센티넬원 리포트

# 기간 : 2023-08-21 ~ 2023-11-21

# scope : [Partner] Comsys>Default site>pgyTest

## 1. OS별 엔드포인트

|  |  |
| --- | --- |
| **OS 유형** | **엔드포인트 수량** |

## 2. 버전별 엔드포인트

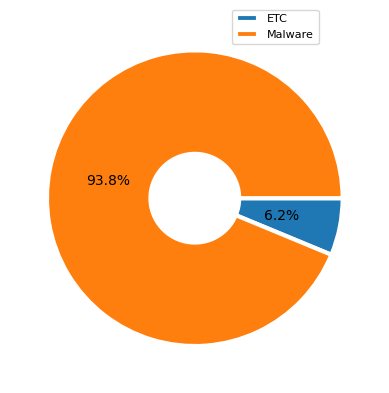
|  |  |
| --- | --- |
| **에이전트 버전** | **엔드포인트 수량** |

## 3. 보호되고 있는 엔드포인트

## 4. 기간내 Top20 탐지 Endpoints

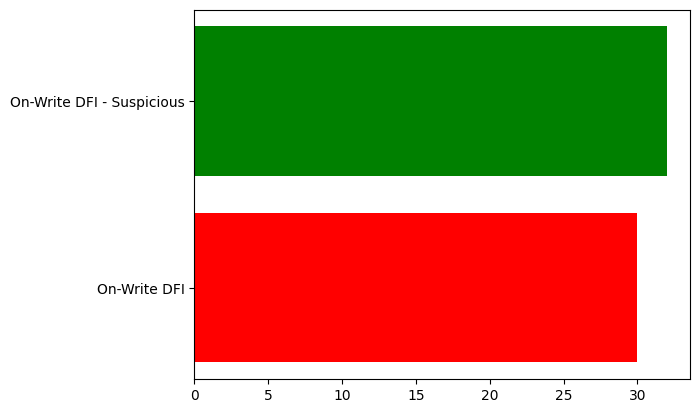
|  |  |  |
| --- | --- | --- |
| **No.** | **Endpoint** | **탐지건수** |
| 1 | PGYVM | 32 |

## 5. 위협별 탐지



|  |  |
| --- | --- |
| **탐지내역** | **탐지수** |
| etc(Trojan, Virus, ) | 2 |
| Malware | 30 |

## 6. 엔진별 탐지



|  |  |
| --- | --- |
| **엔진명** | **탐지수** |
| On-Write DFI | 30 |
| On-Write DFI - Suspicious | 32 |

## 7. 해결된 위협 정보

|  |  |
| --- | --- |
| **해결 상태** | **엔드포인트 수량** |
| mitigated | 30 |
| marked\_as\_benign | 0 |

## 8. 주요 탐지 내역 세부 사항

|  |  |
| --- | --- |
| 파일명 | e04b40547680e3f4c8cae491a2e77bf3e10c2d42805c103b67e2c06ab7a18735 |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\Gunyoung\Desktop\e04b40547680e3f4c8cae491a2e77bf3e10c2d42805c103b67e2c06ab7a18735 |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Abnormalities This binary contains abnormal section names which could be an indication that it was created with non-standard development tools  Abnormalities The Entry point for this binary has an uncommon section name  Abnormalities The Entry point for this binary is an RWX section. It might contain self-modifying code  Hiding/Stealthiness The majority of sections in this PE have high entropy, a sign of obfuscation or packing  Abnormalities This binary has an RWX section. It might contain self-modifying code  Abnormalities This binary uses non-standard DOS stubs  Abnormalities This binary has non-English version info  Hiding/Stealthiness This binary may contain encrypted or compressed data as measured by high entropy of the sections (greater than 6.8) |

|  |  |
| --- | --- |
| 파일명 | e09a8473566df9ff28ea70ad97ed63de6c71ce0725b7e8134d646660c9254323 |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\Gunyoung\Desktop\e09a8473566df9ff28ea70ad97ed63de6c71ce0725b7e8134d646660c9254323 |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Abnormalities The Entry point for this binary has an uncommon section name  Abnormalities This binary has an RWX section. It might contain self-modifying code  General This binary imports debugger functions |