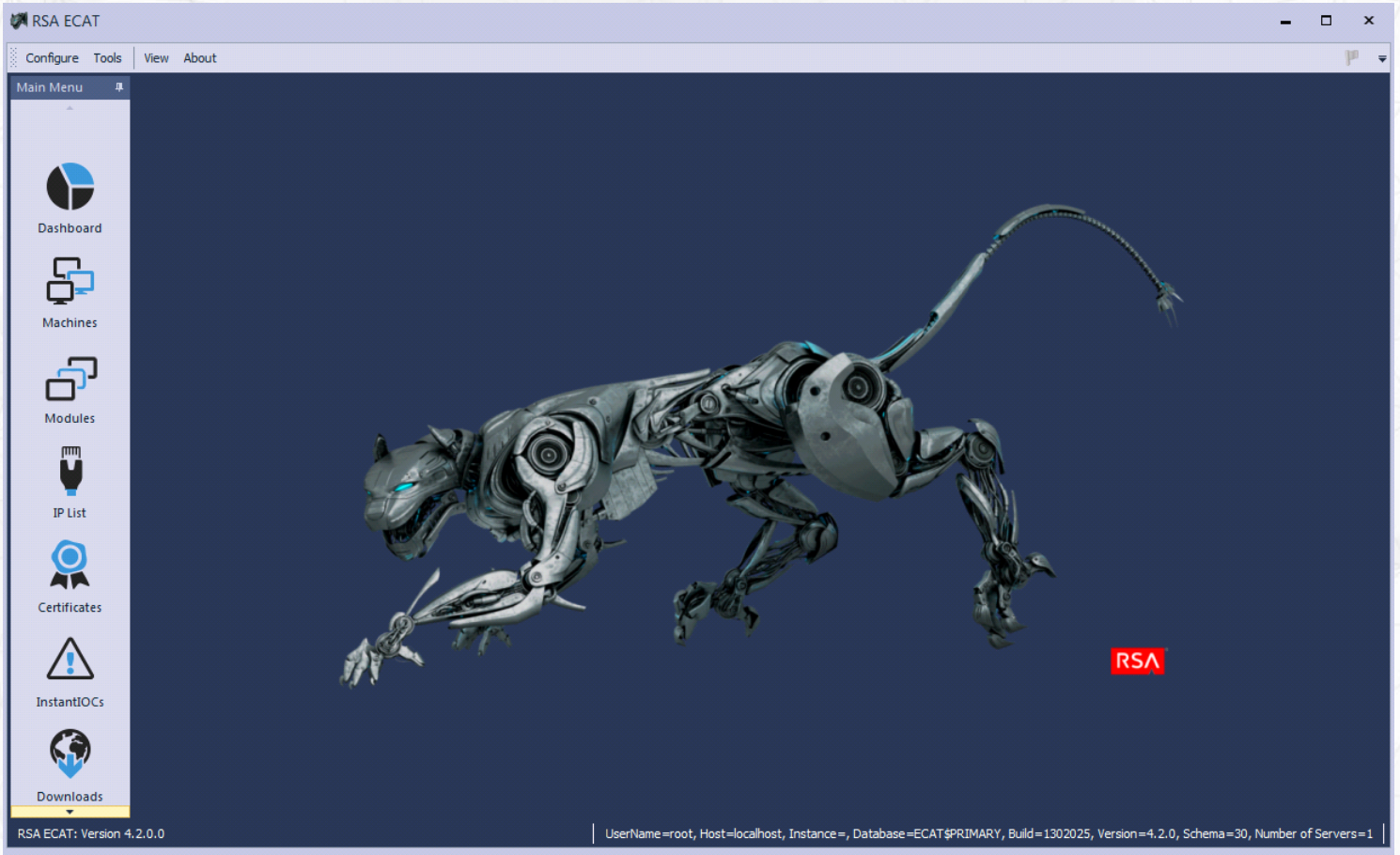
RSA INCIDENT RESPONSE

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

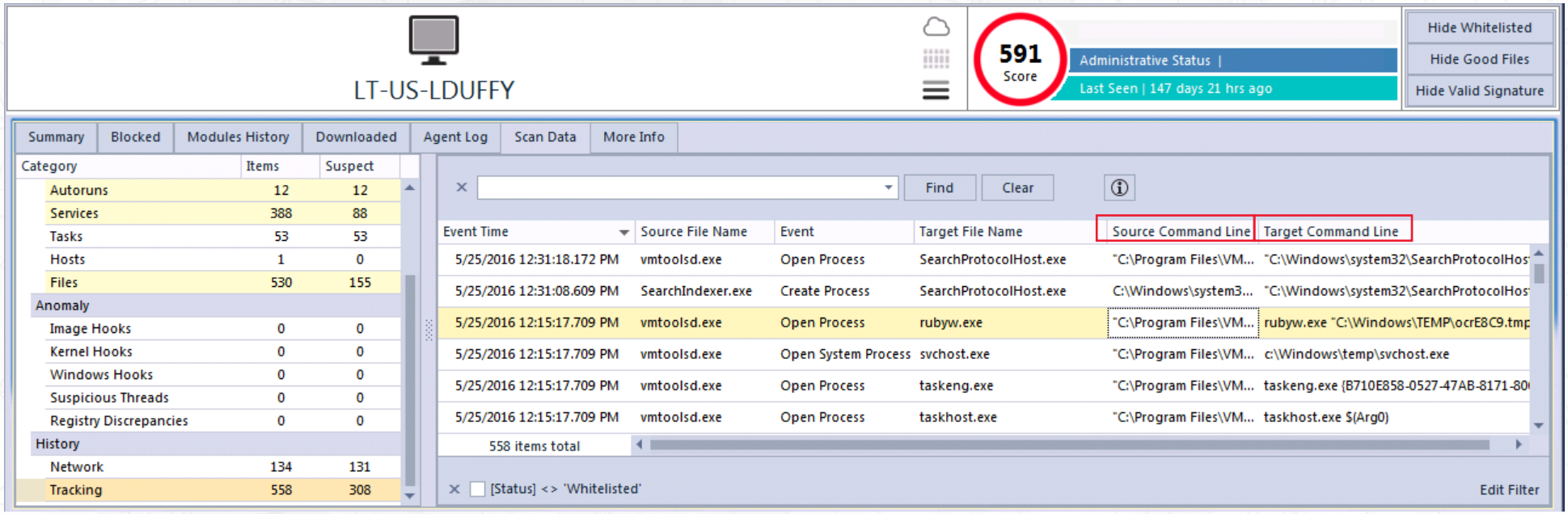
RSA

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

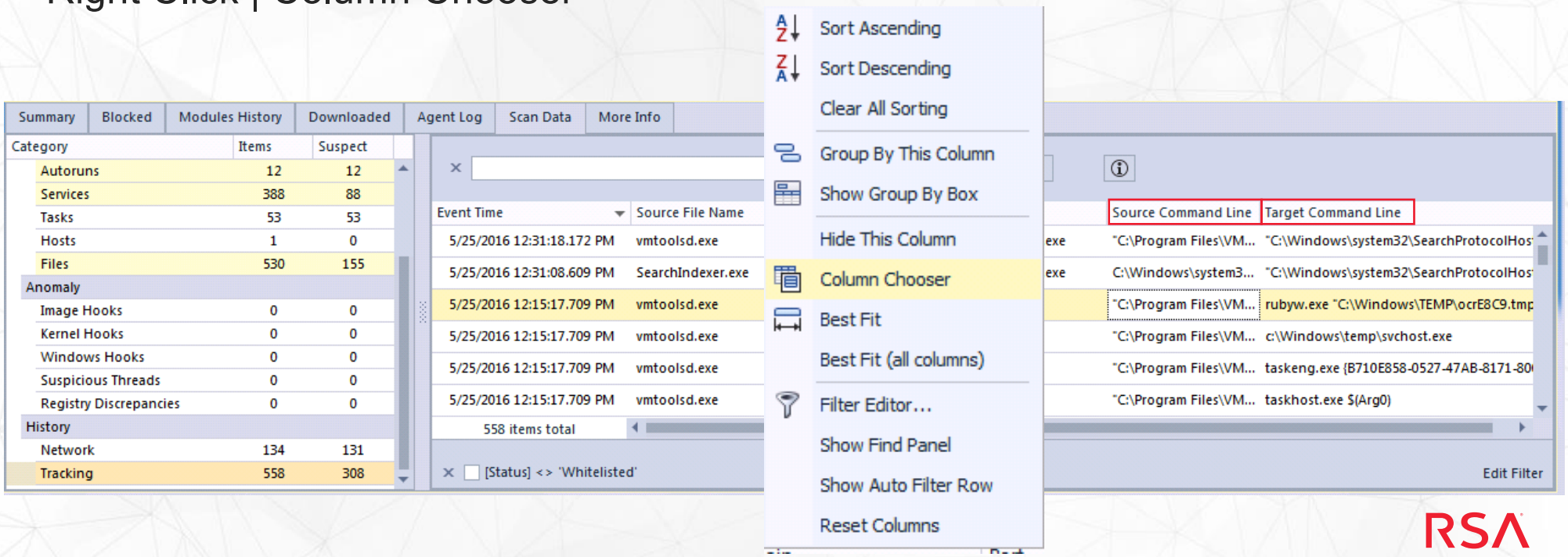
NWE TRACKING EVENTS UI VIEW



NWE TRACKING EVENTS UI VIEW

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

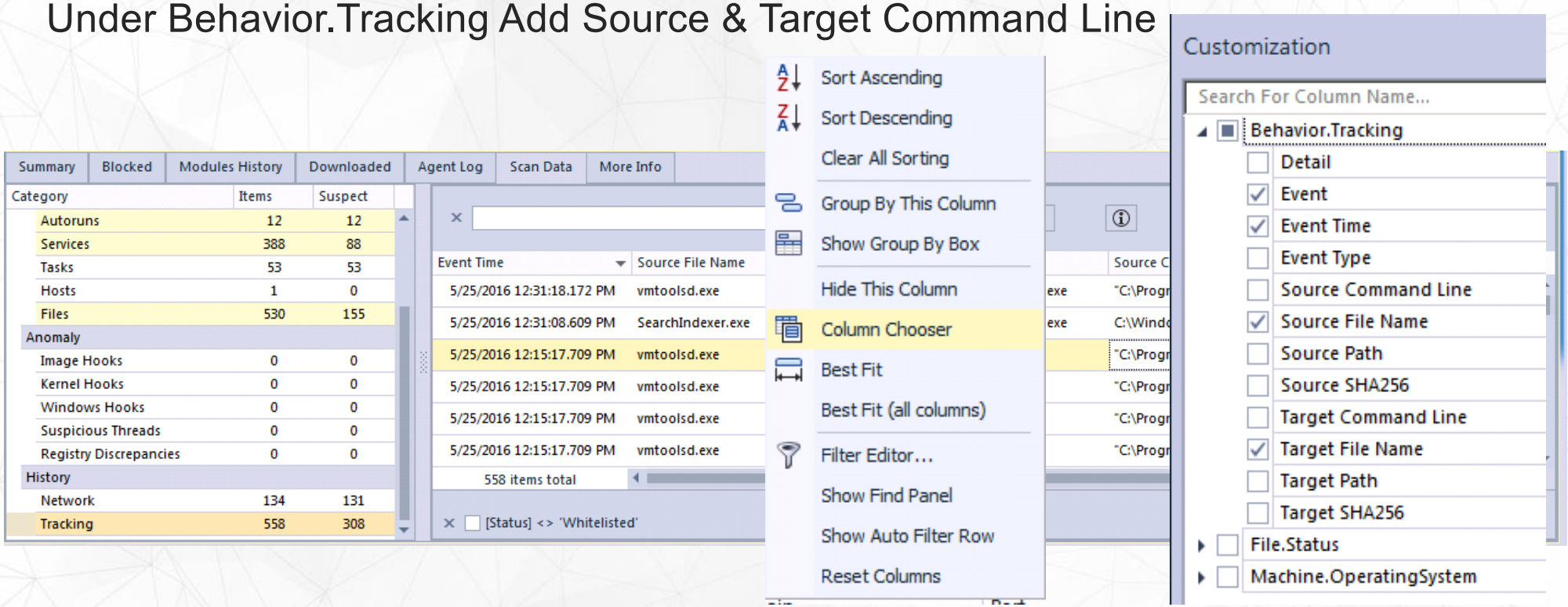
Right Click | Column Chooser



NETWITNESS ENDPOINT (NWE)

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

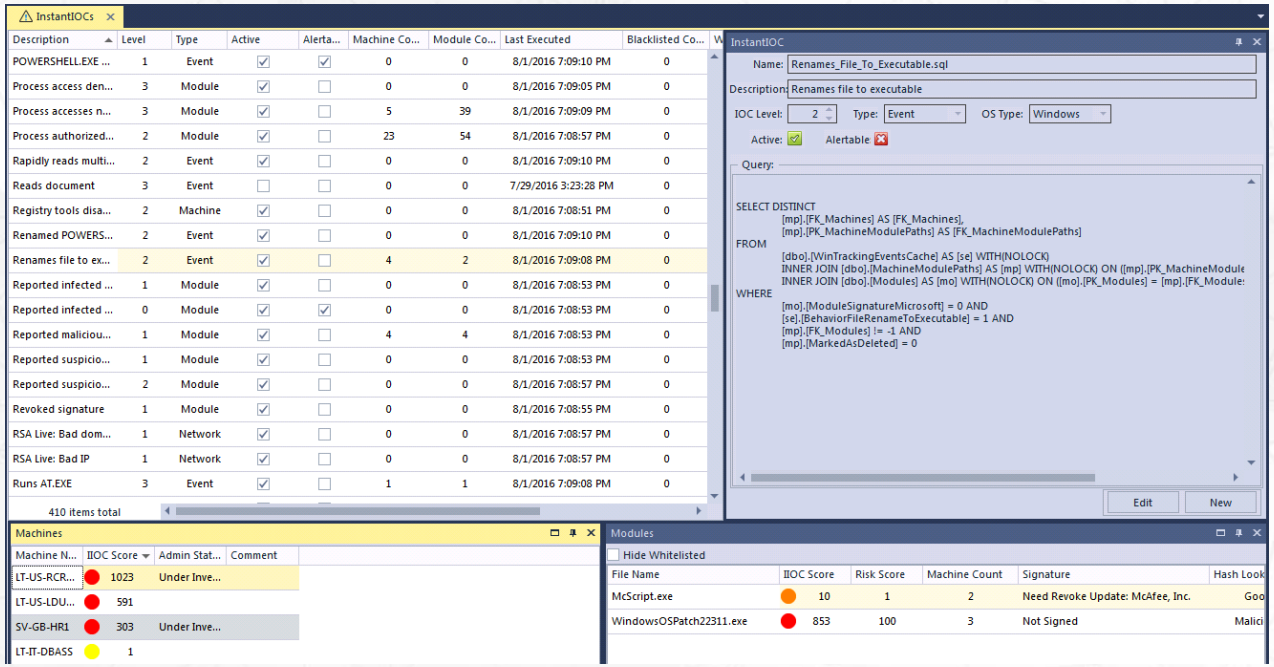
Under Behavior.Tracking Add Source & Target Command Line



INSTANT INDICATOR OF COMPROMISE (IIOC)

Event IIOC are based on tracking events

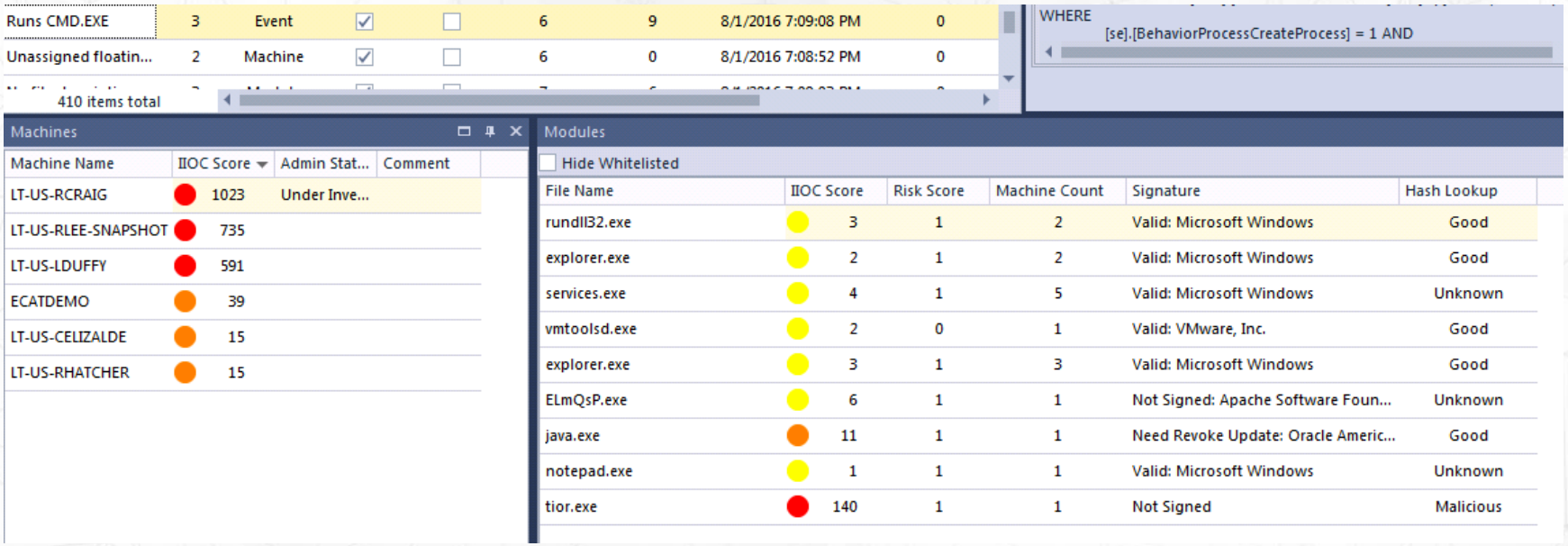
IIOC view is the closest we have to a ‘global’ tracking events view



THE 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



Runs CMD.EXE	3	Event	☑	☐	6	9	8/1/2016 7:09:08 PM	0
Unassigned floatin...	2	Machine	☑	☐	6	0	8/1/2016 7:08:52 PM	0

410 items total

```
WHERE
    [se].[BehaviorProcessCreateProcess] = 1 AND
```

Machines

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

☐ Hide Whitelisted

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

RSA

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’

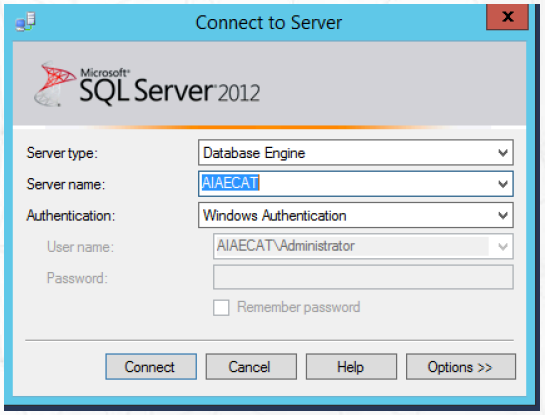
DBHUNTING!

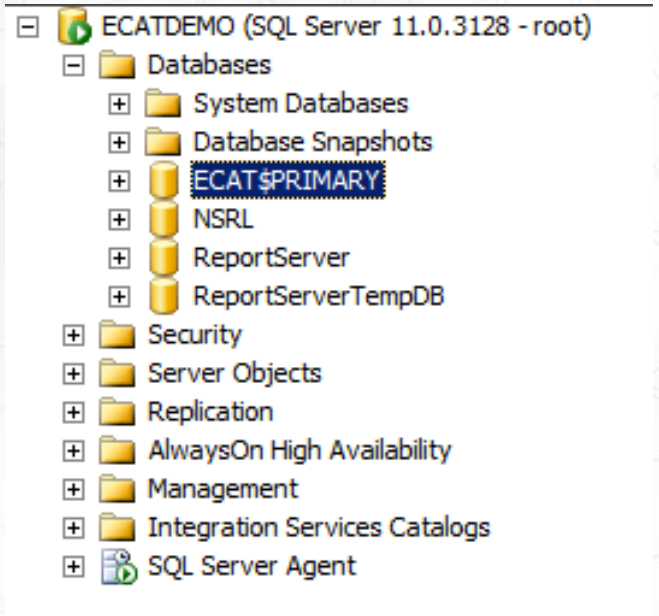
RSA

MANUAL DB HUNTING (MSSQL)

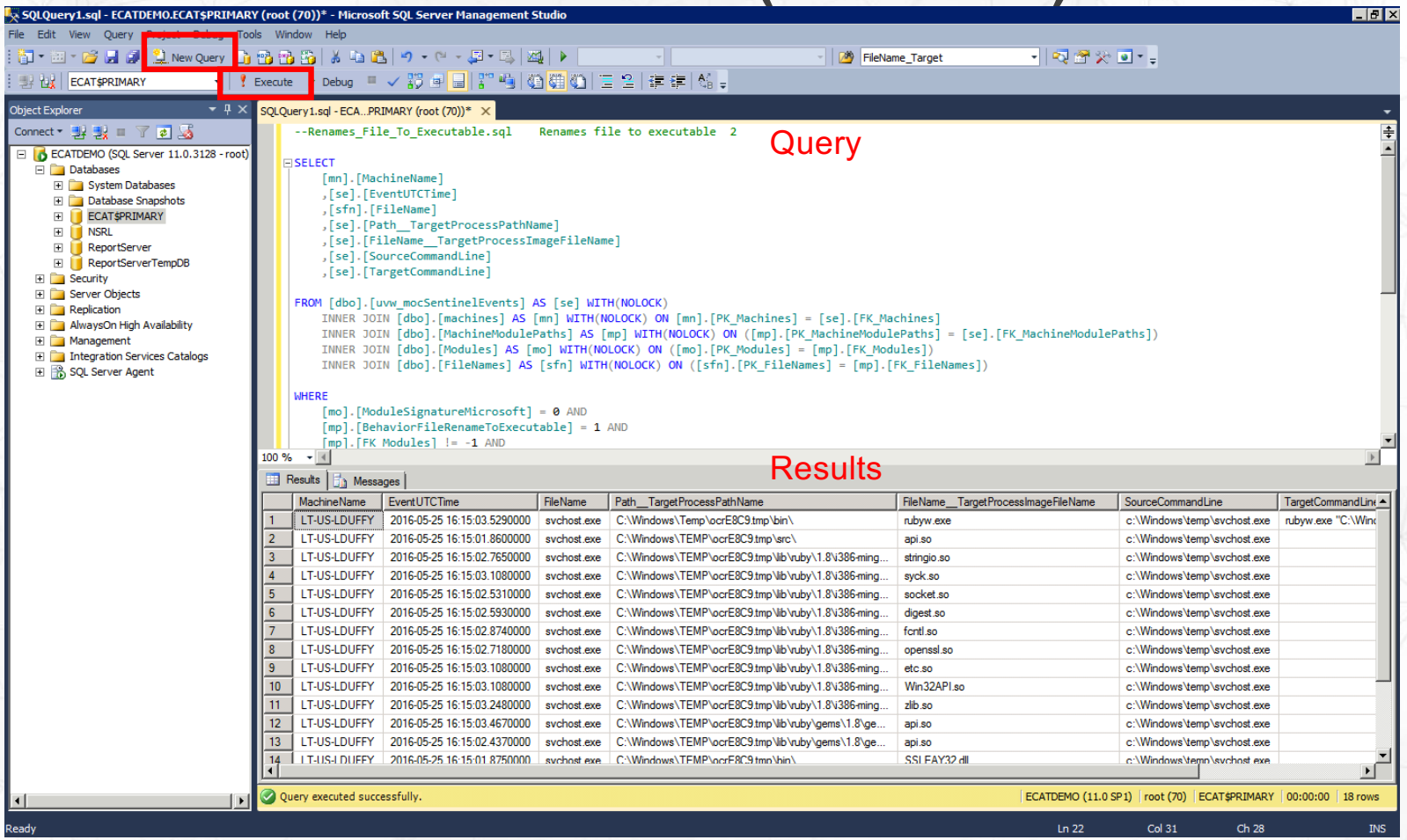
Microsoft SQL Server Management Studio (894mb)

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





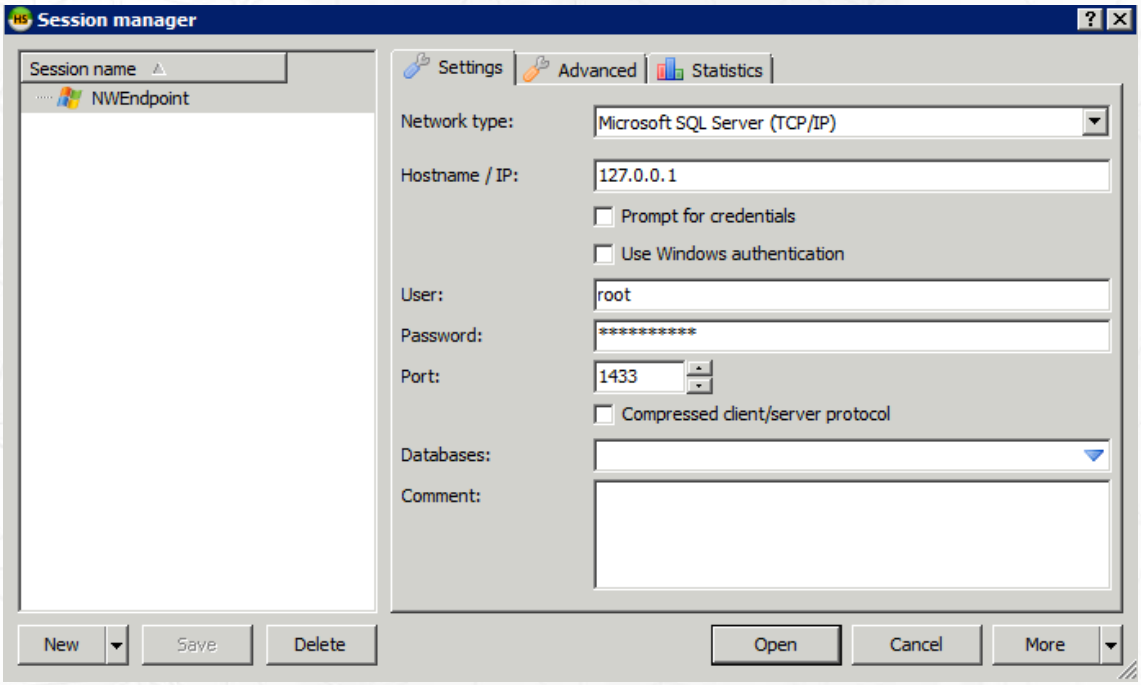
MANUAL DB HUNTING (MSSQL)

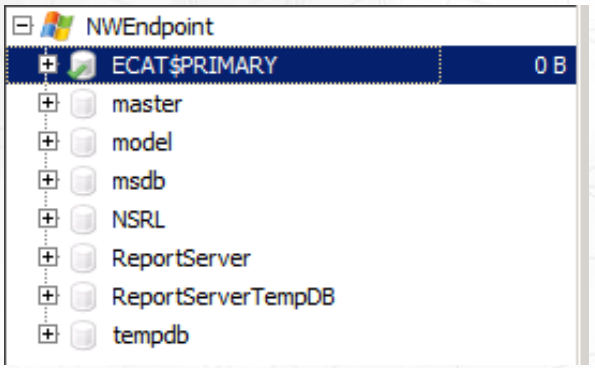


MANUAL DB HUNTING (HEIDI SQL)

HeidiSQL (9.9mb)

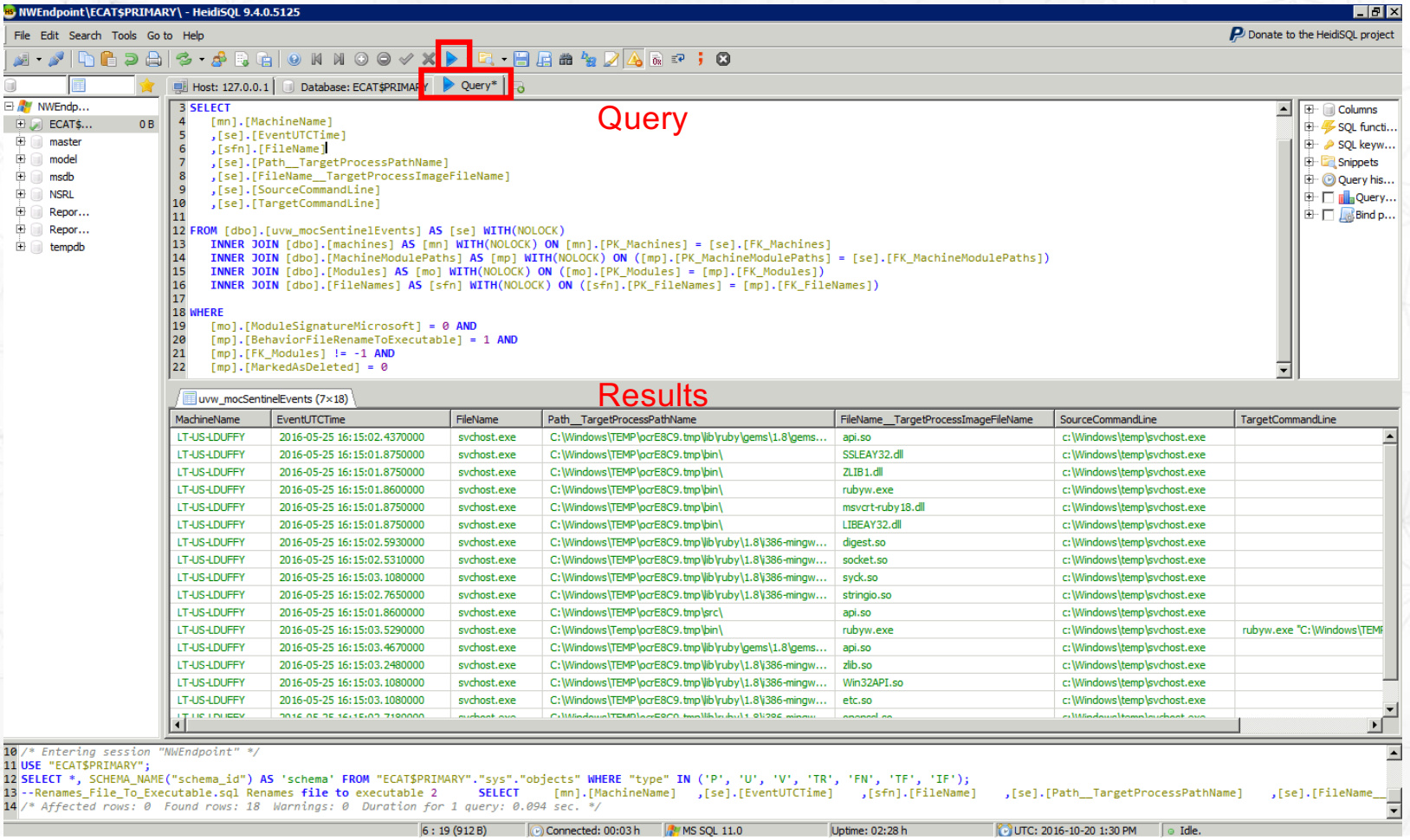
http://www.heidisql.com/download.php





RSA

MANUAL DB HUNTING (HEIDI SQL)



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]
    ,[sfn].[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 [sfn] WITH(NOLOCK) ON ([sfn].[PK_FileNames] = [mp].[FK_FileNames])

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

RSA

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
```

RSA

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

RSA

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.

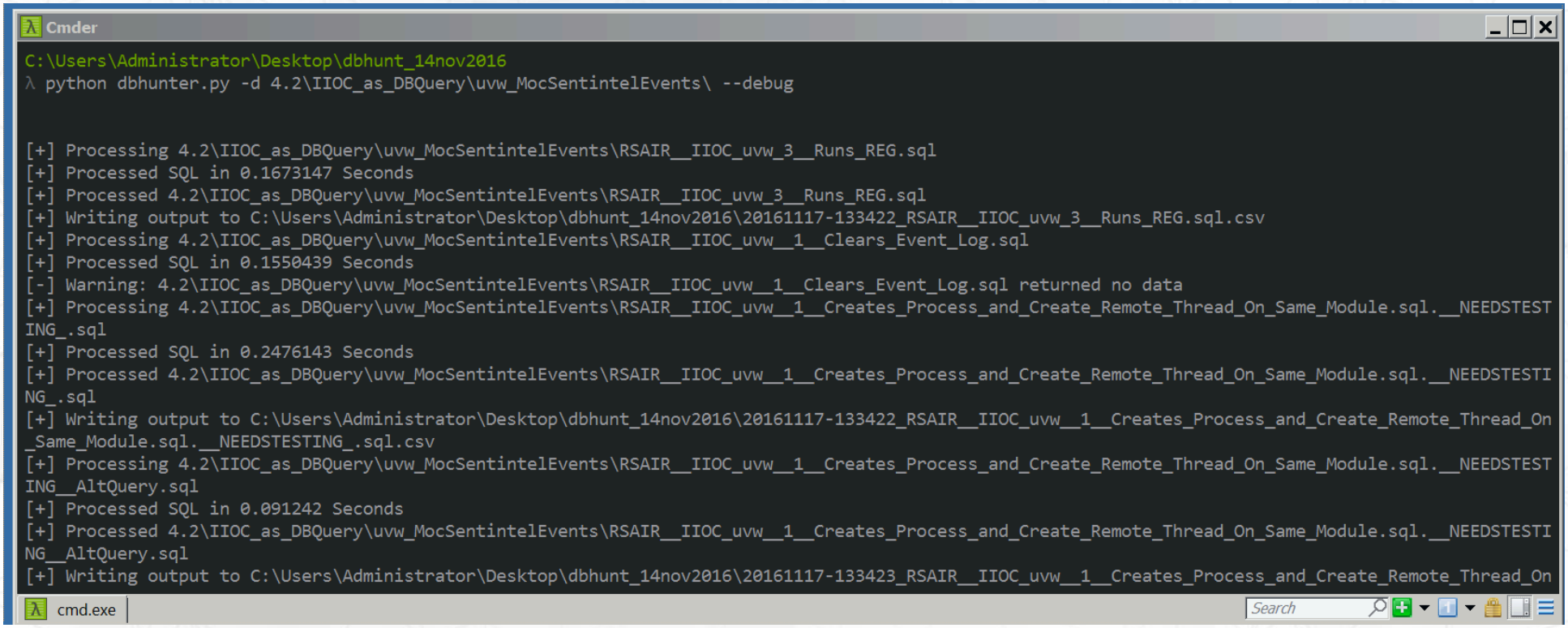
RSA

DBHUNTER.PY

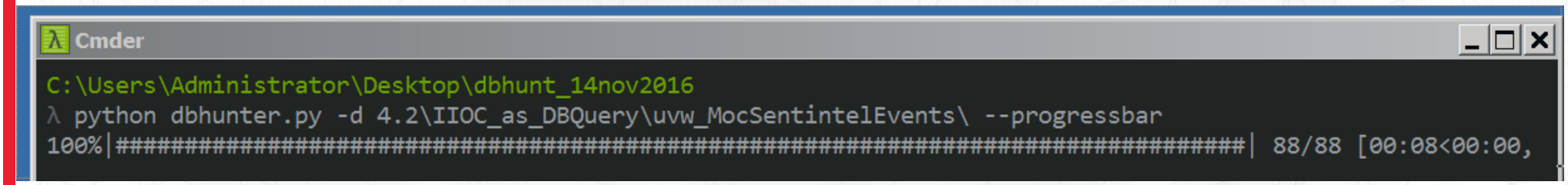
```
C:\Users\Administrator\Desktop\dbhunt>python NWE_DBHunter.9.py -h
usage: NWE_DBHunter.9.py [-h] -d <directory> [-u <user>] [-p <password>]
                         [-s <hostname or IP>] [-db <database>]
                         [-o <output_dir>] [-r] [--debug] [--progressbar]

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

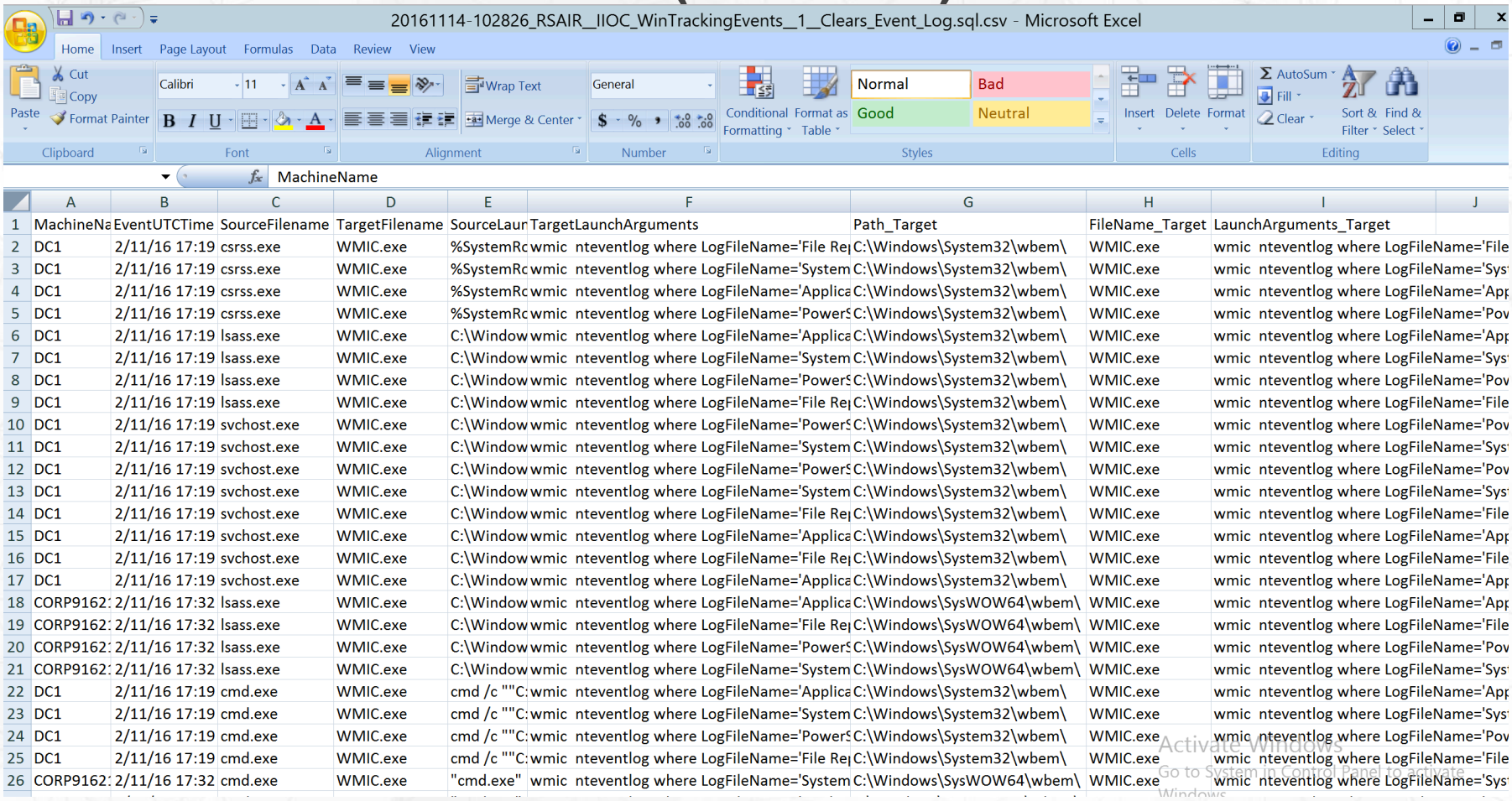


DBHUNTER.PY --PROGRESSBAR



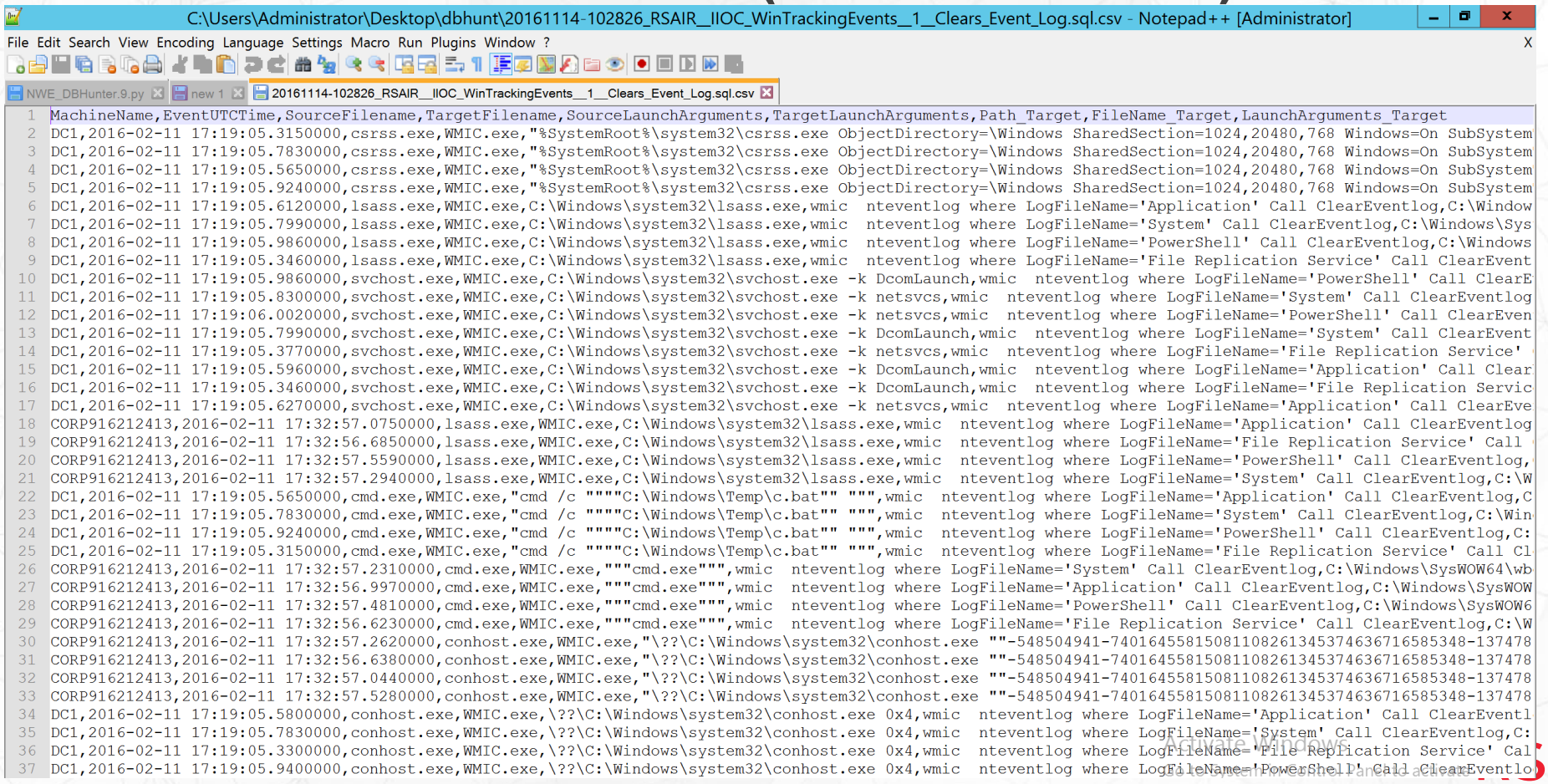
RSA

DBHUNTER OUTPUT (EXCEL)



	A	B	C	D	E	F	G	H	I	J
1	MachineNa	EventUTCTime	SourceFilename	TargetFilename	SourceLaun	TargetLaunchArguments	Path_Target	FileName_Target	LaunchArguments_Target	
2	DC1	2/11/16 17:19	csrss.exe	WMIC.exe	%SystemRc	wmic nteventlog where LogFileName='File Re	C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='File	
3	DC1	2/11/16 17:19	csrss.exe	WMIC.exe	%SystemRc	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	%SystemRc	wmic nteventlog where LogFileName='Applica	C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='App	
5	DC1	2/11/16 17:19	csrss.exe	WMIC.exe	%SystemRc	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='Applica	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 Re	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 Re	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='Applica	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 Re	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='Applica	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='Applica	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 Re	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 ""C:	wmic nteventlog where LogFileName='Applica	C:\Windows\System32\wbem\	WMIC.exe	wmic nteventlog where LogFileName='App	
23	DC1	2/11/16 17:19	cmd.exe	WMIC.exe	cmd /c ""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 ""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 ""C:	wmic nteventlog where LogFileName='File Re	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 ?

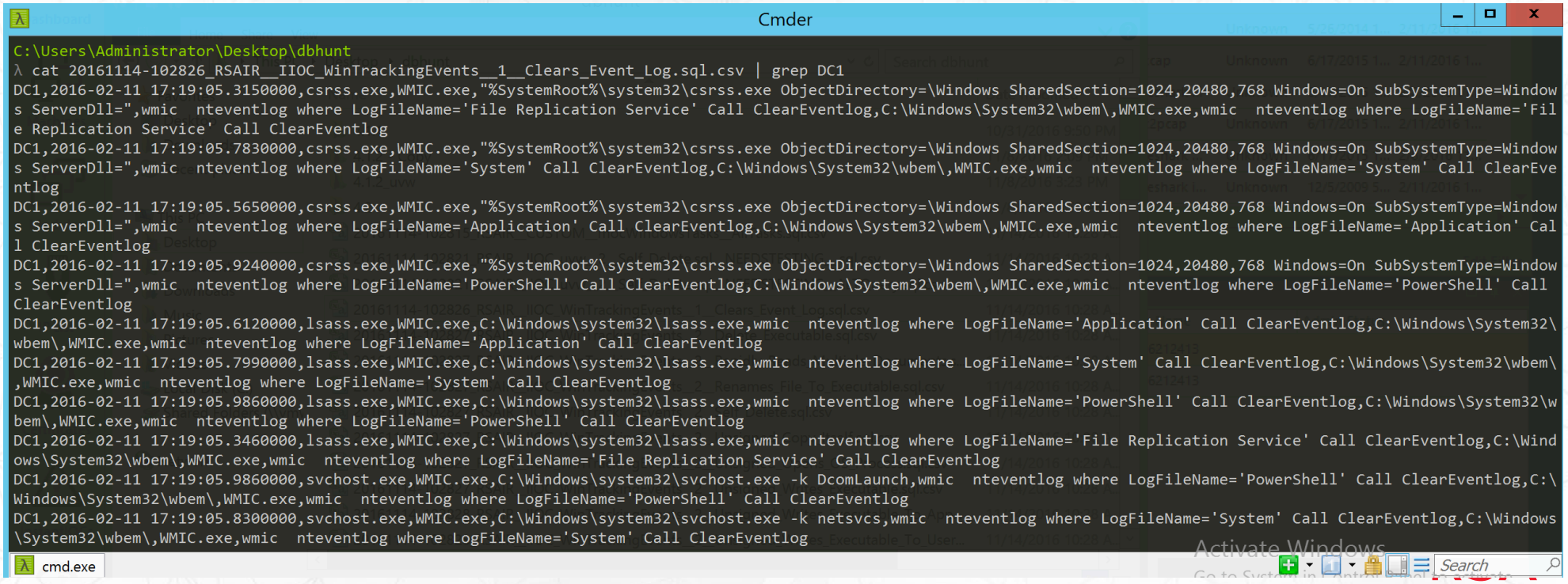
NWE_DBHunter.9.py | new 1 | 20161114-102826_RSAIR__IIOC_WinTrackingEvents__1__Clears_Event_Log.sql.csv

```
MachineName,EventUTCTime,SourceFilename,TargetFilename,SourceLaunchArguments,TargetLaunchArguments,Path_Target,FileName_Target,LaunchArguments_Target
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
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
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
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
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
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
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
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
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
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
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
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
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'
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
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
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
CORP916212413,2016-02-11 17:32:57.0750000,lsass.exe,WMIC.exe,C:\Windows\system32\lsass.exe,wmic  nteventlog where LogFileName='Application' Call ClearEventlog
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
CORP916212413,2016-02-11 17:32:57.5590000,lsass.exe,WMIC.exe,C:\Windows\system32\lsass.exe,wmic  nteventlog where LogFileName='PowerShell' Call ClearEventlog,
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
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
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
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:
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
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
CORP916212413,2016-02-11 17:32:56.9970000,cmd.exe,WMIC.exe,""""cmd.exe"""",wmic  nteventlog where LogFileName='Application' Call ClearEventlog,C:\Windows\SysWOW
CORP916212413,2016-02-11 17:32:57.4810000,cmd.exe,WMIC.exe,""""cmd.exe"""",wmic  nteventlog where LogFileName='PowerShell' Call ClearEventlog,C:\Windows\SysWOW6
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
CORP916212413,2016-02-11 17:32:57.2620000,conhost.exe,WMIC.exe,"\??\C:\Windows\system32\conhost.exe ""-548504941-740164558150811082613453746367165853 48-137478
CORP916212413,2016-02-11 17:32:56.6380000,conhost.exe,WMIC.exe,"\??\C:\Windows\system32\conhost.exe ""-548504941-740164558150811082613453746367165853 48-137478
CORP916212413,2016-02-11 17:32:57.0440000,conhost.exe,WMIC.exe,"\??\C:\Windows\system32\conhost.exe ""-548504941-740164558150811082613453746367165853 48-137478
CORP916212413,2016-02-11 17:32:57.5280000,conhost.exe,WMIC.exe,"\??\C:\Windows\system32\conhost.exe ""-548504941-740164558150811082613453746367165853 48-137478
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
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:
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
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)

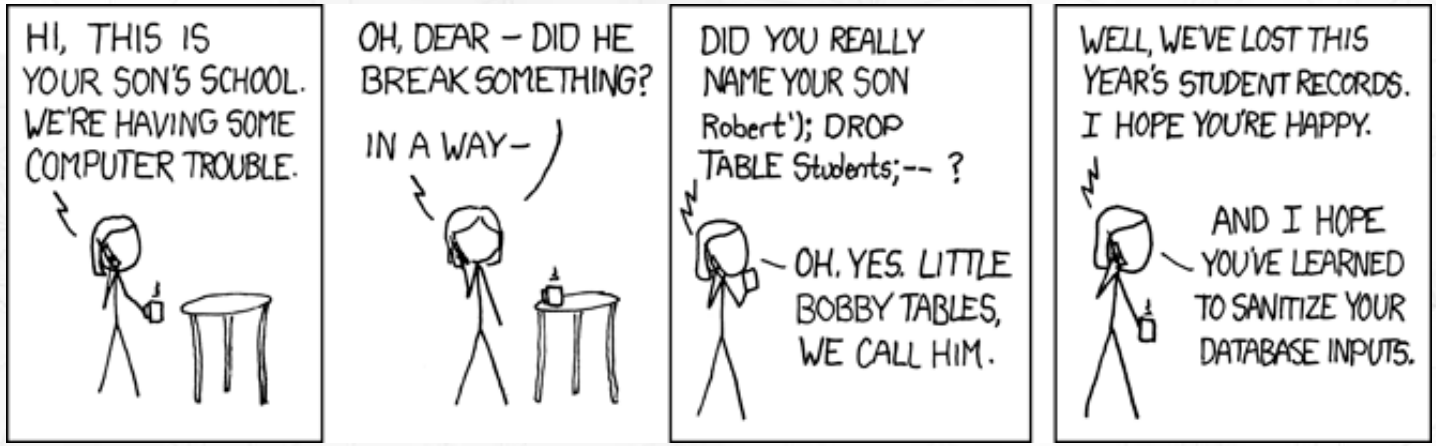
Cmder (http://cmder.net/)

UnixUtils (https://sourceforge.net/projects/unxutils/)



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?

RSA

NETWITNESS ENDPOINT (NWE)

RSA