## 檢測可疑二進制文件

Wazuh 具有異常和惡意軟件檢測功能，可在端點上檢測可疑的二進制文件。二進制文件是用於執行自動任務的可執行代碼。惡意攻擊者主要使用它們來進行利用，以避免被檢測。

在這個用例中，我們演示了 Wazuh rootcheck 模塊如何在 Ubuntu 端點上檢測特洛伊木馬系統二進制文件。您可以通過將合法二進制文件的內容替換為惡意代碼來進行演示，以欺騙端點將其認為是合法的二進制文件並運行它。

Wazuh rootcheck 模塊還檢查隱藏的進程、端口和文件。

## 基礎設施

### 端點

描述

Ubuntu 22.04

Wazuh rootcheck 模塊會檢測此端點上的可疑二進制文件的執行。

## 配置

在 Ubuntu 端點上執行以下步驟，啟用 Wazuh rootcheck 模塊並進行異常和惡意軟件檢測。

Wazuh rootcheck 模塊在 Wazuh 代理配置文件中默認是啟用的。檢查受監視端點的 /var/ossec/etc/ossec.conf 配置文件中的 <rootcheck> 塊，確保它具有以下配置：

```
<rootcheck>
  <disabled>no</disabled>
  <check_files>yes</check_files>

  <!-- 用於特洛伊木馬檢測的行 -->
  <check_trojans>yes</check_trojans>

  <check_dev>yes</check_dev>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>
  <check_ports>yes</check_ports>
  <check_if>yes</check_if>

  <!-- rootcheck 執行的頻率 - 每 12 小時 -->
  <frequency>43200</frequency>
  <rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>
  <skip_nfs>yes</skip_nfs>
</rootcheck>
```

rootcheck 部分解釋了 rootcheck 模塊中的選項。

## 攻擊模擬

創建原始系統二進制文件的副本：

sudo cp -p /usr/bin/w /usr/bin/w.copy

用以下 shell 腳本替換原始系統二進制文件 /usr/bin/w：
sudo tee /usr/bin/w << EOF
#!/bin/bash
echo "`date` this is evil" > /tmp/trojan_created_file
echo 'test for /usr/bin/w trojaned file' >> /tmp/trojan_created_file
Now running original binary
/usr/bin/w.copy
EOF

rootcheck 掃描默認每 12 小時運行一次。強制運行掃描，重啟 Wazuh 代理以查看相關警報：
sudo systemctl restart wazuh-agent

警報視覺化
您可以在 Wazuh 儀表板中查看警報數據。為此，轉到安全事件模塊並在搜索欄中添加過濾器以查詢警報：

location:rootcheck AND rule.id:510 AND data.title:Trojaned version of file detected.

此外，使用「按類型篩選」搜索欄，應用 full_log 篩選器。