센티넬원 리포트

# 기간 : 2023-06-01 ~ 2023-11-21

# scope : Wonik>0-머트리얼즈>01.서버

## 1. OS별 엔드포인트

|  |  |
| --- | --- |
| **OS 유형** | **엔드포인트 수량** |
| windows | 54 |
| linux | 11 |

## 2. 버전별 엔드포인트

|  |  |
| --- | --- |
| **에이전트 버전** | **엔드포인트 수량** |
| 22.3.5.887 | 52 |
| 22.2.4.558 | 1 |
| 22.1.2.7 | 9 |
| 22.3.3.11 | 1 |
| 22.4.2.4 | 1 |
| 22.1.4.10010 | 1 |

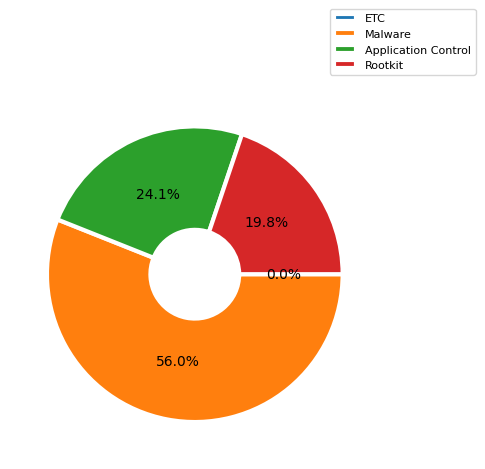
## 3. 보호되고 있는 엔드포인트

|  |  |
| --- | --- |
| **감염여부** | **엔드포인트 수량** |
| Healthy | 65 |

## 4. 기간내 Top20 탐지 Endpoints

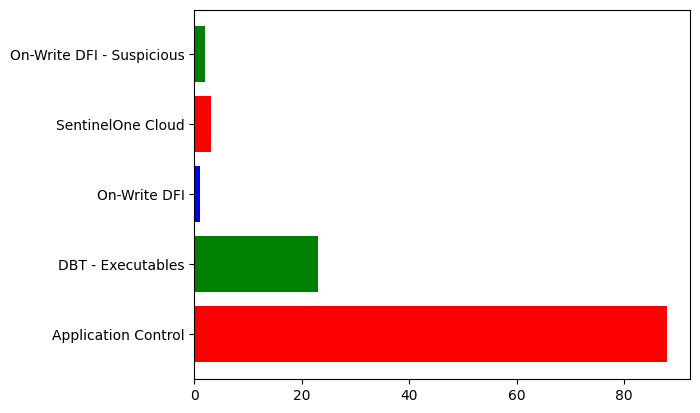
|  |  |  |
| --- | --- | --- |
| **No.** | **Endpoint** | **탐지건수** |
| 1 | anode0 | 111 |
| 2 | DESKTOP-66AOO53 | 2 |
| 3 | calling | 1 |
| 4 | ERP-APP | 1 |
| 5 | wics-pdf-viewer-svr | 1 |

## 5. 위협별 탐지



|  |  |
| --- | --- |
| **탐지내역** | **탐지수** |
| etc() | 0 |
| Malware | 65 |
| Application Control | 28 |
| Rootkit | 23 |

## 6. 엔진별 탐지



|  |  |
| --- | --- |
| **엔진명** | **탐지수** |
| Application Control | 88 |
| DBT - Executables | 23 |
| On-Write DFI | 1 |
| SentinelOne Cloud | 3 |
| On-Write DFI - Suspicious | 2 |

## 7. 해결된 위협 정보

|  |  |
| --- | --- |
| **해결 상태** | **엔드포인트 수량** |
| mitigated | 1 |
| marked\_as\_benign | 3 |

## 8. 주요 탐지 내역 세부 사항

|  |  |
| --- | --- |
| 파일명 | ansyswbu.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | /home/apps/opt/ansys\_inc/v231/aisol/CommonFiles/linx64/ansyswbu.exe |
| Originator Process | sshd |
| 엔진 | Application Control |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Suspicious access to logon info  MITRE : Defense Evasion [T1070.002] Evasion Suspicious access to logon info  MITRE : Defense Evasion [T1070.002] |

|  |  |
| --- | --- |
| 파일명 | rpm |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | /home/apps/opt/ansys\_inc/v232/aisol/CommonFiles/linx64/rpm |
| Originator Process | None |
| 엔진 | Application Control |
| 탐지 횟수 | 2회 |
| 구조/행위분석 |  |

|  |  |
| --- | --- |
| 파일명 | h\_2ms |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | /home/users/gichan/Desktop/Working/vent/h\_2ms |
| Originator Process | systemd |
| 엔진 | Application Control |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Suspicious access to logon info  MITRE : Defense Evasion [T1070.002] Evasion Suspicious access to logon info  MITRE : Defense Evasion [T1070.002] |

|  |  |
| --- | --- |
| 파일명 | ansyslmd |
| 분류 | Application Control |
| 조치여부 | not\_mitigated |
| 탐지경로 | /home/apps/opt/ansys\_inc/shared\_files/licensing/linx64/ansyslmd |
| Originator Process | systemd |
| 엔진 | Application Control |
| 탐지 횟수 | 2회 |
| 구조/행위분석 |  |

|  |  |
| --- | --- |
| 파일명 | insmod |
| 분류 | Rootkit |
| 조치여부 | not\_mitigated |
| 탐지경로 | /dkCAE/devicemapper/mnt/f88e311bebdf700b20070b5b632bc5c1c94eb895a65ffc8d8fa34bcb9aa0094d/rootfssbin/insmod |
| Originator Process | systemd |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Persistence Unsigned kernel module was loaded  MITRE : Persistence [T1547.006] MITRE : Defense Evasion [T1014] Persistence Unsigned kernel module was loaded  MITRE : Persistence [T1547.006] MITRE : Defense Evasion [T1014] |

|  |  |
| --- | --- |
| 파일명 | xstartup |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | /home/users/gichan/.vnc/xstartup |
| Originator Process | sshd |
| 엔진 | Application Control |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Suspicious access to logon info  MITRE : Defense Evasion [T1070.002] Evasion Suspicious access to logon info  MITRE : Defense Evasion [T1070.002] |

|  |  |
| --- | --- |
| 파일명 | ansyscl |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | /home/apps/opt/ansys\_inc/v231/licensingclient/linx64/ansyscl |
| Originator Process | sshd |
| 엔진 | Application Control |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Suspicious access to logon info  MITRE : Defense Evasion [T1070.002] Evasion Suspicious access to logon info  MITRE : Defense Evasion [T1070.002] |

|  |  |
| --- | --- |
| 파일명 | QtWebEngineProcess |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | /home/apps/opt/ansys\_inc/v231/tp/qt/5.9.6/linx64/libexec/QtWebEngineProcess |
| Originator Process | sshd |
| 엔진 | Application Control |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Suspicious access to logon info  MITRE : Defense Evasion [T1070.002] |

|  |  |
| --- | --- |
| 파일명 | m3\_fw.mdt.dpkg-new |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | /usr/lib/firmware/ath11k/IPQ6018/hw1.0/m3\_fw.mdt.dpkg-new |
| Originator Process | dpkg |
| 엔진 | On-Write DFI |
| 탐지 횟수 | 1회 |
| 구조/행위분석 |  |

|  |  |
| --- | --- |
| 파일명 | cports-현재작동중인 port 알기.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume2\Users\Administrator\Desktop\cports-현재작동중인 port 알기.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] Packer A UPX packed process was detected  MITRE : Defense Evasion [T1027][T1480.001] General Detected by the Static Engine |

|  |  |
| --- | --- |
| 파일명 | LicensingSettingsUtilityLinux |
| 분류 | Application Control |
| 조치여부 | not\_mitigated |
| 탐지경로 | /home/apps/opt/ansys\_inc/v232/licensingclient/linx64/LicensingSettingsUtility/LicensingSettingsUtilityLinux |
| Originator Process | None |
| 엔진 | Application Control |
| 탐지 횟수 | 1회 |
| 구조/행위분석 |  |

|  |  |
| --- | --- |
| 파일명 | runwb2 |
| 분류 | Application Control |
| 조치여부 | not\_mitigated |
| 탐지경로 | /home/apps/opt/ansys\_inc/v232/Framework/bin/Linux64/runwb2 |
| Originator Process | None |
| 엔진 | Application Control |
| 탐지 횟수 | 1회 |
| 구조/행위분석 |  |