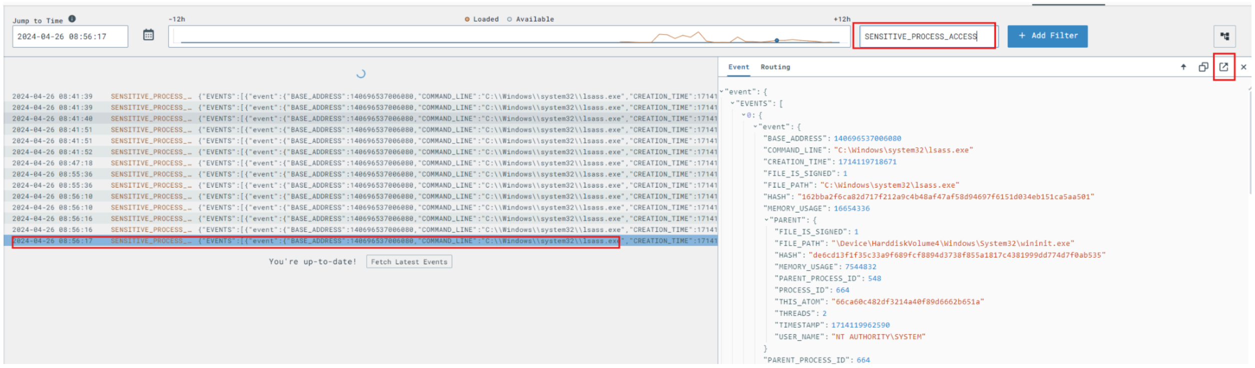
Let’s Get Adversarial

Let’s jump back to Sliver C2 session launched in Part 2 and do some shady stuff that we would want to be able to detect.

1. Get back onto an SSH session on the Linux VM, and drop into a C2 session on your victim.
    a. Retrace your steps from Part 2 if need be.
2. Run the following commands within the Sliver session on your victim host
    a. First, we need to check our privileges to make sure we can perform privileged actions on the host
       Enter “getprivs”
        i. A powerful privilege to check for is SeDebugPrivilege which opens the door for many things.
3. Next, let’s do something adversaries love to do for stealing credentials on a system — dump the lsass.exe process from memory. Read more about this technique here.
   Enter “procdump -n lsass.exe -s lsass.dmp”
    a. This will dump the remote process from memory, and save it locally on your Sliver C2 server. We are not going to further process the lsass dump, but I’ll leave it as an exercise for the reader if you want to try your hand at it.
    b. **NOTE**: This will fail if you did not launch your C2 payload with admin rights on the Windows system. If it still fails for an unknown reason (RPC error, etc), don’t fret, it likely still generated the telemetry we needed. Move on and see if you can still detect the attempt.

Now that we’ve done something adversarial, let’s switch over to LimaCharlie to find the relevant telemetry

a. Since lsass.exe is a known sensitive process often targeted by credential dumping tools, any good EDR will generate events for this.
b. Drill into the Timeline of your Windows VM sensor and use the “Event Type Filters” to filter for “SENSITIVE_PROCESS_ACCESS” events.
    i. There will likely be many of these, but pick any one of them as there isn’t much else on this system that will be legitimately accessing lsass.



Jump to Time: 2024-04-26 08:56:17

SENSITIVE_PROCESS_ACCESS

```
2024-04-26 08:41:39   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass.exe","CREATION_TIME":17141
2024-04-26 08:41:39   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass.exe","CREATION_TIME":17141
2024-04-26 08:41:40   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass.exe","CREATION_TIME":17141
2024-04-26 08:41:51   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass.exe","CREATION_TIME":17141
2024-04-26 08:41:51   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass.exe","CREATION_TIME":17141
2024-04-26 08:41:52   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass.exe","CREATION_TIME":17141
2024-04-26 08:47:18   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass.exe","CREATION_TIME":17141
2024-04-26 08:55:36   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass.exe","CREATION_TIME":17141
2024-04-26 08:55:36   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass.exe","CREATION_TIME":17141
2024-04-26 08:56:10   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass.exe","CREATION_TIME":17141
2024-04-26 08:56:10   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass.exe","CREATION_TIME":17141
2024-04-26 08:56:16   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass.exe","CREATION_TIME":17141
2024-04-26 08:56:16   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass.exe","CREATION_TIME":17141
2024-04-26 08:56:17   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass.exe","CREATION_TIME":17141
```

You're up-to-date!

```
"event": {
  "EVENTS": [
    0: {
      "event": {
        "BASE_ADDRESS": 140696537006080
        "COMMAND_LINE": "C:\Windows\system32\lsass.exe"
        "CREATION_TIME": 1714119718671
        "FILE_IS_SIGNED": 1
        "FILE_PATH": "C:\Windows\system32\lsass.exe"
        "HASH": "162bba2f6ca82d717f212a9c4b48af47af58d94697f6151d034eb151ca5aa501"
        "MEMORY_USAGE": 16654336
        "PARENT": {
          "FILE_IS_SIGNED": 1
          "FILE_PATH": "\Device\HarddiskVolume4\Windows\System32\wininit.exe"
          "HASH": "de6cd13f1f35c33a9f689fcf8894d3738f855a1817c4381999dd774d7f0ab535"
          "MEMORY_USAGE": 7544832
          "PARENT_PROCESS_ID": 548
          "PROCESS_ID": 664
          "THIS_ATOM": "66ca60c482df3214a40f89d6662b651a"
          "THREADS": 2
          "TIMESTAMP": 1714119962590
          "USER_NAME": "NT AUTHORITY\SYSTEM"
        }
        "PARENT_PROCESS_ID": 664
```

4. Input the following into the detect and Respond respectively
5. Detect: “event: SENSITIVE_PROCESS_ACCESS

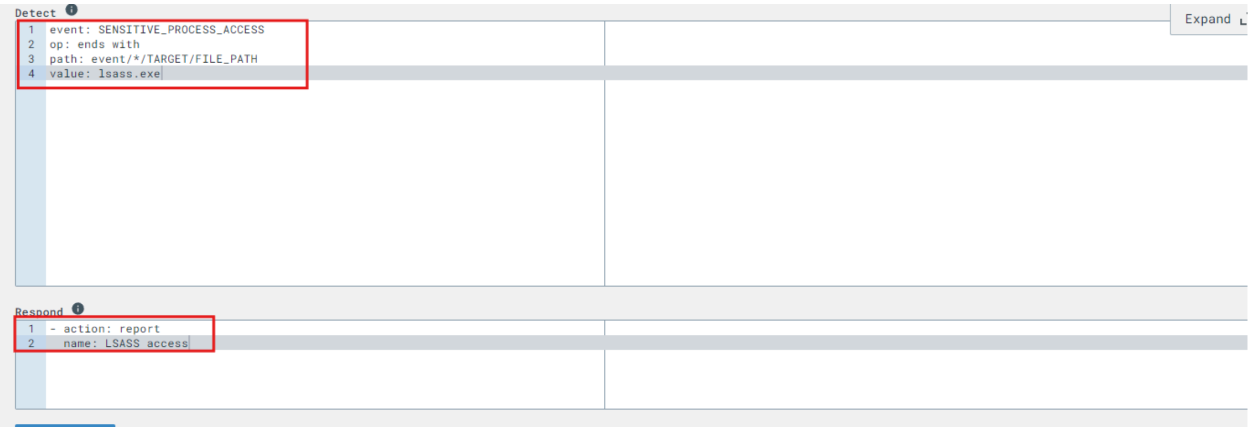
   op: ends with

   path: event/*/TARGET/FILE_PATH

   value: lsass.exe”

6. Respond: “- action: report

   name: LSASS access”



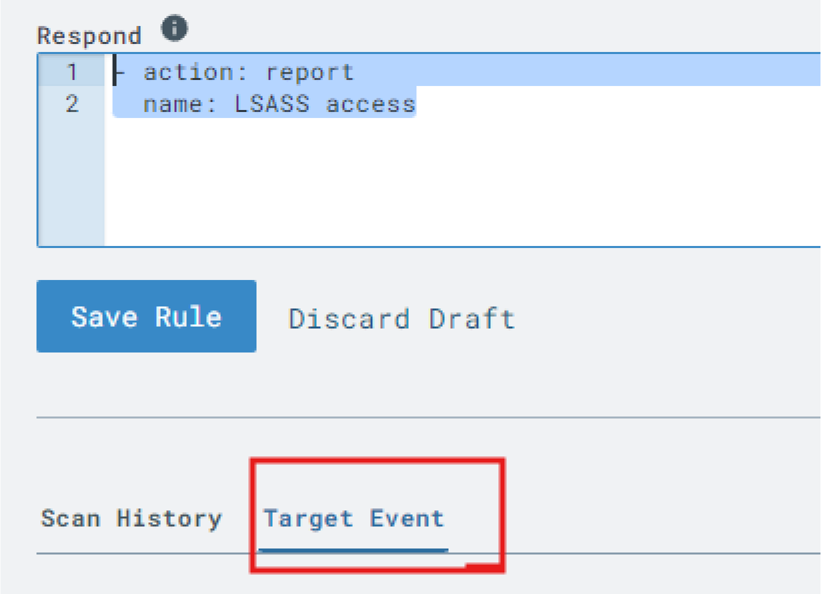
Detect

```
event: SENSITIVE_PROCESS_ACCESS
op: ends with
path: event/*/TARGET/FILE_PATH
value: lsass.exe
```

Respond

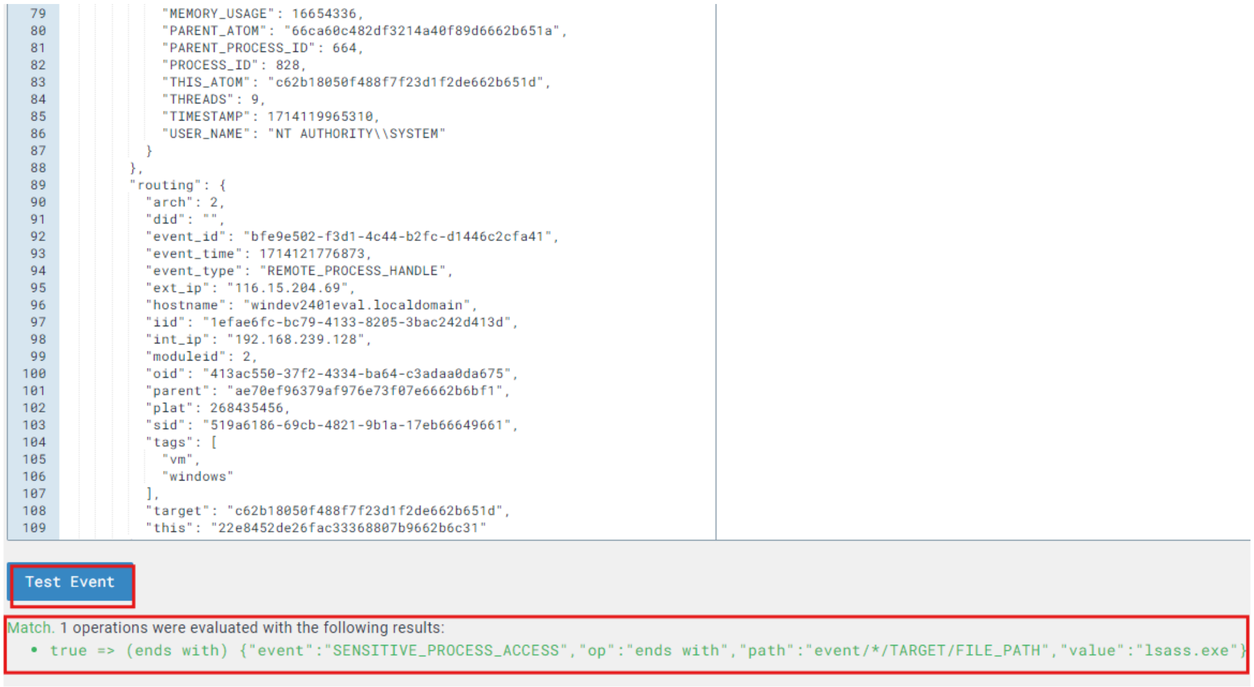
```
- action: report
  name: LSASS access
```

7. The following should be your results
    a. Click on target events



```
- action: report
  name: LSASS access
```

    b. Scroll all the way down and click on test events
        i. The following should be your results

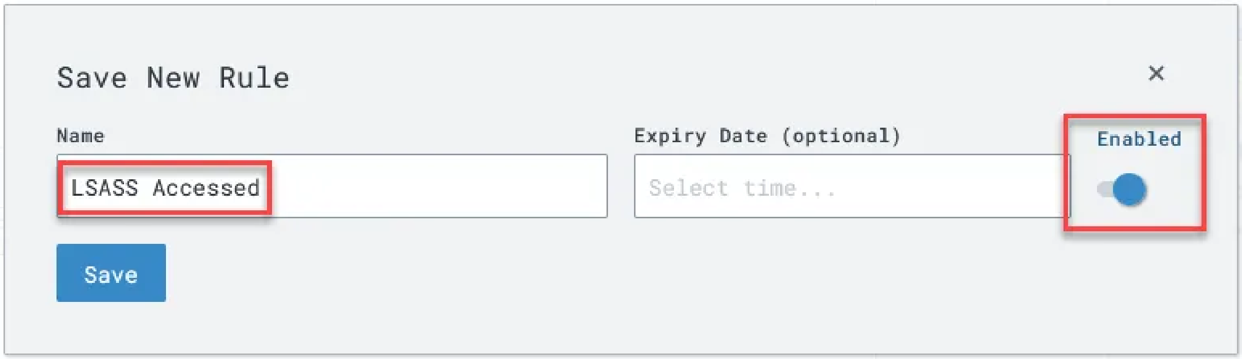


```
        "MEMORY_USAGE": 16654336,
        "PARENT_ATOM": "66ca60c482df3214a40f89d6662b651a",
        "PARENT_PROCESS_ID": 664,
        "PROCESS_ID": 828,
        "THIS_ATOM": "c62b18050f488f7f23d1f2de662b651d",
        "THREADS": 9,
        "TIMESTAMP": 1714119965310,
        "USER_NAME": "NT AUTHORITY\\SYSTEM"
      }
    },
    "routing": {
      "arch": 2,
      "did": "",
      "event_id": "bfe9e502-f3d1-4c44-b2fc-d1446c2cfa41",
      "event_time": 1714121776873,
      "event_type": "REMOTE_PROCESS_HANDLE",
      "ext_ip": "116.15.204.69",
      "hostname": "windev2401eval.localdomain",
      "iid": "1efae6fc-bc79-4133-8205-3bac242d413d",
      "int_ip": "192.168.239.128",
      "moduleid": 2,
      "oid": "413ac550-37f2-4334-ba64-c3adaa0da675",
      "parent": "ae70ef96379af976e73f07e6662b6bf1",
      "plat": 268435456,
      "sid": "519a6186-69cb-4821-9b1a-17eb66649661",
      "tags": [
        "vm",
        "windows"
      ],
      "target": "c62b18050f488f7f23d1f2de662b651d",
      "this": "22e8452de26fac33368807b9662b6c31"
```

Match. 1 operations were evaluated with the following results:

- true => (ends with) {"event":"SENSITIVE_PROCESS_ACCESS","op":"ends with","path":"event/*/TARGET/FILE_PATH","value":"lsass.exe"}

8. Save the rule as LSASS Accessed


Save New Rule

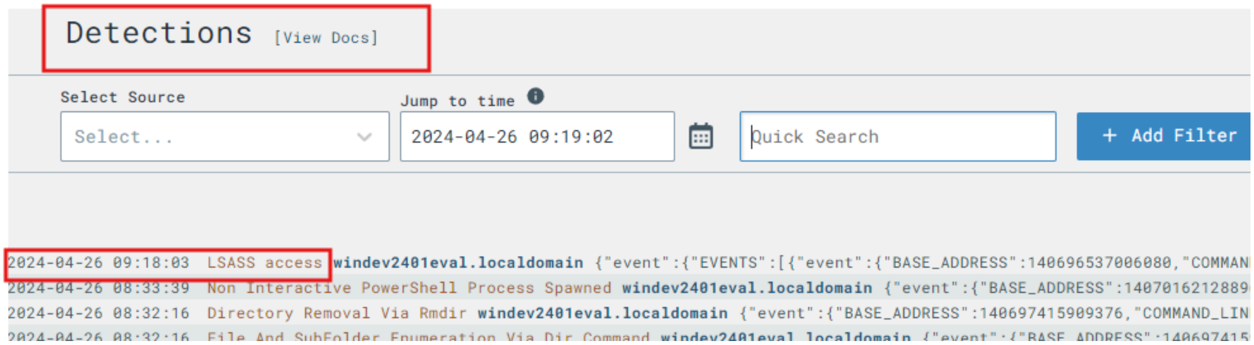
Name: LSASS Accessed

Expiry Date (optional): Select time...

Enabled

Let’s Be Bad Again, Now with Detections!

1. Return to your Sliver server console, back into your C2 session, and rerun our same procdump command from the beginning of this post
    a. If at some point your C2 session dies, just relaunch your malware with the steps in Part 2
2. After rerunning the procdump command, go to the “Detections” tab on the LimaCharlie main left-side menu.
    a. If you are still in the context of your sensor, click “Back to Sensors” at the top of the menu, then you will see the “Detections” option.

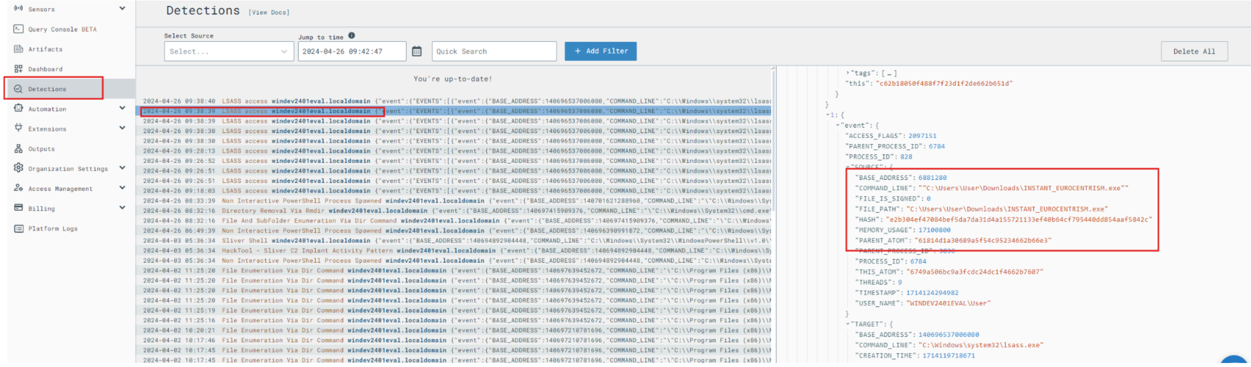

Detections [View Docs]

Select Source: Select...

Jump to time: 2024-04-26 09:19:02

```
2024-04-26 09:18:03  LSASS access windev2401eval.localdomain {"event":{"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAN
2024-04-26 08:33:39  Non Interactive PowerShell Process Spawned windev2401eval.localdomain {"event":{"BASE_ADDRESS":1407016212889
2024-04-26 08:32:16  Directory Removal Via Rmdir windev2401eval.localdomain {"event":{"BASE_ADDRESS":140697415909376,"COMMAND_LIN
2024-04-26 08:32:16  File And SubFolder Enumeration Via Dir Command windev2401eval.localdomain {"event":{"BASE_ADDRESS":14069741
```

3. You’ve just detected a threat with your own detection signature!
    a. Expand a detection to see the raw event



Detections [View Docs]

Select Source: Select...
Jump to time: 2024-04-26 09:42:47
Quick Search

You're up-to-date!

```
2024-04-26 09:38:40 LSASS access windev2401eval.localdomain {"event":{"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass
2024-04-26 09:38:39 LSASS access windev2401eval.localdomain {"event":{"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass
2024-04-26 09:38:39 LSASS access windev2401eval.localdomain {"event":{"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass
2024-04-26 09:38:30 LSASS access windev2401eval.localdomain {"event":{"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass
2024-04-26 09:38:30 LSASS access windev2401eval.localdomain {"event":{"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass
2024-04-26 09:28:13 LSASS access windev2401eval.localdomain {"event":{"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass
2024-04-26 09:26:52 LSASS access windev2401eval.localdomain {"event":{"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass
2024-04-26 09:26:51 LSASS access windev2401eval.localdomain {"event":{"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass
2024-04-26 09:26:51 LSASS access windev2401eval.localdomain {"event":{"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass
2024-04-26 09:18:03 LSASS access windev2401eval.localdomain {"event":{"EVENTS":[{"event":{"BASE_ADDRESS":140696537006080,"COMMAND_LINE":"C:\\Windows\\system32\\lsass
2024-04-26 08:33:39 Non Interactive PowerShell Process Spawned windev2401eval.localdomain {"event":{"BASE_ADDRESS":140701621288960,"COMMAND_LINE":"\"C:\\Windows\\Sys
2024-04-26 08:32:16 Directory Removal Via Rmdir windev2401eval.localdomain {"event":{"BASE_ADDRESS":140697415909376,"COMMAND_LINE":"\"C:\\Windows\\System32\\cmd.exe\
2024-04-26 08:32:16 File And SubFolder Enumeration Via Dir Command windev2401eval.localdomain {"event":{"BASE_ADDRESS":140697415909376,"COMMAND_LINE":"\"C:\\Windows\
2024-04-26 06:49:39 Non Interactive PowerShell Process Spawned windev2401eval.localdomain {"event":{"BASE_ADDRESS":140696390991872,"COMMAND_LINE":"\"C:\\Windows\\Sys
2024-04-03 05:36:34 Sliver Shell windev2401eval.localdomain {"event":{"BASE_ADDRESS":140694892904448,"COMMAND_LINE":"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\
2024-04-03 05:36:34 HackTool - Sliver C2 Implant Activity Pattern windev2401eval.localdomain {"event":{"BASE_ADDRESS":140694892904448,"COMMAND_LINE":"C:\\Windows\\Sy
2024-04-03 05:36:34 Non Interactive PowerShell Process Spawned windev2401eval.localdomain {"event":{"BASE_ADDRESS":140694892904448,"COMMAND_LINE":"C:\\Windows\\Syste
2024-04-02 11:25:20 File Enumeration Via Dir Command windev2401eval.localdomain {"event":{"BASE_ADDRESS":140697639452672,"COMMAND_LINE":"\"C:\\Program Files (x86)\\
2024-04-02 11:25:20 File Enumeration Via Dir Command windev2401eval.localdomain {"event":{"BASE_ADDRESS":140697639452672,"COMMAND_LINE":"\"C:\\Program Files (x86)\\
2024-04-02 11:25:20 File Enumeration Via Dir Command windev2401eval.localdomain {"event":{"BASE_ADDRESS":140697639452672,"COMMAND_LINE":"\"C:\\Program Files (x86)\\
2024-04-02 11:25:20 File Enumeration Via Dir Command windev2401eval.localdomain {"event":{"BASE_ADDRESS":140697639452672,"COMMAND_LINE":"\"C:\\Program Files (x86)\\
2024-04-02 11:25:19 File Enumeration Via Dir Command windev2401eval.localdomain {"event":{"BASE_ADDRESS":140697639452672,"COMMAND_LINE":"\"C:\\Program Files (x86)\\
2024-04-02 11:25:16 File Enumeration Via Dir Command windev2401eval.localdomain {"event":{"BASE_ADDRESS":140697639452672,"COMMAND_LINE":"\"C:\\Program Files (x86)\\
2024-04-02 10:20:21 File Enumeration Via Dir Command windev2401eval.localdomain {"event":{"BASE_ADDRESS":140697210781696,"COMMAND_LINE":"\"C:\\Program Files (x86)\\
2024-04-02 10:17:46 File Enumeration Via Dir Command windev2401eval.localdomain {"event":{"BASE_ADDRESS":140697210781696,"COMMAND_LINE":"\"C:\\Program Files (x86)\\
2024-04-02 10:17:45 File Enumeration Via Dir Command windev2401eval.localdomain {"event":{"BASE_ADDRESS":140697210781696,"COMMAND_LINE":"\"C:\\Program Files (x86)\\
2024-04-02 10:17:45 File Enumeration Via Dir Command windev2401eval.localdomain {"event":{"BASE_ADDRESS":140697210781696,"COMMAND_LINE":"\"C:\\Program Files (x86)\\
```

```
  › "tags": [ … ]
    "this": "c62b18050f488f7f23d1f2de662b651d"
  }
}
˅ 1: {
  ˅ "event": {
      "ACCESS_FLAGS": 2097151
      "PARENT_PROCESS_ID": 6784
      "PROCESS_ID": 828
    ˅ "SOURCE": {
        "BASE_ADDRESS": 6881280
        "COMMAND_LINE": ""C:\Users\User\Downloads\INSTANT_EUROCENTRISM.exe""
        "FILE_IS_SIGNED": 0
        "FILE_PATH": "C:\Users\User\Downloads\INSTANT_EUROCENTRISM.exe"
        "HASH": "e2b304ef47084bef5da7da31d4a155721133ef40b64cf795440dd854aaf5842c"
        "MEMORY_USAGE": 17100800
        "PARENT_ATOM": "61814d1a30689a5f54c95234662b66e3"
        "PARENT_PROCESS_ID": 3036
        "PROCESS_ID": 6784
        "THIS_ATOM": "6749a506bc9a3fcdc24dc1f4662b7607"
        "THREADS": 9
        "TIMESTAMP": 1714124294982
        "USER_NAME": "WINDEV2401EVAL\User"
      }
    ˅ "TARGET": {
        "BASE_ADDRESS": 140696537006080
        "COMMAND_LINE": "C:\Windows\system32\lsass.exe"
        "CREATION_TIME": 1714119718671
```