SOAR-EDR Project

Project Description

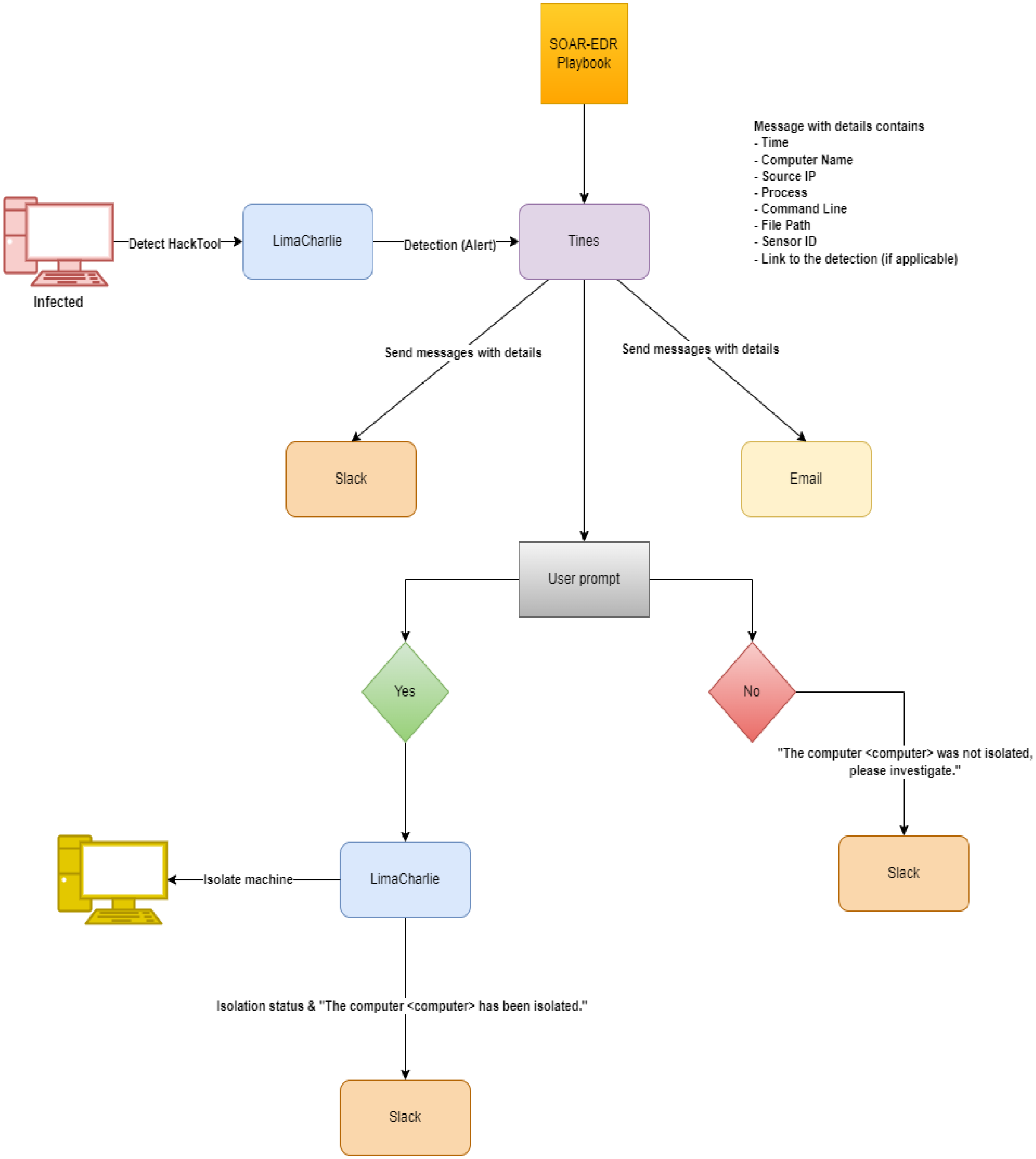
In this project, I will be creating a detection rule in LimaCharlie (an EDR platform) that will detect a tool used to recover passwords on a machine and send it over to Tines (a SOAR platform), which will have a playbook that I created. The playbook will send the user an email, a Slack message, and finally ask if they want to isolate the machine. If the user says “Yes”, LimaCharlie will isolate the machine automatically.

Software and Tools

- LimaCharlie
- LaZagne
- Slack
- Tines
- Square X

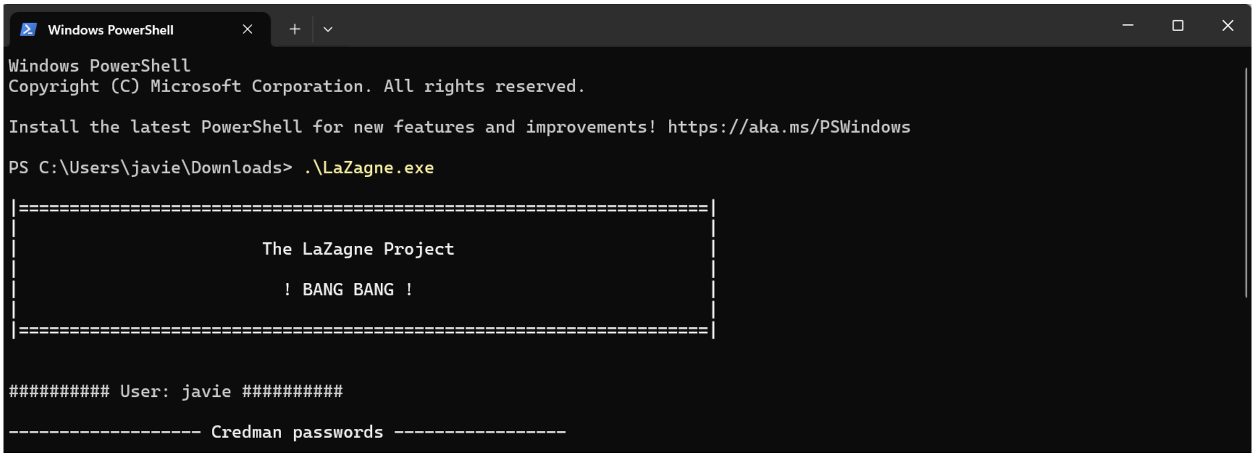
Walkthrough

Before I start, I will create a playbook workflow to help me accomplish my objectives. The following illustrated image should demonstrate the mentioned workflow:


SOAR-EDR Playbook
Infected
Detect HackTool
LimaCharlie
Detection (Alert)
Tines
Send messages with details
Send messages with details
Slack
Email
User prompt
Yes
No
"The computer <computer> was not isolated, please investigate."
Slack
Isolate machine
LimaCharlie
Isolation status & "The computer <computer> has been isolated."
Slack

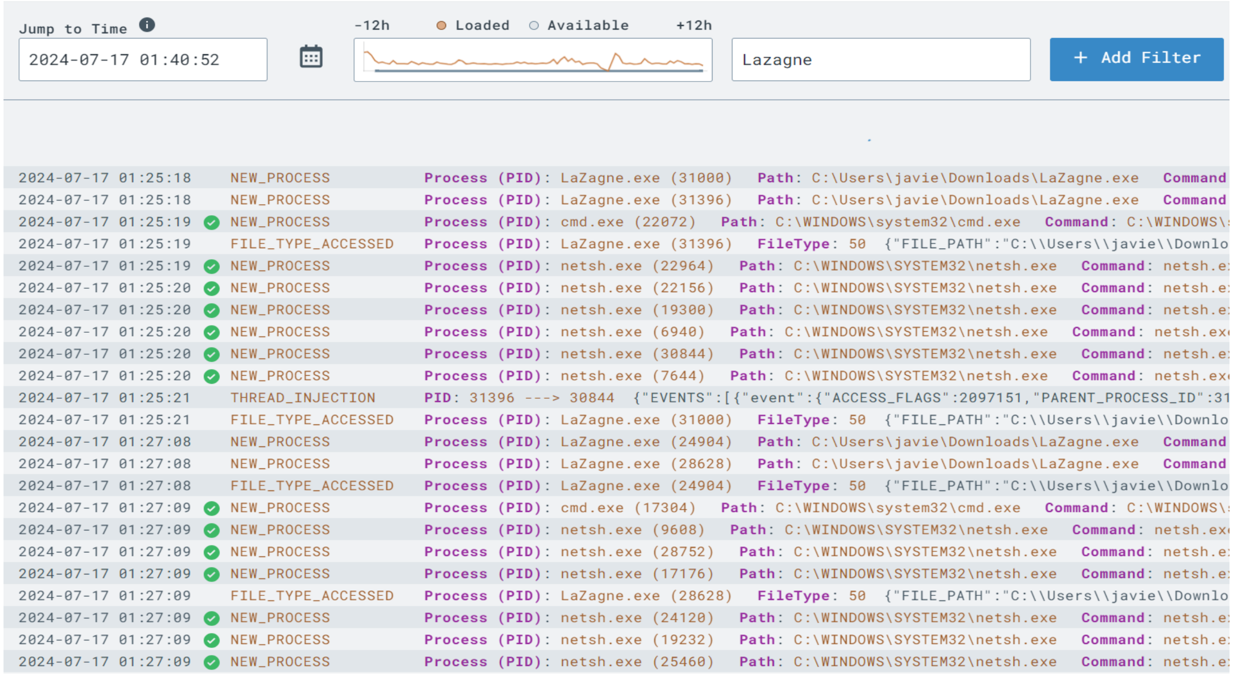
Message with details contains
- Time
- Computer Name
- Source IP
- Process
- Command Line
- File Path
- Sensor ID
- Link to the detection (if applicable)

I proceeded to download LaZagne, which is a password recovery tool. Once downloaded, I opened Windows Powershell and executed the application. The reason I did this is for LimaCharlie to detect the process for LaZagne.



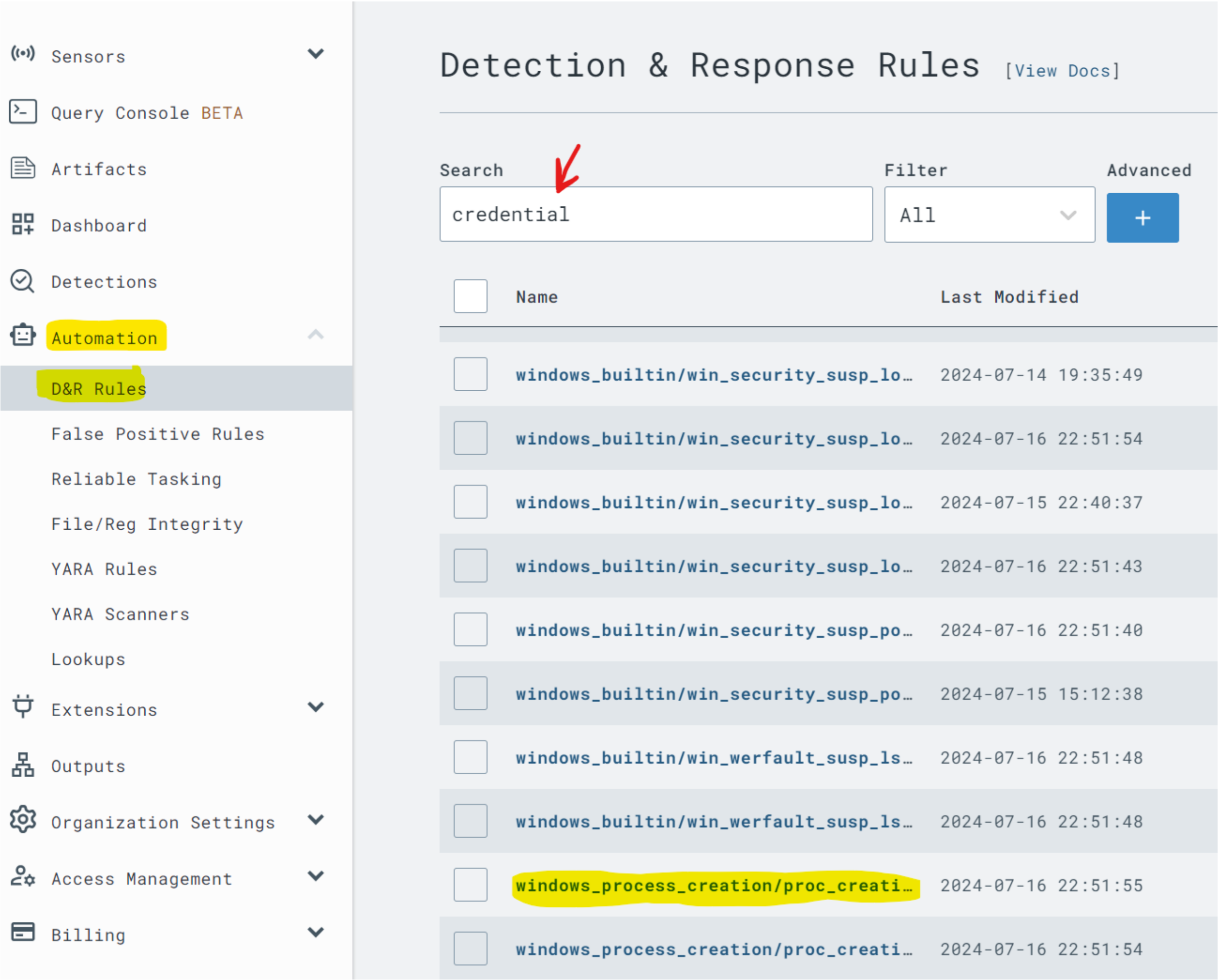
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\javie\Downloads> .\LaZagne.exe

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|


########## User: javie ##########

------------------- Credman passwords -----------------
```

Once I visited LimaCharlie, I went to *Sensor > Sensor List > selected my machine > Timeline*. To simplify the results, I typed “Lazagne” on the Quick Search tab to only see events related to the application.



```
2024-07-17 01:40:52
Lazagne

2024-07-17 01:25:18    NEW_PROCESS           Process (PID): LaZagne.exe (31000)   Path: C:\Users\javie\Downloads\LaZagne.exe   Command
2024-07-17 01:25:18    NEW_PROCESS           Process (PID): LaZagne.exe (31396)   Path: C:\Users\javie\Downloads\LaZagne.exe   Command
2024-07-17 01:25:19 ✓  NEW_PROCESS           Process (PID): cmd.exe (22072)   Path: C:\WINDOWS\system32\cmd.exe   Command: C:\WINDOWS\
2024-07-17 01:25:19    FILE_TYPE_ACCESSED    Process (PID): LaZagne.exe (31396)   FileType: 50  {"FILE_PATH":"C:\\Users\\javie\\Downlo
2024-07-17 01:25:19 ✓  NEW_PROCESS           Process (PID): netsh.exe (22964)   Path: C:\WINDOWS\SYSTEM32\netsh.exe   Command: netsh.e
2024-07-17 01:25:20 ✓  NEW_PROCESS           Process (PID): netsh.exe (22156)   Path: C:\WINDOWS\SYSTEM32\netsh.exe   Command: netsh.e
2024-07-17 01:25:20 ✓  NEW_PROCESS           Process (PID): netsh.exe (19300)   Path: C:\WINDOWS\SYSTEM32\netsh.exe   Command: netsh.e
2024-07-17 01:25:20 ✓  NEW_PROCESS           Process (PID): netsh.exe (6940)   Path: C:\WINDOWS\SYSTEM32\netsh.exe   Command: netsh.exe
2024-07-17 01:25:20 ✓  NEW_PROCESS           Process (PID): netsh.exe (30844)   Path: C:\WINDOWS\SYSTEM32\netsh.exe   Command: netsh.e
2024-07-17 01:25:20 ✓  NEW_PROCESS           Process (PID): netsh.exe (7644)   Path: C:\WINDOWS\SYSTEM32\netsh.exe   Command: netsh.exe
2024-07-17 01:25:21    THREAD_INJECTION      PID: 31396 ---> 30844  {"EVENTS":[{"event":{"ACCESS_FLAGS":2097151,"PARENT_PROCESS_ID":31
2024-07-17 01:25:21    FILE_TYPE_ACCESSED    Process (PID): LaZagne.exe (31000)   FileType: 50  {"FILE_PATH":"C:\\Users\\javie\\Downlo
2024-07-17 01:27:08    NEW_PROCESS           Process (PID): LaZagne.exe (24904)   Path: C:\Users\javie\Downloads\LaZagne.exe   Command
2024-07-17 01:27:08    NEW_PROCESS           Process (PID): LaZagne.exe (28628)   Path: C:\Users\javie\Downloads\LaZagne.exe   Command
2024-07-17 01:27:08    FILE_TYPE_ACCESSED    Process (PID): LaZagne.exe (24904)   FileType: 50  {"FILE_PATH":"C:\\Users\\javie\\Downlo
2024-07-17 01:27:09 ✓  NEW_PROCESS           Process (PID): cmd.exe (17304)   Path: C:\WINDOWS\system32\cmd.exe   Command: C:\WINDOWS\
2024-07-17 01:27:09 ✓  NEW_PROCESS           Process (PID): netsh.exe (9608)   Path: C:\WINDOWS\SYSTEM32\netsh.exe   Command: netsh.exe
2024-07-17 01:27:09 ✓  NEW_PROCESS           Process (PID): netsh.exe (28752)   Path: C:\WINDOWS\SYSTEM32\netsh.exe   Command: netsh.e
2024-07-17 01:27:09 ✓  NEW_PROCESS           Process (PID): netsh.exe (17176)   Path: C:\WINDOWS\SYSTEM32\netsh.exe   Command: netsh.e
2024-07-17 01:27:09    FILE_TYPE_ACCESSED    Process (PID): LaZagne.exe (28628)   FileType: 50  {"FILE_PATH":"C:\\Users\\javie\\Downlo
2024-07-17 01:27:09 ✓  NEW_PROCESS           Process (PID): netsh.exe (24120)   Path: C:\WINDOWS\SYSTEM32\netsh.exe   Command: netsh.e
2024-07-17 01:27:09 ✓  NEW_PROCESS           Process (PID): netsh.exe (19232)   Path: C:\WINDOWS\SYSTEM32\netsh.exe   Command: netsh.e
2024-07-17 01:27:09 ✓  NEW_PROCESS           Process (PID): netsh.exe (25460)   Path: C:\WINDOWS\SYSTEM32\netsh.exe   Command: netsh.e
```

As seen in the image above, most of the app's events fall into the *NEW_PROCESS* event type. Now that I know the event type, I will proceed in creating a rule related to this event. I went to *Sensors > Automation > D&R Rules* and searched for rules that had to do with credentials. Then, I picked one that includes "process" in its name since the event type gathered from Lazagne includes the same word.

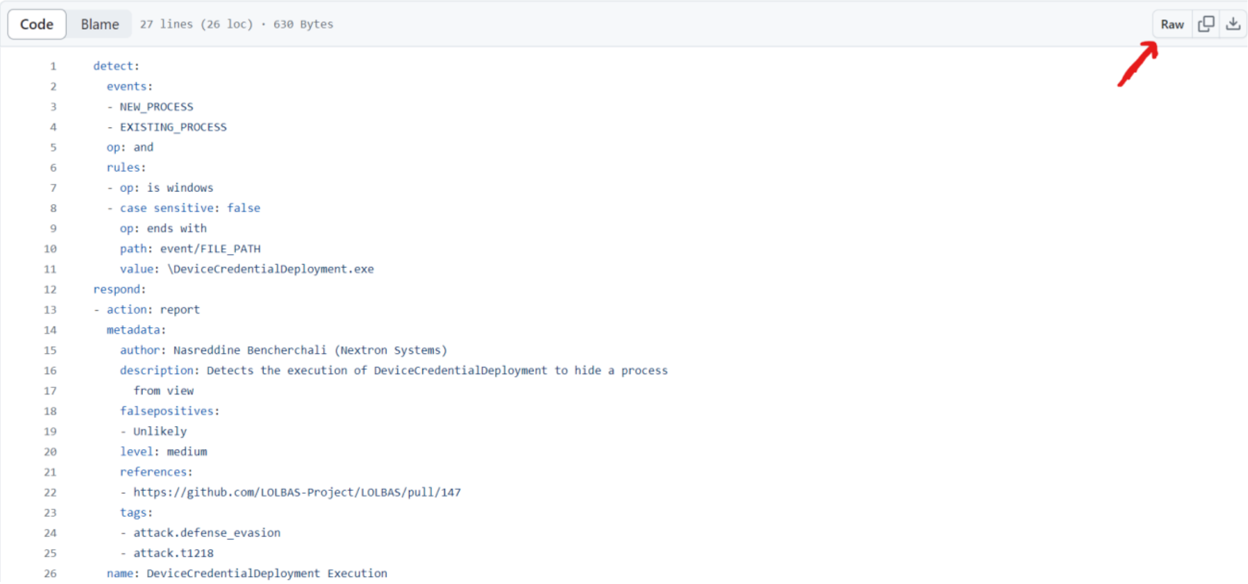


Search: credential

Filter: All

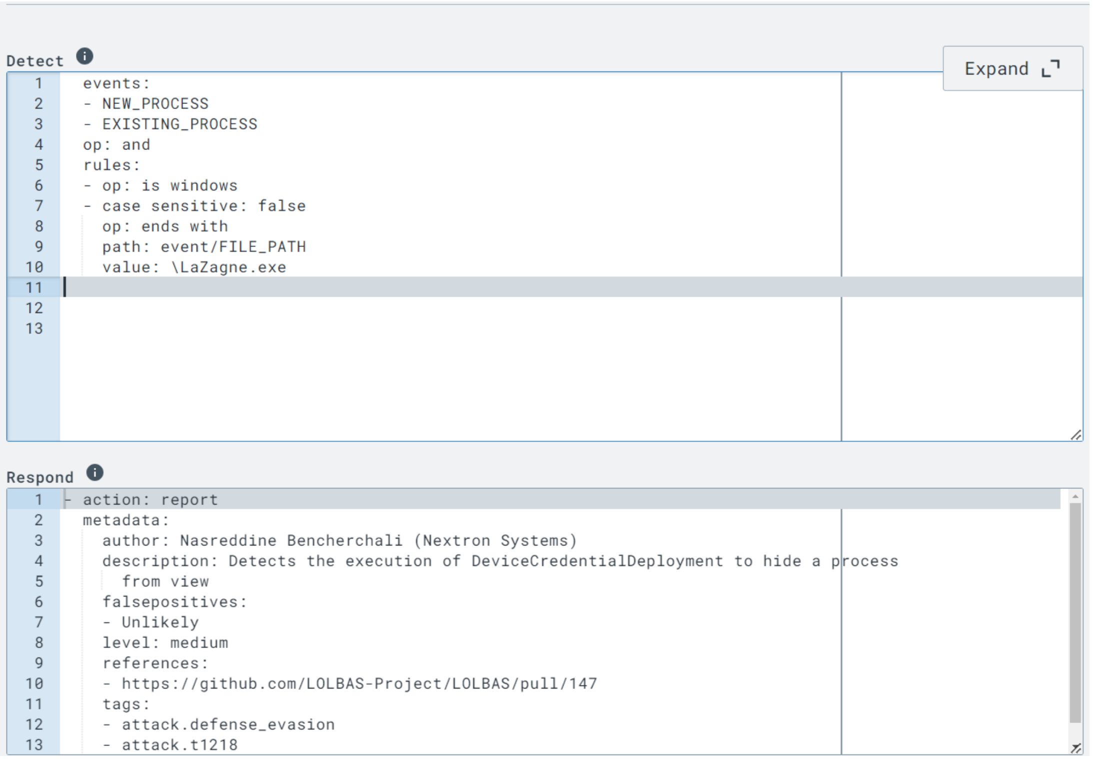
□	Name	Last Modified
□	windows_builtin/win_security_susp_lo…	2024-07-14 19:35:49
□	windows_builtin/win_security_susp_lo…	2024-07-16 22:51:54
□	windows_builtin/win_security_susp_lo…	2024-07-15 22:40:37
□	windows_builtin/win_security_susp_lo…	2024-07-16 22:51:43
□	windows_builtin/win_security_susp_po…	2024-07-16 22:51:40
□	windows_builtin/win_security_susp_po…	2024-07-15 15:12:38
□	windows_builtin/win_werfault_susp_ls…	2024-07-16 22:51:48
□	windows_builtin/win_werfault_susp_ls…	2024-07-16 22:51:48
□	windows_process_creation/proc_creati…	2024-07-16 22:51:55
□	windows_process_creation/proc_creati…	2024-07-16 22:51:54

Then, I proceeded in viewing the rule on GitHub. I clicked the Raw tab so I can copy the code.



```
detect:
  events:
  - NEW_PROCESS
  - EXISTING_PROCESS
  op: and
  rules:
  - op: is windows
  - case sensitive: false
    op: ends with
    path: event/FILE_PATH
    value: \DeviceCredentialDeployment.exe
respond:
- action: report
  metadata:
    author: Nasreddine Bencherchali (Nextron Systems)
    description: Detects the execution of DeviceCredentialDeployment to hide a process
      from view
    falsepositives:
    - Unlikely
    level: medium
    references:
    - https://github.com/LOLBAS-Project/LOLBAS/pull/147
    tags:
    - attack.defense_evasion
    - attack.t1218
  name: DeviceCredentialDeployment Execution
```

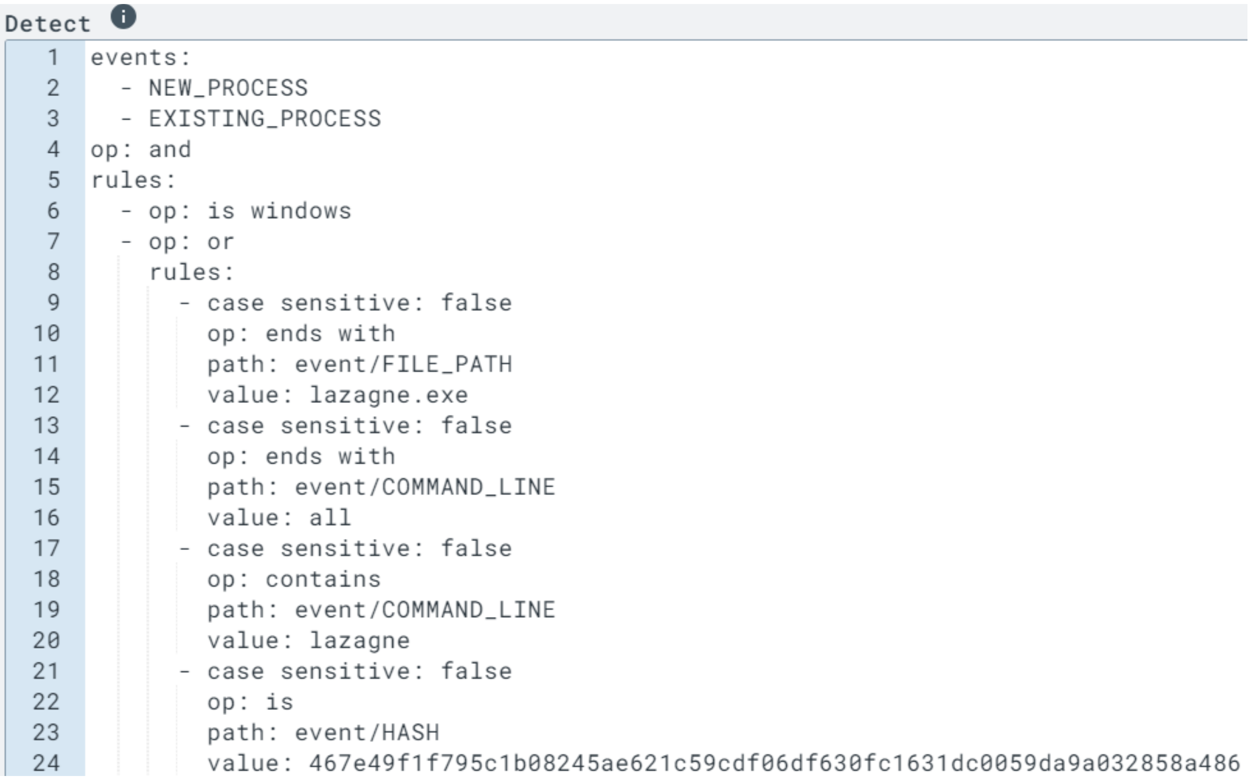
I went back to *D&R Rules*, clicked the "+ New Rule" button, and pasted the raw code, allocating the code blocks to their corresponding sections (Detect and Response) as seen below.



```
events:
- NEW_PROCESS
- EXISTING_PROCESS
op: and
rules:
- op: is windows
- case sensitive: false
  op: ends with
  path: event/FILE_PATH
  value: \LaZagne.exe
```

```
- action: report
metadata:
  author: Nasreddine Bencherchali (Nextron Systems)
  description: Detects the execution of DeviceCredentialDeployment to hide a process
    from view
  falsepositives:
  - Unlikely
  level: medium
  references:
  - https://github.com/LOLBAS-Project/LOLBAS/pull/147
  tags:
  - attack.defense_evasion
  - attack.t1218
```

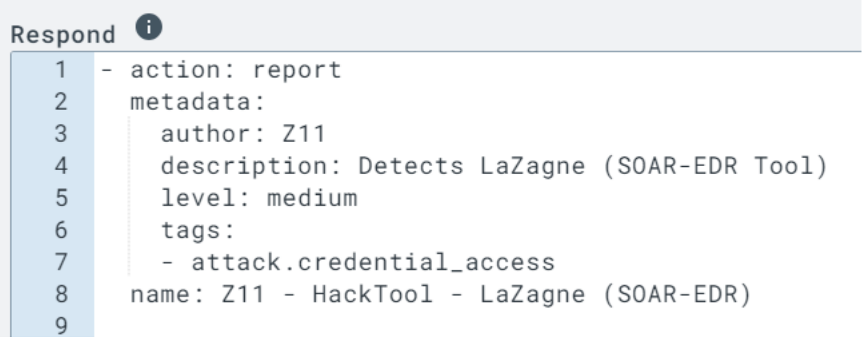
In the ***Detect*** block, I modified the rule to include other elements. This new rule, while ignoring case sensitive, now states that the event type must be either *NEW_PROCESS* or *EXISTING_PROCESS* and must be Windows; *FILE_PATH* ends with *Lazagne.exe*, or *COMMAND_LINE* ends with either *all* or contains *lazagne*; or *HASH* equals the lazagne hash value. This new rule can be seen below.



Detect

```
events:
  - NEW_PROCESS
  - EXISTING_PROCESS
op: and
rules:
  - op: is windows
  - op: or
    rules:
      - case sensitive: false
        op: ends with
        path: event/FILE_PATH
        value: lazagne.exe
      - case sensitive: false
        op: ends with
        path: event/COMMAND_LINE
        value: all
      - case sensitive: false
        op: contains
        path: event/COMMAND_LINE
        value: lazagne
      - case sensitive: false
        op: is
        path: event/HASH
        value: 467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486
```

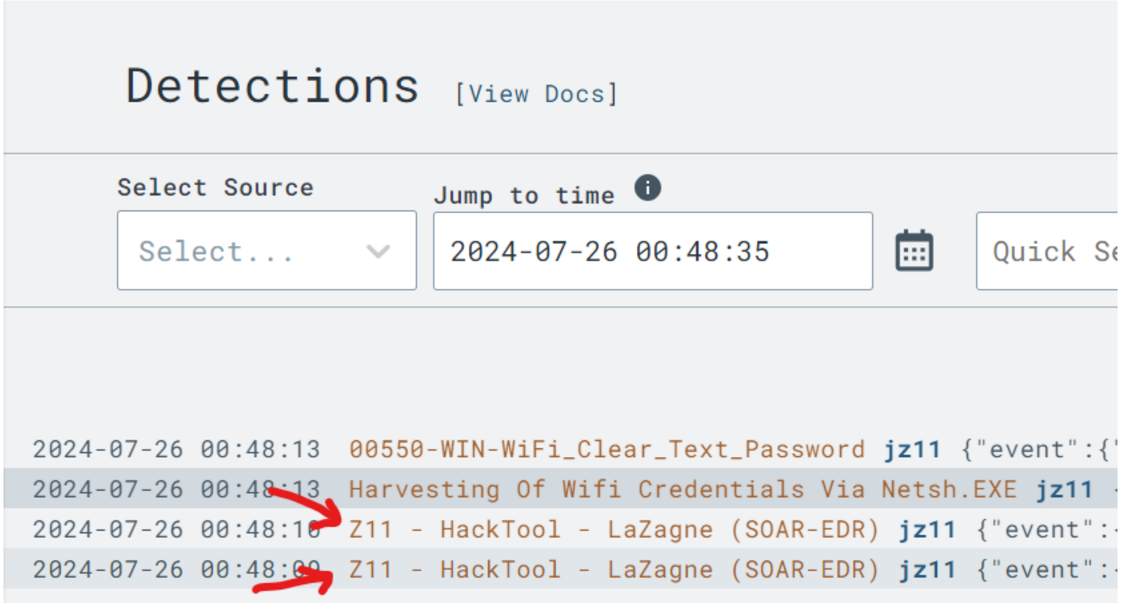
The ***Respond*** block is modified as shown below:



Respond

```
- action: report
  metadata:
    author: Z11
    description: Detects LaZagne (SOAR-EDR Tool)
    level: medium
    tags:
    - attack.credential_access
  name: Z11 - HackTool - LaZagne (SOAR-EDR)

```

Then, I went to test this rule by first clearing out my detection list from LimaCharlie, and then run ***LaZagne.exe*** through Windows Powershell. Once I ran it, I went back to LimaCharlie to see the new detections. As seen below, at the bottom of the list, there's two detections obtained from the new rule.



Detections [View Docs]

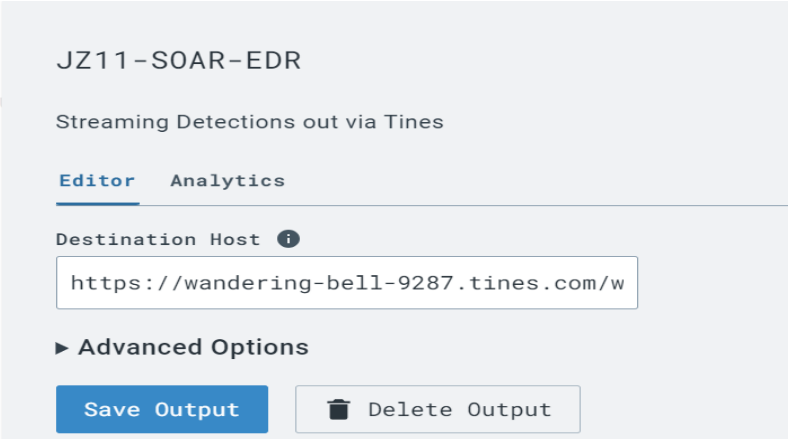
Select Source: Select...

Jump to time: 2024-07-26 00:48:35

Quick Se

```
2024-07-26 00:48:13  00550-WIN-WiFi_Clear_Text_Password jz11 {"event":{"
2024-07-26 00:48:13  Harvesting Of Wifi Credentials Via Netsh.EXE jz11
2024-07-26 00:48:10  Z11 - HackTool - LaZagne (SOAR-EDR) jz11 {"event":
2024-07-26 00:48:09  Z11 - HackTool - LaZagne (SOAR-EDR) jz11 {"event":
```

The next step will be linking up LimaCharlie with Tines. From LimaCharlie's dashboard, I went to *Outputs > Add output > Detections >* selected *Tines*, named the output as *JZ11-SOAR-EDR* and pasted the webhook URL from Tines to the ***Destination Host*** field, as seen below.

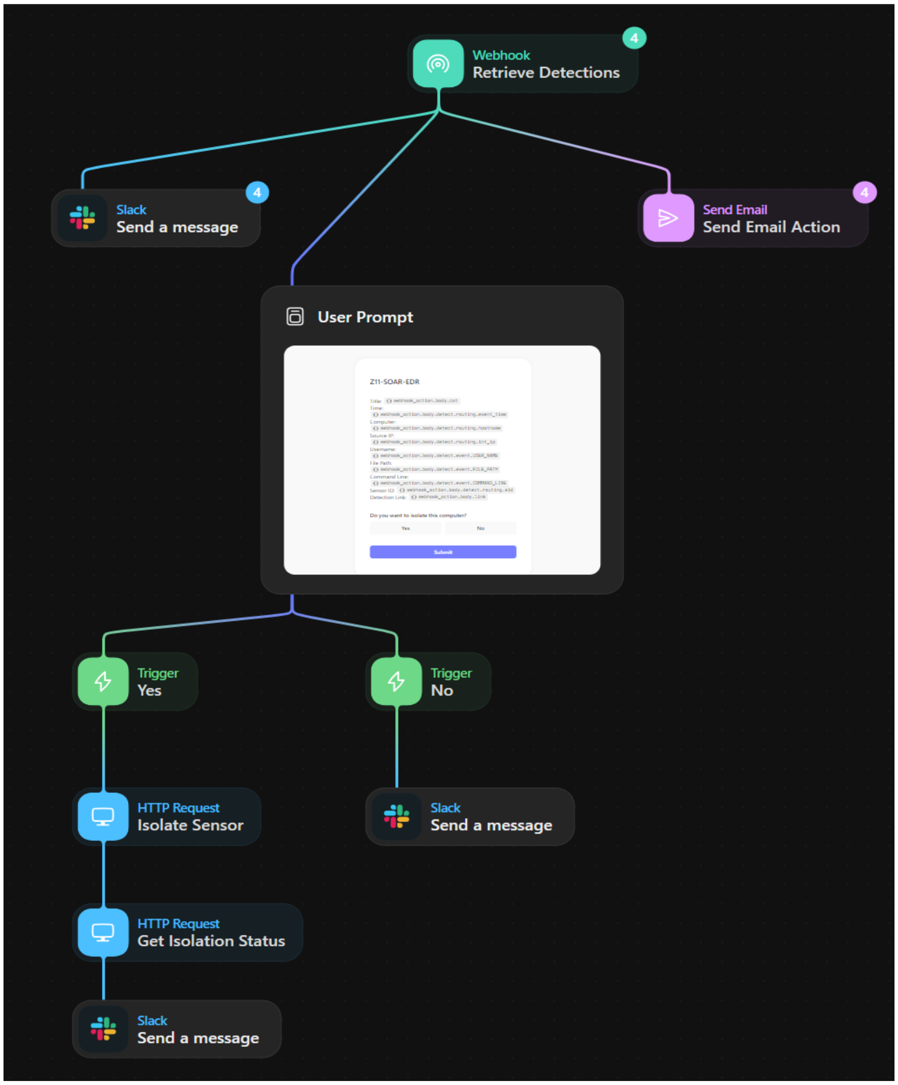


JZ11-SOAR-EDR

Streaming Detections out via Tines

Destination Host: https://wandering-bell-9287.tines.com/w

Then, I went to Tines to create my story (also known as *playbook*). It is important to mention that I have already created an account on Slack, which is a messaging application for businesses. On Slack, I created a new channel called *Alerts*. When I receive a detection from LimaCharlie on Tines, Tines will send a message over to Slack, specifically within the *Alerts* channel. As for the email message, I will be using a temporary email generated by Square X. I added the user prompt, which will ask the user if they want to isolate the computer. The following information will be sent to the email, Slack and the user prompt: title, ***`time, computer, source IP, username, file path, command line, sensor ID`***, and the ***`detection link`***. Below we can see how the story looks like on Tines.



Z11-SOAR-EDR

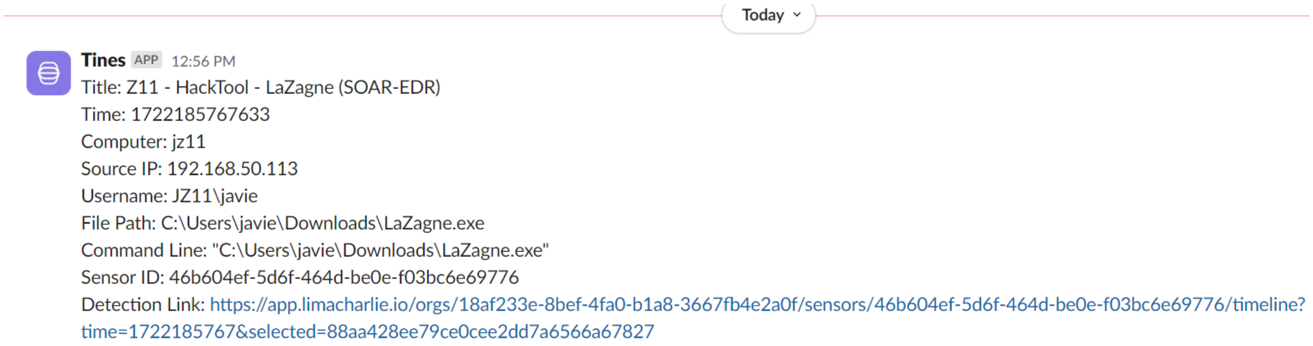
Title: webhook_action.body.cat
Time:
webhook_action.body.detect.routing.event_time
Computer:
webhook_action.body.detect.routing.hostname
Source IP:
webhook_action.body.detect.routing.int_ip
Username:
webhook_action.body.detect.event.USER_NAME
File Path:
webhook_action.body.detect.event.FILE_PATH
Command Line:
webhook_action.body.detect.event.COMMAND_LINE
Sensor ID: webhook_action.body.detect.routing.sid
Detection Link: webhook_action.body.link

Do you want to isolate this computer?

Yes No

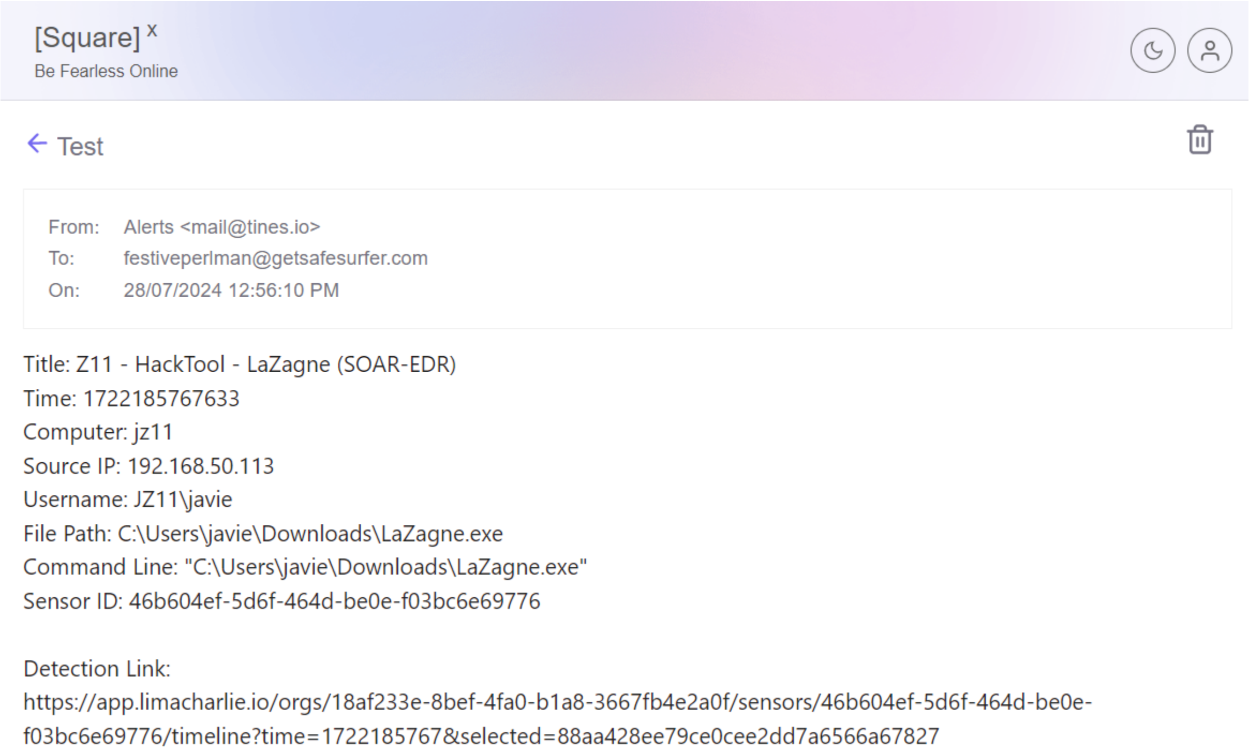
Submit

Now that everything is set up, I’ll proceed and start generating events to test the workflow. I ran ***LaZagne.exe*** from my Windows Powershell, then checked Slack to see if I got an email. As seen in the picture below, we can see that I received an email alert with all the information I have previously listed.



Title: Z11 - HackTool - LaZagne (SOAR-EDR)
Time: 1722185767633
Computer: jz11
Source IP: 192.168.50.113
Username: JZ11\javie
File Path: C:\Users\javie\Downloads\LaZagne.exe
Command Line: "C:\Users\javie\Downloads\LaZagne.exe"
Sensor ID: 46b604ef-5d6f-464d-be0e-f03bc6e69776
Detection Link: https://app.limacharlie.io/orgs/18af233e-8bef-4fa0-b1a8-3667fb4e2a0f/sensors/46b604ef-5d6f-464d-be0e-f03bc6e69776/timeline?time=1722185767&selected=88aa428ee79ce0cee2dd7a6566a67827

Then, I checked my disposable email inbox from Square X. Just like Slack, I received an email with all the information about the detection:

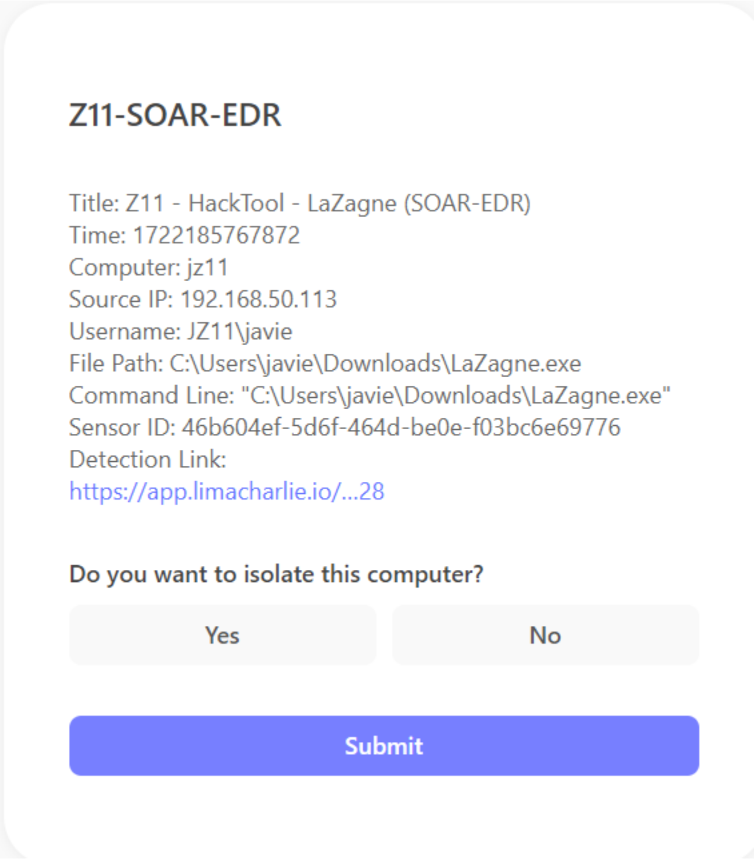


From: Alerts <mail@tines.io>
To: festiveperlman@getsafesurfer.com
On: 28/07/2024 12:56:10 PM

Title: Z11 - HackTool - LaZagne (SOAR-EDR)
Time: 1722185767633
Computer: jz11
Source IP: 192.168.50.113
Username: JZ11\javie
File Path: C:\Users\javie\Downloads\LaZagne.exe
Command Line: "C:\Users\javie\Downloads\LaZagne.exe"
Sensor ID: 46b604ef-5d6f-464d-be0e-f03bc6e69776

Detection Link:
https://app.limacharlie.io/orgs/18af233e-8bef-4fa0-b1a8-3667fb4e2a0f/sensors/46b604ef-5d6f-464d-be0e-f03bc6e69776/timeline?time=1722185767&selected=88aa428ee79ce0cee2dd7a6566a67827

From the user prompt, I opened the most recent event and it opened a new tab displaying the following information:

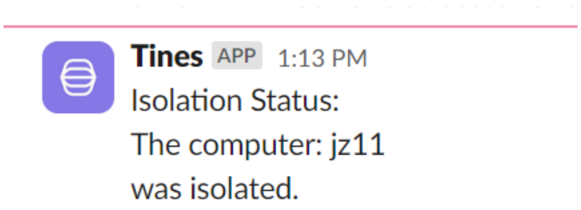


Z11-SOAR-EDR

Title: Z11 - HackTool - LaZagne (SOAR-EDR)
Time: 1722185767872
Computer: jz11
Source IP: 192.168.50.113
Username: JZ11\javie
File Path: C:\Users\javie\Downloads\LaZagne.exe
Command Line: "C:\Users\javie\Downloads\LaZagne.exe"
Sensor ID: 46b604ef-5d6f-464d-be0e-f03bc6e69776
Detection Link:
https://app.limacharlie.io/...28

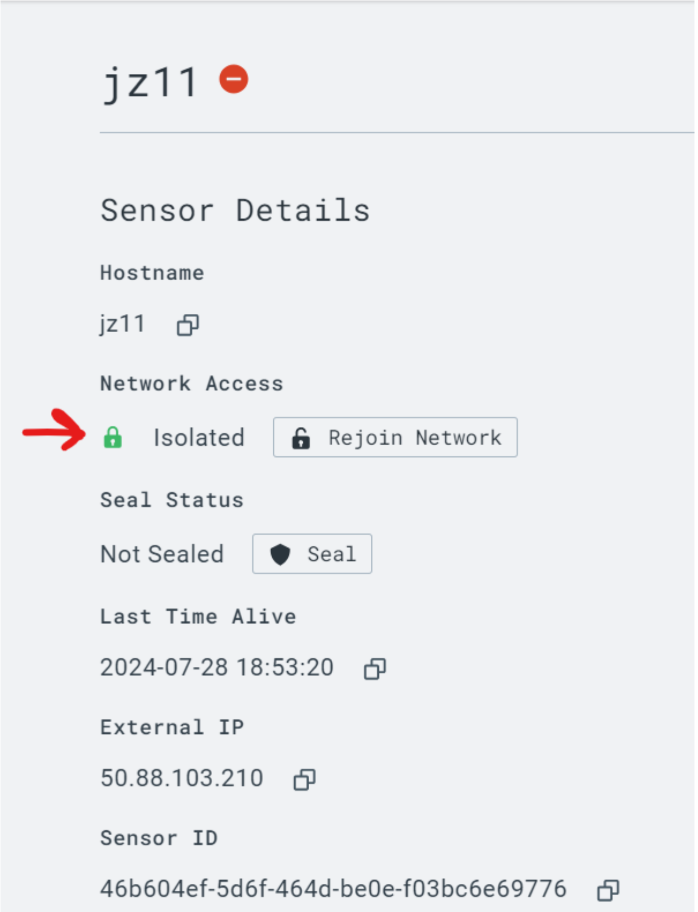
Do you want to isolate this computer?

I proceeded in clicking “Yes” first to see if I receive an isolation message on Slack. When I went to Slack, I received an email saying that the computer was isolated, as expected.



Tines APP 1:13 PM
Isolation Status:
The computer: jz11
was isolated.

To further confirm if the computer was isolated. I went back to ***LimaCharlie > Sensors > Overview*** and, as seen below, the network access for the computer has been isolated.



jz11

Sensor Details

Hostname

jz11

Network Access

Isolated

Seal Status

Not Sealed

Last Time Alive

2024-07-28 18:53:20

External IP

50.88.103.210

Sensor ID

46b604ef-5d6f-464d-be0e-f03bc6e69776