficult to block automatically. The result is that invisible malicious code could be introduced, and that code could then download further LOLBIN components ultimately leading to the implementation of dangerous malware.

“MSHTA provides attackers with a built-in, Microsoft-signed utility that can retrieve and execute remote script content during the initial or intermediate stages of an infection chain,” reports Bitdefender.

Attackers start the process through basic social engineering.

Read More -

<https://www.securityweek.com/legacy-windows-tool-mshta-fuels-surge-in-silent-malware-attacks/>