RSA®Conference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: SDS-R04

Distributed Forensic Collection and Analysis: Fast, Surgical, at Scale and Free!

Dr Michael Cohen

Digital Paleontologist
Velocidex Enterprises

Nick Klein

Director, Velocidex Enterprises
Director, Klein & Co. Computer Forensics
SANS DFIR Certified Instructor

Who are we?

Dr Michael Cohen

- Experienced digital forensic software developer
- Developer of foundation forensic tools including Volatility and Rekall
- Former lead developer of Grr Rapid Response at Google Inc.

Nick Klein

- Director of Klein & Co. digital forensic and cyber response team
- SANS DFIR Certified Instructor.

What’s the challenge?

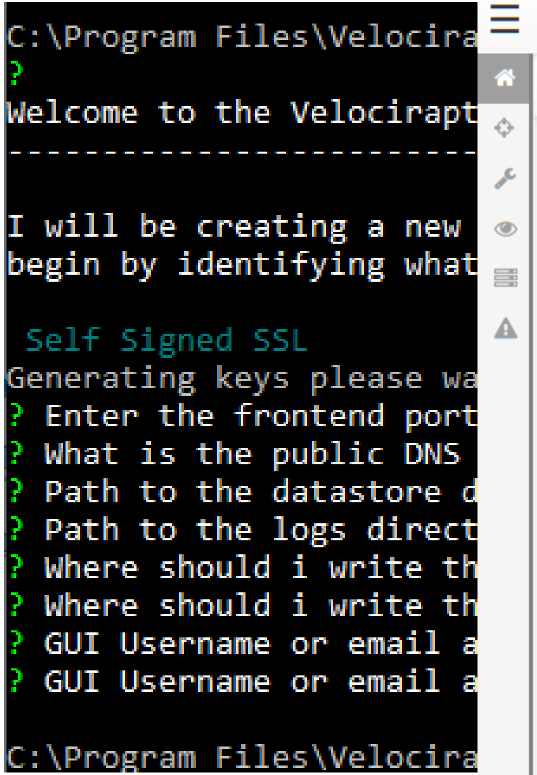
- **Deep visibility of endpoints** is a game changer for digital forensic investigations, threat hunting and cyber breach response.
- Many endpoint monitoring products now exist, but there are few powerful tools to **truly interrogate and collect historic evidence** from across a network.
- For example, an EDR tool may show network connections, but can it also interrogate the Internet history of all users?
- We’re building Velociraptor to address these limitations.

Why Velociraptor?

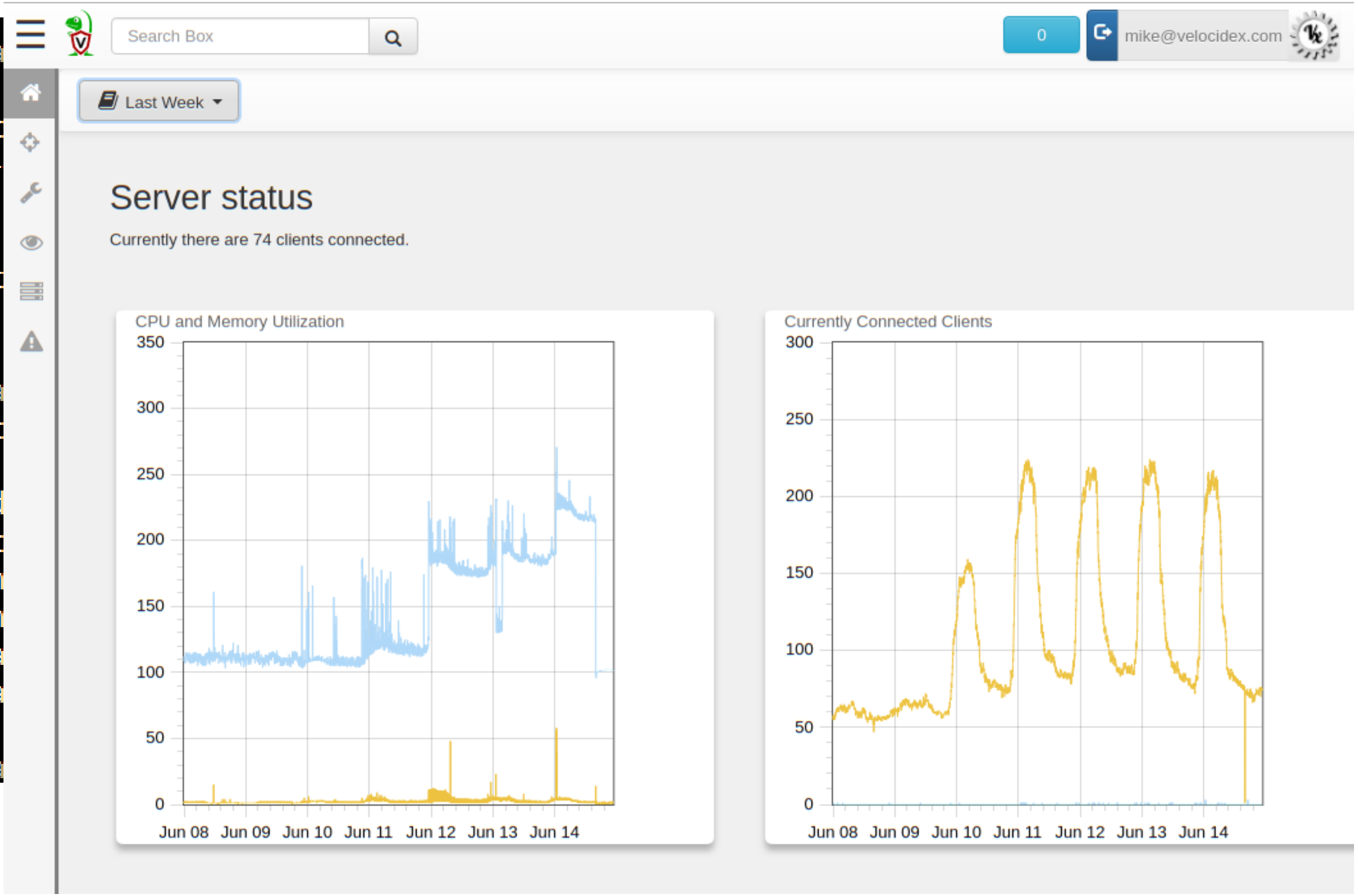
Velociraptor is a unique DFIR tool, giving *you* power and flexibility through the Velociraptor Query Language (VQL)

- VQL is used for everything:
  - Collecting information from endpoints
  - Controlling monitoring and response
  - Controlling and managing the server.

Easy server setup



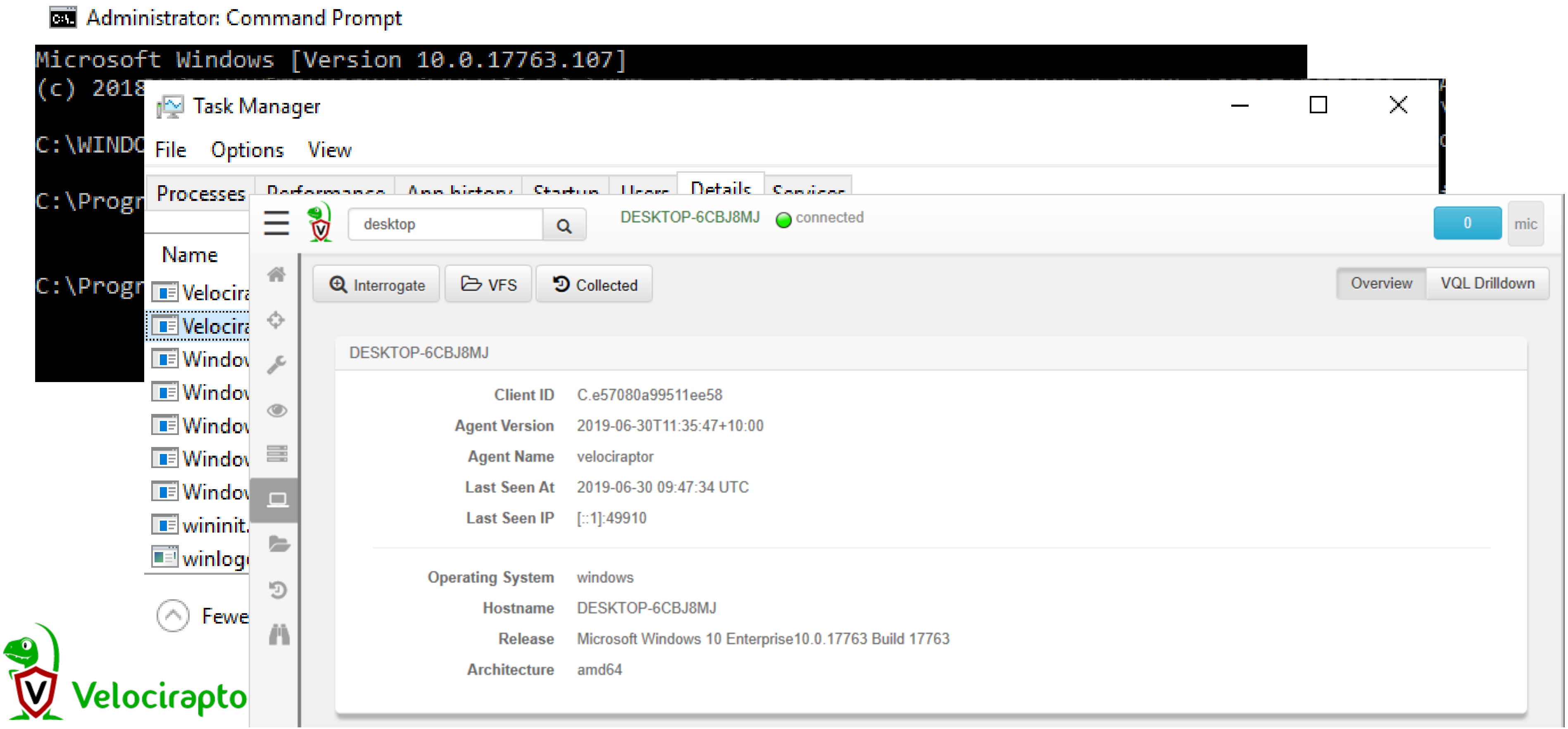
```
C:\Program Files\Velocira
?
Welcome to the Velocirapt
-------------------------

I will be creating a new
begin by identifying what

 Self Signed SSL
Generating keys please wa
? Enter the frontend port
? What is the public DNS
? Path to the datastore d
? Path to the logs direct
? Where should i write th
? Where should i write th
? GUI Username or email a
? GUI Username or email a

C:\Program Files\Velocira
```



Server status

Currently there are 74 clients connected.

Deploying clients



```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018

C:\WINDO

C:\Progr


C:\Progr
```

Name
Velocira
Velocira
Windov
Windov
Windov
Windov
Windov
wininit.
winlog

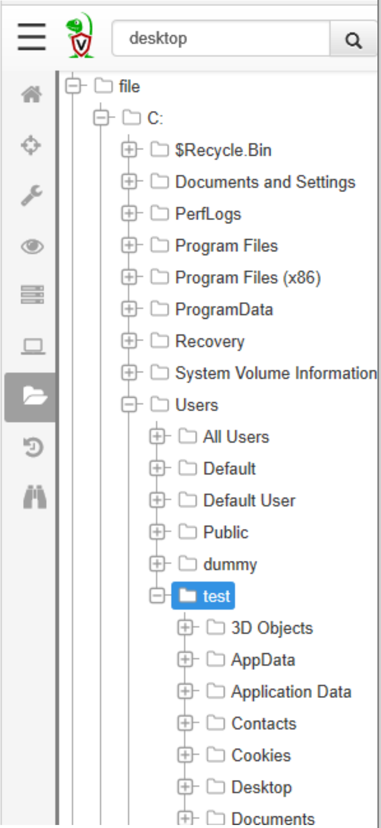
DESKTOP-6CBJ8MJ ● connected

DESKTOP-6CBJ8MJ

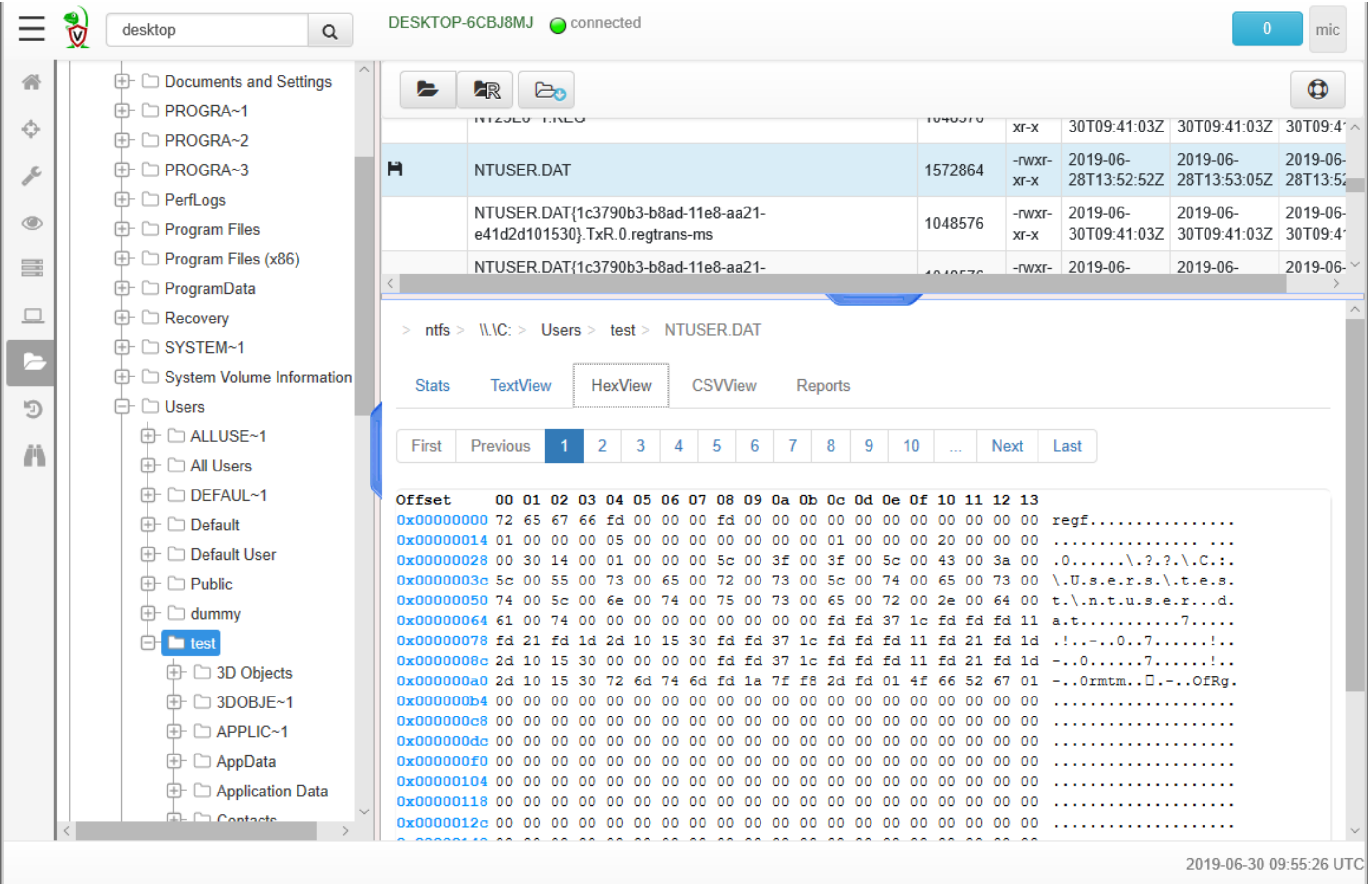
Client ID	C.e57080a99511ee58
Agent Version	2019-06-30T11:35:47+10:00
Agent Name	velociraptor
Last Seen At	2019-06-30 09:47:34 UTC
Last Seen IP	[::1]:49910
Operating System	windows
Hostname	DESKTOP-6CBJ8MJ
Release	Microsoft Windows 10 Enterprise10.0.17763 Build 17763
Architecture	amd64

Velocirapto

Browse remote computers



- file
  - C:
    - $Recycle.Bin
    - Documents and Settings
    - PerfLogs
    - Program Files
    - Program Files (x86)
    - ProgramData
    - Recovery
    - System Volume Information
    - Users
      - All Users
      - Default
      - Default User
      - Public
      - dummy
      - test
        - 3D Objects
        - AppData
        - Application Data
        - Contacts
        - Cookies
        - Desktop
        - Documents



- Documents and Settings
- PROGRA~1
- PROGRA~2
- PROGRA~3
- PerfLogs
- Program Files
- Program Files (x86)
- ProgramData
- Recovery
- SYSTEM~1
- System Volume Information
- Users
  - ALLUSE~1
  - All Users
  - DEFAUL~1
  - Default
  - Default User
  - Public
  - dummy
  - test
    - 3D Objects
    - 3DOBJE~1
    - APPLIC~1
    - AppData
    - Application Data
    - Contacts

			xr-x	30T09:41:03Z	30T09:41:03Z	30T09:4
💾	NTUSER.DAT	1572864	-rwxr-xr-x	2019-06-28T13:52:52Z	2019-06-28T13:53:05Z	2019-06-28T13:5
	NTUSER.DAT{1c3790b3-b8ad-11e8-aa21-e41d2d101530}.TxR.0.regtrans-ms	1048576	-rwxr-xr-x	2019-06-30T09:41:03Z	2019-06-30T09:41:03Z	2019-06-30T09:4
	NTUSER.DAT{1c3790b3-b8ad-11e8-aa21-		-rwxr-	2019-06-	2019-06-	2019-06-

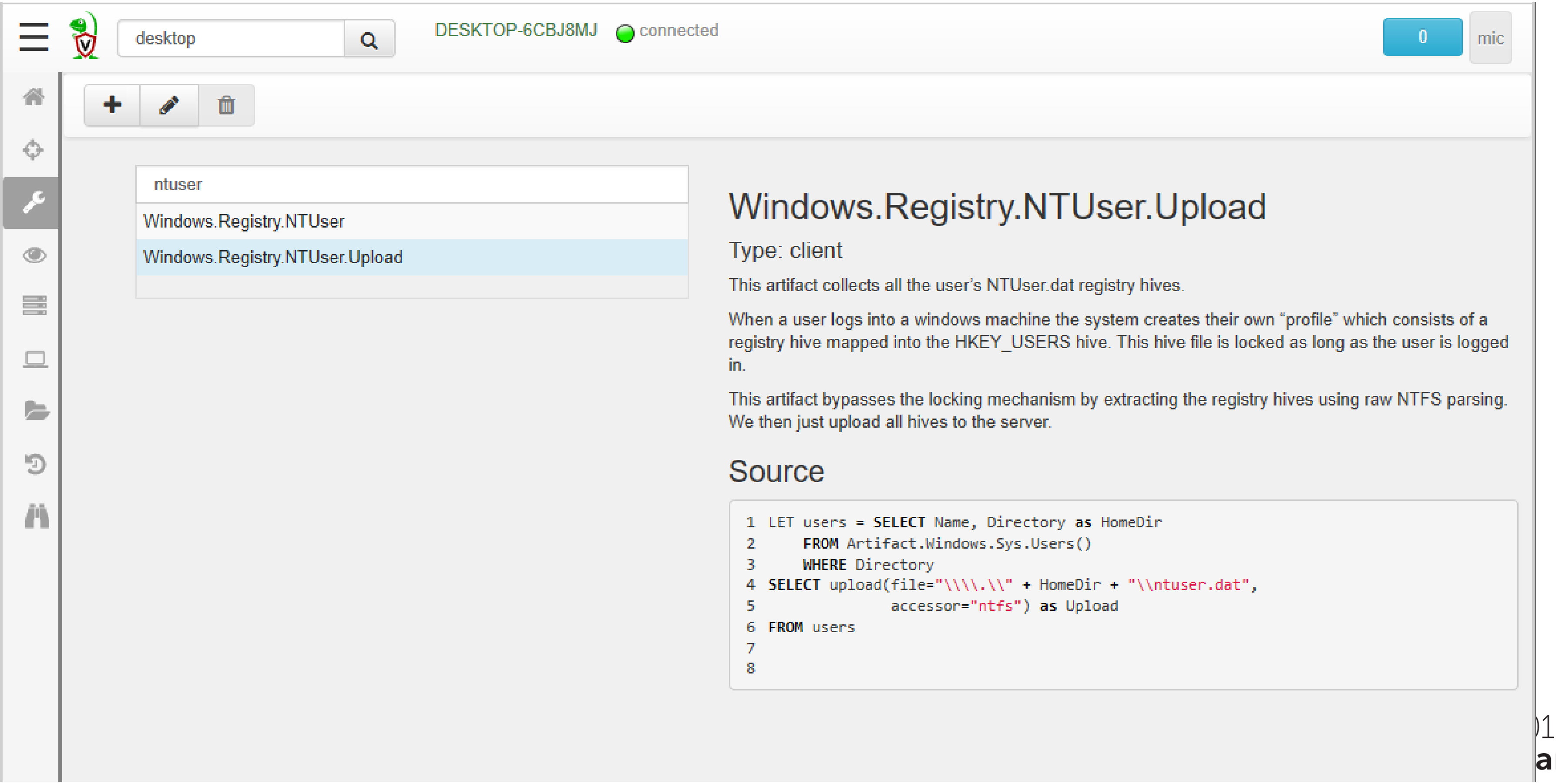
> ntfs > \\.\C: > Users > test > NTUSER.DAT

```
Offset     00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13
0x00000000 72 65 67 66 fd 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 regf................
0x00000014 01 00 00 00 05 00 00 00 00 00 00 00 01 00 00 00 20 00 00 00 ................ ...
0x00000028 00 30 14 00 01 00 00 00 5c 00 3f 00 3f 00 5c 00 43 00 3a 00 .0......\.?.?.\.C.:.
0x0000003c 5c 00 55 00 73 00 65 00 72 00 73 00 5c 00 74 00 65 00 73 00 \.U.s.e.r.s.\.t.e.s.
0x00000050 74 00 5c 00 6e 00 74 00 75 00 73 00 65 00 72 00 2e 00 64 00 t.\.n.t.u.s.e.r...d.
0x00000064 61 00 74 00 00 00 00 00 00 00 00 00 fd fd 37 1c fd fd fd 11 a.t.........7.....
0x00000078 fd 21 fd 1d 2d 10 15 30 fd fd 37 1c fd fd fd 11 fd 21 fd 1d .!..-..0..7......!..
0x0000008c 2d 10 15 30 00 00 00 00 fd fd 37 1c fd fd fd 11 fd 21 fd 1d -..0......7......!..
0x000000a0 2d 10 15 30 72 6d 74 6d fd 1a 7f f8 2d fd 01 4f 66 52 67 01 -..0rmtm..□.-..OfRg.
0x000000b4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....................
0x000000c8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....................
0x000000dc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....................
0x000000f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....................
0x00000104 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....................
0x00000118 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....................
0x0000012c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....................
```

2019-06-30 09:55:26 UTC

Velociraptor

Single endpoint collection



ntuser

Windows.Registry.NTUser

Windows.Registry.NTUser.Upload

Windows.Registry.NTUser.Upload

Type: client

This artifact collects all the user's NTUser.dat registry hives.

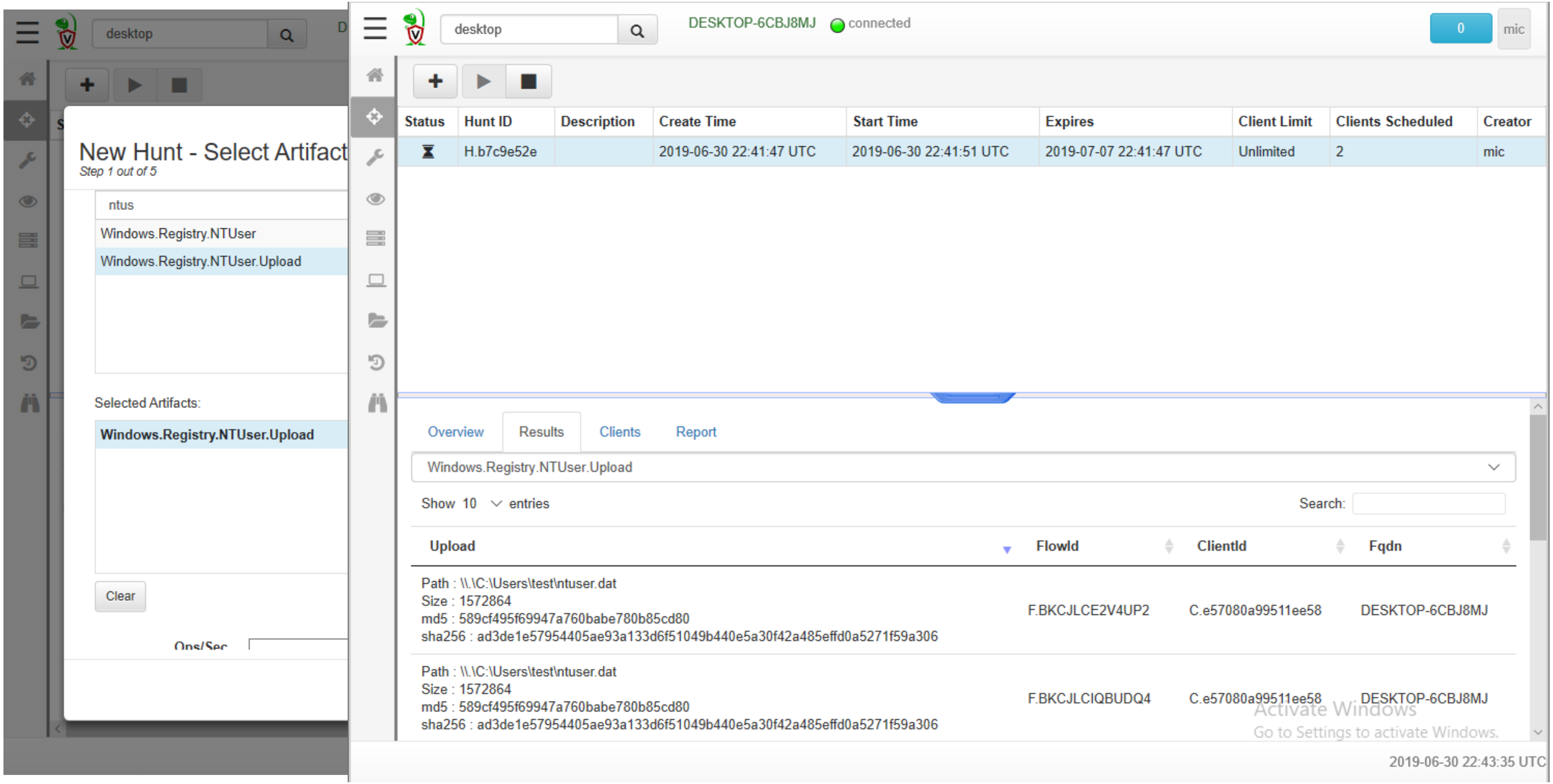
When a user logs into a windows machine the system creates their own "profile" which consists of a registry hive mapped into the HKEY_USERS hive. This hive file is locked as long as the user is logged in.

This artifact bypasses the locking mechanism by extracting the registry hives using raw NTFS parsing. We then just upload all hives to the server.

Source

```
LET users = SELECT Name, Directory as HomeDir
    FROM Artifact.Windows.Sys.Users()
    WHERE Directory
SELECT upload(file="\\\\.\\" + HomeDir + "\\ntuser.dat",
              accessor="ntfs") as Upload
FROM users


```

Network-wide hunts



New Hunt - Select Artifact
Step 1 out of 5

ntus

Windows.Registry.NTUser
Windows.Registry.NTUser.Upload

Selected Artifacts:

Windows.Registry.NTUser.Upload

Ops/Sec

Status	Hunt ID	Description	Create Time	Start Time	Expires	Client Limit	Clients Scheduled	Creator
⧗	H.b7c9e52e		2019-06-30 22:41:47 UTC	2019-06-30 22:41:51 UTC	2019-07-07 22:41:47 UTC	Unlimited	2	mic

Windows.Registry.NTUser.Upload

Show 10 entries

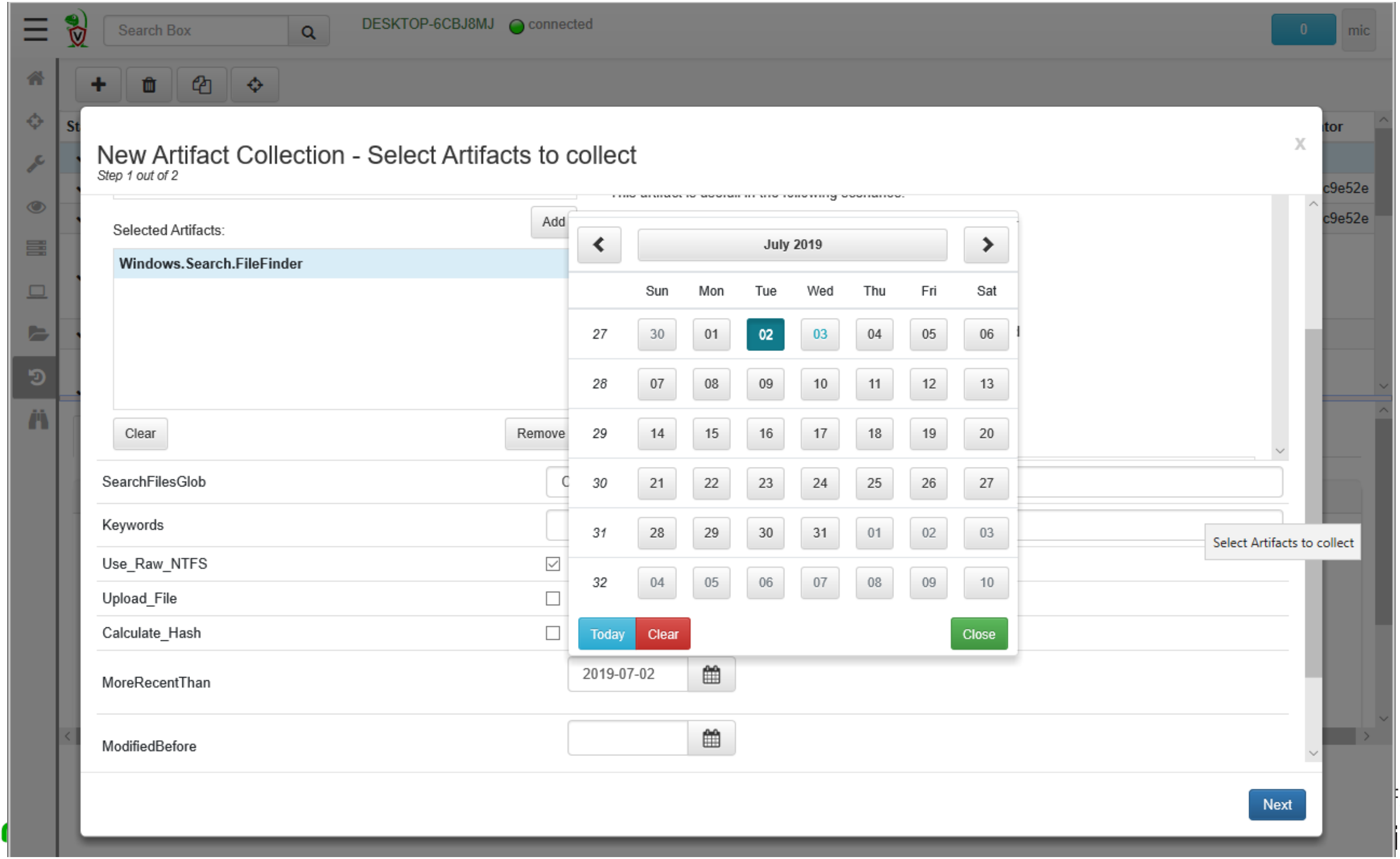
Search:

Upload	FlowId	ClientId	Fqdn
Path : \\.\C:\Users\test\ntuser.dat Size : 1572864 md5 : 589cf495f69947a760babe780b85cd80 sha256 : ad3de1e57954405ae93a133d6f51049b440e5a30f42a485effd0a5271f59a306	F.BKCJLCE2V4UP2	C.e57080a99511ee58	DESKTOP-6CBJ8MJ
Path : \\.\C:\Users\test\ntuser.dat Size : 1572864 md5 : 589cf495f69947a760babe780b85cd80 sha256 : ad3de1e57954405ae93a133d6f51049b440e5a30f42a485effd0a5271f59a306	F.BKCJLCIQBUDQ4	C.e57080a99511ee58	DESKTOP-6CBJ8MJ

Activate Windows
Go to Settings to activate Windows.

2019-06-30 22:43:35 UTC

Scenario: Finding files across endpoints



New Artifact Collection - Select Artifacts to collect

Step 1 out of 2

Selected Artifacts:

Windows.Search.FileFinder

‹	July 2019						›
	Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	30	01	02	03	04	05	06
28	07	08	09	10	11	12	13
29	14	15	16	17	18	19	20
30	21	22	23	24	25	26	27
31	28	29	30	31	01	02	03
32	04	05	06	07	08	09	10

SearchFilesGlob

Keywords

Use_Raw_NTFS ☑

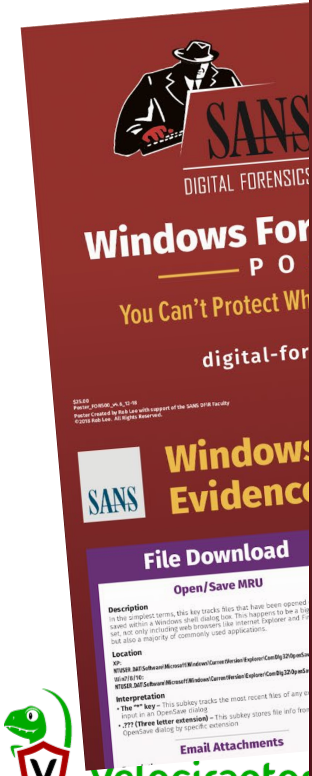
Upload_File □

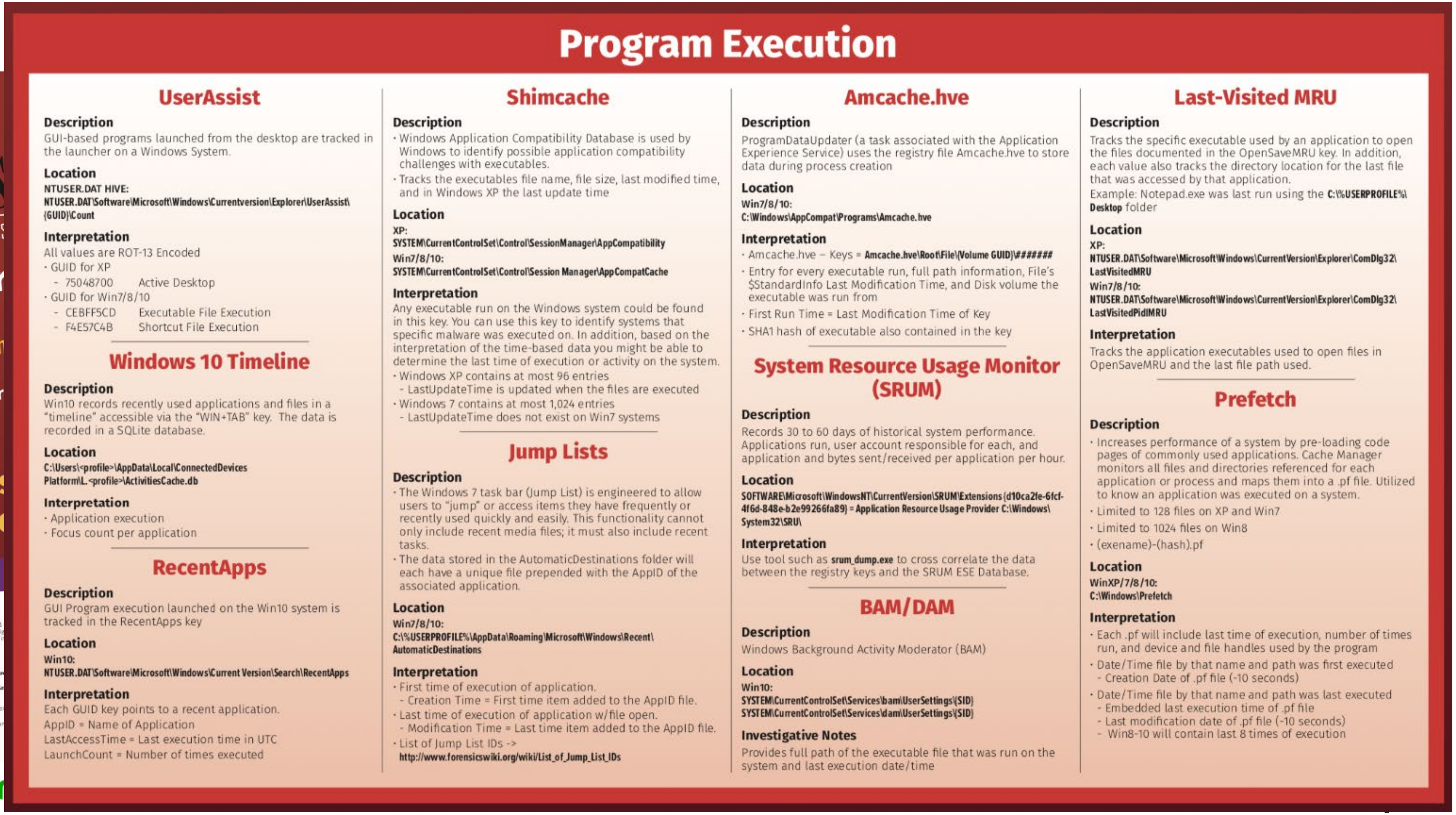
Calculate_Hash □

MoreRecentThan 2019-07-02

ModifiedBefore

Scenario: Hunt for evidence of program execution





Program Execution

UserAssist

Description

GUI-based programs launched from the desktop are tracked in the launcher on a Windows System.

Location

NTUSER.DAT HIVE:
NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count

Interpretation

All values are ROT-13 Encoded
- GUID for XP
  - 75048700 Active Desktop
- GUID for Win7/8/10
  - CEBFF5CD Executable File Execution
  - F4E57C4B Shortcut File Execution

Windows 10 Timeline

Description

Win10 records recently used applications and files in a "timeline" accessible via the "WIN+TAB" key. The data is recorded in a SQLite database.

Location

C:\Users\<profile>\AppData\Local\ConnectedDevices Platform\L.<profile>\ActivitiesCache.db

Interpretation

- Application execution
- Focus count per application

RecentApps

Description

GUI Program execution launched on the Win10 system is tracked in the RecentApps key

Location

Win10:
NTUSER.DAT\Software\Microsoft\Windows\Current Version\Search\RecentApps

Interpretation

Each GUID key points to a recent application.
AppID = Name of Application
LastAccessTime = Last execution time in UTC
LaunchCount = Number of times executed

Shimcache

Description

- Windows Application Compatibility Database is used by Windows to identify possible application compatibility challenges with executables.
- Tracks the executables file name, file size, last modified time, and in Windows XP the last update time

Location

XP:
SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility
Win7/8/10:
SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

Interpretation

Any executable run on the Windows system could be found in this key. You can use this key to identify systems that specific malware was executed on. In addition, based on the interpretation of the time-based data you might be able to determine the last time of execution or activity on the system.
- Windows XP contains at most 96 entries
  - LastUpdateTime is updated when the files are executed
- Windows 7 contains at most 1,024 entries
  - LastUpdateTime does not exist on Win7 systems

Jump Lists

Description

- The Windows 7 task bar (Jump List) is engineered to allow users to "jump" or access items they have frequently or recently used quickly and easily. This functionality cannot only include recent media files; it must also include recent tasks.
- The data stored in the AutomaticDestinations folder will each have a unique file prepended with the AppID of the associated application.

Location

Win7/8/10:
C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Interpretation

- First time of execution of application.
  - Creation Time = First time item added to the AppID file.
- Last time of execution of application w/file open.
  - Modification Time = Last time item added to the AppID file.
- List of Jump List IDs -> **http://www.forensicswiki.org/wiki/List_of_Jump_List_IDs**

Amcache.hve

Description

ProgramDataUpdater (a task associated with the Application Experience Service) uses the registry file Amcache.hve to store data during process creation

Location

Win7/8/10:
C:\Windows\AppCompat\Programs\Amcache.hve

Interpretation

- Amcache.hve – Keys = **Amcache.hve\Root\File\{Volume GUID}\#######**
- Entry for every executable run, full path information, File's $StandardInfo Last Modification Time, and Disk volume the executable was run from
- First Run Time = Last Modification Time of Key
- SHA1 hash of executable also contained in the key

System Resource Usage Monitor (SRUM)

Description

Records 30 to 60 days of historical system performance. Applications run, user account responsible for each, and application and bytes sent/received per application per hour.

Location

SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SRUM\Extensions {d10ca2fe-6fcf-4f6d-848e-b2e99266fa89} = Application Resource Usage Provider C:\Windows\System32\SRU\

Interpretation

Use tool such as **srum_dump.exe** to cross correlate the data between the registry keys and the SRUM ESE Database.

BAM/DAM

Description

Windows Background Activity Moderator (BAM)

Location

Win10:
SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}
SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}

Investigative Notes

Provides full path of the executable file that was run on the system and last execution date/time

Last-Visited MRU

Description

Tracks the specific executable used by an application to open the files documented in the OpenSaveMRU key. In addition, each value also tracks the directory location for the last file that was accessed by that application.

Example: Notepad.exe was last run using the **C:\%USERPROFILE%\Desktop** folder

Location

XP:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
Win7/8/10:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

Interpretation

Tracks the application executables used to open files in OpenSaveMRU and the last file path used.

Prefetch

Description

- Increases performance of a system by pre-loading code pages of commonly used applications. Cache Manager monitors all files and directories referenced for each application or process and maps them into a .pf file. Utilized to know an application was executed on a system.
- Limited to 128 files on XP and Win7
- Limited to 1024 files on Win8
- (exename)-(hash).pf

Location

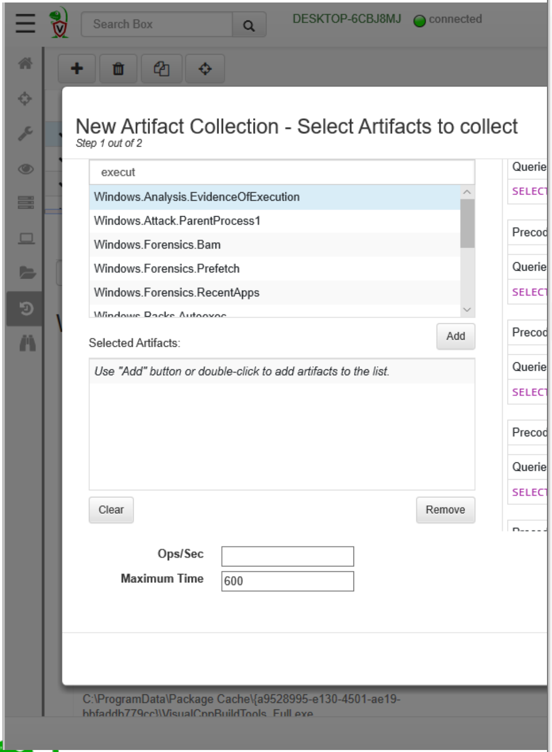
WinXP/7/8/10:
C:\Windows\Prefetch

Interpretation

- Each .pf will include last time of execution, number of times run, and device and file handles used by the program
- Date/Time file by that name and path was first executed
  - Creation Date of .pf file (-10 seconds)
- Date/Time file by that name and path was last executed
  - Embedded last execution time of .pf file
  - Last modification date of .pf file (-10 seconds)
  - Win8-10 will contain last 8 times of execution

Velociraptor

Scenario: Hunt for evidence of program execution



New Artifact Collection - Select Artifacts to collect

Step 1 out of 2

execut

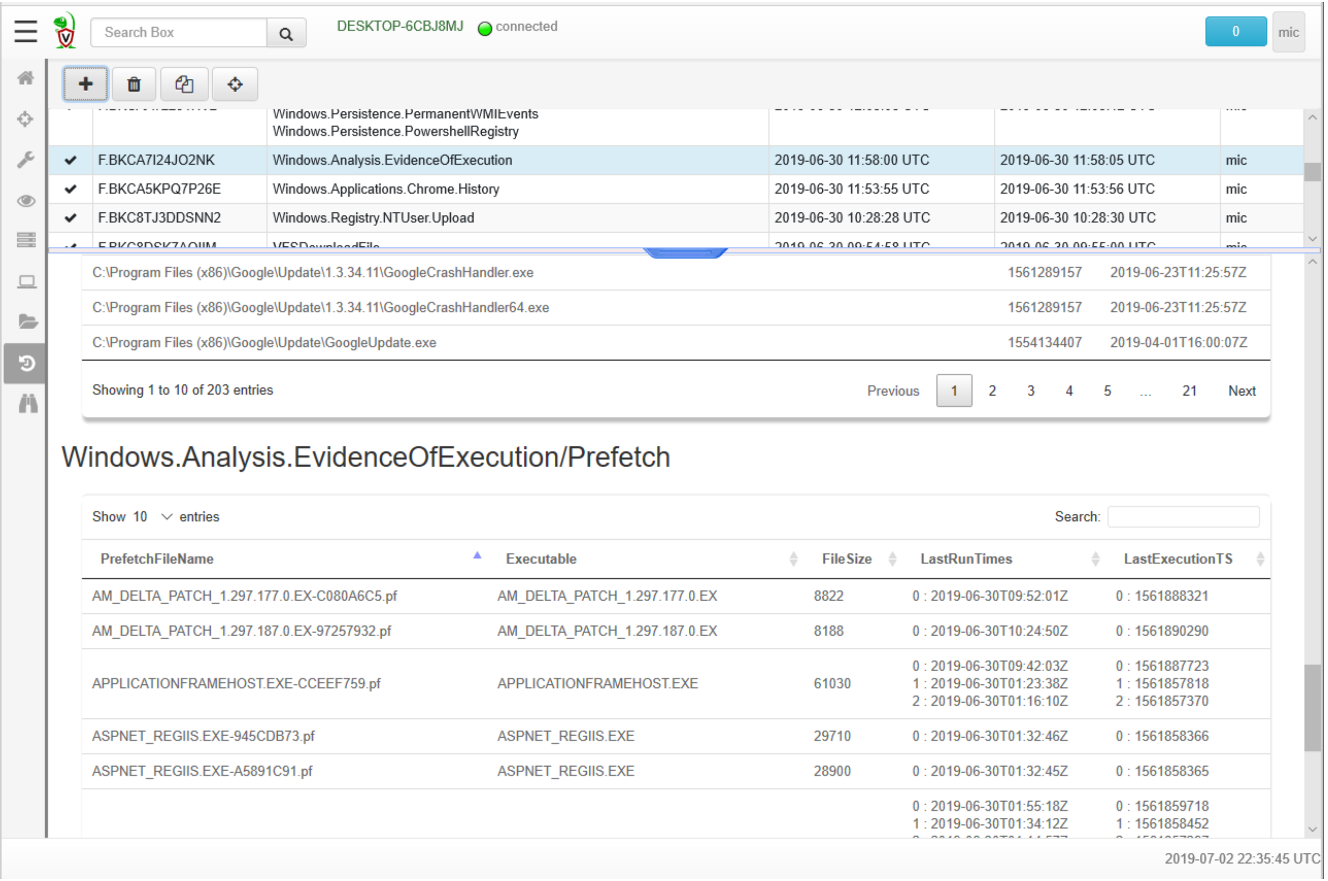
- Windows.Analysis.EvidenceOfExecution
- Windows.Attack.ParentProcess1
- Windows.Forensics.Bam
- Windows.Forensics.Prefetch
- Windows.Forensics.RecentApps
- Windows.Packs.Autoexec

Selected Artifacts:

Use "Add" button or double-click to add artifacts to the list.

Ops/Sec	
Maximum Time	600

C:\ProgramData\Package Cache\{a9528995-e130-4501-ae19-bbfaddb779cc}\VisualCppBuildTools_Full.exe



		Windows.Persistence.PermanentWMIEvents Windows.Persistence.PowershellRegistry			
✓	F.BKCA7I24JO2NK	Windows.Analysis.EvidenceOfExecution	2019-06-30 11:58:00 UTC	2019-06-30 11:58:05 UTC	mic
✓	F.BKCA5KPQ7P26E	Windows.Applications.Chrome.History	2019-06-30 11:53:55 UTC	2019-06-30 11:53:56 UTC	mic
✓	F.BKC8TJ3DDSNN2	Windows.Registry.NTUser.Upload	2019-06-30 10:28:28 UTC	2019-06-30 10:28:30 UTC	mic
✓	F.BKC8DSK7AQIIM	VFSDownloadFile	2019-06-30 09:54:58 UTC	2019-06-30 09:55:00 UTC	mic

C:\Program Files (x86)\Google\Update\1.3.34.11\GoogleCrashHandler.exe	1561289157	2019-06-23T11:25:57Z
C:\Program Files (x86)\Google\Update\1.3.34.11\GoogleCrashHandler64.exe	1561289157	2019-06-23T11:25:57Z
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe	1554134407	2019-04-01T16:00:07Z

Showing 1 to 10 of 203 entries

Windows.Analysis.EvidenceOfExecution/Prefetch

Show 10 entries

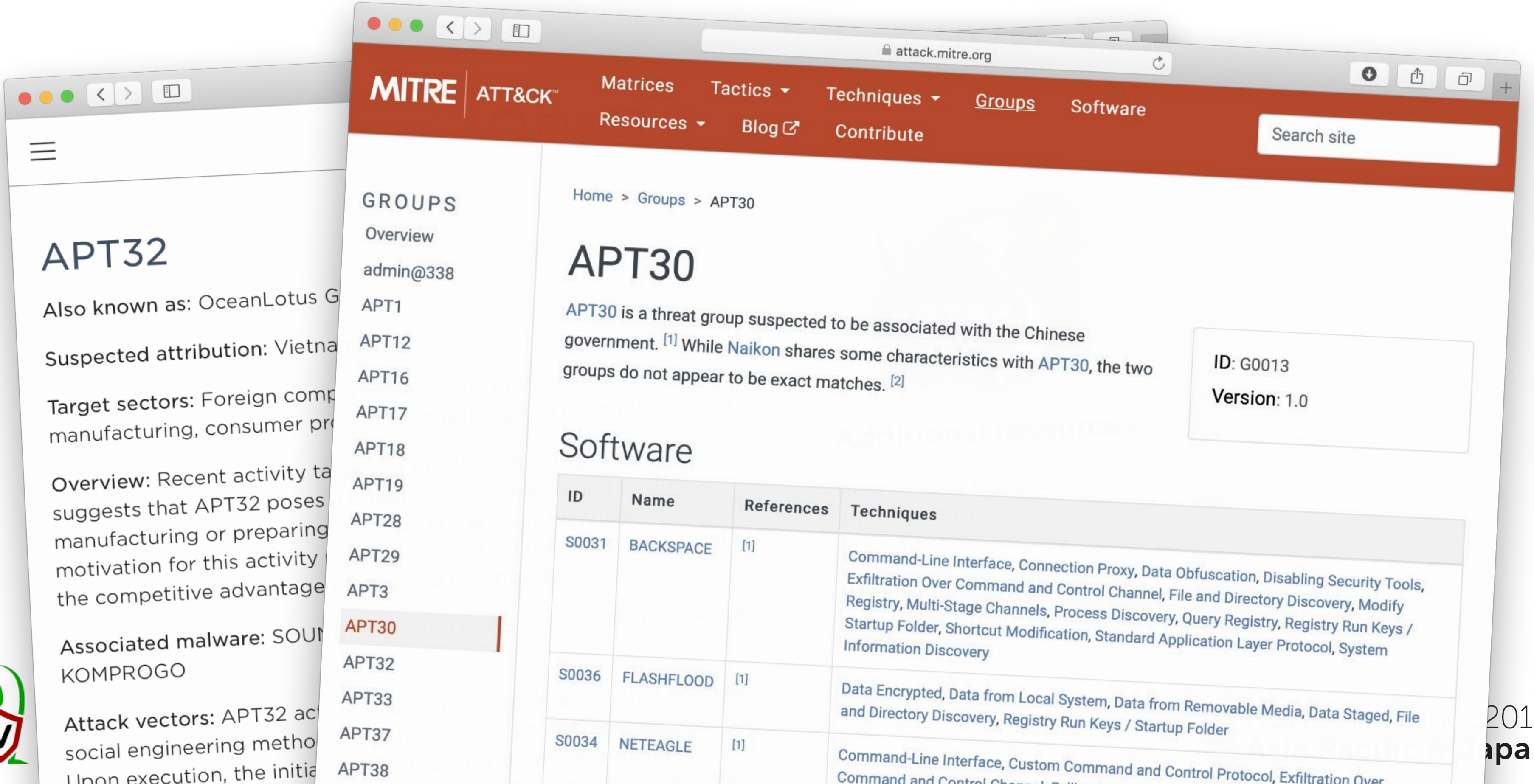
Search:

PrefetchFileName	Executable	FileSize	LastRunTimes	LastExecutionTS
AM_DELTA_PATCH_1.297.177.0.EX-C080A6C5.pf	AM_DELTA_PATCH_1.297.177.0.EX	8822	0 : 2019-06-30T09:52:01Z	0 : 1561888321
AM_DELTA_PATCH_1.297.187.0.EX-97257932.pf	AM_DELTA_PATCH_1.297.187.0.EX	8188	0 : 2019-06-30T10:24:50Z	0 : 1561890290
APPLICATIONFRAMEHOST.EXE-CCEEF759.pf	APPLICATIONFRAMEHOST.EXE	61030	0 : 2019-06-30T09:42:03Z 1 : 2019-06-30T01:23:38Z 2 : 2019-06-30T01:16:10Z	0 : 1561887723 1 : 1561857818 2 : 1561857370
ASPNET_REGIIS.EXE-945CDB73.pf	ASPNET_REGIIS.EXE	29710	0 : 2019-06-30T01:32:46Z	0 : 1561858366
ASPNET_REGIIS.EXE-A5891C91.pf	ASPNET_REGIIS.EXE	28900	0 : 2019-06-30T01:32:45Z	0 : 1561858365
			0 : 2019-06-30T01:55:18Z 1 : 2019-06-30T01:34:12Z	0 : 1561859718 1 : 1561858452

2019-07-02 22:35:45 UTC

Velociraptor

Scenario: Hunt for an APT group using threat intel



APT32

Also known as: OceanLotus G

Suspected attribution: Vietna

Target sectors: Foreign comp manufacturing, consumer pr

Overview: Recent activity ta suggests that APT32 poses manufacturing or preparing motivation for this activity the competitive advantage

Associated malware: SOUI KOMPROGO

Attack vectors: APT32 ac social engineering metho Upon execution, the initia

Home > Groups > APT30

APT30

APT30 is a threat group suspected to be associated with the Chinese government. [1] While Naikon shares some characteristics with APT30, the two groups do not appear to be exact matches. [2]

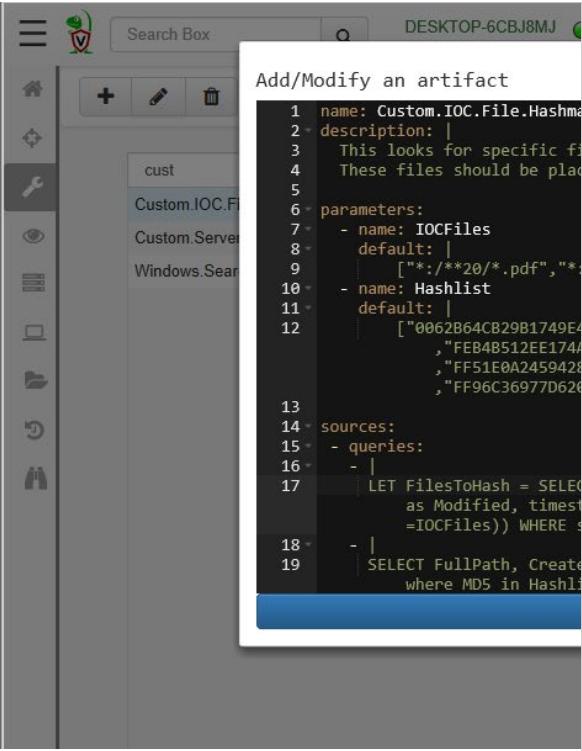
ID: G0013

Version: 1.0

Software

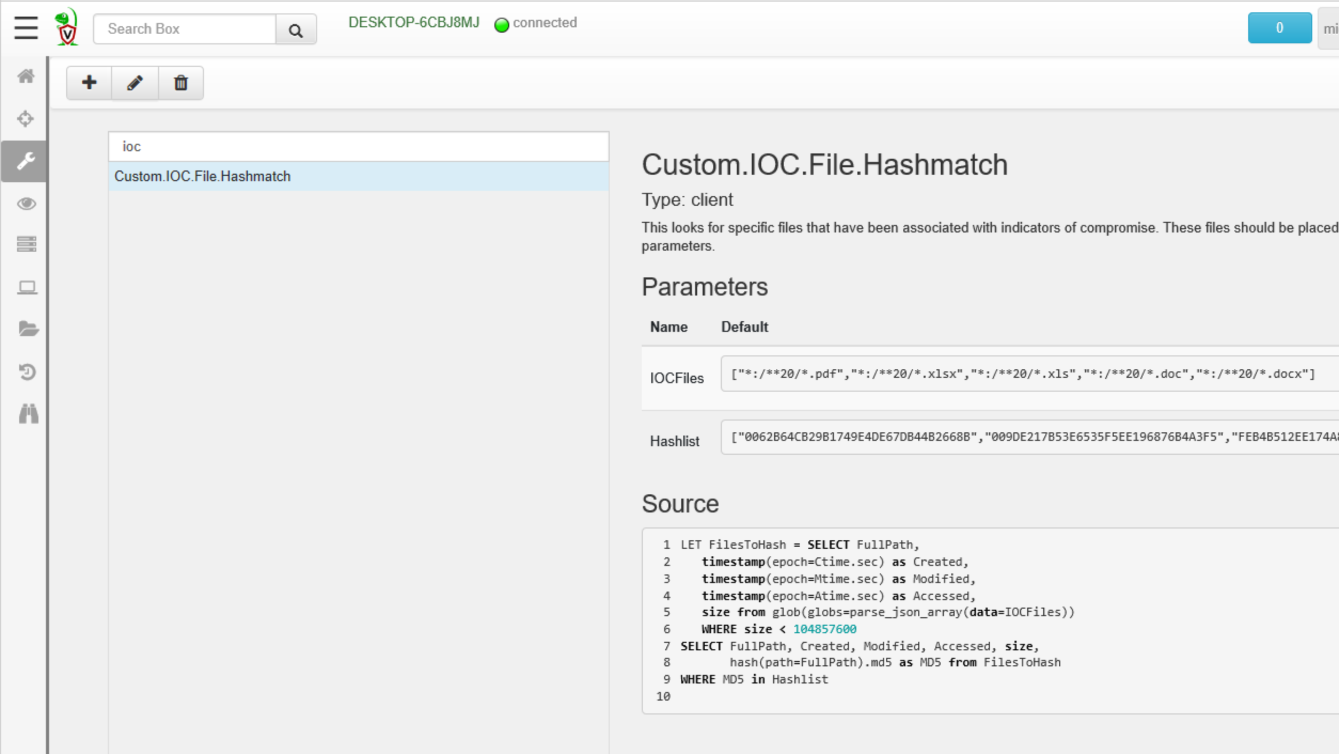
ID	Name	References	Techniques
S0031	BACKSPACE	[1]	Command-Line Interface, Connection Proxy, Data Obfuscation, Disabling Security Tools, Exfiltration Over Command and Control Channel, File and Directory Discovery, Modify Registry, Multi-Stage Channels, Process Discovery, Query Registry, Registry Run Keys / Startup Folder, Shortcut Modification, Standard Application Layer Protocol, System Information Discovery
S0036	FLASHFLOOD	[1]	Data Encrypted, Data from Local System, Data from Removable Media, Data Staged, File and Directory Discovery, Registry Run Keys / Startup Folder
S0034	NETEAGLE	[1]	Command-Line Interface, Custom Command and Control Protocol, Exfiltration Over Command and Control Channel

Scenario: Hunt for an APT group using threat intel



Add/Modify an artifact

```
name: Custom.IOC.File.Hashma
description: |
  This looks for specific fi
  These files should be plac

parameters:
  - name: IOCFiles
    default: |
       ["*:/**20/*.pdf","*:
  - name: Hashlist
    default: |
       ["0062B64CB29B1749E4
           ,"FEB4B512EE174A
           ,"FF51E0A2459428
           ,"FF96C36977D620

sources:
 - queries:
   - |
     LET FilesToHash = SELEC
         as Modified, timest
         =IOCFiles)) WHERE s
   - |
     SELECT FullPath, Create
         where MD5 in Hashli
```



Custom.IOC.File.Hashmatch

Type: client

This looks for specific files that have been associated with indicators of compromise. These files should be placed parameters.

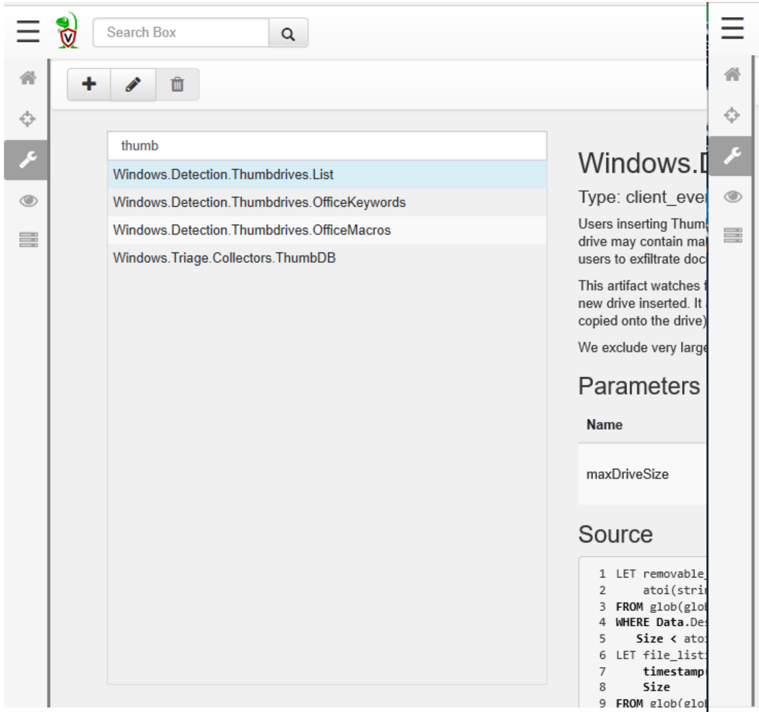
Parameters

Name	Default
IOCFiles	`["*:/**20/*.pdf","*:/**20/*.xlsx","*:/**20/*.xls","*:/**20/*.doc","*:/**20/*.docx"]`
Hashlist	`["0062B64CB29B1749E4DE67DB44B2668B","009DE217B53E6535F5EE196876B4A3F5","FEB4B512EE174A`

Source

```
LET FilesToHash = SELECT FullPath,
   timestamp(epoch=Ctime.sec) as Created,
   timestamp(epoch=Mtime.sec) as Modified,
   timestamp(epoch=Atime.sec) as Accessed,
   size from glob(globs=parse_json_array(data=IOCFiles))
   WHERE size < 104857600
SELECT FullPath, Created, Modified, Accessed, size,
       hash(path=FullPath).md5 as MD5 from FilesToHash
WHERE MD5 in Hashlist

```

Scenario: Monitor documents on all USB devices



thumb

- Windows.Detection.Thumbdrives.List
- Windows.Detection.Thumbdrives.OfficeKeywords
- Windows.Detection.Thumbdrives.OfficeMacros
- Windows.Triage.Collectors.ThumbDB

Windows.D

Type: client_eve

Users inserting Thum
drive may contain ma
users to exfiltrate doc

This artifact watches f
new drive inserted. It
copied onto the drive)

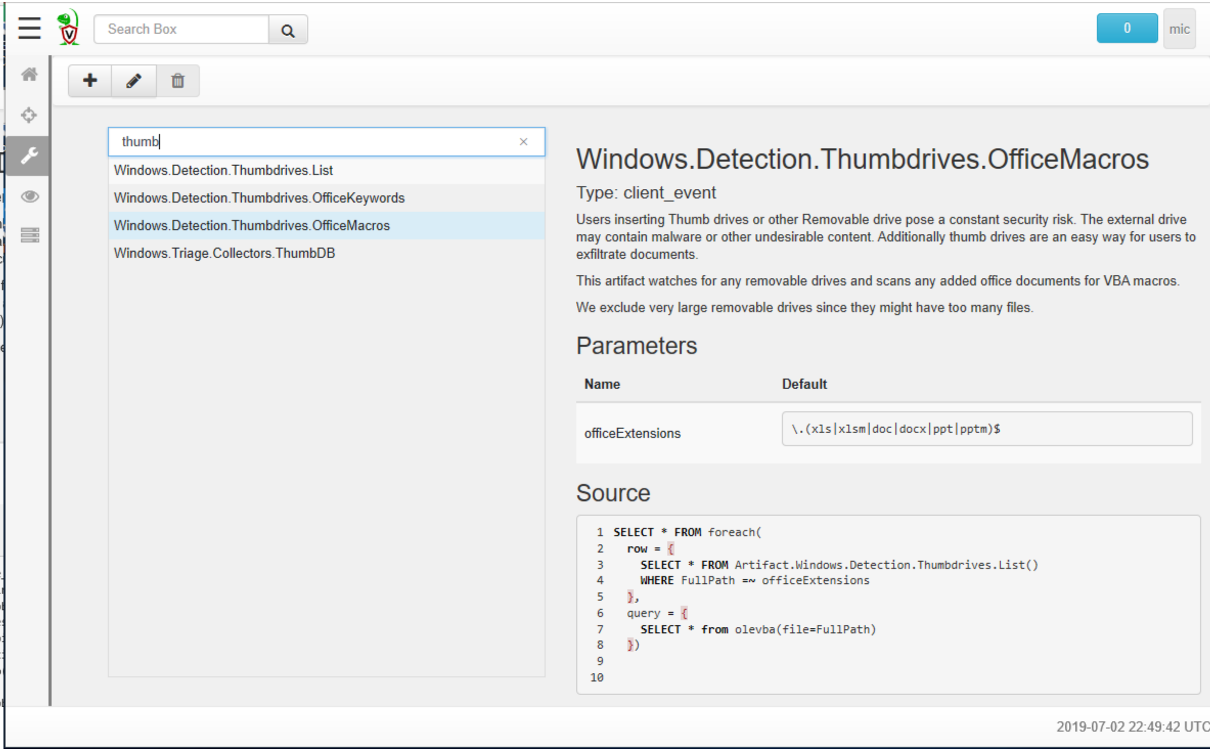
We exclude very large

Parameters

Name
maxDriveSize

Source

```
LET removable_
     atoi(strin
FROM glob(glob
WHERE Data.Des
    Size < atoi
LET file_listi
     timestamp(
     Size
FROM glob(glob
```



thumb

- Windows.Detection.Thumbdrives.List
- Windows.Detection.Thumbdrives.OfficeKeywords
- Windows.Detection.Thumbdrives.OfficeMacros
- Windows.Triage.Collectors.ThumbDB

Windows.Detection.Thumbdrives.OfficeMacros

Type: client_event

Users inserting Thumb drives or other Removable drive pose a constant security risk. The external drive may contain malware or other undesirable content. Additionally thumb drives are an easy way for users to exfiltrate documents.

This artifact watches for any removable drives and scans any added office documents for VBA macros.

We exclude very large removable drives since they might have too many files.

Parameters

Name	Default
officeExtensions	`\.(xls|xlsm|doc|docx|ppt|pptm)$`

Source

```
SELECT * FROM foreach(
  row = {
    SELECT * FROM Artifact.Windows.Detection.Thumbdrives.List()
    WHERE FullPath =~ officeExtensions
  },
  query = {
    SELECT * from olevba(file=FullPath)
  })


```

2019-07-02 22:49:42 UTC

Velociraptor

Velociraptor can hunt for whatever information exists across your endpoints.

So what do *you* want to find?

Watch this space

- Velociraptor is **free and open source** - download and use it today.
- Ongoing professional development, plus contributions from the DFIR community.
- Velociraptor is commercially backed - professional services and training are also available.

Start hunting today!

- Download Velociraptor from www.velocidex.com or GitHub
- Review the quick start documentation
- Setup a server and deploy some test agents
- Start by hunting for some pre-built artefacts
- Then customise some hunts to your own requirements
- Contribute back with your feedback and ideas.

RSAConference2019
Asia Pacific & Japan

Thank you.

www.velocidex.com