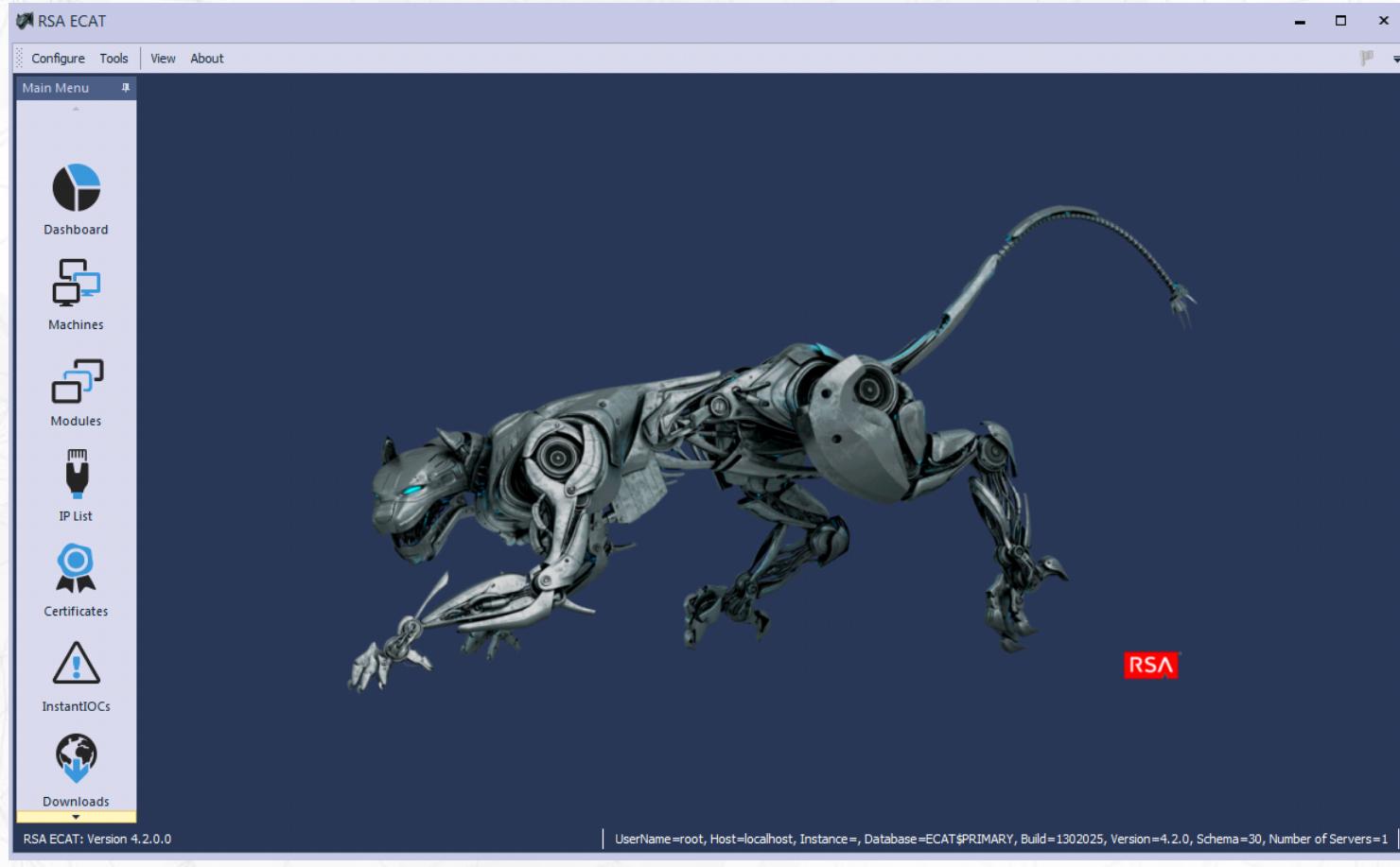


RSA INCIDENT RESPONSE

NetWitness Endpoint (ECAT) Database Hunting

RSA

NETWITNESS ENDPOINT (NWE)



RSA

NETWITNESS ENDPOINT (NWE)

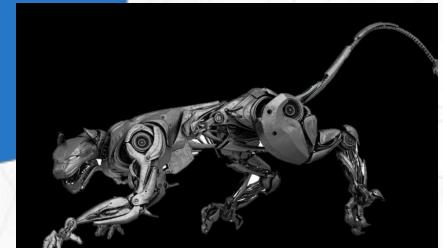
NWEndpoint is more than just a UI

Two forms of visibility:

- Endpoint Scanning
 - Modules focused
- Tracking Data
 - Behavioral Tracking
 - Network Tracking

DB Hunting focuses on

Behavior Tracking Data
Network Tracking Data



RSA

TRACKING DATA

- Requires Full User-Mode Monitoring and Tracking
- Can Include both Network Monitoring and Behavior Tracking
- Behavior Tracking system is an active system that monitors operations performed in user-mode
- Monitors key behaviors related to processes, files, and networks.
- Does not require a scan for collection



RSA

TRACKING BEHAVIORS

- Windows
 - OpenProcess, CreateRemoteThread, OpenLogicalDrive, OpenPhysicalDrive, ReadDocument, WriteToExecutable, RenameToExecutable, NewIPAddress, Network - incoming, and Network - outgoing
- Mac OS
 - OpenProcess, CreateRemoteThread, WriteToExecutable, RenameExecutable, and CreateAutorun



RSA

BEHAVIOR TRACKING PURPOSES

- To identify the perpetrators of common malware-like behaviors, such as floating code allocation and suspicious thread creation (for more information, see Floating Code). This is available to allow you to better pinpoint the owner of an action.
- To report common behaviors, such as network activity and inter-process operations, that could be indicative of malware or other threats.



RSA

NWE TRACKING EVENTS UI VIEW

The screenshot shows a user interface for tracking events. At the top, there's a navigation bar with icons for computer, cloud, and file system, followed by the host name "LT-US-LDUFFY". To the right is a "Score" indicator (591) enclosed in a red circle, with "Administrative Status" and "Last Seen" information below it. On the far right are three buttons: "Hide Whitelisted", "Hide Good Files", and "Hide Valid Signature".

The main area contains several tabs: "Summary", "Blocked", "Modules History", "Downloaded", "Agent Log", "Scan Data", and "More Info". The "Summary" tab is active, displaying a table of anomalies:

Category	Items	Suspect
Autoruns	12	12
Services	388	88
Tasks	53	53
Hosts	1	0
Files	530	155

Below this is a section titled "Anomaly" with sub-categories: "Image Hooks", "Kernel Hooks", "Windows Hooks", "Suspicious Threads", and "Registry Discrepancies", all showing 0 items.

The "History" section shows network and tracking statistics:

Category	Items	Suspect
Network	134	131
Tracking	558	308

The "Agent Log" tab is expanded, showing a table of event logs:

Event Time	Source File Name	Event	Target File Name	Source Command Line	Target Command Line
5/25/2016 12:31:18.172 PM	vmtoolsd.exe	Open Process	SearchProtocolHost.exe	"C:\Program Files\VM...	"C:\Windows\system32\SearchProtocolHost...
5/25/2016 12:31:08.609 PM	SearchIndexer.exe	Create Process	SearchProtocolHost.exe	C:\Windows\system3...	"C:\Windows\system32\SearchProtocolHost...
5/25/2016 12:15:17.709 PM	vmtoolsd.exe	Open Process	rubyw.exe	"C:\Program Files\VM...	rubyw.exe "C:\Windows\TEMP\ocrE8C9.tmp
5/25/2016 12:15:17.709 PM	vmtoolsd.exe	Open System Process	svchost.exe	"C:\Program Files\VM...	c:\Windows\temp\svchost.exe
5/25/2016 12:15:17.709 PM	vmtoolsd.exe	Open Process	taskeng.exe	"C:\Program Files\VM...	taskeng.exe (B710E858-0527-47AB-8171-80
5/25/2016 12:15:17.709 PM	vmtoolsd.exe	Open Process	taskhost.exe	"C:\Program Files\VM...	taskhost.exe \${Arg0}

At the bottom of the log table, it says "558 items total". There are also filter and edit filter buttons at the bottom right of the log table.

RSA

NWE TRACKING EVENTS UI VIEW

If you don't normally see Source Command Line & Target Command Line in your view

Right Click | Column Chooser

Category	Items	Suspect
Autoruns	12	12
Services	388	88
Tasks	53	53
Hosts	1	0
Files	530	155
Anomaly		
Image Hooks	0	0
Kernel Hooks	0	0
Windows Hooks	0	0
Suspicious Threads	0	0
Registry Discrepancies	0	0
History		
Network	134	131
Tracking	558	308

The screenshot shows a context menu for the 'Column Chooser' option, which is highlighted in yellow. The menu includes options for sorting (Sort Ascending, Sort Descending, Clear All Sorting), grouping (Group By This Column, Show Group By Box), hiding columns, and applying filters. The 'Source Command Line' and 'Target Command Line' columns are specifically highlighted with red boxes in the main table area.

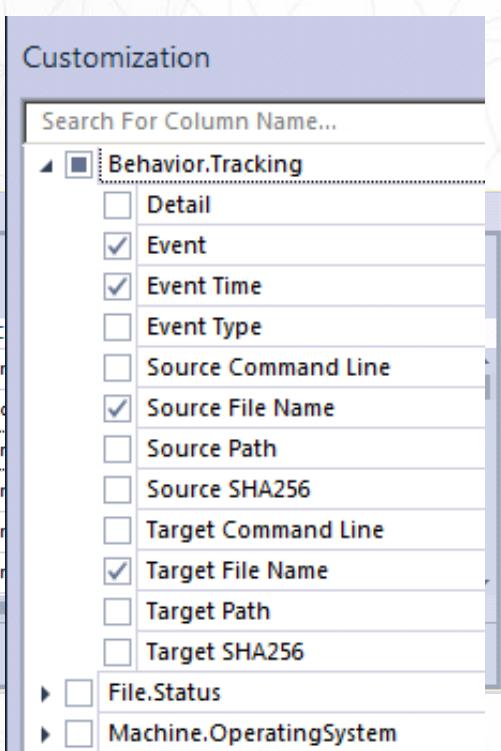
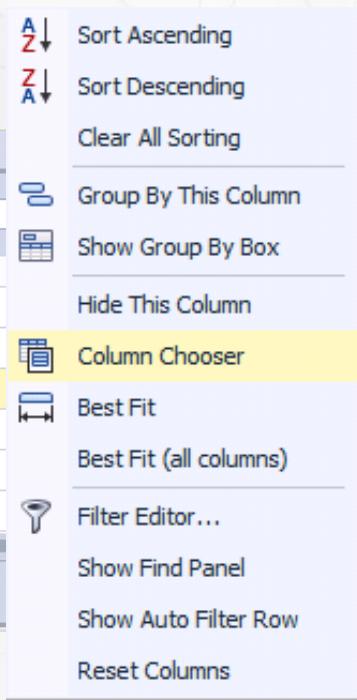
Event Time	Source File Name
5/25/2016 12:31:18.172 PM	vmtoolsd.exe
5/25/2016 12:31:08.609 PM	SearchIndexer.exe
5/25/2016 12:15:17.709 PM	vmtoolsd.exe

NETWITNESS ENDPOINT (NWE)

If you don't normally see Source Command Line & Target Command Line in your view

Under Behavior.Tracking Add Source & Target Command Line

Category	Items	Suspect
Autoruns	12	12
Services	388	88
Tasks	53	53
Hosts	1	0
Files	530	155
Anomaly		
Image Hooks	0	0
Kernel Hooks	0	0
Windows Hooks	0	0
Suspicious Threads	0	0
Registry Discrepancies	0	0
History		
Network	134	131
Tracking	558	308



INSTANT INDICATOR OF COMPROMISE (IIOC)

Event IIOC are based on tracking events

IIOC view is the closest we have to a 'global' tracking events view

The screenshot displays the InstantIocs application interface. On the left, a table titled "InstantIocs" lists various IOCs with columns for Description, Level, Type, Active, Alerta..., Machine Co..., Module Co..., Last Executed, and Blacklisted Co... . A total of 410 items are shown. In the center, a modal window titled "InstantIOC" shows a query editor with the following SQL code:

```
SELECT DISTINCT
    [imp].[FK_Machines] AS [FK_Machines],
    [imp].[PK_MachineModulePaths] AS [FK_MachineModulePaths]
FROM
    [dbo].[WinTracingEventsCast] AS [se] WITH(NOLOCK)
    INNER JOIN [dbo].[MachineModulePaths] AS [mp] WITH(NOLOCK) ON ([mp].[PK_MachineModulePaths] = [se].[MachineModulePath])
    INNER JOIN [dbo].[Modules] AS [mo] WITH(NOLOCK) ON ([mo].[PK_Modules] = [mp].[FK_Module])
WHERE
    [mo].[ModuleSignatureMicrosoft] = 0 AND
    [se].[BehaviorFileRenameToExecutable] = 1 AND
    [mp].[FK_Modules] != -1 AND
    [mp].[MarkedAsDeleted] = 0
```

On the right, there are two detail panes: "Machines" and "Modules". The "Machines" pane shows a list of machines with their IIOC scores (e.g., LT-US-RCR... 1023, LT-US-LDU... 591, SV-GB-HR1 303, LT-IT-DBASS 1) and status. The "Modules" pane shows a list of modules with their IIOC scores (e.g., McScript.exe 10, WindowsOSPatch22311.exe 855), Risk Scores, Machine Count, and Signature status.

THE PROBLEM WITH IIoC

IIoC doesn't display command line, path, or module directly associated with the source system. Additional steps are needed to dig into each item.

This is a good start, but there are other ways of presenting this data

The screenshot displays a user interface for security analysis, likely using a tool like Mandiant's ATLAS. It features two main tables: 'Machines' and 'Modules'.

Machines Table:

Machine Name	IIoC Score	Admin Stat...	Comment
LT-US-RCRAIG	1023	Under Inve...	
LT-US-RLEE-SNAPSHOT	735		
LT-US-LDUFFY	591		
ECATDEMO	39		
LT-US-CELIZALDE	15		
LT-US-RHATCHER	15		

Modules Table:

File Name	IIoC Score	Risk Score	Machine Count	Signature	Hash Lookup
rundll32.exe	3	1	2	Valid: Microsoft Windows	Good
explorer.exe	2	1	2	Valid: Microsoft Windows	Good
services.exe	4	1	5	Valid: Microsoft Windows	Unknown
vmtoolsd.exe	2	0	1	Valid: VMware, Inc.	Good
explorer.exe	3	1	3	Valid: Microsoft Windows	Good
ELmQsP.exe	6	1	1	Not Signed: Apache Software Foun...	Unknown
java.exe	11	1	1	Need Revoke Update: Oracle Americ...	Good
notepad.exe	1	1	1	Valid: Microsoft Windows	Unknown
tior.exe	140	1	1	Not Signed	Malicious

A WHERE clause is visible in the background: [se].[BehaviorProcessCreateProcess] = 1 AND

NETWITNESS ENDPOINT (NWE)

There is no 'global' view similar to the machine tracking view (for a very good reason)

So how can we get some of that 'global view'

DBHUNTING!

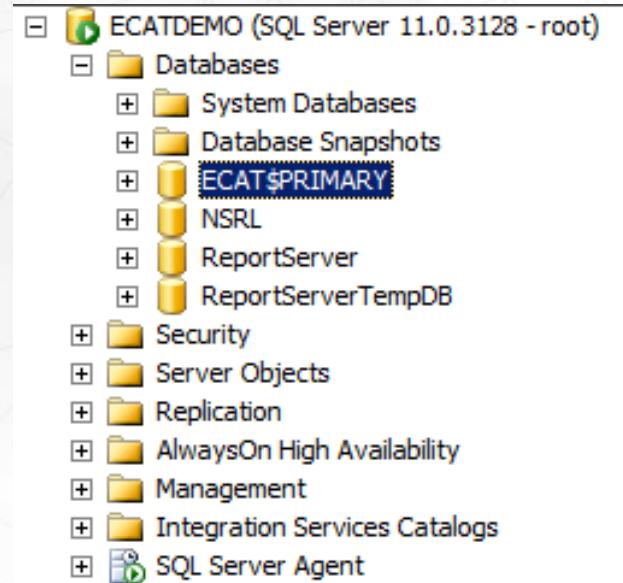
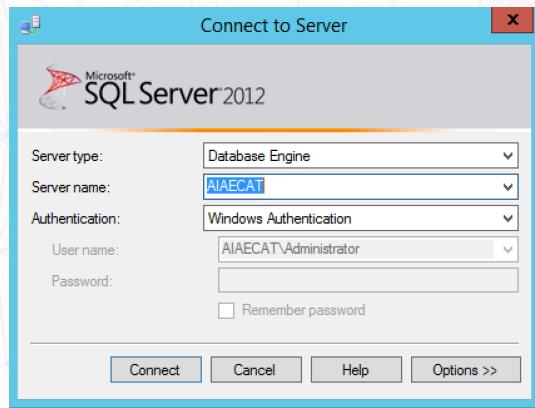


RSA

MANUAL DB HUNTING (MSSQL)

Microsoft SQL Server Management Studio (894mb)

<https://msdn.microsoft.com/en-us/library/mt238290.aspx>



MANUAL DB HUNTING (MSSQL)

The screenshot shows the Microsoft SQL Server Management Studio interface. A red box highlights the 'New Query' button in the toolbar. Another red box highlights the 'Execute' button in the toolbar. The 'Object Explorer' pane on the left shows a connection to 'ECATDEMO (SQL Server 11.0.3128 - root)'. The 'Query' pane contains a T-SQL script named 'SQLQuery1.sql' which renames files to executable files. The 'Results' pane displays the output of the query, titled 'Results' in red. The results table has columns: MachineName, EventUTCTime, FileName, Path_TargetProcessPathName, FileName_TargetProcessImageFileName, SourceCommandLine, and TargetCommandLine. The table contains 18 rows of data.

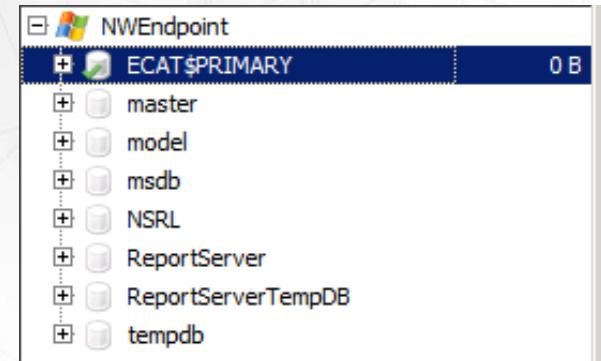
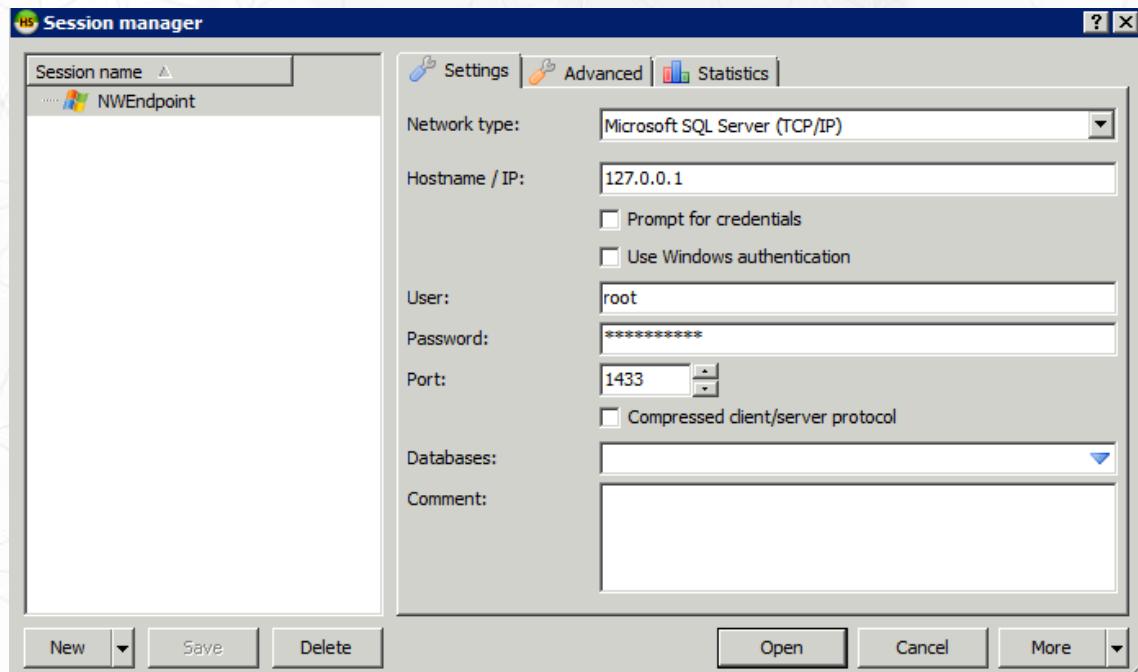
MachineName	EventUTCTime	FileName	Path_TargetProcessPathName	FileName_TargetProcessImageFileName	SourceCommandLine	TargetCommandLine
LT-US-LDUFFY	2016-05-25 16:15:03.5290000	svchost.exe	C:\Windows\Temp\ocrE8C9tmp\bin\	rubyw.exe	c:\Windows\temp\svchost.exe	rubyw.exe "C:\Winc
LT-US-LDUFFY	2016-05-25 16:15:01.8600000	svchost.exe	C:\Windows\TEMP\ocrE8C9tmp\src\	api so	c:\Windows\temp\svchost.exe	
LT-US-LDUFFY	2016-05-25 16:15:02.7650000	svchost.exe	C:\Windows\TEMP\ocrE8C9tmp\lib\uby\1.8\386 ming...	stringio.so	c:\Windows\temp\svchost.exe	
LT-US-LDUFFY	2016-05-25 16:15:03.1080000	svchost.exe	C:\Windows\TEMP\ocrE8C9tmp\lib\uby\1.8\386 ming...	syck.so	c:\Windows\temp\svchost.exe	
LT-US-LDUFFY	2016-05-25 16:15:02.5310000	svchost.exe	C:\Windows\TEMP\ocrE8C9tmp\lib\uby\1.8\386 ming...	socket.so	c:\Windows\temp\svchost.exe	
LT-US-LDUFFY	2016-05-25 16:15:02.5930000	svchost.exe	C:\Windows\TEMP\ocrE8C9tmp\lib\uby\1.8\386 ming...	digest.so	c:\Windows\temp\svchost.exe	
LT-US-LDUFFY	2016-05-25 16:15:02.8740000	svchost.exe	C:\Windows\TEMP\ocrE8C9tmp\lib\uby\1.8\386 ming...	fcntl.so	c:\Windows\temp\svchost.exe	
LT-US-LDUFFY	2016-05-25 16:15:02.7180000	svchost.exe	C:\Windows\TEMP\ocrE8C9tmp\lib\uby\1.8\386 ming...	openssl.so	c:\Windows\temp\svchost.exe	
LT-US-LDUFFY	2016-05-25 16:15:03.1080000	svchost.exe	C:\Windows\TEMP\ocrE8C9tmp\lib\uby\1.8\386 ming...	etc.so	c:\Windows\temp\svchost.exe	
LT-US-LDUFFY	2016-05-25 16:15:03.1080000	svchost.exe	C:\Windows\TEMP\ocrE8C9tmp\lib\uby\1.8\386 ming...	Win32API.so	c:\Windows\temp\svchost.exe	
LT-US-LDUFFY	2016-05-25 16:15:03.2480000	svchost.exe	C:\Windows\TEMP\ocrE8C9tmp\lib\uby\1.8\386 ming...	zlib.so	c:\Windows\temp\svchost.exe	
LT-US-LDUFFY	2016-05-25 16:15:03.4670000	svchost.exe	C:\Windows\TEMP\ocrE8C9tmp\lib\uby\gems\1.8\ge...	api so	c:\Windows\temp\svchost.exe	
LT-US-LDUFFY	2016-05-25 16:15:02.4370000	svchost.exe	C:\Windows\TEMP\ocrE8C9tmp\lib\uby\gems\1.8\ge...	api so	c:\Windows\temp\svchost.exe	
LT-US-LDUFFY	2016-05-25 16:15:01.8750000	svchost.exe	C:\Windows\TFMP\ocrE8C9tmp\bin\	SSI FAY32.dll	c:\Windows\temp\svchost.exe	

RSA

MANUAL DB HUNTING (HEIDI SQL)

HeidiSQL (9.9mb)

<http://www.heidisql.com/download.php>



RSA

MANUAL DB HUNTING (HEIDI SQL)

NWEndpoint\ECAT\$PRIMARY - HeidiSQL 9.4.0.5125

File Edit Search Tools Go to Help

Host: 127.0.0.1 Database: ECAT\$PRIMARY Query*

Query

```

3 SELECT
4     [mn].[MachineName]
5     ,[se].[EventUTCTime]
6     ,[sf].,[fileName]
7     ,[se].[Path__TargetProcessPathName]
8     ,[se].[FileName__TargetProcessImageFileName]
9     ,[se].[SourceCommandLine]
10    ,[se].[TargetCommandLine]
11
12 FROM [dbo].[uvw_mocSentinelEvents] AS [se] WITH(NOLOCK)
13 INNER JOIN [dbo].[machines] AS [mn] WITH(NOLOCK) ON [mn].[PK_Machines] = [se].[FK_Machines]
14 INNER JOIN [dbo].[MachineModulePaths] AS [mp] WITH(NOLOCK) ON ([mp].[PK_MachineModulePaths] = [se].[FK_MachineModulePaths])
15 INNER JOIN [dbo].[Modules] AS [mo] WITH(NOLOCK) ON ([mo].[PK_Modules] = [mp].[FK_Modules])
16 INNER JOIN [dbo].[FileNames] AS [sf] WITH(NOLOCK) ON ([sf].[PK_FileNames] = [mp].[FK_FileNames])
17
18 WHERE
19     [mo].[ModuleSignatureMicrosoft] = 0 AND
20     [mp].[BehaviorFileRenameToExecutable] = 1 AND
21     [mp].[FK_Modules] != -1 AND
22     [mp].[MarkedAsDeleted] = 0

```

Results

MachineName	EventUTCTime	FileName	Path__TargetProcessPathName	FileName__TargetProcessImageFileName	SourceCommandLine	TargetCommandLine
LT-US-LDUFFY	2016-05-25 16:15:02.4370000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\lib\ruby\gems\1.8\gems...	api.so	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:01.8750000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\bin\	SSLEAY32.dll	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:01.8750000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\bin\	ZLIB1.dll	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:01.8600000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\bin\	rubyw.exe	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:01.8750000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\bin\	msvcr7-ruby18.dll	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:01.8750000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\bin\	LIBEAY32.dll	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:02.5930000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\lib\ruby\1.8\386-mingw...	digest.so	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:02.5310000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\lib\ruby\1.8\386-mingw...	socket.so	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:03.1080000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\lib\ruby\1.8\386-mingw...	syck.so	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:02.7650000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\lib\ruby\1.8\386-mingw...	stringio.so	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:01.8600000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\src\	api.so	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:03.5290000	svhost.exe	C:\Windows\Temp\ocrE8C9.tmp\bin\	rubyw.exe	c:\Windows\temp\svhost.exe	rubyw.exe "C:\Windows\TEMP\
LT-US-LDUFFY	2016-05-25 16:15:03.4670000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\lib\ruby\gems\1.8\gems...	api.so	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:03.2480000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\lib\ruby\1.8\386-mingw...	zlib.so	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:03.1080000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\lib\ruby\1.8\386-mingw...	Win32API.so	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:03.1080000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\lib\ruby\1.8\386-mingw...	etc.so	c:\Windows\temp\svhost.exe	
LT-US-LDUFFY	2016-05-25 16:15:03.1080000	svhost.exe	C:\Windows\TEMP\ocrE8C9.tmp\lib\ruby\1.8\386-mingw...	openssl.so	c:\Windows\temp\svhost.exe	

```

10 /* Entering session "NWEndpoint" */
11 USE "ECAT$PRIMARY";
12 SELECT *, SCHEMA_NAME("schema_id") AS 'schema' FROM "ECAT$PRIMARY"."sys"."objects" WHERE "type" IN ('P', 'U', 'V', 'TR', 'FN', 'TF', 'IF');
13 --Renames_File_To_Executable.sql Renames file to executable 2      SELECT [mn].[MachineName] , [se].[EventUTCTime] , [sf].,[fileName] , [se].[Path__TargetProcessPathName] , [se].[FileName__TargetProcessImageFileName]
14 /* Affected rows: 0 Found rows: 18 Warnings: 0 Duration for 1 query: 0.094 sec. */

```

6 : 19 (912B) Connected: 00:03 h MS SQL 11.0 Uptime: 02:28 h UTC: 2016-10-20 1:30 PM Idle.

RSA

DATABASE QUERIES

RSA IR has converted IIOC into DB Queries and also created custom DB queries

((Download Link))

As of NWE 4.2.0.2 several places to query

- [dbo].[WinTrackingEvents_P0]
- [dbo].[WinTrackingEvents_P1]
- **[dbo].[uvw_mocSentinelEvents]**

Which is a view that combines two existing tables

- [dbo].[WinTrackingEvents_P0]
- [dbo].[WinTrackingEvents_P1]

SIMPLE COMMAND LINE SEARCH

```
--Template to search for a given string in the Source or Target Command Line

SELECT
    [mn].[MachineName]
    ,[se].[EventUTCTime]
    ,[sfm].[FileName]
    ,[se].[Path__TargetProcessPathName]
    ,[se].[FileName__TargetProcessImageFileName]
    ,[se].[SourceCommandLine]
    ,[se].[TargetCommandLine]

FROM [dbo].[uvw_mocSentinelEvents] AS [se] WITH(NOLOCK)
    INNER JOIN [dbo].[machines] AS [mn] WITH(NOLOCK) ON [mn].[PK_Machines] = [se].[FK_Machines]
    INNER JOIN [dbo].[MachineModulePaths] AS [mp] WITH(NOLOCK) ON ([mp].[PK_MachineModulePaths] = [se].[FK_MachineModulePaths])
    INNER JOIN [dbo].[Modules] AS [mo] WITH(NOLOCK) ON ([mo].[PK_Modules] = [mp].[FK_Modules])
    INNER JOIN [dbo].[FileNames] AS [sfm] WITH(NOLOCK) ON ([sfm].[PK_FileNames] = [mp].[FK_FileNames])

WHERE
    [se].[SourceCommandLine] LIKE N'%SEARCHSTRING%'
    OR
    [se].[TargetCommandLine] LIKE N'%SEARCHSTRING%'
```

TRACKING DATA FOR A SINGLE SYSTEM

```
--Returns tracking data (sentinel events) for the given MachineName

select [mn].[MachineName]
      ,[se].[EventUTCTime]
      ,[se].[EventType]
      ,[sfn].[FileName]
      ,[se].[Path__TargetProcessPathName]
      ,[se].[FileName__TargetProcessImageFileName]
      ,[se].[SourceCommandLine]
      ,[se].[TargetCommandLine]
      ,[se].[MarkedAsDeleted]

FROM [dbo].[uvw_mocSentinelEvents] AS [se] WITH(NOLOCK)
INNER JOIN [dbo].[Machines] AS [mn] WITH(NOLOCK) ON [mn].[PK_Machines] = [se].[FK_Machines]
INNER JOIN [dbo].[MachineModulePaths] AS [mp] WITH(NOLOCK) ON ([mp].[PK_MachineModulePaths] = [se].[FK_MachineModulePaths])
INNER JOIN [dbo].[FileNames] AS [sfn] WITH(NOLOCK) ON ([sfn].[PK_FileNames] = [mp].[FK_FileNames])

WHERE
    --Enter the MachineName Below
    mn.MachineName = N'<MachineName_Goes_Here>'

order by EventUTCTime desc
```

MANUAL QUERY EXECUTION

1. Execute individual DB Queries against the Database
2. Review the output
3. Repeat

Problem:

Some queries can take a significant time to process

Solution:

Automate the processing to allow for background processing

AUTOMATED QUERY PROCESSING

DBHunter.py

<https://github.com/timetology/ecat/blob/master/scripts/dbhunt/dbhunter.py>

Python script to take a directory of .sql files and execute them against the database serially. Each query will produce it's own .csv output file.

Use excel, your favorite text editor, or even grep to view the results.

DBHUNTER.PY

```
C:\Users\Administrator\Desktop\dbhunt>python NWE_DBHunter.9.py -h
usage: NWE_DBHunter.9.py [-h] -d <directory> [-u <user>] [-p <password>]
                         [-s <hostname or IP>] [-db <database>]
                         [-o <output_dir>] [-r] [--debug] [--progressbar]
```

For each SQL file in the supplied directory, script run the SQL Query and return the requested Data in a CSV

optional arguments:

```
-h, --help            show this help message and exit
-d <directory>, --dir <directory>
                      Directory where .SQL files are stored
-u <user>, --user <user>
                      Username for SQL Database. Default: Windows
                      Credentials
-p <password>, --pass <password>
                      Password for SQL Database. (If user specified with no
                      pass then you will be prompted for the pass)
-s <hostname or IP>, --server <hostname or IP>
                      Hostname or IP for SQL Server. Default: localhost
-db <database>, --database <database>
                      ECAT database
-o <output_dir>, --output <output_dir>
                      Output Directory
-r, --recursive      Recursively traverse directory for .sql files
--debug              Enable Debug Messages
--progressbar        Include Progress bar (requires tqdm)
```

```
C:\dbhunt>python dbhunter.py -r -d 4.2 -o
output --progressbar
100%#####
#####| 306/306 [00:14<00:00, 21.04it/s]
```

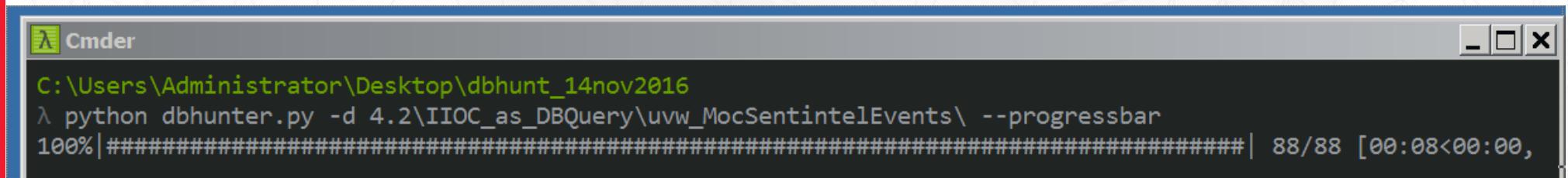
DBHUNTER.PY --DEBUG

```
C:\Users\Administrator\Desktop\dbhunt_14nov2016
\ python dbhunter.py -d 4.2\IIOC_as_DBQuery\uvw_MocSentintelEvents\ --debug

[+] Processing 4.2\IIOC_as_DBQuery\uvw_MocSentintelEvents\RSAIR_IIOC_uvw_3_Runs_REG.sql
[+] Processed SQL in 0.1673147 Seconds
[+] Processing 4.2\IIOC_as_DBQuery\uvw_MocSentintelEvents\RSAIR_IIOC_uvw_3_Runs_REG.sql
[+] Writing output to C:\Users\Administrator\Desktop\dbhunt_14nov2016\20161117-133422_RSAIR_IIOC_uvw_3_Runs_REG.sql.csv
[+] Processing 4.2\IIOC_as_DBQuery\uvw_MocSentintelEvents\RSAIR_IIOC_uvw_1_Clears_Event_Log.sql
[+] Processed SQL in 0.1550439 Seconds
[-] Warning: 4.2\IIOC_as_DBQuery\uvw_MocSentintelEvents\RSAIR_IIOC_uvw_1_Clears_Event_Log.sql returned no data
[+] Processing 4.2\IIOC_as_DBQuery\uvw_MocSentintelEvents\RSAIR_IIOC_uvw_1Creates_Process_and_Create_Remote_Thread_On_Same_Module.sql.__NEEDSTESTING_.sql
[+] Processed SQL in 0.2476143 Seconds
[+] Processing 4.2\IIOC_as_DBQuery\uvw_MocSentintelEvents\RSAIR_IIOC_uvw_1Creates_Process_and_Create_Remote_Thread_On_Same_Module.sql.__NEEDSTESTING_.sql
[+] Writing output to C:\Users\Administrator\Desktop\dbhunt_14nov2016\20161117-133422_RSAIR_IIOC_uvw_1Creates_Process_and_Create_Remote_Thread_On_Same_Module.sql.__NEEDSTESTING_.sql.csv
[+] Processing 4.2\IIOC_as_DBQuery\uvw_MocSentintelEvents\RSAIR_IIOC_uvw_1Creates_Process_and_Create_Remote_Thread_On_Same_Module.sql.__NEEDSTESTING_AltQuery.sql
[+] Processed SQL in 0.091242 Seconds
[+] Processing 4.2\IIOC_as_DBQuery\uvw_MocSentintelEvents\RSAIR_IIOC_uvw_1Creates_Process_and_Create_Remote_Thread_On_Same_Module.sql.__NEEDSTESTING_AltQuery.sql
[+] Writing output to C:\Users\Administrator\Desktop\dbhunt_14nov2016\20161117-133423_RSAIR_IIOC_uvw_1Creates_Process_and_Create_Remote_Thread_On_Same_Module.sql.__NEEDSTESTING_AltQuery.sql
```

RSA

DBHUNTER.PY --PROGRESSBAR



A screenshot of a terminal window titled "Cmder". The window shows the command line output of running "dbhunter.py" with the "--progressbar" option. The output includes the path "C:\Users\Administrator\Desktop\dbhunt_14nov2016", the command "python dbhunter.py -d 4.2\IIOC_as_DBQuery\uvw_MocSentintelEvents\ --progressbar", and a progress bar indicating 100% completion with 88/88 items processed in 00:08<00:00.

```
C:\Users\Administrator\Desktop\dbhunt_14nov2016
λ python dbhunter.py -d 4.2\IIOC_as_DBQuery\uvw_MocSentintelEvents\ --progressbar
100%|#####| 88/88 [00:08<00:00,
```

DBHUNTER OUTPUT (EXCEL)

20161114-102826_RSAIR_IIOC_WinTrackingEvents_1_Clears_Event_Log.sql.csv - Microsoft Excel

	A	B	C	D	E	F	G	H	I	J
1	MachineName	EventUTCTime	SourceFilename	TargetFilename	SourceLaunched	TargetLaunchArguments	Path_Target	FileName_Target	LaunchArguments_Target	
2	DC1	2/11/16 17:19	csrss.exe	WMIC.exe	%SystemRoot%	wmic nteventlog where LogFileName='File Rej' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='File		
3	DC1	2/11/16 17:19	csrss.exe	WMIC.exe	%SystemRoot%	wmic nteventlog where LogFileName='System' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='Sys		
4	DC1	2/11/16 17:19	csrss.exe	WMIC.exe	%SystemRoot%	wmic nteventlog where LogFileName='Applic' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='App		
5	DC1	2/11/16 17:19	csrss.exe	WMIC.exe	%SystemRoot%	wmic nteventlog where LogFileName='Power' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='Pov		
6	DC1	2/11/16 17:19	lsass.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='Applic' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='App		
7	DC1	2/11/16 17:19	lsass.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='System' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='Sys		
8	DC1	2/11/16 17:19	lsass.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='Power' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='Pov		
9	DC1	2/11/16 17:19	lsass.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='File Rej' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='File		
10	DC1	2/11/16 17:19	svchost.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='Power' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='Pov		
11	DC1	2/11/16 17:19	svchost.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='System' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='Sys		
12	DC1	2/11/16 17:19	svchost.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='Power' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='Pov		
13	DC1	2/11/16 17:19	svchost.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='System' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='Sys		
14	DC1	2/11/16 17:19	svchost.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='File Rej' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='File		
15	DC1	2/11/16 17:19	svchost.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='Applic' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='App		
16	DC1	2/11/16 17:19	svchost.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='File Rej' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='File		
17	DC1	2/11/16 17:19	svchost.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='Applic' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='App		
18	CORP9162:	2/11/16 17:32	lsass.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='Applic' C:\Windows\SysWOW64\wbem\	WMIC.exe	wmic nteventlog where LogFileName='App		
19	CORP9162:	2/11/16 17:32	lsass.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='File Rej' C:\Windows\SysWOW64\wbem\	WMIC.exe	wmic nteventlog where LogFileName='File		
20	CORP9162:	2/11/16 17:32	lsass.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='Power' C:\Windows\SysWOW64\wbem\	WMIC.exe	wmic nteventlog where LogFileName='Pov		
21	CORP9162:	2/11/16 17:32	lsass.exe	WMIC.exe	C:\Window	wmic nteventlog where LogFileName='System' C:\Windows\SysWOW64\wbem\	WMIC.exe	wmic nteventlog where LogFileName='Sys		
22	DC1	2/11/16 17:19	cmd.exe	WMIC.exe	cmd / ""C:	wmic nteventlog where LogFileName='Applic' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='App		
23	DC1	2/11/16 17:19	cmd.exe	WMIC.exe	cmd / ""C:	wmic nteventlog where LogFileName='System' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='Sys		
24	DC1	2/11/16 17:19	cmd.exe	WMIC.exe	cmd / ""C:	wmic nteventlog where LogFileName='Power' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='Pov		
25	DC1	2/11/16 17:19	cmd.exe	WMIC.exe	cmd / ""C:	wmic nteventlog where LogFileName='File Rej' C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='File		
26	CORP9162:	2/11/16 17:32	cmd.exe	WMIC.exe	"cmd.exe"	wmic nteventlog where LogFileName='System' C:\Windows\SysWOW64\wbem\	WMIC.exe	wmic nteventlog where LogFileName='Sys		

DBHUNTER OUTPUT (NOTEPAD++)

C:\Users\Administrator\Desktop\dbhunt\20161114-102826_RSAIR_IIOC_WinTrackingEvents_1_Clears_Event_Log.sql.csv - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

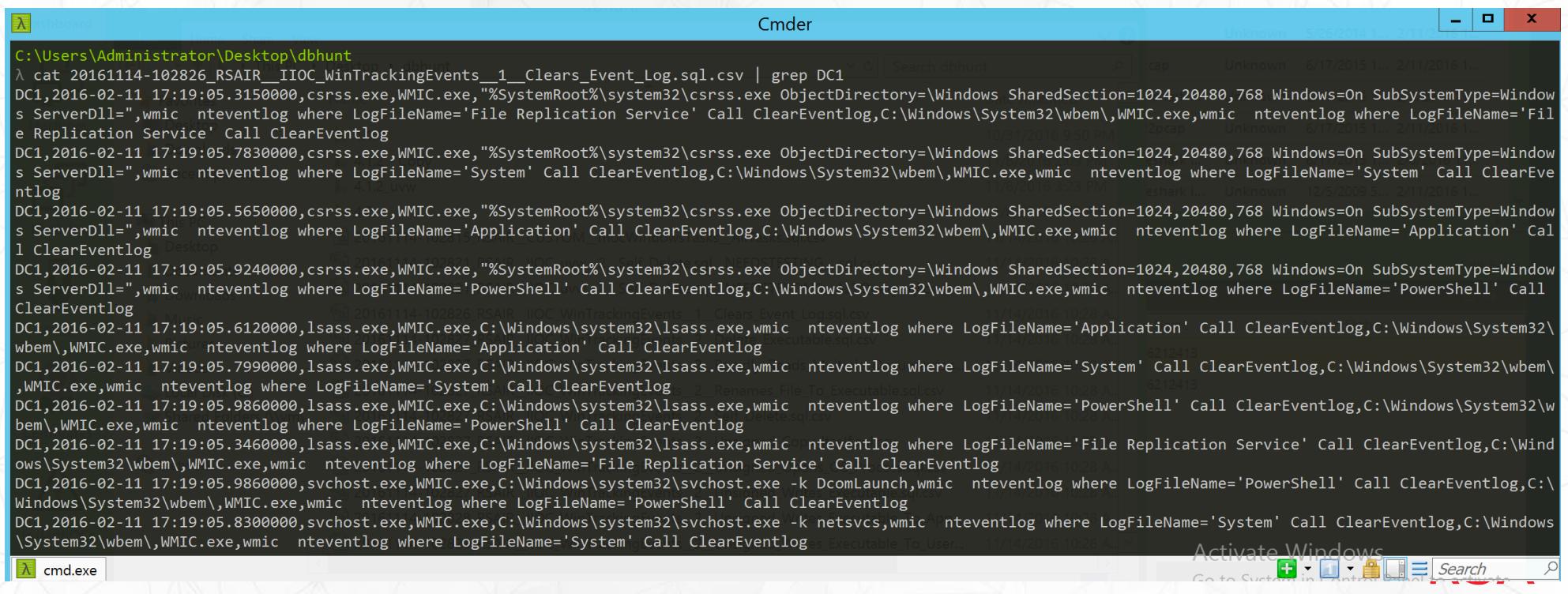
NWE_DBHunter.9.py new 1 20161114-102826_RSAIR_IIOC_WinTrackingEvents_1_Clears_Event_Log.sql.csv

```
1 MachineName,EventUTCTime,SourceFilename,TargetFilename,SourceLaunchArguments,TargetLaunchArguments,Path_Target,FileName_Target,LaunchArguments_Target
2 DC1,2016-02-11 17:19:05.3150000,csrss.exe,WMIC.exe,"%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystem
3 DC1,2016-02-11 17:19:05.7830000,csrss.exe,WMIC.exe,"%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystem
4 DC1,2016-02-11 17:19:05.5650000,csrss.exe,WMIC.exe,"%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystem
5 DC1,2016-02-11 17:19:05.9240000,csrss.exe,WMIC.exe,"%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystem
6 DC1,2016-02-11 17:19:05.6120000,lsass.exe,WMIC.exe,C:\Windows\system32\lsass.exe,wmic nteventlog where LogFileName='Application' Call ClearEventlog,C:\Window
7 DC1,2016-02-11 17:19:05.7990000,lsass.exe,WMIC.exe,C:\Windows\system32\lsass.exe,wmic nteventlog where LogFileName='System' Call ClearEventlog,C:\Windows\Sys
8 DC1,2016-02-11 17:19:05.9860000,lsass.exe,WMIC.exe,C:\Windows\system32\lsass.exe,wmic nteventlog where LogFileName='PowerShell' Call ClearEventlog,C:\Windows
9 DC1,2016-02-11 17:19:05.3460000,lsass.exe,WMIC.exe,C:\Windows\system32\lsass.exe,wmic nteventlog where LogFileName='File Replication Service' Call ClearEvent
10 DC1,2016-02-11 17:19:05.9860000,svchost.exe,WMIC.exe,C:\Windows\system32\svchost.exe -k DcomLaunch,wmic nteventlog where LogFileName='PowerShell' Call ClearE
11 DC1,2016-02-11 17:19:05.8300000,svchost.exe,WMIC.exe,C:\Windows\system32\svchost.exe -k netsvcs,wmic nteventlog where LogFileName='System' Call ClearEventlog
12 DC1,2016-02-11 17:19:06.0020000,svchost.exe,WMIC.exe,C:\Windows\system32\svchost.exe -k netsvcs,wmic nteventlog where LogFileName='PowerShell' Call ClearEven
13 DC1,2016-02-11 17:19:05.7990000,svchost.exe,WMIC.exe,C:\Windows\system32\svchost.exe -k DcomLaunch,wmic nteventlog where LogFileName='System' Call ClearEvent
14 DC1,2016-02-11 17:19:05.3770000,svchost.exe,WMIC.exe,C:\Windows\system32\svchost.exe -k netsvcs,wmic nteventlog where LogFileName='File Replication Service'
15 DC1,2016-02-11 17:19:05.5960000,svchost.exe,WMIC.exe,C:\Windows\system32\svchost.exe -k DcomLaunch,wmic nteventlog where LogFileName='Application' Call Clear
16 DC1,2016-02-11 17:19:05.3460000,svchost.exe,WMIC.exe,C:\Windows\system32\svchost.exe -k DcomLaunch,wmic nteventlog where LogFileName='File Replication Servic
17 DC1,2016-02-11 17:19:05.6270000,svchost.exe,WMIC.exe,C:\Windows\system32\svchost.exe -k netsvcs,wmic nteventlog where LogFileName='Application' Call ClearEve
18 CORP916212413,2016-02-11 17:32:57.0750000,lsass.exe,WMIC.exe,C:\Windows\system32\lsass.exe,wmic nteventlog where LogFileName='Application' Call ClearEventlog
19 CORP916212413,2016-02-11 17:32:56.6850000,lsass.exe,WMIC.exe,C:\Windows\system32\lsass.exe,wmic nteventlog where LogFileName='File Replication Service' Call
20 CORP916212413,2016-02-11 17:32:57.5590000,lsass.exe,WMIC.exe,C:\Windows\system32\lsass.exe,wmic nteventlog where LogFileName='PowerShell' Call ClearEventlog,
21 CORP916212413,2016-02-11 17:32:57.2940000,lsass.exe,WMIC.exe,C:\Windows\system32\lsass.exe,wmic nteventlog where LogFileName='System' Call ClearEventlog,C:\W
22 DC1,2016-02-11 17:19:05.5650000,cmd.exe,WMIC.exe,"cmd /c ""C:\Windows\Temp\c.bat"" "",wmic nteventlog where LogFileName='Application' Call ClearEventlog,C
23 DC1,2016-02-11 17:19:05.7830000,cmd.exe,WMIC.exe,"cmd /c ""C:\Windows\Temp\c.bat"" "",wmic nteventlog where LogFileName='System' Call ClearEventlog,C:\Win
24 DC1,2016-02-11 17:19:05.9240000,cmd.exe,WMIC.exe,"cmd /c ""C:\Windows\Temp\c.bat"" "",wmic nteventlog where LogFileName='PowerShell' Call ClearEventlog,C:
25 DC1,2016-02-11 17:19:05.3150000,cmd.exe,WMIC.exe,"cmd /c ""C:\Windows\Temp\c.bat"" "",wmic nteventlog where LogFileName='File Replication Service' Call Cl
26 CORP916212413,2016-02-11 17:32:57.2310000,cmd.exe,WMIC.exe,"""cmd.exe""",wmic nteventlog where LogFileName='System' Call ClearEventlog,C:\Windows\SysWOW64\wb
27 CORP916212413,2016-02-11 17:32:56.9970000,cmd.exe,WMIC.exe,"""cmd.exe""",wmic nteventlog where LogFileName='Application' Call ClearEventlog,C:\Windows\SysWOW
28 CORP916212413,2016-02-11 17:32:57.4810000,cmd.exe,WMIC.exe,"""cmd.exe""",wmic nteventlog where LogFileName='PowerShell' Call ClearEventlog,C:\Windows\SysWOW6
29 CORP916212413,2016-02-11 17:32:56.6230000,cmd.exe,WMIC.exe,"""cmd.exe""",wmic nteventlog where LogFileName='File Replication Service' Call ClearEventlog,C:\W
30 CORP916212413,2016-02-11 17:32:57.2620000,conhost.exe,WMIC.exe,"\\?\C:\Windows\system32\conhost.exe ""-548504941-74016455815081108261345374636716585348-137478
31 CORP916212413,2016-02-11 17:32:56.6380000,conhost.exe,WMIC.exe,"\\?\C:\Windows\system32\conhost.exe ""-548504941-74016455815081108261345374636716585348-137478
32 CORP916212413,2016-02-11 17:32:57.0440000,conhost.exe,WMIC.exe,"\\?\C:\Windows\system32\conhost.exe ""-548504941-74016455815081108261345374636716585348-137478
33 CORP916212413,2016-02-11 17:32:57.5280000,conhost.exe,WMIC.exe,"\\?\C:\Windows\system32\conhost.exe ""-548504941-74016455815081108261345374636716585348-137478
34 DC1,2016-02-11 17:19:05.5800000,conhost.exe,WMIC.exe,"\\?\C:\Windows\system32\conhost.exe 0x4,wmic nteventlog where LogFileName='Application' Call ClearEventl
35 DC1,2016-02-11 17:19:05.7830000,conhost.exe,WMIC.exe,"\\?\C:\Windows\system32\conhost.exe 0x4,wmic nteventlog where LogFileName='System' Call ClearEventlog,C:
36 DC1,2016-02-11 17:19:05.3300000,conhost.exe,WMIC.exe,"\\?\C:\Windows\system32\conhost.exe 0x4,wmic nteventlog where LogFileName='File Replication Service' Cal
37 DC1,2016-02-11 17:19:05.9400000,conhost.exe,WMIC.exe,"\\?\C:\Windows\system32\conhost.exe 0x4,wmic nteventlog where LogFileName='PowerShell' Call ClearEventlo
```

DBHUNTER OUTPUT (CMDER / GREP)

Cmder (<http://cmder.net/>)

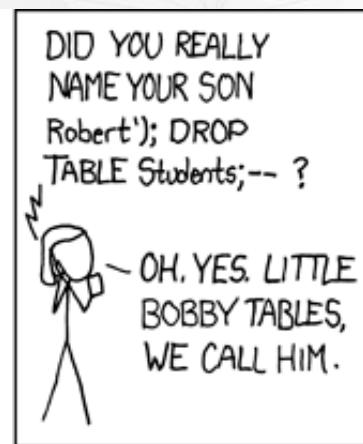
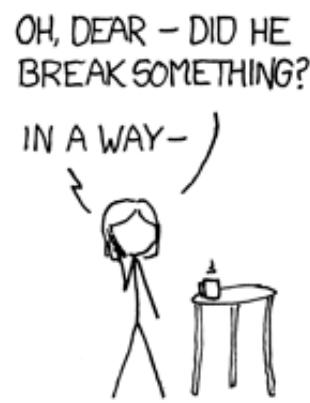
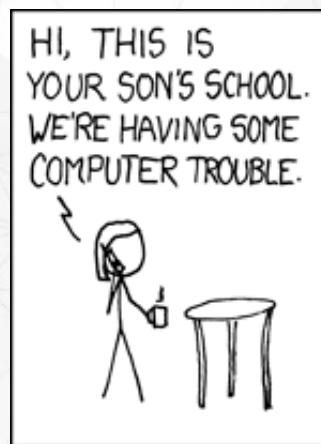
UnixUtils (<https://sourceforge.net/projects/uxutils/>)



```
C:\Users\Administrator\Desktop\dbhunt
λ cat 20161114-102826_RSAIR_IIOC_WinTrackingEvents_1_Clears_Event_Log.sql.csv | grep DC1
DC1,2016-02-11 17:19:05.315000,csrss.exe,WMIC.exe,"%SystemRoot%\system32\csrss.exe ObjectDirectory=\\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Window
s ServerDll=",wmic nteventlog where LogFileName='File Replication Service' Call ClearEventlog,C:\Windows\System32\wbem\,WMIC.exe,wmic nteventlog where LogFileName='Fil
e Replication Service' Call ClearEventlog
DC1,2016-02-11 17:19:05.783000,csrss.exe,WMIC.exe,"%SystemRoot%\system32\csrss.exe ObjectDirectory=\\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Window
s ServerDll=",wmic nteventlog where LogFileName='System' Call ClearEventlog,C:\Windows\System32\wbem\,WMIC.exe,wmic nteventlog where LogFileName='System' Call ClearEve
ntlog
DC1,2016-02-11 17:19:05.565000,csrss.exe,WMIC.exe,"%SystemRoot%\system32\csrss.exe ObjectDirectory=\\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Window
s ServerDll=",wmic nteventlog where LogFileName='Application' Call ClearEventlog,C:\Windows\System32\wbem\,WMIC.exe,wmic nteventlog where LogFileName='Application' Cal
l ClearEventlog
DC1,2016-02-11 17:19:05.924000,csrss.exe,WMIC.exe,"%SystemRoot%\system32\csrss.exe ObjectDirectory=\\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Window
s ServerDll=",wmic nteventlog where LogFileName='PowerShell' Call ClearEventlog,C:\Windows\System32\wbem\,WMIC.exe,wmic nteventlog where LogFileName='PowerShell' Call
ClearEventlog
DC1,2016-02-11 17:19:05.612000,lsass.exe,WMIC.exe,C:\Windows\system32\lsass.exe,wmic nteventlog where LogFileName='Application' Call ClearEventlog,C:\Windows\System32\w
bem\,WMIC.exe,wmic nteventlog where LogFileName='Application' Call ClearEventlog
DC1,2016-02-11 17:19:05.799000,lsass.exe,WMIC.exe,C:\Windows\system32\lsass.exe,wmic nteventlog where LogFileName='System' Call ClearEventlog,C:\Windows\System32\wbem\,
WMIC.exe,wmic nteventlog where LogFileName='System' Call ClearEventlog
DC1,2016-02-11 17:19:05.986000,lsass.exe,WMIC.exe,C:\Windows\system32\lsass.exe,wmic nteventlog where LogFileName='PowerShell' Call ClearEventlog,C:\Windows\System32\w
bem\,WMIC.exe,wmic nteventlog where LogFileName='PowerShell' Call ClearEventlog
DC1,2016-02-11 17:19:05.346000,lsass.exe,WMIC.exe,C:\Windows\system32\lsass.exe,wmic nteventlog where LogFileName='File Replication Service' Call ClearEventlog,C:\Wind
ows\System32\wbem\,WMIC.exe,wmic nteventlog where LogFileName='File Replication Service' Call ClearEventlog
DC1,2016-02-11 17:19:05.986000,svchost.exe,WMIC.exe,C:\Windows\system32\svchost.exe -k DcomLaunch,wmic nteventlog where LogFileName='PowerShell' Call ClearEventlog,C:\W
indows\System32\wbem\,WMIC.exe,wmic nteventlog where LogFileName='PowerShell' Call ClearEventlog
DC1,2016-02-11 17:19:05.830000,svchost.exe,WMIC.exe,C:\Windows\system32\svchost.exe -k netsvcs,wmic nteventlog where LogFileName='System' Call ClearEventlog,C:\Windows
\System32\wbem\,WMIC.exe,wmic nteventlog where LogFileName='System' Call ClearEventlog
cmd.exe | Activate Windows | Go to System in Internet Explorer | Search | + | - | x
```

CAVEATS AND WARNINGS

You are executing queries against the actual NetWitness Endpoint Database. Be careful what you run. One drop table and your day could get less fun real quick.



QUESTIONS?



NETWITNESS ENDPOINT (NWE)