Hunting In On-Premises Exchange Server Logs

Posted on October 7, 2022 | by m365guy | 2 comments

This will be a high-level summary of the different logs that can be found on an On-Premises Exchange server, which can be useful during an IR. For each log, I'll try to explain what we can achieve with it. Not all logs are useful, so I've only picked the one's that I'm aware of and believe are useful.

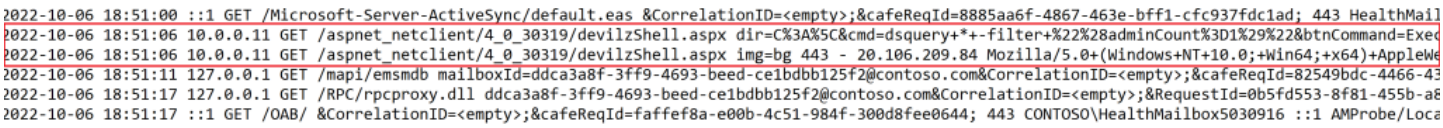
IIS logs

One of the useful logs on an Exchange server are the IIS logs. From hunting down **ProxyLogon** to **Webshell** activities. IIS logs can play a huge role in finding these suspicious activities. IIS logs are by default stored at the following location: **C:\inetpub\logs\LogFiles** and come with two folders. **W3SVC1** and **W3SVC2**. Both of these IIS log files contain all the GET and POST requests that are made. It also includes basic items such as IP and username, request date and time, service status and number of bytes received, as well as detailed items of target files.

This how the structure of the IIS log looks like with the all the fields.

```
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2022-10-06 07:13:03
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username
c-ip cs(User-Agent) cs(Referer) sc-status sc-substatus sc-win32-status time-
taken
```

Let's take a quick example of an **GET** request that was made by an attacker. The two lines that I've marked in highlight is the Webshell activity.



This how the entire result looks like:

```
2022-10-06 18:51:06 10.0.0.11 GET
/aspnet_netclient/4_0_30319/devilzShell.aspx dir=C%3A%5C&cmd=dsquery+*+-
filter+%22%28adminCount%3D1%29%22&btnCommand=Execute 443 - 20.106.209.84
Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+
(KHTML,+like+Gecko)+Chrome/106.0.0.0+Safari/537.36+Edg/106.0.1370.34
https://20.62.174.61/aspnet_netclient/4_0_30319/devilzShell.aspx?
dir=C%3A%5C&cmd=nltest+%2Fdomain_trusts+%2Fall_trusts&btnCommand=Execute 200
0 0 432
```

This is how we can interpret the data.

Date time	2022-10-06 18:51:06
s-ip	10.0.0.11 (This is the internal IP of the server)
cs-method	GET
cs-uri-stem	/aspnet_netclient/4_0_30319/devilzShell.aspx
cs-uri-query	dir=C%3A%5C&cmd=**dsquery**+*+-**filter**+%22%28**adminCount**%3D**1**%29%22&btnCommand=Execute
s-port	443
c-ip	20.106.209.84 (IP address of the attacker that initiated this request)
cs(User-Agent)	Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/106.0.0.0+Safari/537.36+Edg/106.0.1370.34
cs(Referer)	https://20.62.174.61/aspnet_netclient/4_0_30319/devilzShell.aspx?dir=C%3A%5C&cmd=nltest+%2Fdomain_trusts+%2Fall_trusts&btnCommand=Execut
sc-status	200

At this example, we are having a different Webshell. However, this time we are initiating a **POST** request.

```
2022-10-06 19:22:20 10.0.0.11 GET /owa/favicon.ico &CorrelationID=<empty>;&cafeReqId=18d2fcb0-7d4d-4a22-8113-0be36c349a57;&LogoffReason=NoCookiesGetOrE14Au
2022-10-06 19:22:20 10.0.0.11 GET /owa/auth/logon.aspx url=https%3a%2f%2f20.62.174.61%2fowa%2ffavicon.ico&reason=0&CorrelationID=<empty>;&cafeReqId=0a737b1
2022-10-06 19:22:22 10.0.0.11 GET /aspnet_netclient/4_0_30319/ - 443 - 20.106.209.84 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+l
2022-10-06 19:22:22 10.0.0.11 GET /favicon.ico &Owa302RedirectUri=/owa/favicon.ico 443 - 20.106.209.84 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKi
2022-10-06 19:22:22 10.0.0.11 GET /owa/favicon.ico &CorrelationID=<empty>;&cafeReqId=e60a4d4c-41e5-4beb-94cb-492ccac7eefc;&LogoffReason=NoCookiesGetOrE14Au
2022-10-06 19:22:22 10.0.0.11 GET /owa/auth/logon.aspx url=https%3a%2f%2f20.62.174.61%2fowa%2ffavicon.ico&reason=0&CorrelationID=<empty>;&cafeReqId=767bbef
2022-10-06 19:22:24 10.0.0.11 GET /aspnet_netclient/4_0_30319/POWERshell.aspx - 443 - 20.106.209.84 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/5
2022-10-06 19:22:24 10.0.0.11 GET /favicon.ico &Owa302RedirectUri=/owa/favicon.ico 443 - 20.106.209.84 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKi
2022-10-06 19:22:24 10.0.0.11 GET /owa/favicon.ico &CorrelationID=<empty>;&cafeReqId=ce463951-e878-4f0a-bdf6-581144fddc08;&LogoffReason=NoCookiesGetOrE14Au
2022-10-06 19:22:24 10.0.0.11 GET /owa/auth/logon.aspx url=https%3a%2f%2f20.62.174.61%2fowa%2ffavicon.ico&reason=0&CorrelationID=<empty>;&cafeReqId=d3dd147
2022-10-06 19:22:30 127.0.0.1 GET /OWA/Calendar/HealthMailbox5030916c27b64154a725d5dbd4e373c1@contoso.com/calendar/calendar.html &CorrelationID=<empty>;&ca
2022-10-06 19:22:30 10.0.0.11 POST /aspnet_netclient/4_0_30319/POWERshell.aspx - 443 - 20.106.209.84 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/
2022-10-06 19:22:30 10.0.0.11 GET /favicon.ico &Owa302RedirectUri=/owa/favicon.ico 443 - 20.106.209.84 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKi
```

This is how the full POST request looks like:

```
2022-10-06 19:22:30 10.0.0.11 POST
/aspnet_netclient/4_0_30319/POWERshell.aspx - 443 - 20.106.209.84
Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+
(KHTML,+like+Gecko)+Chrome/106.0.0.0+Safari/537.36+Edg/106.0.1370.34
https://20.62.174.61/aspnet_netclient/4_0_30319/POWERshell.aspx 200 0 0 767
```

This is how we can interpret the data:

Date time	2022-10-06 19:22:30
s-ip	10.0.0.11 (This is the internal IP of the server)
cs-method	POST
cs-uri-stem	/aspnet_netclient/4_0_30319/POWERshell.aspx
s-port	443
c-ip	20.106.209.84 (IP address of the attacker)
cs(User-Agent)	Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/106.0.0.0+Safari/537.36+Edg/106.0.1370.34
cs(Referer)	https://20.62.174.61/aspnet_netclient/4_0_30319/POWERshell.aspx
sc-status	200

Exchange Setup logs

During an installation of Exchange, there will be a new folder created in the **C:** drive. By default, the Exchange setup logs are located at: **C:\ExchangeSetupLogs**.

The Setup log tracks the progress of every task during the Exchange installation and configuration. The file contains information about the status of the prerequisite and system readiness checks before installation starts, the application installation progress, and the configuration changes that are made to the system.

2022-10-01 – Exchange was installed which contains a specific version 15.1.1713.5.

Exchange Server 2016 CU12	February 12, 2019	15.1.1713.5	15.01.1713.005

This means that on this date, we saw that Exchange Server 2016 CU12 was installed.

```
[10/01/2022 08:58:47.0783] [0] ********************************************
[10/01/2022 08:58:47.0798] [0] Starting Microsoft Exchange Server 2016 Setup
[10/01/2022 08:58:47.0798] [0] ********************************************
[10/01/2022 08:58:47.0798] [0] Local time zone: (UTC) Coordinated Universal Time.
[10/01/2022 08:58:47.0798] [0] Operating system version: Microsoft Windows NT 6.2.9200.0.
[10/01/2022 08:58:47.0814] [0] Setup version: 15.1.1713.5.
[10/01/2022 08:58:47.0814] [0] Logged on user: CONTOSO\Usman.
[10/01/2022 08:58:47.0830] [0] The registry key, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ExchangeServer\V15\Setup, wasn't found.
[10/01/2022 08:58:47.0845] [0] The registry key, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ExchangeServer\V15\Setup, wasn't found.
[10/01/2022 08:58:47.0876] [0] Command Line Parameter Name='sourcedir', Value='F:\'.
[10/01/2022 08:58:47.0876] [0] Command Line Parameter Name='mode', Value='Install'.
[10/01/2022 08:58:47.0892] [0] RuntimeAssembly was started with the following command: '/sourcedir:F: /mode:Install'.
[10/01/2022 08:58:47.0892] [0] The registry key, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ExchangeServer\V15\Setup, wasn't found.
[10/01/2022 08:58:48.0970] [0] Finished loading screen CheckForUpdatesPage.
[10/01/2022 08:58:51.0965] [0] Finished loading screen UpdatesDownloadsPage.
[10/01/2022 08:58:54.0513] [0] Starting file's copying...
[10/01/2022 08:58:54.0528] [0] Setup copy files from 'F:\Setup\ServerRoles\Common' to 'C:\Windows\Temp\ExchangeSetup'
[10/01/2022 08:58:54.0575] [0] Disk space required: 2104368763 bytes.
[10/01/2022 08:58:54.0575] [0] Disk space available: 114456432640 bytes.
[10/01/2022 08:58:54.0716] [0] Finished loading screen CopyFilesPage.
[10/01/2022 08:59:47.0543] [0] File's copying finished.
```

2022-10-04 – Exchange has been upgraded to version 15.1.2507.6.

Here we can see that Exchange has been upgraded to CU23.

Exchange PowerShell cmdlet History

Commands that were ran in Exchange PowerShell will be logged in the following location: **C:\Program Files\Microsoft\Exchange Server\V15\Logging\CmdletInfra\LocalPowerShell\Cmdlet**. The filenames look similar to something like **powershell.exe_19516_Cmdlet_2022100116-1**.

This is how the structure of the Exchange PowerShell history logs look like:

```
#Software: Microsoft Exchange Server
#Version: 15.01.1713.001
#Log-type: Rps Cmdlet Logs
#Date: 2022-10-01T14:45:19.673Z
#Fields:
DateTime,StartTime,RequestId,ClientRequestId,MajorVersion,MinorVersion,BuildV
ersion,RevisionVersion,ServerHostName,ProcessId,ProcessName,ThreadId,CultureI
nfo,Organization,AuthenticatedUser,ExecutingUserSid,EffectiveOrganization,Use
rServicePlan,IsAdmin,ClientApplication,Cmdlet,Parameters,CmdletUniqueId,UserB
udgetOnStart,ContributeToFailFast,RunspaceSettingsCreationHint,ADViewEntireFo
rest,ADRecipientViewRoot,ADConfigurationDomainControllers,ADPreferredGlobalCa
talogs,ADPreferredDomainControllers,ADUserConfigurationDomainController,ADUse
rPreferredGlobalCatalog,ADuserPreferredDomainControllers,ThrottlingInfo,Delay
Info,ThrottlingDelay,IsOutputObjectRedacted,CmdletProxyStage,CmdletProxyRemot
eServer,CmdletProxyRemoteServerVersion,CmdletProxyMethod,ProxiedObjectCount,C
mdletProxyLatency,OutputObjectCount,ParameterBinding,BeginProcessing,ProcessR
ecord,EndProcessing,StopProcessing,BizLogic,PowerShellLatency,UserInteraction
Latency,ProvisioningLayerLatency,ActivityContextLifeTime,TotalTime,ErrorType,
ExecutionResult,CacheHitCount,CacheMissCount,GenericLatency,GenericInfo,Gener
icErrors,ObjectGuid,ExternalDirectoryOrganizationId,ExternalDirectoryObjectId
,NonPiiParameters
```

I’ve decided to take a snippet of an history log file. It contains which user ran which commands and so on. This can be very useful if someone cleaned the MSExchangeManagement event logs. Since all the history logs will be still there on disk.

As we can see here, there is a user that is exporting all the mailboxes to the C:\Temp directory.

At the second example, we can see that a SMTP forwarding rule is created to forward the e-mails from Leon Edwards to an external domain.

Last example, we can see that a role assignment was initiated to assign a user to the Recipient Management role in Exchange.

Exchange CosmosQueue Logs

Exchange CosmosQueue logs are like the audit logs in Exchange. It shows more of the operational activities that were performed in Exchange. This can include examples such as creating a new Database Availability Group (DAG) or removing a Mailbox database, putting the Exchange server in maintenance mode, and so on. All the logs are located at: **C:\Program Files\Microsoft\Exchange Server\V15\Logging\CosmosQueue** and have a similar filename such as **audit20221004-4**.

This is how the structure of the Exchange CosmosQueue logs look like:

```
#Software: Microsoft Exchange
#Version: 15.01.1713.001
#Log-type: audit
#Date: 2022-10-04T13:29:22.251Z
#Fields:
```

```
Timestamp,Server,TenantId,RecordType,Data,UserKey,RecordId,Operation,Workload
,ResultStatus,Version,Scope
```

Here we can a snippet of some of the operational tasks in Exchange being logged:

This includes also the associated user that performed this operational activity.

Exchange Control Panel – Activity Logs

Exchange Control Panel is like the admin panel for Exchange. Administrative tasks can be performed in this panel, and this activity is logged as well. All the activity logs of ECP are stored at the following location: **C:\Program Files\Microsoft\Exchange Server\V15\Logging\ECP\Activity** and it has similar filename as **ECPActivity_9296_20221004-1**.

This is how the structure of the ECP activity logs look like:

```
#Software: Microsoft Exchange Server
#Version: 15.0.0.0
```

```
#Log-type: ECP Activity Context Log
#Date: 2022-10-04T09:20:35.883Z
#Fields: TimeStamp,ServerName,EventId,EventData
```

This is how the logs may look like:

Let's take a closer look at some of the ECP activity logs. I will include a couple of examples.

Here we can see that the user Testing was creating a new user mailbox in ECP.

```
2022-10-01T10:47:36.658Z,EXCHANGE,Request,S:PSA=
<PII>Testing@contoso.com</PII>;S:FE=EXCHANGE.CONTOSO.COM;S:URL=https://exchan
ge.contoso.com:444/ecp/UsersGroups/NewMailboxOnPremises.aspx?
pwmcid=3&ReturnObjectType=1(https://exchange.contoso.com/ecp/UsersGroups/NewM
ailboxOnPremises.aspx?
pwmcid=3&ReturnObjectType=1);S:Bld=15.1.1713.5;S:ActID=3bbbf798-1dc1-40f8-
a56b-
0611baa1065d;Dbl:BudgUse.T[]=7.00040006637573;I32:ADS.C[DC]=1;F:ADS.AL[DC]=1.
592;I32:ATE.C[DC.contoso.com]=0;F:ATE.AL[DC.contoso.com]=0;S:WLM.Bal=2.147484
E+09;Dbl:WLM.TS=259
```

A new mailbox database was created by Testing.

```
2022-10-04T18:23:44.745Z,EXCHANGE,Request,S:PSA=
<PII>Testing@contoso.com</PII>;S:FE=EXCHANGE.CONTOSO.COM;S:URL=https://exchan
ge.contoso.com:444/ecp/DBMgmt/NewDatabase.aspx?
pwmcid=16&ReturnObjectType=1(https://exchange.contoso.com/ecp/DBMgmt/NewDatab
```

```
ase.aspx?pwmcid=16&ReturnObjectType=1);S:Bld=15.1.1713.5;S:ActID=d9a2ef05-
ef68-4e47-a4d9-d2a80d6180ac;Dbl:WLM.TS=40
```

New Database Availability Group (DAG) was created in ECP.

```
2022-10-04T18:11:54.303Z,EXCHANGE,Request,S:PSA=
<PII>Testing@contoso.com</PII>;S:FE=EXCHANGE.CONTOSO.COM;S:URL=https://exchan
ge.contoso.com:444/ecp/DBMgmt/NewDAG.aspx?
pwmcid=2&ReturnObjectType=1(https://exchange.contoso.com/ecp/DBMgmt/NewDAG.as
px?pwmcid=2&ReturnObjectType=1);S:Bld=15.1.1713.5;S:ActID=7abb1d23-ee8d-44a5-
a3ac-536cdbaeffc2;Dbl:WLM.TS=53
```

Share this:

Related

Hunting and Responding to ProxyShell Attacks
October 18, 2022
In "Incident Response"

Hunting Webshell Activity
October 9, 2022
In "Incident Response"

Investigating ProxyLogon Attacks and how to mitigate it
October 16, 2022
In "Incident Response"

2 COMMENTS

Ban December 19, 2022 2:38 am

Thank you for amazing writeup

★ Like

Reply

RSA July 12, 2024 3:27 am

Thanks a lot this was helpful

★ Like

Reply

LEAVE A COMMENT

Search ...

BUY ME A COFFEE

POPULAR THIS WEEK

- Hunting in On-Premises Exchange Server logs
- Investigating Certificate Template Enrollment Attacks - (ADCS)
- Everything about Service Principals, Applications, and API Permissions
- Practical Compromise Recovery Guidance for Active Directory
- History of Exchange with having wide permissions in AD

CATEGORIES

- M365 Advanced Hunting
- Azure Sentinel
- Azure Active Directory
- KQL
- Microsoft Identity
- Windows OS
- Jupyter Notebooks

CONTACT

RECENT POSTS

- Investigating Certificate Template Enrollment Attacks – (ADCS)
- How one misconfiguration in ADCS can lead to full AD Forest compromise
- Investigating Ransomware Deployments that happened via Group Policy
- Hunting and Responding to ProxyShell Attacks

- Investigating ProxyLogon Attacks and how to mitigate it

TAGS

Jupyter Notebooks