**Kịch bản mã hoá file**

3.1.1 Mô tả các kịch bản ứng phó

3.1.1.1 Mã hoá file khi có hành vi gửi file

* Phát hiện hành vi gửi file của máy agent và thực hiện mã hoá file sau đưa ra cảnh báo với máy server

3.1.2 Cách thức xây dựng kịch bản ứng phó

3.1.2.5 Mã hoá file khi có hành vi gửi file

* Sử dụng proxy để chặn khi người dùng thực hiện gửi file
* Sau đó tiến hành sửa đổi nội dung gói tin bằng nội dung đã được mã hoá
* Cuối cùng tạo log để gửi cảnh báo lên server

if flow.request.method == "POST":

content\_type = flow.request.headers.get("Content-Type", "")

request\_body = flow.request.get\_text()

if is\_valid\_filename(content\_type, request\_body) :

filename = extract\_filename(request\_body)

old\_content = extract\_content(request\_body)

if filename != "blob" and check\_file\_format\_encode(filename):

matches = [m.start() for m in re.finditer(re.escape(extract\_content(request\_body)), request\_body)]

if len(matches) >= 2:

second\_occurrence\_index = matches[1]

request\_body= request\_body[:second\_occurrence\_index] + encode\_content(extract\_content(request\_body)) + request\_body[second\_occurrence\_index + len(request\_body):]

else:

request\_body = request\_body.replace(extract\_content(request\_body),encode\_content(extract\_content(request\_body)))

new\_content = extract\_content(request\_body)

flow.request.text = request\_body

log\_data = f'{{"url-log": "{flow.request.pretty\_host}",

"event\_type": "alert", "Method": "{flow.request.method}",

"Filename": "{filename}",

"Old\_content": "{old\_content}",

"New\_content": "{new\_content}"}}'

log\_data = json.loads(log\_data)

send\_syslog\_message(log\_data,syslog\_host,syslog\_port)

* Công nghệ sử dụng chính là mitmproxy để thực hiện chặn các gói tin http và sửa đổi nội dung gói tin

4. Thực nghiệm và đánh giá

4.1 Kịch bản thu thập hành vi gửi file từ máy người dùng

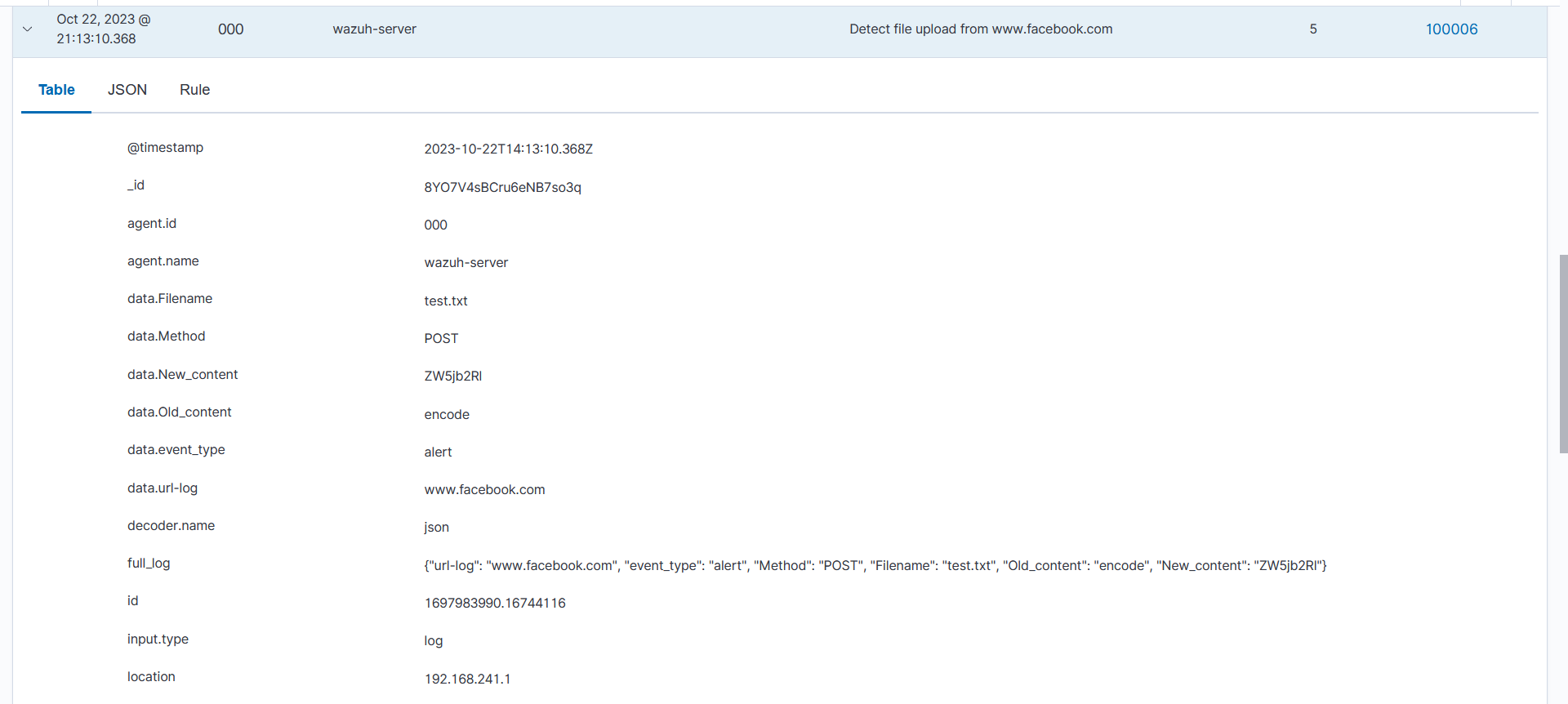
* Giả sử người dùng bị attacker chiếm quyền điều khiển máy tính, và thực hiện gửi các file quan trọng qua ứng dụng facebook.Bên máy agent sẽ thực hiện phát hiện hành vi này mã hoá các file attacker gửi và thông báo lên server

4.2 Kịch bản phát hiện gửi file của người dùng

* Khi attacker thực hiện gửi file trên ứng dụng facebook phía máy agent sẽ ngay lập tức tạo một log khi lại hành vi gửi file này sau đó gửi lên máy server với rule như sau



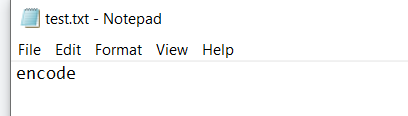
* Khi hành vi gửi file được thực hiện, bên máy server sẽ nhận được thông báo



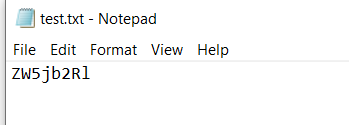
* Ở phần full\_log ta nhận được thông tin bao gồm vị trí mà attacker gửi file, tên file gửi, nội dung trước và sau khi thực hiện mã hoá

4.3 Kịch bản ứng phó

* Khi thực hiện gửi log về việc gửi file từ máy agent lên server, thì máy agent cũng sẽ đồng thời tự động mã hoá file
* Giả sử phía agent attacker gửi một file txt có nội dung như sau



* Lúc này trong quá trình gửi, nội dung của gói tin upload file đã được thay đổi, và khi gửi xong nội dung sẽ bị mã hoá như sau



* Đối với trường hợp attacker gửi các file docx hay pdf thì sau khi nội dung file bị mã hoá sẽ dẫn tới việc file sau khi gửi sẽ không thể truy cập vào được

**Kịch bản ngắt kết nối mạng(IP)**

1. Mô tả

* Agent thực hiện các hành động truy cập đến các địa chỉ IP gây hại hoặc các kết nối C2C

1. Cách thức xây dựng kịch bản ứng phó

* Trước tiên, thực hiện cấu hình rule sao cho phát hiện được việc sử dụng các câu lệnh kết nối tới địa chỉ IP bên ngoài từ máy agent hoặc máy agent tự động kết nối tới một địa chỉ ip nằm trong blacklist và gửi lên wazuh server
* Sau đó wazuh server sẽ thực hiện gửi yêu cầu về phía máy agent và thực hiện đoạn code sau
* Đây là đoạn code giả sử cho việc sử dụng rule firewall để tiến hành kiểm soát tới địa chỉ ip gây nguy hiểm cụ thể là 172.31.245.42

inbound\_args = [

"netsh", "advfirewall", "firewall", "add", "rule", "name=MyRuleInbound",

"dir=in", "action=block", "enable=yes", "remoteip=172.31.245.42/32"

]

subprocess.run(inbound\_args, shell=True)

outbound\_args = [

"netsh", "advfirewall", "firewall", "add", "rule", "name=MyRuleOutbound",

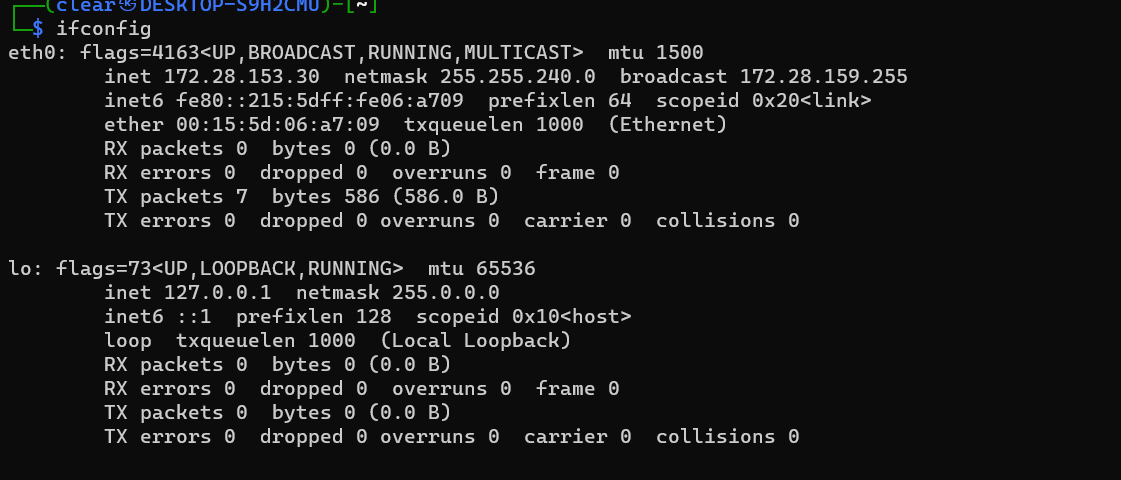
"dir=out", "action=block", "enable=yes", "remoteip=172.31.245.42/32"

]

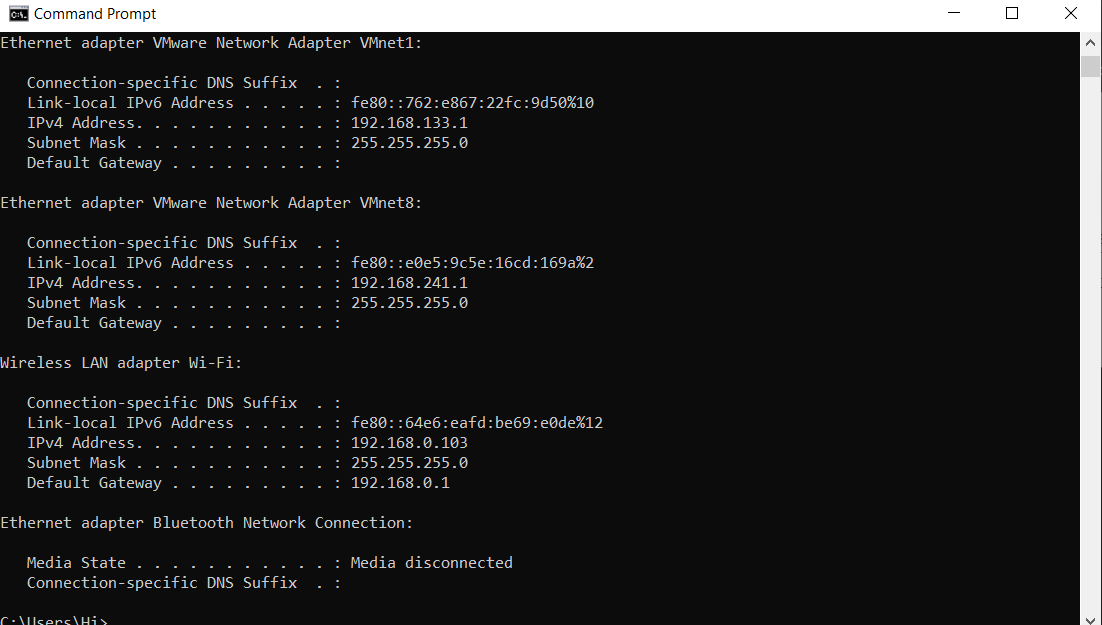
subprocess.run(outbound\_args, shell=True)

1. Demo

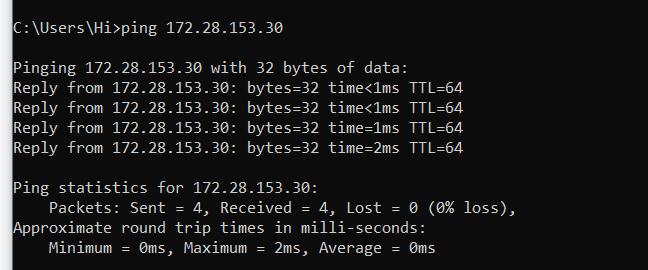
* Giả sử ta có một máy kali làm máy kẻ tấn công sử dụng để tiến hành kết nối tới máy agent có địa chỉ ip như sau



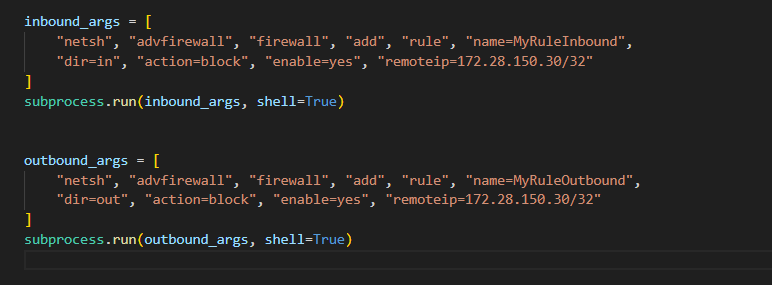
* Địa chỉ Ip của máy agent như sau



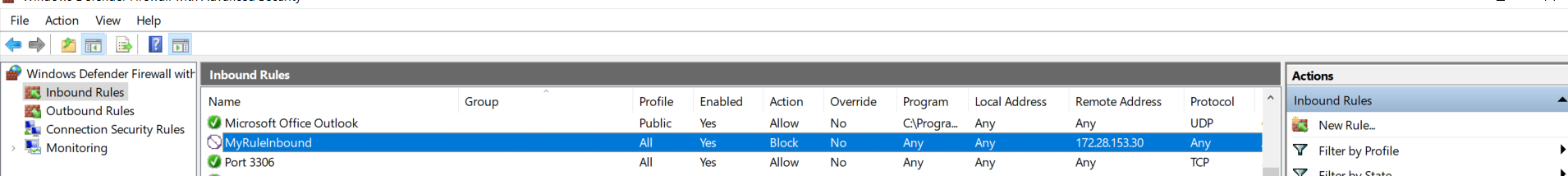
* Thử ping để kiểm tra kết nối mạng giữa 2 máy này

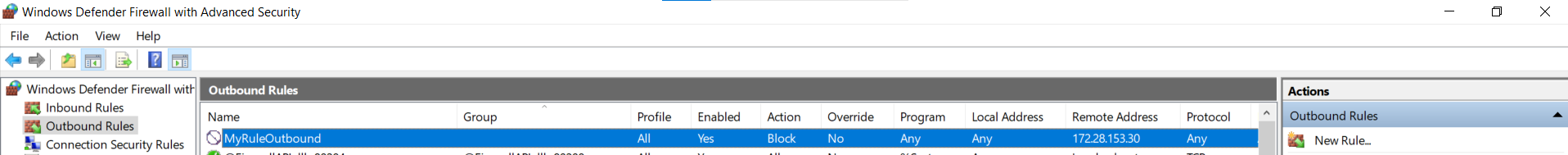


* Giả sử khi kẻ tấn công thực hiện hành vi kết nối mạng từ agent đến địa chỉ ip của máy attacker sau đó thông báo sẽ được hiện lên wazuh server => wazuh server thực hiện yêu cầu máy agent thực hiện cấu hình rule firewall để thực hiện ngăn cản kết nối này thông qua đoạn code

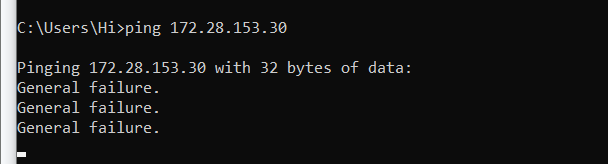


* Sau khi thực hiện kiểm tra cấu hình firewall xem đã thành công chưa





* Rule đã được kích hoạt thành công, ta tiến hành ping lại đến địa chỉ ip của máy attacker

****

**Kịch bản phục hồi thanh ghi**

1. Mô tả

* Máy agent có sự thay đổi trong các thanh ghi khởi động
* Ví dụ: một giá trị đã được thêm vào registry

1. Cách thức xây dựng kịch bản ứng phó

* Ngay khi có sự thay đổi trong các thanh ghi khởi động => wauzh server sẽ nhận được alert về sự thay đổi này của máy agent thông qua rule như sau

<rule id="100000" level="10">

<mitre>

<id>T1547.001</id>

</mitre>

<description>CurrentVersion Autorun Keys Modification</description>

<if\_group>sysmon\_eid13\_detections</if\_group>

<field name="win.eventdata.targetObject" negate="no" type="pcre2">(?i)(\\\\SOFTWARE\\\\Microsoft\\\\Windows\\\\CurrentVersion)</field>

<field name="win.eventdata.targetObject" negate="no" type="pcre2">(?i)(\\\\ShellServiceObjectDelayLoad|\\\\Run\\\\|\\\\RunOnce\\\\|\\\\RunOnceEx\\\\|\\\\RunServices\\\\|\\\\RunServicesOnce\\\\|\\\\Policies\\\\System\\\\Shell|\\\\Policies\\\\Explorer\\\\Run|\\\\Group\ Policy\\\\Scripts\\\\Startup|\\\\Group\ Policy\\\\Scripts\\\\Shutdown|\\\\Group\ Policy\\\\Scripts\\\\Logon|\\\\Group\ Policy\\\\Scripts\\\\Logoff|\\\\Explorer\\\\ShellServiceObjects|\\\\Explorer\\\\ShellIconOverlayIdentifiers|\\\\Explorer\\\\ShellExecuteHooks|\\\\Explorer\\\\SharedTaskScheduler|\\\\Explorer\\\\Browser\ Helper\ Objects|\\\\Authentication\\\\PLAP\ Providers|\\\\Authentication\\\\Credential\ Providers|\\\\Authentication\\\\Credential\ Provider\ Filters)</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:\(Empty\))$</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(?:\\\\NgcFirst\\\\ConsecutiveSwitchCount)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)(?:\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\Update\\\\OneDriveSetup\.exe)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)(?:\\\\AppData\\\\Roaming\\\\Spotify\\\\Spotify\.exe)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)(?:\\\\AppData\\\\Local\\\\WebEx\\\\WebexHost\.exe)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\WINDOWS\\\\system32\\\\devicecensus\.exe)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Windows\\\\system32\\\\winsat\.exe)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\\\\Microsoft\ OneDrive\\\\StandaloneUpdater\\\\OneDriveSetup\.exe)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\\\\Microsoft\ OneDrive\\\\Update\\\\OneDriveSetup\.exe)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\ \(x86\)\\\\Microsoft\ OneDrive\\\\Update\\\\OneDriveSetup\.exe)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\\\\KeePass\ Password\ Safe\ 2\\\\ShInstUtil\.exe)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\\\\Everything\\\\Everything\.exe)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\ \(x86\)\\\\Microsoft\ Office\\\\root\\\\integration\\\\integrator\.exe)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Windows\\\\system32\\\\LogonUI\.exe)$</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(\\\\Authentication\\\\Credential\ Providers\\\\\{D6886603\-9D2F\-4EB2\-B667\-1971041FA96B\}\\\\)</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(\\\\Authentication\\\\Credential\ Providers\\\\\{BEC09223\-B018\-416D\-A0AC\-523971B639F5\}\\\\)</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(\\\\Authentication\\\\Credential\ Providers\\\\\{8AF662BF\-65A0\-4D0A\-A540\-A338A999D36F\}\\\\)</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(\\\\Authentication\\\\Credential\ Providers\\\\\{27FBDB57\-B613\-4AF2\-9D7E\-4FA7A66C21AD\}\\\\)</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\ \(x86\)\\\\Microsoft\\\\EdgeUpdate\\\\Install\\\\)</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\ \(x86\)\\\\Microsoft\\\\EdgeWebView\\\\)</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\ \(x86\)\\\\Microsoft\\\\Edge\\\\Application\\\\msedge\.exe)</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Windows\\\\system32\\\\regsvr32\.exe)$</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(DropboxExt)</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)(?:A251\-47B7\-93E1\-CDD82E34AF8B\})$</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(?:\\\\SOFTWARE\\\\Microsoft\\\\Windows\\\\CurrentVersion\\\\Run\\\\Opera\ Browser\ Assistant)$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\\\\Opera\\\\assistant\\\\browser\_assistant\.exe)$</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(?:\\\\SOFTWARE\\\\Microsoft\\\\Windows\\\\CurrentVersion\\\\Run\\\\iTunesHelper)$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:"C:\\\\Program\ Files\\\\iTunes\\\\iTunesHelper\.exe")$</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(?:\\\\SOFTWARE\\\\Microsoft\\\\Windows\\\\CurrentVersion\\\\RunOnce\\\\zoommsirepair)$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:"C:\\\\Program\ Files\\\\Zoom\\\\bin\\\\installer\.exe"\ \/repair)$</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(?:\\\\SOFTWARE\\\\Microsoft\\\\Windows\\\\CurrentVersion\\\\Run\\\\Greenshot)$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\\\\Greenshot\\\\Greenshot\.exe)$</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(?:\\\\Software\\\\Microsoft\\\\Windows\\\\CurrentVersion\\\\Run\\\\GoogleDriveFS)$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\\\\Google\\\\Drive\ File\ Stream\\\\)</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)(\\\\GoogleDriveFS\.exe)</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(GoogleDrive)</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:\{CFE8B367\-77A7\-41D7\-9C90\-75D16D7DC6B6\})$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:\{A8E52322\-8734\-481D\-A7E2\-27B309EF8D56\})$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:\{C973DA94\-CBDF\-4E77\-81D1\-E5B794FBD146\})$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:\{51EF1569\-67EE\-4AD6\-9646\-E726C3FFC8A2\})$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:C:\\\\Windows\\\\system32\\\\cmd\.exe\ \/q\ \/c\ rmdir\ \/s\ \/q\ "C:\\\\Users\\\\)</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:C:\\\\Windows\\\\system32\\\\cmd\.exe\ \/q\ \/c\ del\ \/q\ "C:\\\\Users\\\\)</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)(\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\)</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(\\\\Microsoft\\\\Windows\\\\CurrentVersion\\\\RunOnce\\\\\{)</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)(\\\\AppData\\\\Local\\\\Package\ Cache\\\\\{)</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)(\}\\\\python\-)</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)(?:\.exe"\ \/burn\.runonce)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\\\\Common\ Files\\\\Microsoft\ Shared\\\\ClickToRun\\\\)</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\\\\Common\ Files\\\\Microsoft\ Shared\\\\ClickToRun\\\\Updates\\\\)</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)(?:\\\\OfficeClickToRun\.exe)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\\\\Windows\ Defender\\\\MsMpEng\.exe)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)(?:\\\\Microsoft\\\\Teams\\\\current\\\\Teams\.exe)$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)(\\\\Microsoft\\\\Teams\\\\Update\.exe\ \-\-processStart\ )</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Windows\\\\system32\\\\userinit\.exe)$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:ctfmon\.exe\ \/n)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\\\\AVG\\\\Antivirus\\\\Setup\\\\)</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:"C:\\\\Program\ Files\\\\AVG\\\\Antivirus\\\\AvLaunch\.exe"\ \/gui)$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:"C:\\\\Program\ Files\ \(x86\)\\\\AVG\\\\Antivirus\\\\AvLaunch\.exe"\ \/gui)$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:\{472083B0\-C522\-11CF\-8763\-00608CC02F24\})$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)(?:\\\\aurora\-agent\-64\.exe)$</field>

<field name="win.eventdata.image" negate="yes" type="pcre2">(?i)(?:\\\\aurora\-agent\.exe)$</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(?:\\\\Microsoft\\\\Windows\\\\CurrentVersion\\\\Run\\\\aurora\-dashboard)$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)^(?:C:\\\\Program\ Files\\\\Aurora\-Agent\\\\tools\\\\aurora\-dashboard\.exe)$</field>

<field name="win.eventdata.targetObject" negate="yes" type="pcre2">(?i)(?:\\\\Microsoft\\\\Windows\\\\CurrentVersion\\\\Run\\\\Everything)$</field>

<field name="win.eventdata.details" negate="yes" type="pcre2">(?i)(?:\\\\Everything\\\\Everything\.exe"\ \-startup)$</field>

</rule>

* Sau đó wazuh server sẽ gửi thông báo tới máy agent yêu cầu việc xoá các thanh ghi này thông qua đoạn code như sau

def delete\_registry\_value(registry\_path, value\_name):

try:

registry\_split = registry\_path.split("\\")

start\_path = registry\_split[0]

key\_path = "\\".join(registry\_split[1:])

if start\_path == "HKLM":

key = winreg.OpenKey(winreg.HKEY\_LOCAL\_MACHINE, key\_path, 0, winreg.KEY\_SET\_VALUE)

elif start\_path == "HKCU":

key = winreg.OpenKey(winreg.HKEY\_CURRENT\_USER, key\_path, 0, winreg.KEY\_SET\_VALUE)

elif start\_path == "HKCR":

key = winreg.OpenKey(winreg.HKEY\_CLASSES\_ROOT, key\_path, 0, winreg.KEY\_SET\_VALUE)

elif start\_path == "HKU":

key = winreg.OpenKey(winreg.HKEY\_USERS, key\_path, 0, winreg.KEY\_SET\_VALUE)

elif start\_path == "HKCC":

key = winreg.OpenKey(winreg.HKEY\_CURRENT\_CONFIG, key\_path, 0, winreg.KEY\_SET\_VALUE)

else:

raise ValueError("Invalid start path")

try:

winreg.DeleteValue(key, value\_name)

print(f"Registry value '{value\_name}' deleted successfully.")

except FileNotFoundError:

print(f"Registry value '{value\_name}' not found.")

except Exception as e:

print(f"Failed to delete registry value: {e}")

# Đóng Registry key

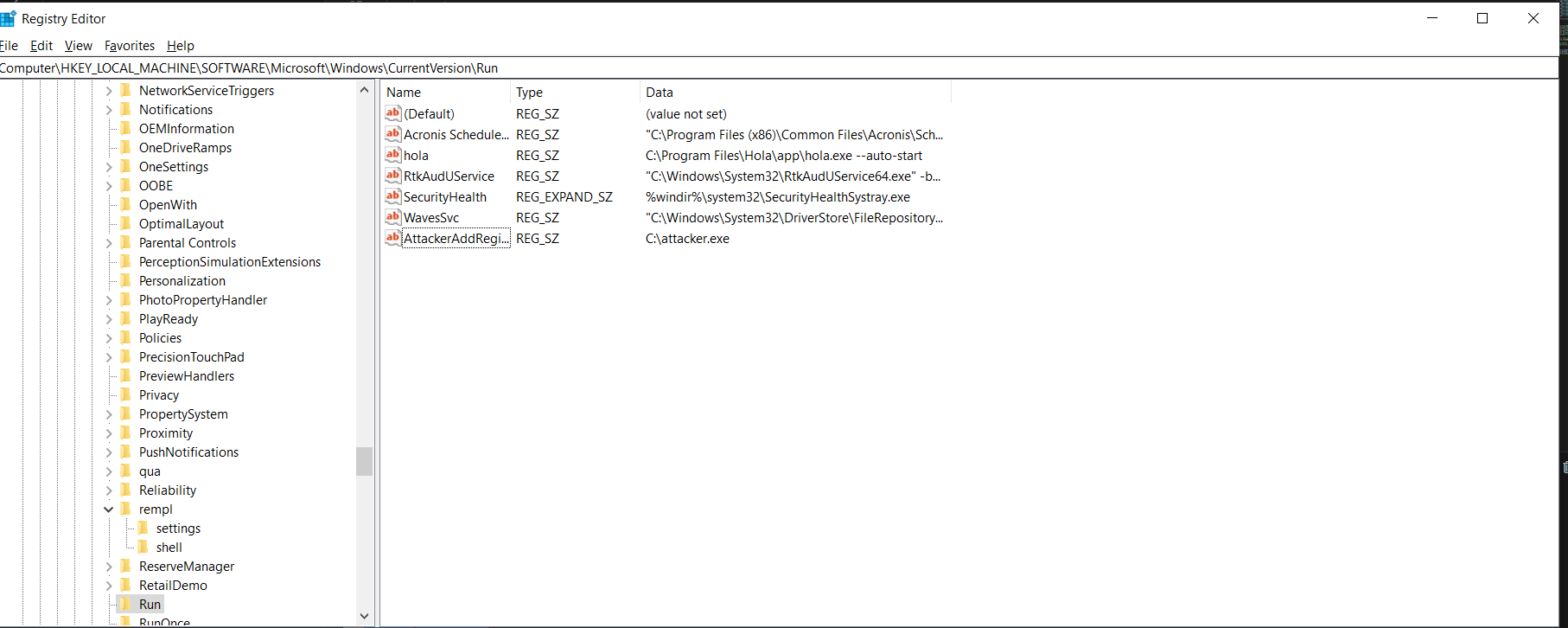
winreg.CloseKey(key)

except Exception as e:

print(f"Error: {e}")

1. Demo

* Giả sử sau khi chiếm quyền điều khiển máy agent, attacker sẽ sử dụng dòng lệnh hoặc trực tiếp tạo một giá trị tại thanh ghi khởi động



* Attacker đã thêm giá trị AttackerAddRegistry với nội dung là C:/attacker.exe vào registry của hệ thống máy agent
* Khi có phát hiện về việc sửa đổi giá trị thanh ghi khởi động, hệ thống sẽ đưa ra phản hồi xuống agent để thực hiện chức năng xóa giá trị thanh ghi vi phạm thông qua đoạn code

def delete\_registry\_value(registry\_path, value\_name):

try:

registry\_split = registry\_path.split("\\")

start\_path = registry\_split[0]

key\_path = "\\".join(registry\_split[1:])

if start\_path == "HKLM":

key = winreg.OpenKey(winreg.HKEY\_LOCAL\_MACHINE, key\_path, 0, winreg.KEY\_SET\_VALUE)

elif start\_path == "HKCU":

key = winreg.OpenKey(winreg.HKEY\_CURRENT\_USER, key\_path, 0, winreg.KEY\_SET\_VALUE)

elif start\_path == "HKCR":

key = winreg.OpenKey(winreg.HKEY\_CLASSES\_ROOT, key\_path, 0, winreg.KEY\_SET\_VALUE)

elif start\_path == "HKU":

key = winreg.OpenKey(winreg.HKEY\_USERS, key\_path, 0, winreg.KEY\_SET\_VALUE)

elif start\_path == "HKCC":

key = winreg.OpenKey(winreg.HKEY\_CURRENT\_CONFIG, key\_path, 0, winreg.KEY\_SET\_VALUE)

else:

raise ValueError("Invalid start path")

try:

winreg.DeleteValue(key, value\_name)

print(f"Registry value '{value\_name}' deleted successfully.")

except FileNotFoundError:

print(f"Registry value '{value\_name}' not found.")

except Exception as e:

print(f"Failed to delete registry value: {e}")

# Đóng Registry key

winreg.CloseKey(key)

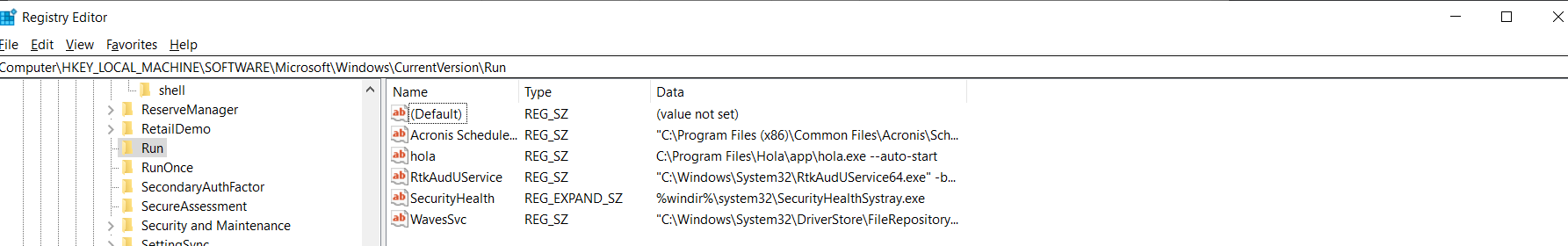
except Exception as e:

print(f"Error: {e}")

registry\_path\_to\_delete = "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run"

value\_name\_to\_delete = "AttackerAddRegistry"

delete\_registry\_value(registry\_path\_to\_delete, value\_name\_to\_delete)



* Giá trị registry attacker thêm đã bị xoá

**Kịch bản xóa file độc hại**

1. **Mô tả**

* Phát hiện file độc hại đang tồn tại trên máy agent và thực hiện hành động xóa file tránh gây thực thi và làm tổn hại hệ thống

1. **Cách thức xây dựng kịch bản ứng phó**

* Khi một file độc hại nằm trong blacklist mà ta cấu hình, wazuh server sẽ nhận được alert về việc tồn tại file malware trong hệ thông của ta
* Sau đó wazuh server sẽ thực hiện gửi yêu cầu xuống agent để xoá file độc hại này thông qua đoạn code sau

try:

os.remove(msg.alert["parameters"]["alert"]["syscheck"]["path"])

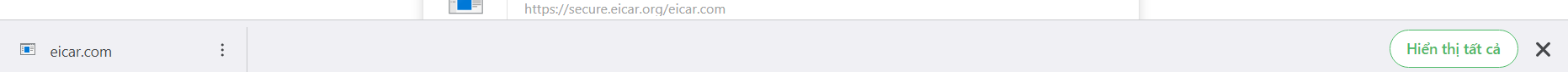
write\_debug\_file(argv[0], json.dumps(msg.alert) + " Successfully removed threat")

except OSError as error:

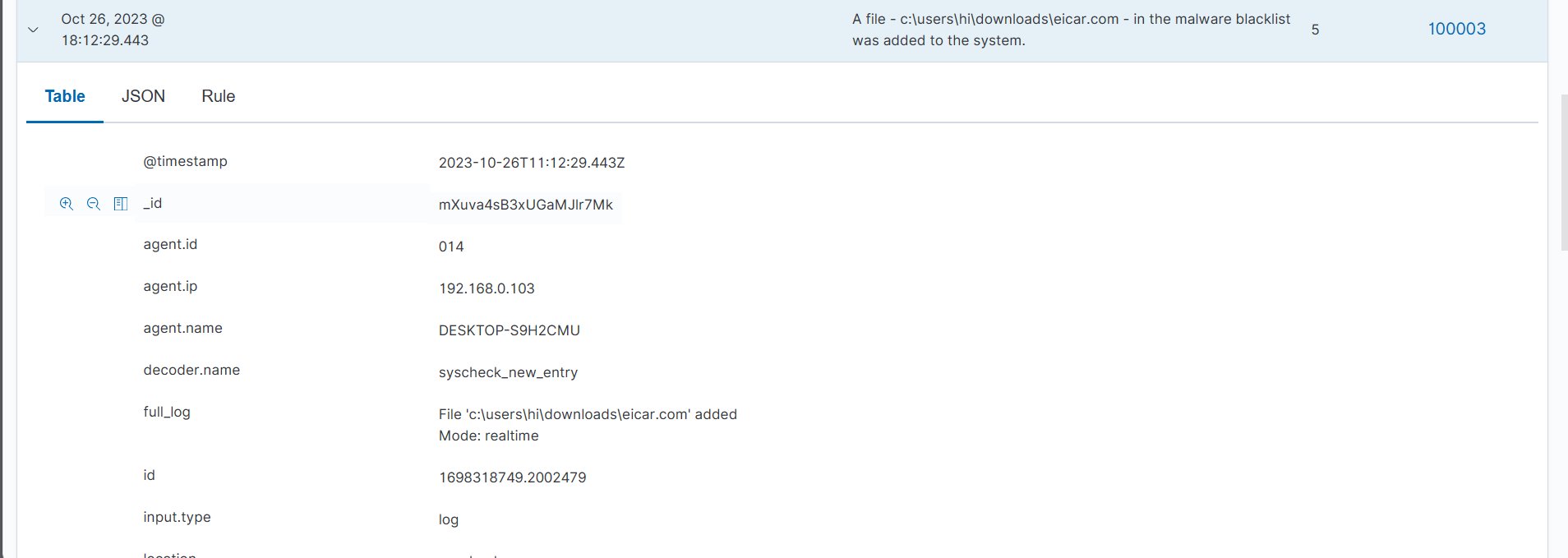
write\_debug\_file(argv[0], json.dumps(msg.alert) + "Error removing threat")

1. **Demo**

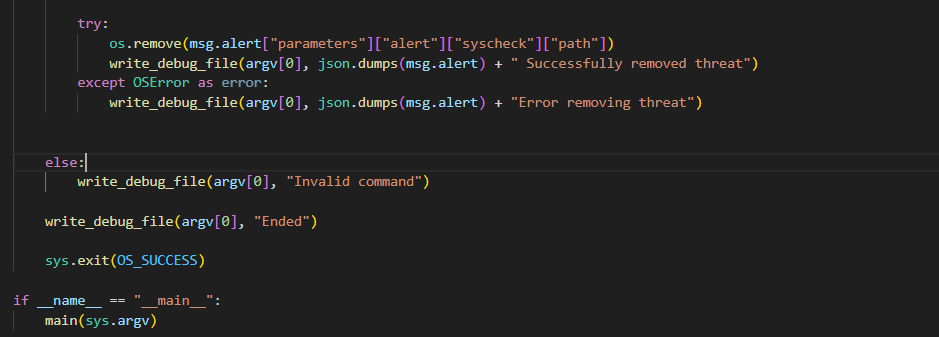
* Giả sử ta sẽ tiến hành dowload một file malware xuống máy agent

****

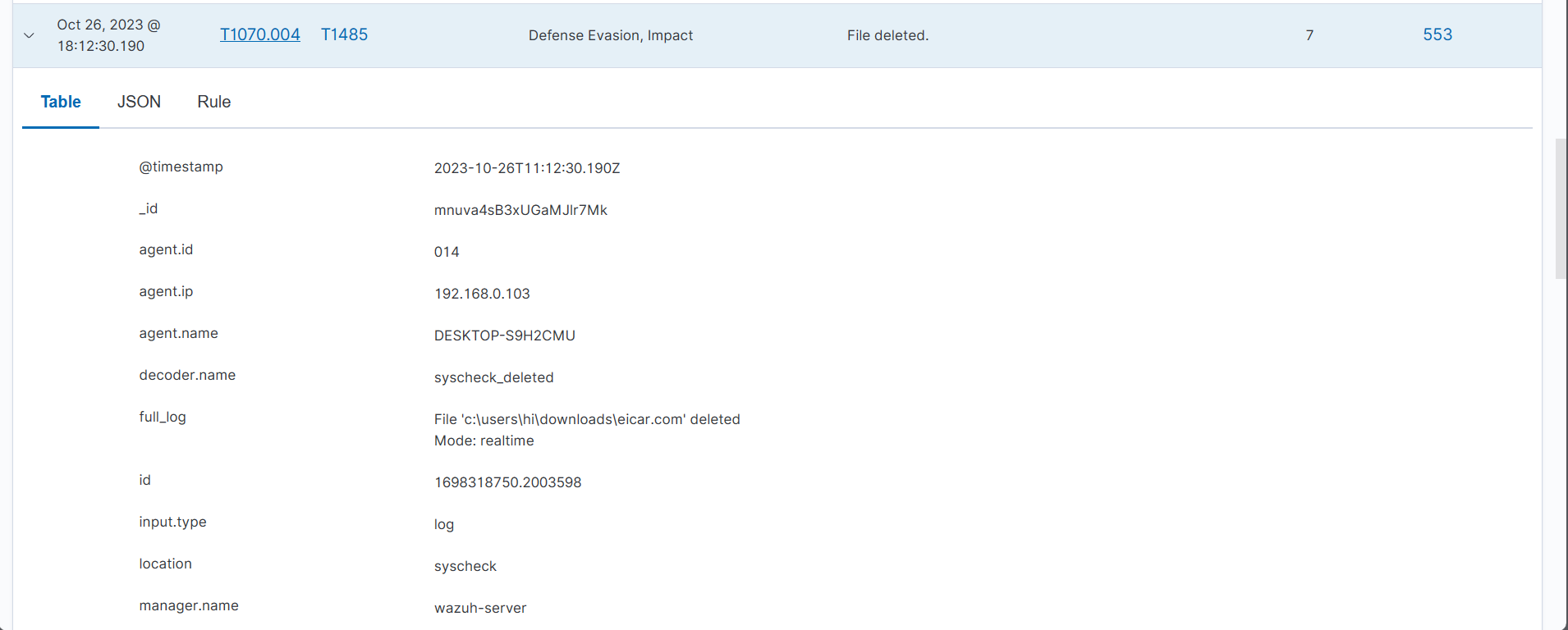
* Ngay sau đó wazuh server sẽ nhận được cảnh báo đây là một file nguy hiểm



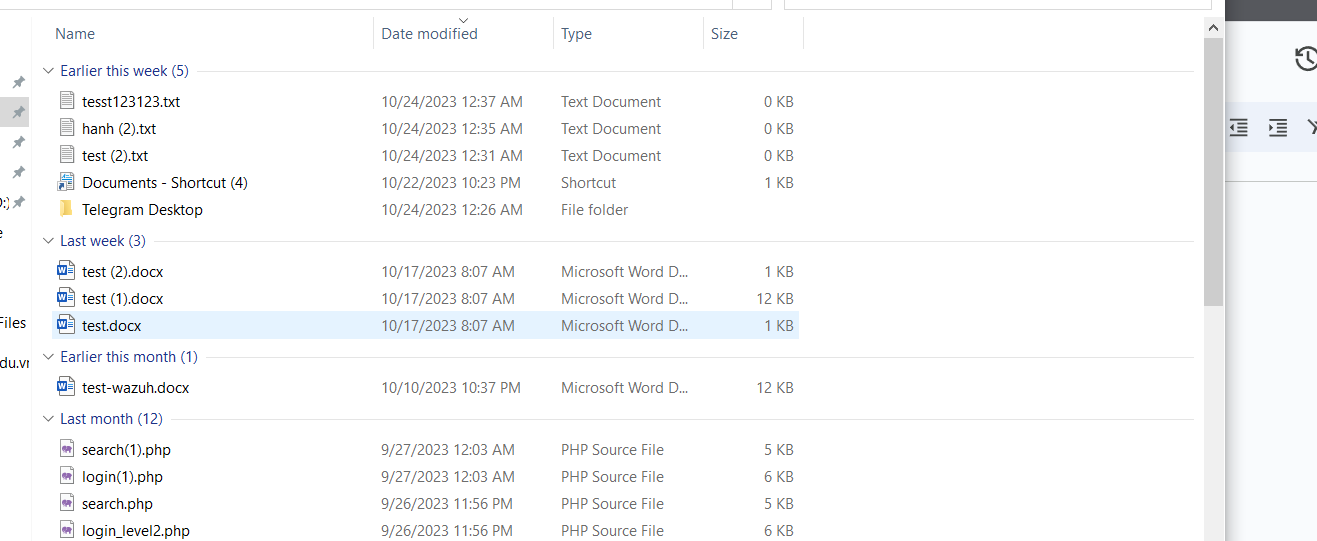
* Ngay lập tức wazuh server sẽ yêu cầu máy agent thực hiện xoá file này thông qua đoạn code

****

* Sau khi xoá xong sẽ đưa ra thông báo về việc đã xoá thành công



* Kiểm tra ta thấy file đã được xoá hoàn toàn



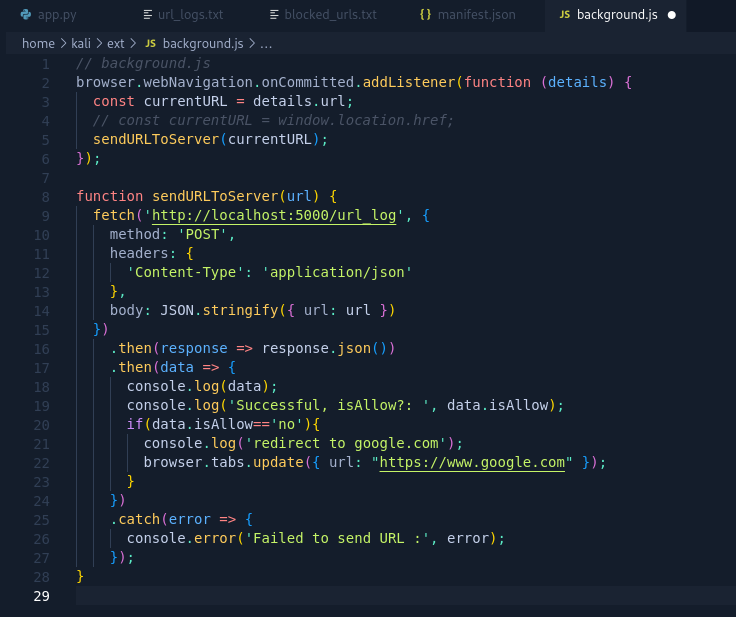
**Kịch bản ngăn chặn việc sử dụng các url trong blacklist của người dùng**

1. **Mô tả**

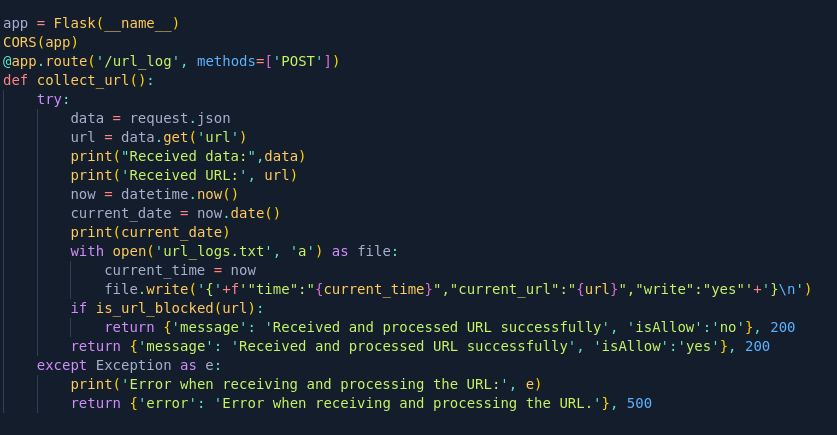
* Khi người dùng truy cập vào đường dẫn url nằm trong blacklist của hệ thống thì sẽ thực hiện chuyển hướng trang đó

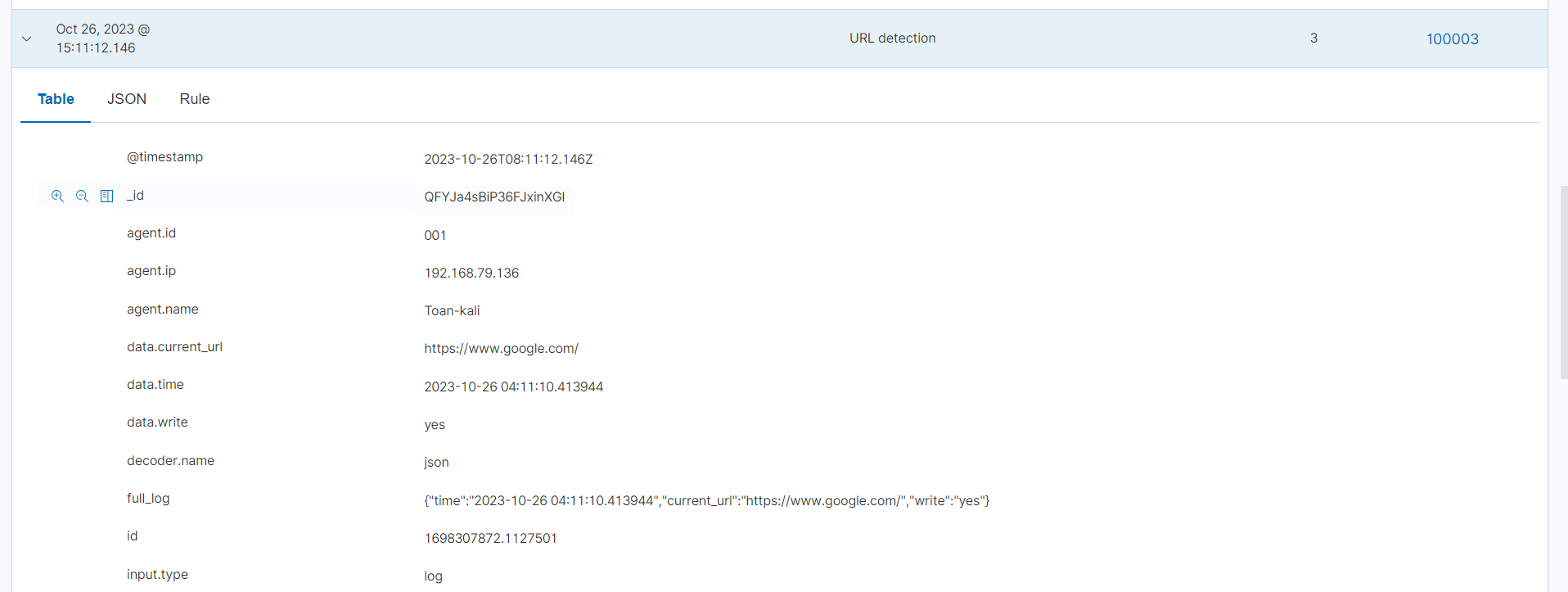
1. **Cách thức xây dựng kịch bản ứng phó**

* **Sử dụng extension để lắng nghe các sự kiện tải trang web**

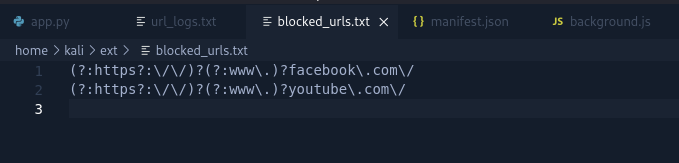


* Sau đó thu thập các url này vào trong file url\_logs.txt và được chuyển tới wazuh server về các hoạt động truy cập url của người dùng

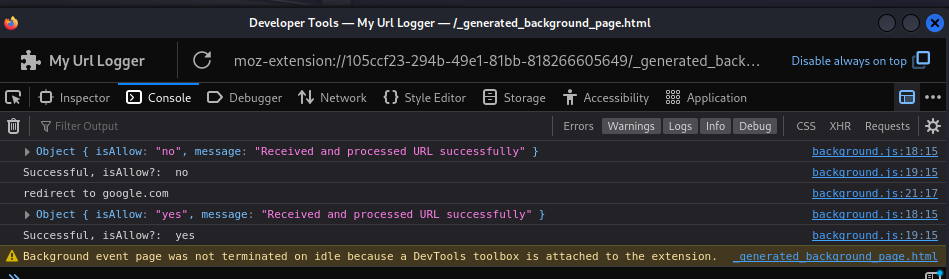




* Sau đó sử dụng 1 file làm blacklist để chứa thông tin các url bị cấm



* Nếu url không được phép truy cập extension tự chuyển hướng tab đó của người dùng tới một trang, vd google.com hoặc một trang rỗng, và in ra thông báo redirect trong Console.



Thông tin mẫu Malware (dựa trên virustotal):

- Tên malware: Bladabindi – njRAT

- MD5: 11b79281a25da1b798574f667c56898b

- SHA-1: 5a2ad92a0413ed15914ee2e38f4a4ab678deb90e

- SHA-256: c959b4ce89d2907e1dbc239d612396d4f63d8bb6b80bc0bfdde6ab80359cdbcf

- Loại tệp: PE32 executable (GUI) Intel 80386, for MS Windows.

Thông tin ghi lại trên Mitre ATT&CK:

| Execution | T1106 | Native API |
| --- | --- | --- |
| Persistence/Privilege Escalation | T1547.001 | Registry Run Keys / Startup Folder |
| Defense Evasion | T1027 | Obfuscated Files or Information |
| Defense Evasion | T1027.002 | Software Packing |
| Defense Evasion | T1036 | Masquerading |
| Defense Evasion | T1140 | Deobfuscate/Decode Files or Information |
| Defense Evasion | T1222 | File and Directory Permissions Modification |
| Defense Evasion/Discovery | T1497 | Virtualization/Sandbox Evasion |
| Defense Evasion | T1562.001 | Disable or Modify Tools |
| Defense Evasion | T1620 | Reflective Code Loading |
| Credential Access/Collection | T1056 | Input Capture |
| Credential Access/ Collection | T1056.001 | Keylogging |
| Discovery | T1010 | Application Window Discovery |
| Discovery | T1012 | Query Registry |
| Discovery | T1018 | Remote System Discovery |
| Discovery | T1033 | System Owner/User Discovery |
| Discovery | T1057 | Process Discovery |
| Discovery | T1082 | System Information Discovery |
| Discovery | T1083 | File and Directory Discovery |
| Discovery | T1087 | Account Discovery |
| Discovery | T1518 | Software Discovery |
| Discovery | T1518.001 | Security Software Discovery |
| Discovery | T1614 | System Location Discovery |
| Discovery | T1614.001 | System Language Discovery |
| Collection | T1113 | Screen Capture |
| Collection | T1560 | Archive Collected Data |
| Collection | T1560.002 | Archive via Library |
| Command and Control | T1071 | Application Layer Protocol |
| Command and Control | T1071.001 | Web Protocols |
| Command and Control | T1095 | Non-Application Layer Protocol |