RTR FOR FORENSICS AND HUNTING

RTR EXAMPLES

SPEAKER

JIM MILLER

Senior Consultant

- CrowdStrike Services – 3 years
- Over a decade of security experience (SOC/IR/Forensics)
- CISSP/GPEN/GCFA/GCFE/GWAPT
- Bachelors in IT from RIT (Go Tigers!)

AGENDA

- DEFINITIONS
- RTR BUILT-IN COMMANDS
- RTR WITH PREBUILT BINARIES
- RTR AND POWERSHELL
- RTR AT SCALE?

DEFINITIONS

- **Real Time Response**

  "RTR" the ability to connect to a host running Falcon via the cloud and execute arbitrary commands

- **PowerShell**

  Command-line shell and scripting language focusing on automation

- **Registry**

  The Windows Registry, a configuration database containing low level options

- **Malware**

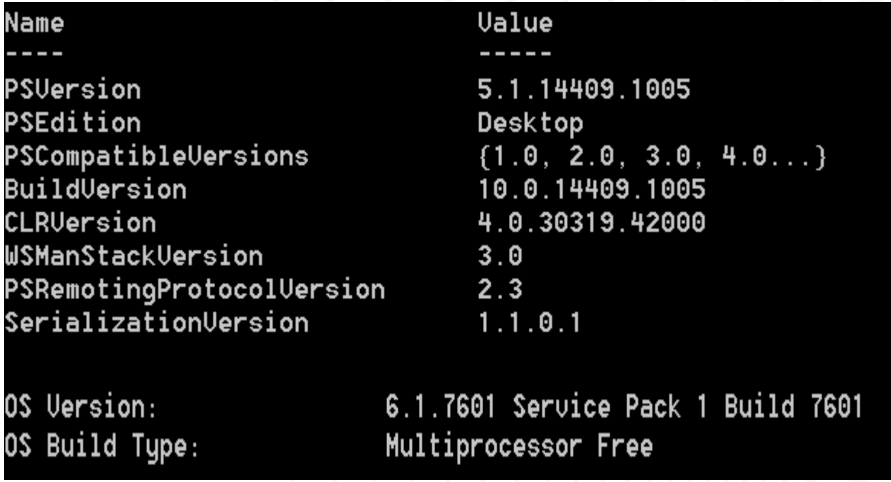
  For this talk, anything we don't want running on the host. (Adware/PUPS/etc)

BUILT-INS

SOME QUICK ASSUMPTIONS

The demo machine for all of this was Win7SP1 x64 PowerShell 5.1

- Some commands (zip) may not work for you
- Additional PowerShell (PS) frameworks may require additional features
- You have the correct Falcon permissions and authority to make the changes on the hosts you are working on



```
Name                           Value
----                           -----
PSVersion                      5.1.14409.1005
PSEdition                      Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.14409.1005
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1

OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Build Type:             Multiprocessor Free
```

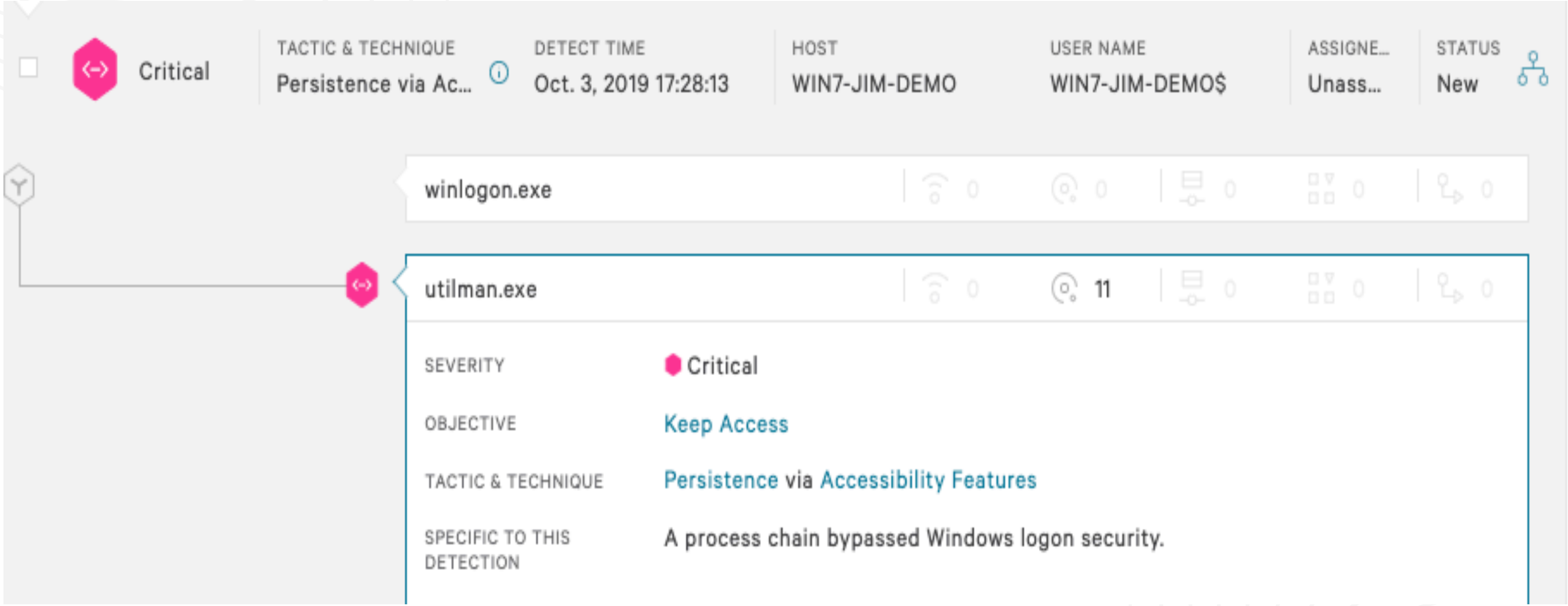
THE BUILT-INS

- cat
- cd
- eventlog
- filehash
- get
- help

- kill
- ls
- map
- memdump
- mv
- ps

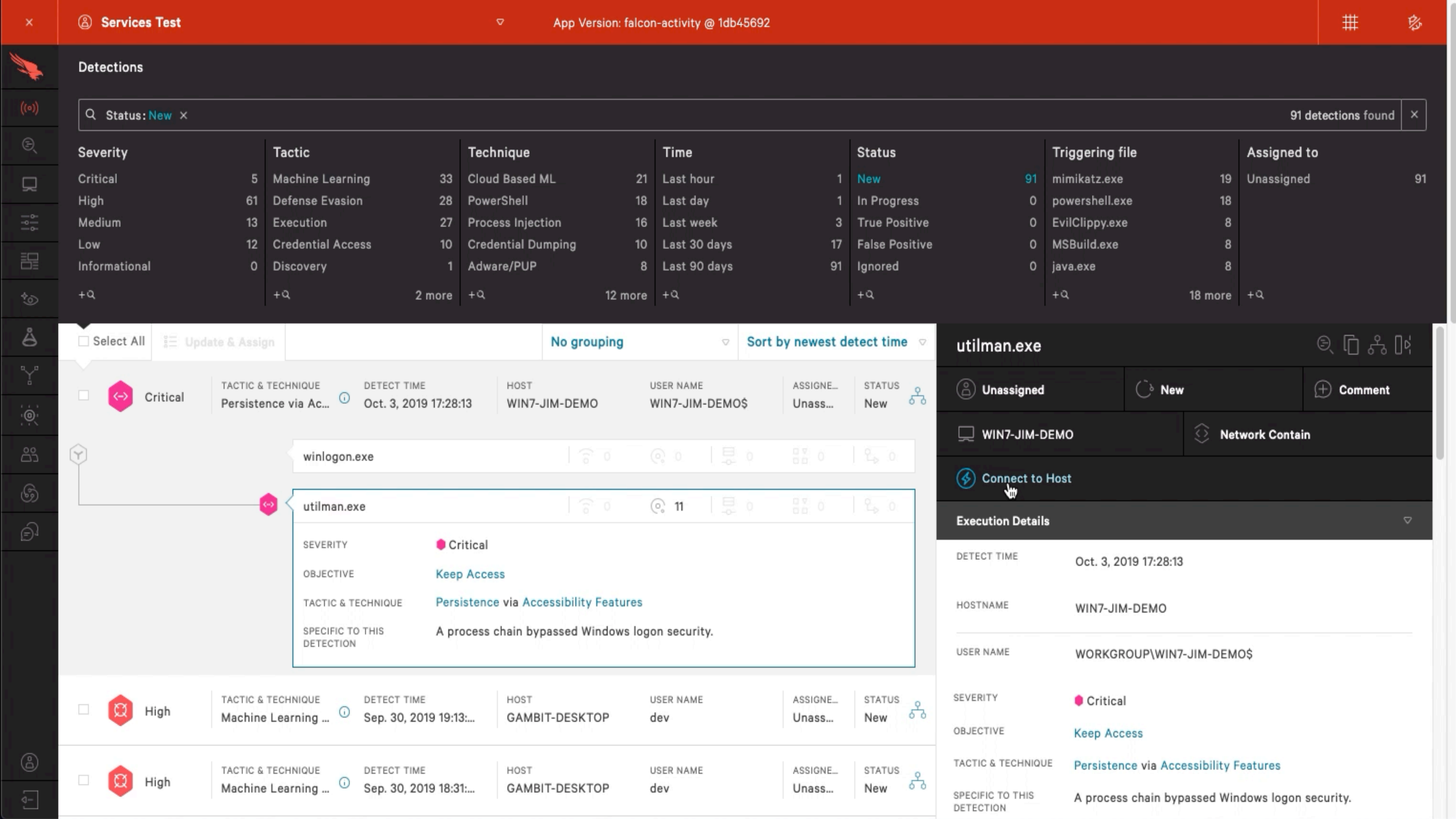
- put
- reg
- rm
- runscript
- xmemdump

A SAMPLE DETECTION



	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNE...	STATUS
Critical	Persistence via Ac...	Oct. 3, 2019 17:28:13	WIN7-JIM-DEMO	WIN7-JIM-DEMO$	Unass...	New

SEVERITY	Critical
OBJECTIVE	Keep Access
TACTIC & TECHNIQUE	Persistence via Accessibility Features
SPECIFIC TO THIS DETECTION	A process chain bypassed Windows logon security.



Services Test

App Version: falcon-activity @ 1db45692

Detections

Status: New ×

91 detections found

Severity		Tactic		Technique		Time		Status		Triggering file		Assigned to	
Critical	5	Machine Learning	33	Cloud Based ML	21	Last hour	1	New	91	mimikatz.exe	19	Unassigned	91
High	61	Defense Evasion	28	PowerShell	18	Last day	1	In Progress	0	powershell.exe	18		
Medium	13	Execution	27	Process Injection	16	Last week	3	True Positive	0	EvilClippy.exe	8		
Low	12	Credential Access	10	Credential Dumping	10	Last 30 days	17	False Positive	0	MSBuild.exe	8		
Informational	0	Discovery	1	Adware/PUP	8	Last 90 days	91	Ignored	0	java.exe	8		
			2 more		12 more						18 more		

□ Select All | Update & Assign | No grouping | Sort by newest detect time

Severity	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNE...	STATUS
Critical	Persistence via Ac...	Oct. 3, 2019 17:28:13	WIN7-JIM-DEMO	WIN7-JIM-DEMO$	Unass...	New
High	Machine Learning ...	Sep. 30, 2019 19:13:...	GAMBIT-DESKTOP	dev	Unass...	New
High	Machine Learning ...	Sep. 30, 2019 18:31:...	GAMBIT-DESKTOP	dev	Unass...	New

winlogon.exe 0 0 0 0 0

utilman.exe 0 11 0 0 0

SEVERITY Critical

OBJECTIVE Keep Access

TACTIC & TECHNIQUE Persistence via Accessibility Features

SPECIFIC TO THIS DETECTION A process chain bypassed Windows logon security.

utilman.exe

Unassigned | New | Comment

WIN7-JIM-DEMO | Network Contain

Connect to Host

Execution Details

DETECT TIME Oct. 3, 2019 17:28:13

HOSTNAME WIN7-JIM-DEMO

USER NAME WORKGROUP\WIN7-JIM-DEMO$

SEVERITY Critical

OBJECTIVE Keep Access

TACTIC & TECHNIQUE Persistence via Accessibility Features

SPECIFIC TO THIS DETECTION A process chain bypassed Windows logon security.

THE COMMANDS

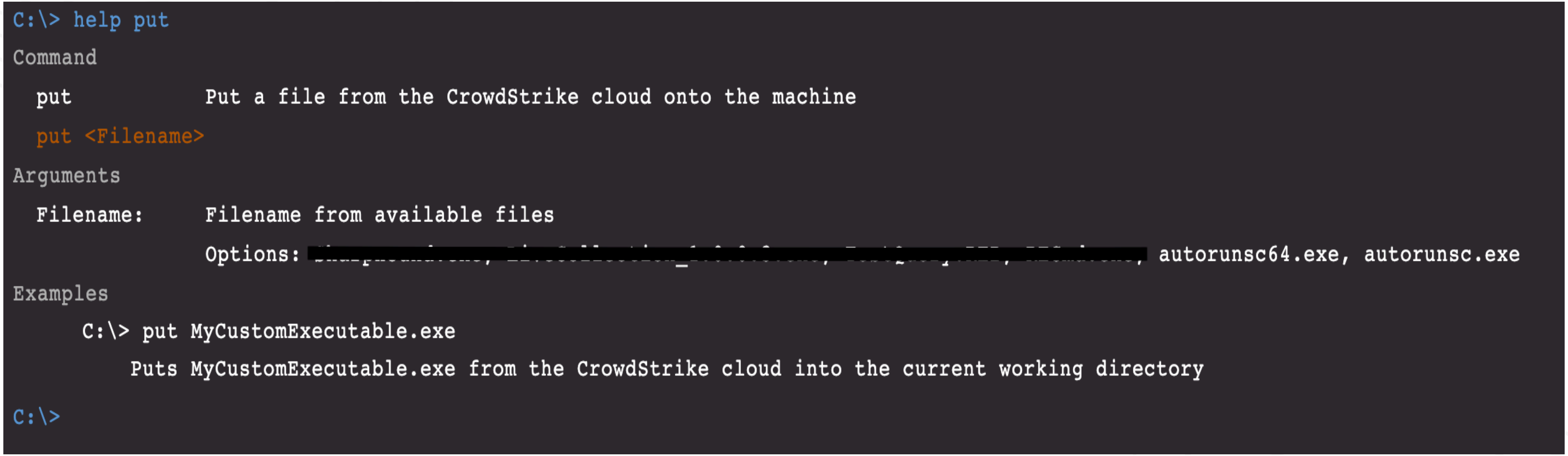
- ls c:\windows\system32\utilma*
- filehash c:\windows\system32\utilman.exe && exe.old
- reg query "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager"
- New-ItemProperty -Path "Registry::HKLM\SYSTEM\CurrentControlSet\Control\Session Manager" -Name PendingFileRenameOperations -PropertyType MultiString -Value ('\??\C:\Windows\System32\utilman.exe.old','\??\C:\Windows\System32\utilman.exe') | Out-Null

WARNING

Untested Code

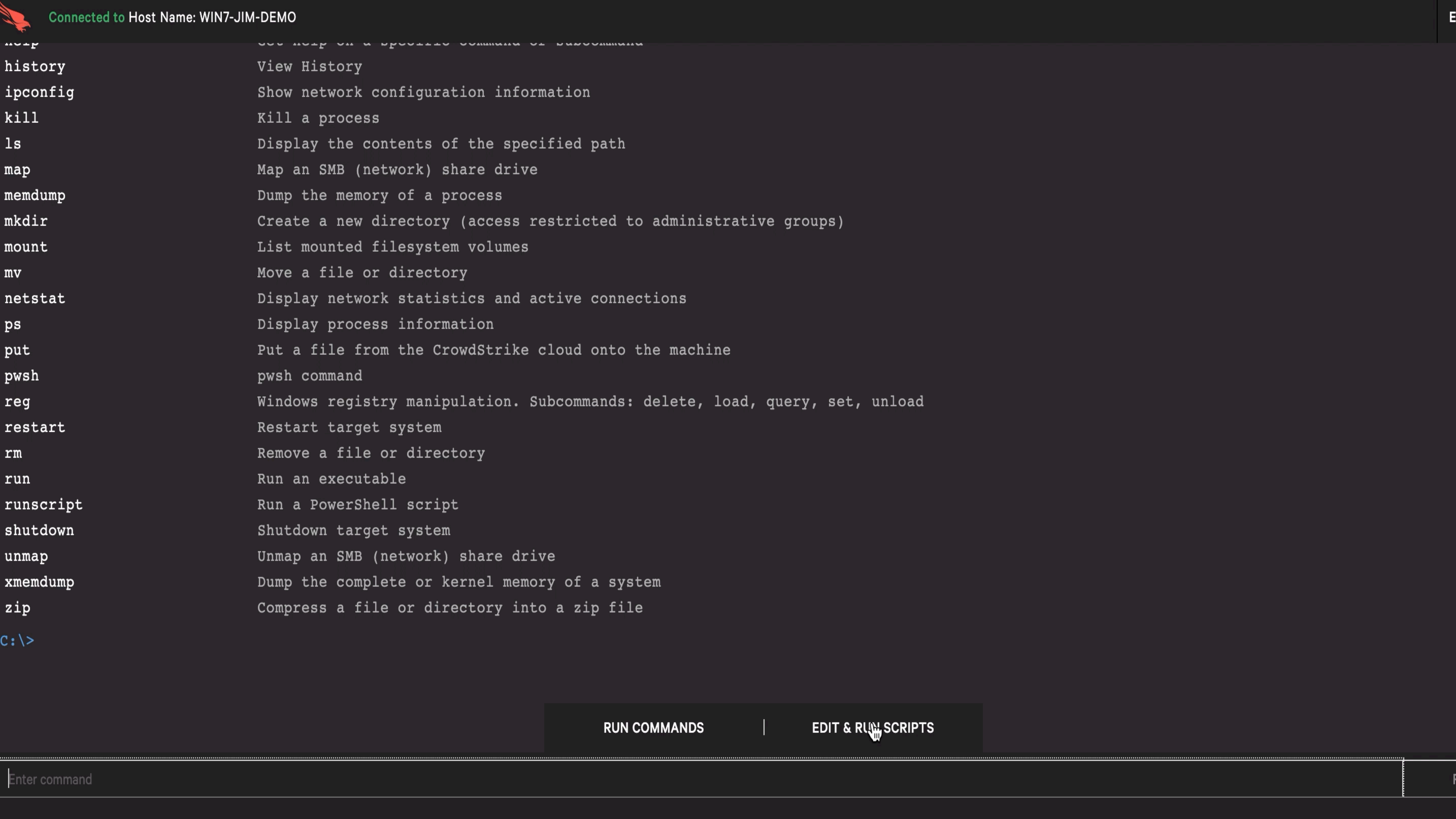
PRE-BUILT BINARIES

AUTORUNS



```
C:\> help put
Command
  put           Put a file from the CrowdStrike cloud onto the machine
  put <Filename>
Arguments
  Filename:     Filename from available files
                Options: [redacted] autorunsc64.exe, autorunsc.exe
Examples
      C:\> put MyCustomExecutable.exe
          Puts MyCustomExecutable.exe from the CrowdStrike cloud into the current working directory
C:\>
```

- NB: Autoruns and Sysinternals are copyright works of Microsoft



Connected to Host Name: WIN7-JIM-DEMO

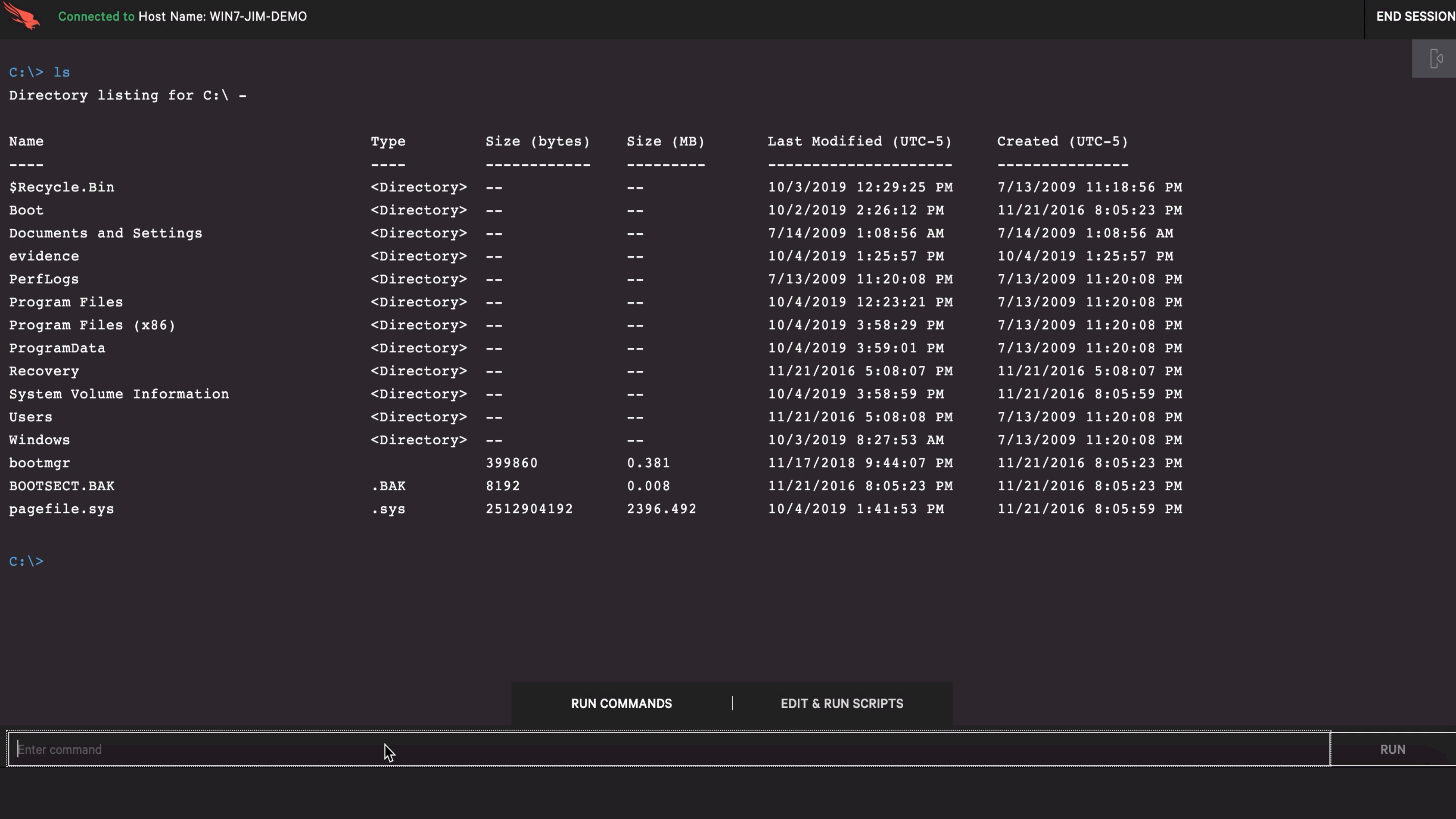
```
help                         Get help on a specific command or subcommand
history                      View History
ipconfig                     Show network configuration information
kill                         Kill a process
ls                           Display the contents of the specified path
map                          Map an SMB (network) share drive
memdump                      Dump the memory of a process
mkdir                        Create a new directory (access restricted to administrative groups)
mount                        List mounted filesystem volumes
mv                           Move a file or directory
netstat                      Display network statistics and active connections
ps                           Display process information
put                          Put a file from the CrowdStrike cloud onto the machine
pwsh                         pwsh command
reg                          Windows registry manipulation. Subcommands: delete, load, query, set, unload
restart                      Restart target system
rm                           Remove a file or directory
run                          Run an executable
runscript                    Run a PowerShell script
shutdown                     Shutdown target system
unmap                        Unmap an SMB (network) share drive
xmemdump                     Dump the complete or kernel memory of a system
zip                          Compress a file or directory into a zip file

C:\>
```

THE COMMANDS

- wmic os get OSArchitecture
- ls/mkdir
- put autorunsc64.exe
- run "C:\Temp\autorunsc64.exe" -CommandLine="-accepteula -avm * -o C:\Temp\autoruns.txt"

POWERSHELL



```
C:\> ls
Directory listing for C:\ -

Name                                    Type         Size (bytes)    Size (MB)       Last Modified (UTC-5)     Created (UTC-5)
----                                    ----         ------------    ---------       ---------------------     ---------------
$Recycle.Bin                            <Directory>  --              --              10/3/2019 12:29:25 PM     7/13/2009 11:18:56 PM
Boot                                    <Directory>  --              --              10/2/2019 2:26:12 PM      11/21/2016 8:05:23 PM
Documents and Settings                  <Directory>  --              --              7/14/2009 1:08:56 AM      7/14/2009 1:08:56 AM
evidence                                <Directory>  --              --              10/4/2019 1:25:57 PM      10/4/2019 1:25:57 PM
PerfLogs                                <Directory>  --              --              7/13/2009 11:20:08 PM     7/13/2009 11:20:08 PM
Program Files                           <Directory>  --              --              10/4/2019 12:23:21 PM     7/13/2009 11:20:08 PM
Program Files (x86)                     <Directory>  --              --              10/4/2019 3:58:29 PM      7/13/2009 11:20:08 PM
ProgramData                             <Directory>  --              --              10/4/2019 3:59:01 PM      7/13/2009 11:20:08 PM
Recovery                                <Directory>  --              --              11/21/2016 5:08:07 PM     11/21/2016 5:08:07 PM
System Volume Information               <Directory>  --              --              10/4/2019 3:58:59 PM      11/21/2016 8:05:59 PM
Users                                   <Directory>  --              --              11/21/2016 5:08:08 PM     7/13/2009 11:20:08 PM
Windows                                 <Directory>  --              --              10/3/2019 8:27:53 AM      7/13/2009 11:20:08 PM
bootmgr                                              399860          0.381           11/17/2018 9:44:07 PM     11/21/2016 8:05:23 PM
BOOTSECT.BAK                            .BAK         8192            0.008           11/21/2016 8:05:23 PM     11/21/2016 8:05:23 PM
pagefile.sys                            .sys         2512904192      2396.492        10/4/2019 1:41:53 PM      11/21/2016 8:05:59 PM

C:\>
```

THE COMMANDS

-
  ```
  [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
  Invoke-WebRequest -URI https://github.com/Invoke-IR/PowerForensics/releases/download/1.1.1/PowerForensicsv2.zip -OutFile "C:\PowerForensicsv2.zip”
  ```

-
  ```
  Expand-Archive -path 'C:\PowerForensicsv2.zip' -destinationpath "C:\Program Files\WindowsPowerShell\Modules\
  ```

-
  ```
  Import-Module PowerForensicsv2
  ```

POWERFORENSICS

- Get-ForensicFileRecord (parse the MFT!)
- Invoke-ForensicDD
- Get-ForensicEventLog
- Get-ForensicPrefetch
- Get-ForensicTimezone

PowerForensics by **Developed by @jaredcatkinson**

OTHER USEFUL ONE-LINERS

- Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0 –Force
- [System.Environment]::Is64BitOperatingSystem
- Get-Childitem –Path C:\ -Include <Your Search String Here> -Recurse -ErrorAction SilentlyContinue
- Get-Item –Path C:\<Path-To-File> -stream *

RTR AT SCALE?

RTR IS POWERFUL

RTR has an API

You can automate doing a forensic collection of the MFT

CrowdCollect

Gather a number of different triage artifacts from a remote host

Map a network share

Xmemdump to copy and you can collect all of your triage information online

DOCUMENT AND ITERATE

Record useful one-liners and longer remediation scripts

Automate responding to common detections (Dridex/Trickbot/Phishing)

Share that knowledge as a community

FALCON Unite

THANK YOU.

ANY QUESTIONS?