



Agenda


- Who are we?
- IIS-sassins
- Atomics
- Detections
- Discussion
- Next time on *Atomics On A Friday*



Who Are We?




Michael Haag
Sr. Threat Connoisseur

 @M_Haggis



Paul Michaud
Principal Handler of Shenanigans

 @Burning_PM



 IIS-sassins



Why is this important?

Internet Information Services (IIS), a web server software produced by Microsoft, which is often used to host websites and web applications on Windows

Adversaries pop-shells on poorly maintained websites running IIS all the time

When the shell is dropped, behaviors happen

Including:

Persistence

Module installation

Post-exploitation

Cmd, PowerShell

Exfiltration

Bye Bye Credit Cards



IIS extensions are on the rise as backdoors to servers

Posted: July 27, 2022 by Pieter Arntz

July 26, 2022 • 13 min read

Malicious IIS extensions quietly open persistent backdoors into servers

Microsoft 365 Defender Research Team

December 12, 2022 • 10 min read

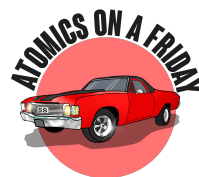
IIS modules: The evolution of web shells and how to detect them

Microsoft Security Threat Intelligence



As defenders:

- We need to understand how adversaries abuse IIS
- We need to know how to find IIS modules
- How to simulate adversary tradecraft
- We need to understand what behaviors occur from IIS when shells drop
- Ultimately, how to prevent this from happening



Related Reading

- <https://www.microsoft.com/en-us/security/blog/2022/07/26/malicious-iis-extensions-quietly-op-en-persistent-backdoors-into-servers/>
- <https://www.microsoft.com/en-us/security/blog/2022/12/12/iis-modules-the-evolution-of-web-s-hells-and-how-to-detect-them/>
- <https://www.crowdstrike.com/wp-content/uploads/2022/05/crowdstrike-iceapple-a-novel-internet-information-services-post-exploitation-framework-1.pdf>
- <https://securelist.com/the-sessionmanager-iis-backdoor/106868/>

Public IIS Modules to Test

MDSec [IIS-Raid](#)



What are IIS Modules?

T1505.004 Server Software Component: IIS Components

Native Modules

A native module is typically going to be a DLL deployed to the server and loaded up via IIS Administration Tool, **PowerShell** or AppCmd.

All three of these installation methods result in the module entry being added to the <globalModules> IIS configuration section in
%windir%\system32\inetsrv\config\applicationhost.config

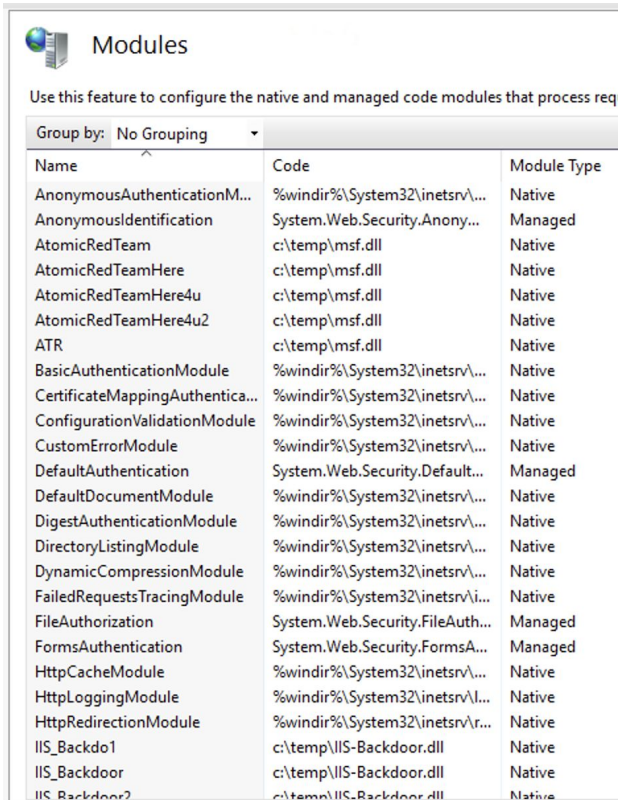
Managed Modules

Do not require installation, and can be enabled directly for each application. This allows applications to include their managed modules directly within the application by registering them in the application's web.config file.

%windir%\system32\inetsrv\config\applicationhost.config, and searching for the string "<modules>".



How do I find IIS Modules?



Name	Code	Module Type
AnonymousAuthenticationM...	%windir%\System32\inetsrv\...	Native
AnonymousIdentification	System.Web.Security.Anony...	Managed
AtomicRedTeam	c:\temp\msf.dll	Native
AtomicRedTeamHere	c:\temp\msf.dll	Native
AtomicRedTeamHere4u	c:\temp\msf.dll	Native
AtomicRedTeamHere4u2	c:\temp\msf.dll	Native
ATR	c:\temp\msf.dll	Native
BasicAuthenticationModule	%windir%\System32\inetsrv\...	Native
CertificateMappingAuthentica...	%windir%\System32\inetsrv\...	Native
ConfigurationValidationModule	%windir%\System32\inetsrv\...	Native
CustomErrorModule	%windir%\System32\inetsrv\...	Native
DefaultAuthentication	System.Web.Security.Default...	Managed
DefaultDocumentModule	%windir%\System32\inetsrv\...	Native
DigestAuthenticationModule	%windir%\System32\inetsrv\...	Native
DirectoryListingModule	%windir%\System32\inetsrv\...	Native
DynamicCompressionModule	%windir%\System32\inetsrv\...	Native
FailedRequestsTracingModule	%windir%\System32\inetsrv\i...	Native
FileAuthorization	System.Web.Security.FileAuth...	Managed
FormsAuthentication	System.Web.Security.FormsA...	Managed
HttpCacheModule	%windir%\System32\inetsrv\...	Native
HttpLoggingModule	%windir%\System32\inetsrv\l...	Native
HttpRedirectionModule	%windir%\System32\inetsrv\r...	Native
IIS_Backdoor1	c:\temp\IIS-Backdoor.dll	Native
IIS_Backdoor	c:\temp\IIS-Backdoor.dll	Native
IIS_Backdoor2	c:\temp\IIS-Backdoor.dll	Native

```
PS C:\Users\Administrator> C:\Windows\System32\inetsrv\appcmd.exe list modules
MODULE "IsapiFilterModule" ( native, preCondition: )
MODULE "BasicAuthenticationModule" ( native, preCondition: )
MODULE "IsapiModule" ( native, preCondition: )
MODULE "HttpLoggingModule" ( native, preCondition: )
MODULE "HttpCacheModule" ( native, preCondition: )
MODULE "DynamicCompressionModule" ( native, preCondition: )
MODULE "StaticCompressionModule" ( native, preCondition: )
```

```
PS C:\Users\Administrator> Get-WebGlobalModule
```

Name	Image
----	-----
HttpLoggingModule	%windir%\System32\inetsrv\loghttp.dll
UriCacheModule	%windir%\System32\inetsrv\cachuri.dll
FileCacheModule	%windir%\System32\inetsrv\cachfile.dll
TokenCacheModule	%windir%\System32\inetsrv\cachtokn.dll
HttpCacheModule	%windir%\System32\inetsrv\cachhttp.dll
DynamicCompressionModule	%windir%\System32\inetsrv\compdyn.dll
StaticCompressionModule	%windir%\System32\inetsrv\compstat.dll
DefaultDocumentModule	%windir%\System32\inetsrv\defdoc.dll



Log Sources

In the Microsoft [blog](#) it is recommended to enable advanced IIS logging to hunt for web shells. The **Microsoft-IIS-Configuration/Operational** log provides details on new modules being added.

- Lists additional logs available for IIS: `wevtutil el | findstr -i IIS`
- Configuration for the selected log: `wevtutil gl Microsoft-IIS-Configuration/Operational`
- Enable the selected log: `wevtutil sl /e:true Microsoft-IIS-Configuration/Operational`

```
PS C:\Windows\System32\inetsrv> wevtutil el | findstr -i IIS
Microsoft-IIS-Configuration/Administrative
Microsoft-IIS-Configuration/Analytic
Microsoft-IIS-Configuration/Debug
Microsoft-IIS-Configuration/Operational
Microsoft-IIS-Logging/Logs
Microsoft-Windows-IIS/Diagnostic
PS C:\Windows\System32\inetsrv> wevtutil gl Microsoft-IIS-Configuration/Operational
name: Microsoft-IIS-Configuration/Operational
enabled: true
type: Operational
owningPublisher: Microsoft-Windows-IIS-Configuration
isolation: Custom
channelAccess: 0:BAG:SYD:PARAI(A;;FA;;;BA)
logging:
  logFileName: %SystemRoot%\System32\winevt\Logs\Microsoft-IIS-Configuration%4Operational.evtx
  retention: false
  autoBackup: false
  maxSize: 1052672
publishing:
  fileMax: 1
PS C:\Windows\System32\inetsrv>
```



Ship The Data

For Splunk: <https://gist.github.com/MHaggis/64396dfd9fc3734e1d1901a8f2f07040>

Once enabled, make a new Splunk App and deploy.

Inputs.conf

```
[WinEventLog://Microsoft-IIS-Configuration/Operational]
index=win
sourcetype=IIS:Configuration:Operational
disabled = false
###
# Modify cron schedule as you like. Default is once daily.
# Modify index as needed.
# We recommend this method over the other options provided.
###
[powershell://IISModules]
script = Get-WebGlobalModule
schedule = */1 * * * *
#schedule = 0 0 * * *
sourcetype = Pwsh:InstalledIISModules
index=iis
```



Atomic Testing

- [T1505.004](#) -testnumbers 1
- [T1505.004](#) -testnumbers 2
- [T1562.002](#) -testnumber 1
- [T1562.002](#) -testnumber 2

T1505.004

```
%windir%\system32\inetsrv\appcmd.exe install module /name:AoaF  
/image:%windir%\system32\inetsrv\defdoc.dll
```

```
New-WebGlobalModule -Name AoaF_module -Image  
%windir%\system32\inetsrv\defdoc.dll
```

T1562.002

```
C:\Windows\System32\inetsrv\appcmd.exe set config "Default Web Site"  
/section:httplogging /dontLog:true
```

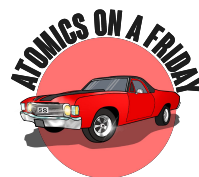
```
set-WebConfigurationProperty -PSPath "IIS:\Sites\Default Web Site\  
-filter "system.webServer/httpLogging" -name dontLog -value $true
```

Bonus points:

```
Set-itemProperty -Path 'IIS:\Sites\Default Web Site' -Name  
Logfile.enabled -Value $false
```

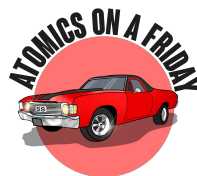


DEMO



AppCmd Add New Module

<div>New Search</div> <pre> tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes where NOT (Processes.parent_process_name IN ("msiexec.exe", "iissetup.exe")) Processes.process_name=appcmd.exe Processes.process IN ("*install.*", "*module.*") AND Processes.process="*image*" by Processes.dest Processes.user Processes.parent_process_name Processes.process_name Processes.original_file_name Processes.process_id Processes.parent_process_id `drop_dm_object_name(Processes)` `security_content_ctime(firstTime)` `security_content_ctime(lastTime)`</pre>							
✓ 30 events (12/1/22 12:00:00.000 AM to 12/31/22 3:11:30.000 PM) No Event Sampling ▼ Jo							
Events (30) Patterns <u>Statistics (30)</u> Visualization							
20 Per Page ▼ ✓ Format Preview ▼							
dest ▼	user ▼	parent_process_name ▼	process_name ▼	original_file_name ▼	process ▼	process_id ▼	parent_proce ▼
win-dc-exch01.attackrange.local	Administrator	cmd.exe	appcmd.exe	appcmd.exe	c:\windows\system32\inetsrv\appcmd.exe install module /name:AtomicRedTeamHere4u2 /image:c:\temp\msf.dll	5552	11172
win-dc-exch01.attackrange.local	administrator	cmd.exe	appcmd.exe	unknown	c:\windows\system32\inetsrv\appcmd.exe install module /name:AtomicRedTeamHere /image:c:\temp\msf.dll	0x3404	0x2ba4
win-dc-exch01.attackrange.local	administrator	cmd.exe	appcmd.exe	unknown	c:\windows\system32\inetsrv\appcmd.exe install module /name:AtomicRedTeam /image:c:\temp\msf.dll	0x352c	0x2ba4
win-dc-exch01.attackrange.local	administrator	cmd.exe	appcmd.exe	unknown	c:\windows\system32\inetsrv\appcmd.exe install module /name:AtomicRedTeam /image:c:\temp\msf.dll	0x4ab0	0x2ba4
win-dc-exch01.attackrange.local	administrator	cmd.exe	appcmd.exe	unknown	C:\Windows\System32\inetsrv\appcmd.exe install module /name:IIS_Backdoor3 /image:"c:\temp\IIS-Backdoor.dll"	0x48c	0x2ba4
win-dc-exch01.attackrange.local	administrator	cmd.exe	appcmd.exe	unknown	C:\Windows\System32\inetsrv\appcmd.exe install module /name:IIS_Backdoor2 /image:"c:\temp\IIS-Backdoor.dll" /add:true	0x2d18	0x2ba4
win-dc-exch01.attackrange.local	administrator	cmd.exe	appcmd.exe	unknown	C:\Windows\System32\inetsrv\appcmd.exe install module /name:IIS_Backdoor /image:"c:\temp\IIS-Backdoor.dll" /add:true	0x3870	0x2ba4
win-host-mhaag-attack-range-622	Administrator	powershell.exe	appcmd.exe	appcmd.exe	"C:\windows\system32\inetsrv\appcmd.exe" install module /name:IIS_Backdoor_no_xml2 /image:c:\windows\system32\inetsrv\IIS-Backdoor.dll	5808	4052
win-host-mhaag-attack-range-622	Administrator	powershell.exe	appcmd.exe	unknown	"C:\windows\system32\inetsrv\appcmd.exe" install module /name:IIS_Backdoor_no_xml2 /image:c:\windows\system32\inetsrv\IIS-Backdoor.dll	0x16b0	0xfd4



PowerShell - WebGlobalModule

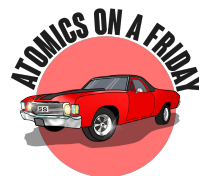
```
'powershell' EventCode=4104 ScriptBlockText IN("*New-WebGlobalModule*", "*Enable-WebGlobalModule*", "*Set-WebGlobalModule*")
| stats count min(_time) as firstTime max(_time) as lastTime by EventCode ScriptBlockText Computer user_id
| 'security_content_ctime(firstTime)'
| 'security_content_ctime(lastTime)'
```

✓ 5 events (12/1/22 12:00:00.000 AM to 12/31/22 3:13:34.000 PM) No Event Sampling ▼

Events (5) Patterns **Statistics (5)** Visualization

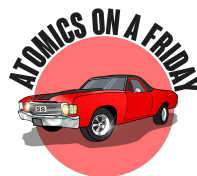
20 Per Page ▼ ✎ Format Preview ▼

EventCode ↕ ✎	ScriptBlockText ↕	Computer ↕
4104	Get-Help Set-WebGlobalModule -Online	win-dc-exch01.attacker
4104	New-WebGlobalModule -Name "testGlobalModule" -Image "c:\test\test.dll"	win-dc-exch01.attacker
4104	get-help Set-WebGlobalModule	win-dc-exch01.attacker
4104	get-help Set-WebGlobalModule -all	win-dc-exch01.attacker
4104	get-help Set-WebGlobalModule -full	win-dc-exch01.attacker



New: IIS Operational Logs

sourcetype="IIS:Configuration:Operational" EventCode=29 stats count min(_time) as firstTime max(_time) as lastTime by OpCode EventCode ComputerName Message rename ComputerName AS dest 'security_content_ctime(firstTime)' 'security_content_ctime(lastTime)'				
✓ 118 events (12/1/22 12:00:00.000 AM to 12/31/22 3:16:29.000 PM) No Event Sampling ▾ Job ▾				
Events (118) Patterns Statistics (73) Visualization				
20 Per Page ▾ Format Preview ▾				
OpCode ▾	EventCode ▾	dest ▾	Message ▾	
Info	29	win-dc-exch01.attackrange.local	Changes to '/system.applicationHost/applicationPools/add[@name="test"]' at 'MACHINE/WEBROOT/APPHOST' have successfully been committed.	
Info	29	win-dc-exch01.attackrange.local	Changes to '/system.applicationHost/applicationPools/add[@name="test"]/@name' at 'MACHINE/WEBROOT/APPHOST' have successfully been committed.	
Info	29	win-dc-exch01.attackrange.local	Changes to '/system.applicationHost/sites/site[@name="shell" and @id="3"]/application[@path="/"]/virtualDirectory[@path="/shell"]' at 'MACHINE/WEBROOT/APPHOST' have successfully been committed.	
Info	29	win-dc-exch01.attackrange.local	Changes to '/system.applicationHost/sites/site[@name="shell" and @id="3"]/application[@path="/"]/virtualDirectory[@path="/shell"]/@path' at 'MACHINE/WEBROOT/APPHOST' have successfully been committed.	
Info	29	win-dc-exch01.attackrange.local	Changes to '/system.applicationHost/sites/site[@name="test" and @id="4"]' at 'MACHINE/WEBROOT/APPHOST' have successfully been committed.	
Info	29	win-dc-exch01.attackrange.local	Changes to '/system.applicationHost/sites/site[@name="test" and @id="4"]/@id' at 'MACHINE/WEBROOT/APPHOST' have successfully been committed.	
Info	29	win-dc-exch01.attackrange.local	Changes to '/system.applicationHost/sites/site[@name="test" and @id="4"]/@name' at 'MACHINE/WEBROOT/APPHOST' have successfully been committed.	
Info	29	win-dc-exch01.attackrange.local	Changes to '/system.applicationHost/sites/site[@name="test" and @id="4"]/application[@path="/"]' at 'MACHINE/WEBROOT/APPHOST' have successfully been committed.	
Info	29	win-dc-exch01.attackrange.local	Changes to '/system.applicationHost/sites/site[@name="test" and @id="4"]/application[@path="/"]/@applicationPool' at 'MACHINE/WEBROOT/APPHOST' have successfully been committed.	
Info	29	win-dc-exch01.attackrange.local	Changes to '/system.applicationHost/sites/site[@name="test" and @id="4"]/application[@path="/"]/@path' at 'MACHINE/WEBROOT/APPHOST' have successfully been committed.	
Info	29	win-dc-exch01.attackrange.local	Changes to '/system.applicationHost/sites/site[@name="test" and @id="4"]/application[@path="/"]/virtualDirectory[@path="/"]' at 'MACHINE/WEBROOT/APPHOST' have successfully been committed.	
Info	29	win-dc-exch01.attackrange.local	Changes to '/system.applicationHost/sites/site[@name="test" and @id="4"]/application[@path="/"]/virtualDirectory[@path="/"]/@path' at 'MACHINE/WEBROOT/APPHOST' have successfully been committed.	
Info	29	win-dc-exch01.attackrange.local	Changes to '/system.applicationHost/sites/site[@name="test" and @id="4"]/application[@path="/"]/virtualDirectory[@path="/"]/@physicalPath' at 'MACHINE/WEBROOT/APPHOST' have successfully been committed.	



Module Failing to Load

```
`wineventlog_application` EventCode=2282 | stats count min(_time) as firstTime max(_time) as lastTime by EventCode dest Name ModuleDll | `security_content_ctime(firstTime)` | `security_cor`
```

82,296 of 82,296 events matched No Event Sampling ▼

Events (82,296) Patterns **Statistics (1)** Visualization

20 Per Page ▼ Format Preview ▼

EventCode ↕	dest ↕	Name ↕	ModuleDll ↕	count ↕
2282	win-dc-exch01.attackrange.local	'Microsoft-Windows-IIS-W3SVC-WP'	c:\temp\msf.dll	69788



Pwsh Script Input

```
[powershell://IISModules]
script = Get-WebGlobalModule
schedule = */1 * * * *
#schedule = 0 0 * * *
sourcetype = Pwsh:InstalledIISModules
index=iis
```

index=iis sourcetype="Pwsh:InstalledIISModules" | stats count min(_time) as firstTime max(_time) as lastTime by host name image | rename host as dest | "security_console"

✓ 204,313 events (12/11/22 12:00:00.000 AM to 12/24/22 12:00:00.000 AM) No Event Sampling ▼

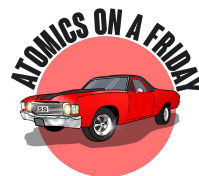
Events (204,313) Patterns **Statistics (44)** Visualization

20 Per Page ▼ Format Preview ▼

dest ↕	name ↕	image ↕
WIN-DC-EXCH01	ATR	c:\temp\msf.dll
WIN-DC-EXCH01	AnonymousAuthenticationModule	%windir%\System32\inetsrv\authanon.dll
WIN-DC-EXCH01	AtomicRedTeam	c:\temp\msf.dll
WIN-DC-EXCH01	AtomicRedTeamHere	c:\temp\msf.dll
WIN-DC-EXCH01	AtomicRedTeamHere4u	c:\temp\msf.dll
WIN-DC-EXCH01	AtomicRedTeamHere4u2	c:\temp\msf.dll
WIN-DC-EXCH01	BasicAuthenticationModule	%windir%\System32\inetsrv\authbas.dll
WIN-DC-EXCH01	CertificateMappingAuthenticationModule	%windir%\System32\inetsrv\authcert.dll
WIN-DC-EXCH01	ConfigurationValidationModule	%windir%\System32\inetsrv\validcfg.dll
WIN-DC-EXCH01	CustomErrorModule	%windir%\System32\inetsrv\custerr.dll
WIN-DC-EXCH01	DefaultDocumentModule	%windir%\System32\inetsrv\defdoc.dll
WIN-DC-EXCH01	DigestAuthenticationModule	%windir%\System32\inetsrv\authmd5.dll
WIN-DC-EXCH01	DirectoryListingModule	%windir%\System32\inetsrv\dirlist.dll
WIN-DC-EXCH01	DynamicCompressionModule	%windir%\System32\inetsrv\compdyn.dll
WIN-DC-EXCH01	FailedRequestsTracingModule	%windir%\System32\inetsrv\iisfrec.dll
WIN-DC-EXCH01	FileCacheModule	%windir%\System32\inetsrv\cachfile.dll
WIN-DC-EXCH01	HttpCacheModule	%windir%\System32\inetsrv\cachhttp.dll
WIN-DC-EXCH01	HttpLoggingModule	%windir%\System32\inetsrv\loghttp.dll
WIN-DC-EXCH01	HttpRedirectionModule	%windir%\System32\inetsrv\redirect.dll
WIN-DC-EXCH01	IIS_Backdoor1	c:\temp\IIS-Backdoor.dll

Mitigations

- Patch web apps
- Move web servers into a DMZ and restrict internal access
- Use application control to dismiss any new binaries on disk
- Use a web application firewall, NGFW
- Move left: prevent the activity first
- <Insert all the tools>
- Inventory your Modules



Thank you

- Atomics
 - [T1505.004](#) -testnumbers 2
 - [T1562.002](#) -testnumber 1
 - [T1562.002](#) -testnumber 2
- Splunk Content
 - https://research.splunk.com/stories/iis_components/
- Reading
 - <https://www.microsoft.com/en-us/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/>
 - <https://www.microsoft.com/en-us/security/blog/2022/12/12/iis-modules-the-evolution-of-web-shells-and-how-to-detect-them/>
 - <https://www.crowdstrike.com/wp-content/uploads/2022/05/crowdstrike-iceapple-a-novel-internet-information-services-post-exploitation-framework-1.pdf>
- Coming REAL soon! Atomics on A Friday Github repo: <https://github.com/Atoms-on-A-Friday>

