Research report: VBScript

Introduction:

Microsoft Visual Basic Scripting Edition, also known as VBScript or just VBS is a deprecated active scripting language, based on Visual Basic. It was developed by Microsoft and used in their Windows operating system, as a tool for system administration, and additional applications. It has effectively been replaced or superseded in its former functions and now exists in legacy products and systems. Specifically, the Powershell scripting language has taken over it's key previous functions for OS interaction and .NET for other tasks (3).

Along with its system admin tasks such as automating processes and writing macros, it can be used in web development and functions similar to JavaScript, albeit only supported by Internet Explorer. Client side, it interacts with HTML pages using the document object model (DOM), server side applications can be developed using active server pages (ASP).

Malware can be written using VBScript which can execute on a victims Windows instance, performing various malicious actions including steps to install malware and establish its persistence (5).

Overview:

Rarity:

This is difficult to quantify due to the broad nature of the malware described, but is likely to increase in rarity as the scattered remnants of VBScript support in the Windows/ IE ecosystem die off piecemeal.

Earlier malware appears to have relied on browser exploits to distribute their malware, but increases to browser security measures and general awareness have led to attackers employing social-engineering to better target victims (3). According to Microsoft research, malicious VBScript files remain the second most encountered by Windows users as recently as 2019, although they conclude that malicious scripts are not a prevalent form of malware (3). While McAfee labs' research suggests that traditional file-based malware remains significant in its scope. (4)

Risk:

Mitigation largely relies on user awareness now due to the rise of socially engineered emails and risk will likely be determined by the general awareness of the user (3).

Impact:

Potentially severe, for individuals, VBScript malware has been used recently in attacks which steal funds, identity and access credentials from users (7). A new loader from 2023 for VBScript malware features hidden VNC and browser history theft (7).

OS affected:

Operating systems affected by VBScript malware are of the Microsoft Windows line, internet exposed instances post 1996 (3).

History:

VBScript was originally released in 1996 and attempted to compete with ECMAscript (more commonly known as JavaScript) in the web market, it was able to run in Internet Explorer serving effectively the same function. In July 2019, with a weekly patch to IE version 11, Microsoft disabled VBScript in browser. Although not fully clarified, it is speculated that the retirement is intended to remove one potential attack surface and close off a loose end (2).

VBScript would also be used across Windows systems for various tasks in the years before the introduction of Powershell and .NET which replaced its original use cases and led to its eventual supersession.

In October 2023 Microsoft announced that VBScript support will be officially deprecated in a future release of Windows (1). It currently exists as a ‘feature on demand’, that is, disabled by default. To be fully removed in a later release (1).

From the time of its release, VBScript would become a vector for malware, with malware such as Lokibots, Qbot, DarkGate and Emotet rising to prominence, some of these continue to be deployed in attacks as of 2023 (8).

Likely the most famous of VBScript malware is the ILOVEYOU worm, a widespread malicious script which spread via IRC messaging and email. It used VBScript to corrupt or erase files on victims’ hard drives, then spread itself to victims’ contacts (6).

Emotet and Lokibots, delivered via DarkGate are modern, notorious examples of malware. Emotet was a prominent botnet shut down in 2021, which resurfaced in 2023 featuring adaptations (8).

Technical:

TBC

Summary:

TBC

References:

1. https://learn.microsoft.com/en-us/windows/whats-new/deprecated-features
2. https://blogs.windows.com/msedgedev/2015/05/06/a-break-from-the-past-part-2-saying-goodbye-to-activex-vbscript-attachevent/

3. https://www.microsoft.com/en-us/research/uploads/prod/2020/12/VbsNet_Icassp2020.pdf
4. https://partners.trellix.com/enterprise/en-us/assets/reports/rp-quarterly-threats-sept-2017.pdf
5. https://doi.org/10.1016/j.procs.2018.10.127
6. https://www.kaspersky.com/blog/cybersecurity-history-iloveyou/45001/
7. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-266a
8. https://www.kaspersky.com/about/press-releases/2023_emotet-returns-lokibot-persists-kaspersky-reports-on-new-infection-methods
9.