

CrownJewel-2,evt(x(gigasheet、EvtxECmd、Timeline Explorer),NTDS

Sherlock Scenario

Forela's Domain environment is pure chaos. Just got another alert from the Domain controller of NTDS.dit database being exfiltrated. Just one day prior you responded to an alert on the same domain controller where an attacker dumped NTDS.dit via vssadmin utility. However, you managed to delete the dumped files kick the attacker out of the DC, and restore a clean snapshot. Now they again managed to access DC with a domain admin account with their persistent access in the environment. This time they are abusing ntdsutil to dump the database. Help Forela in these chaotic times!!

* * *

About CrownJewel-2

In this very easy sherlock, you will learn how to detect NTDS.dit dumping which is one of the most critical Active directory attacks. You will get your hands on event logs to respond to an attack where the attacker utilized ntdsutil utility to dump the NTDS.dit database.

文件：SYSTEM.evt(x、SECURITY.evt(x、APPLICATION.evt(x

使用工具：<https://app.gigasheet.com/>、EvtxECmd、Timeline Explorer

指令：

```
- EvtxECmd.exe -f "C:\Users\TS0\Downloads\APPLICATION.evt(x" --csv
"C:\Users\TS0\Downloads\LOG" --csvf APPLICATION.csv
- EvtxECmd.exe -f "C:\Users\TS0\Downloads\SECURITY.evt(x" --csv
"C:\Users\TS0\Downloads\LOG" --csvf SECURITY.csv
- EvtxECmd.exe -f "C:\Users\TS0\Downloads\SYSTEM.evt(x" --csv
"C:\Users\TS0\Downloads\LOG" --csvf SYSTEM.csv
```

Task 1

When utilizing ntdsutil.exe to dump NTDS on disk, it simultaneously employs the Microsoft Shadow Copy Service. What is the most recent timestamp at which this service entered the running state, signifying the possible initiation of the NTDS dumping process?

查詢包括ntdsutil.exe

FileEditInsertFormatDataAutomationHelp

SECURITY.evtx ⓘ

🗨️🔗🔄📈

Views📄🔄Reset

Manage Columns🔗

Filtered by 1 field🔍

Group📁

Sorted by 2 fields📶

Enrich Data🔗

Chart Data📊

#	...	#	EventRecordID	TimeCreated	#	EventID	#	Level	T	Provider	T	Channel
16		5978		2024-05-15 05:39:55.636	4799	0			Microsoft-Windows-Security			
15		5977		2024-05-15 05:39:55.636	4799	0			Microsoft-Windows-Security			
18		5980		2024-05-15 05:39:55.638	4799	0			Microsoft-Windows-Security			
17		5979		2024-05-15 05:39:55.638	4799	0			Microsoft-Windows-Security			
02		5984		2024-05-15 05:39:55.648	4799	0			Microsoft-Windows-Security			
01		5983		2024-05-15 05:39:55.648	4799	0			Microsoft-Windows-Security			
00		5982		2024-05-15 05:39:55.648	4799	0			Microsoft-Windows-Security			
19		5981		2024-05-15 05:39:55.648	4799	0			Microsoft-Windows-Security			
05		5987		2024-05-15 05:39:55.649	4799	0			Microsoft-Windows-Security			
04		5986		2024-05-15 05:39:55.649	4799	0			Microsoft-Windows-Security			
03		5985		2024-05-15 05:39:55.649	4799	0			Microsoft-Windows-Security			
08		5990		2024-05-15 05:39:55.650	4799	0			Microsoft-Windows-Security			
07		5989		2024-05-15 05:39:55.650	4799	0			Microsoft-Windows-Security			
06		5988		2024-05-15 05:39:55.650	4799	0			Microsoft-Windows-Security			
09		5991		2024-05-15 05:39:55.655	4799	0			Microsoft-Windows-Security			
10		5992		2024-05-15 05:39:55.656	4799	0			Microsoft-Windows-Security			
11		5993		2024-05-15 05:39:55.721	4799	0			Microsoft-Windows-Security			
12		5994		2024-05-15 05:39:55.722	4799	0			Microsoft-Windows-Security			
13		5995		2024-05-15 05:39:55.723	4799	0			Microsoft-Windows-Security			
14		5996		2024-05-15 05:39:55.724	4799	0			Microsoft-Windows-Security			
16		5998		2024-05-15 05:39:55.726	4799	0			Microsoft-Windows-Security			
15		5997		2024-05-15 05:39:55.726	4799	0			Microsoft-Windows-Security			
		Sum	715,285									

2024-05-15 05:39:55

Sheet Assistant

查詢包括ntdsutil.exe

It seems like you're looking to query specific data. Could you please clarify what particular information or criteria you're interested in? For example, are you looking for events related to a specific user, event types, timestamps, or something else?

I will filter the dataset to include only rows where the ProcessID is 'ntdsutil.exe'.

Applied filters on the following columns: EventData/CallerProcessName.

Show me...

BETA Share your feedback or connect with support

Task 2

Identify the full path of the dumped NTDS file.

參考：<https://docs.velociraptor.app/exchange/artifacts/pages/ntdsutil/>

event id：

325、327

但完全找不到event id...，我改用桌面版就正常了

Timeline Explorer v2.0.0.1

FileToolsTabsViewHelp

APPLICATION.csv

Enter text to search...Find

	Event Record Id	Time Created	Payload Data	Event Id
244	244	2023-03-08 10:05:39	Database: DFSRs, 2328,D,35, \\.\C:\System Volume Information\DFSR\database...	325
293	293	2023-03-09 09:16:08	Database: DFSRs, 2044,D,50, \\.\C:\System Volume Information\DFSR\database...	326
307	307	2023-03-09 09:25:32	Database: B: , 1, C:\Windows\system32\config\systemprofile\AppData\Local\D...	325
367	367	2023-03-10 02:00:59	Database: DFSRs, 2224,D,50, \\.\C:\System Volume Information\DFSR\database...	326
473	473	2023-03-25 14:33:22	Database: DFSRs, 2572,D,50, \\.\C:\System Volume Information\DFSR\database...	326
483	483	2023-03-25 14:37:58	Database: B: , 1, C:\Windows\system32\config\systemprofile\AppData\Local\D...	326
508	508	2023-03-27 14:03:25	Database: DFSRs, 3052,D,50, \\.\C:\System Volume Information\DFSR\database...	326
530	530	2023-03-27 14:13:03	Database: B: , 1, C:\Windows\system32\config\systemprofile\AppData\Local\D...	326
540	540	2024-05-14 04:01:50	Database: DFSRs, 7344,D,35, \\.\C:\System Volume Information\DFSR\database...	325
644	644	2024-05-15 05:39:56	Database: C:\\$SNAP_202405151039_VOLUMEC\$\Windows\NTDS\ntds.dit	326
646	646	2024-05-15 05:39:56	Database: C:\Windows\Temp\dump_tmp\Active Directory\ntds.dit	325
648	648	2024-05-15 05:39:58	Database: C:\Windows\Temp\dump_tmp\Active Directory\ntds.dit	327
649	649	2024-05-15 05:39:58	Database: C:\\$SNAP_202405151039_VOLUMEC\$\Windows\NTDS\ntds.dit	327
653	653	2024-05-15 05:40:47	Database: DFSRs, 3064,D,50, \\.\C:\System Volume Information\DFSR\database...	326

Event Id In

325326327

C:\Windows\Temp\dump_tmp\Active Directory\ntds.dit

啟用
移至

Task 3

When was the database dump created on the disk?

同上event id : 325

2024-05-15 05:39:56

Task 4

When was the newly dumped database considered complete and ready for use?

同上Task2 event id : 327

2024-05-15 05:39:58

Task 5

Event logs use event sources to track events coming from different sources. Which event source provides database status data like creation and detachment?

我記得web有出現過

APPLICATION.evtx ⓘ									
Views ▾ ⌂ Reset Manage Columns Filter Group ⬆️ Sorted by 2 fields ⌘ Enrich Data 📊 Chart Data									
#	EventRecordID	TimeCreated	#	EventID	#	Level	T	Provider	T
634		2024-05-15 05:39:56.189			4		ESENT	Applicat	
633		2024-05-15 05:39:56.189			4		ESENT	Applicat	
632		2024-05-15 05:39:56.189			4		ESENT	Applicat	
631		2024-05-15 05:39:56.189			4		ESENT	Applicat	
638		2024-05-15 05:39:56.205			4		ESENT	Applicat	
637		2024-05-15 05:39:56.205			4		ESENT	Applicat	
640		2024-05-15 05:39:56.221			4		ESENT	Applicat	
639		2024-05-15 05:39:56.221			4		ESENT	Applicat	
641		2024-05-15 05:39:56.252			4		ESENT	Applicat	
642		2024-05-15 05:39:56.392			4		ESENT	Applicat	
644		2024-05-15 05:39:56.408			4		ESENT	Applicat	
643		2024-05-15 05:39:56.408			4		ESENT	Applicat	
645		2024-05-15 05:39:56.486			4		ESENT	Applicat	
647		2024-05-15 05:39:56.502			4		ESENT	Applicat	
646		2024-05-15 05:39:56.502			4		ESENT	Applicat	
648		2024-05-15 05:39:58.549			4		ESENT	Applicat	
650		2024-05-15 05:39:58.564			4		ESENT	Applicat	
649		2024-05-15 05:39:58.564			4		ESENT	Applicat	
651		2024-05-15 05:40:47.080			4		ESENT	Applicat	
653		2024-05-15 05:40:47.096			4		ESENT	Applicat	
652		2024-05-15 05:40:47.096			4		ESENT	Applicat	
Sum 213,531									

View 100 ▾ ⏪ ⏩ Page 7 of 7 ⏪ ⏩ Rows: 653 Cols: 50 of 51

ESENT

Task 6

When ntdsutil.exe is used to dump the database, it enumerates certain user groups to validate the privileges of the account being used. Which two groups are enumerated by the ntdsutil.exe process? Give the groups in alphabetical order joined by comma space.

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

APPLICATION.csv SYSTEM.csv SECURITY.csv

ntdsutil.exe x Find

	Event Record Id	Time Created	Payload Data1	Payload Data2
261	6143	2024-05-15 05:39:56	Target: Builtin\Administrators (S-1-5-32-544)	SubjectLogonId: 0x8DE3D
96	5978	2024-05-15 05:39:55	Target: Builtin\Backup Operators (S-1-5-32-551)	SubjectLogonId: 0x8DE3D

Administrators, Backup Operators

Task 7

Now you are tasked to find the Login Time for the malicious Session. Using the Logon ID, find the Time when the user logon session started.

event id : 4768

APPLICATION.csv SYSTEM.csv SECURITY.csv

4768 x Find

	Time Created	Payload Data1	Payload Data2	Event Id	Payload Data6
7	2024-05-15 05:36:31	Target: FORELA\Administrator	ServiceName: krbtgt	4768	PreAuthType: PA-ENC-TIMESTAMP - This type is normal for standard password authentication
3	2024-05-15 05:35:57	Target: FORELA.LOCAL\DC01\$	ServiceName: krbtgt	4768	PreAuthType: PA-ENC-TIMESTAMP - This type is normal for standard password authentication
7	2024-05-15 05:35:57	Target: FORELA.LOCAL\DC01\$	ServiceName: krbtgt	4768	PreAuthType: PA-ENC-TIMESTAMP - This type is normal for standard password authentication

2024-05-15 05:36:31