센티넬원 리포트

# 기간 : 2023-08-21 ~ 2023-11-21

# scope : Wonik>0-머트리얼즈>Default Group

## 1. OS별 엔드포인트

|  |  |
| --- | --- |
| **OS 유형** | **엔드포인트 수량** |
| windows | 681 |
| linux | 1 |

## 2. 버전별 엔드포인트

|  |  |
| --- | --- |
| **에이전트 버전** | **엔드포인트 수량** |
| 22.3.5.887 | 489 |
| 22.2.4.558 | 47 |
| 22.3.4.612 | 20 |
| 4.6.12.241 | 2 |
| 4.0.3.53 | 13 |
| 21.7.5.1080 | 94 |
| 22.1.4.10010 | 15 |
| 22.1.2.217 | 1 |
| 22.1.2.7 | 1 |

## 3. 보호되고 있는 엔드포인트

|  |  |
| --- | --- |
| **감염여부** | **엔드포인트 수량** |
| Healthy | 660 |
| Infected | 22 |

## 4. 기간내 Top20 탐지 Endpoints

|  |  |  |
| --- | --- | --- |
| **No.** | **Endpoint** | **탐지건수** |
| 1 | C3H6분석 | 15 |
| 2 | 2210104WBA00687 | 12 |
| 3 | 2200701WBA00631 | 10 |
| 4 | 2200103WBB00464 | 7 |
| 5 | DESKTOP-VC1OEU0 | 7 |
| 6 | 2180802WBA00060 | 6 |
| 7 | 2211203WBA00570 | 6 |
| 8 | DESKTOP-R4NAJEK | 6 |
| 9 | DESKTOP-3D8S9UI | 6 |
| 10 | DESKTOP-V5U3VDE | 5 |
| 11 | DESKTOP-SA9VJNH | 5 |
| 12 | LIQIANKUN | 5 |
| 13 | PC-20190715CHXN | 4 |
| 14 | DESKTOP-17E4NS6 | 4 |
| 15 | DESKTOP-14G866U | 4 |
| 16 | 2170403WBA00735 | 4 |
| 17 | 2220107WBA00757 | 4 |
| 18 | DESKTOP-FL478JF | 4 |
| 19 | DESKTOP-HPB1FKH | 3 |
| 20 | DESKTOP-F3T4VNU | 3 |

## 7. 해결된 위협 정보

|  |  |
| --- | --- |
| **해결 상태** | **엔드포인트 수량** |
| mitigated | 203 |
| marked\_as\_benign | 3 |

## 8. 주요 탐지 내역 세부 사항

|  |  |
| --- | --- |
| 파일명 | StormPlayer.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume5\Program Files (x86)\Baofeng\StormPlayer\StormPlayer.exe |
| Originator Process | explorer.exe |
| 엔진 | Reputation |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Infostealer Chrome's private memory was accessed  MITRE : Credential Access [T1555.003] Infostealer Attempts to read sensitive information from LSASS  MITRE : Credential Access [T1003.001][T1555.004] MITRE : Initial Access [T1078] MITRE : Defense Evasion [T1078] MITRE : Persistence [T1078] MITRE : Privilege Escalation [T1078] General Detected by the Static Engine  Infostealer Blocked read access to LSASS  MITRE : Credential Access [T1003.001] MITRE : Initial Access [T1078] MITRE : Defense Evasion [T1078] MITRE : Persistence [T1078] MITRE : Privilege Escalation [T1078] Reconnaissance Suspicious WMI query was identified  MITRE : Execution [T1047] MITRE : Discovery [T1518.001] MITRE : Collection [T1119] MITRE : Defense Evasion [T1480.001] Persistence Application registered itself to become persistent via service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] Evasion Process tampered with Windows user interface  Direct Syscall Attempt to evade monitoring with a syscall directly from a remote allocation  MITRE : Defense Evasion [T1562.001] Injection Code injection to a remote process  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Anti-VM technique was used  MITRE : Defense Evasion  Evasion Anti-debug technique was used  MITRE : Defense Evasion  Discovery Identified attempt to access a raw volume  MITRE : Discovery [T1082] Evasion Application added firewall rules to allow network traffic  MITRE : Exfiltration [T1041][T1048][T1020][T1030][T1029] MITRE : Defense Evasion [T1562.004] Persistence A process registered a custom extension that spawns a suspicious executable  MITRE : Persistence [T1546.001][T1547.001] MITRE : Privilege Escalation [T1547.001][T1546.001] Persistence Application registered itself to become persistent via an autorun  MITRE : Persistence [T1547.001] MITRE : Privilege Escalation [T1547.001] Persistence Application registered itself to become persistent via COM object  MITRE : Persistence [T1546.015] MITRE : Privilege Escalation [T1546.015] Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Injection Suspicious library loaded into the process memory  Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | GnStart.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Geni\Genian\GnStart.exe |
| Originator Process | services.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Internal process resource was manipulated in memory  MITRE : Defense Evasion  Reconnaissance Suspicious WMI query was identified  MITRE : Execution [T1047] MITRE : Discovery [T1518.001] MITRE : Collection [T1119] MITRE : Defense Evasion [T1480.001] |