센티넬원 리포트

# 기간 : 2023-08-21 ~ 2023-11-21

# scope : Wonik>1-QnC>Default Group

## 1. OS별 엔드포인트

|  |  |
| --- | --- |
| **OS 유형** | **엔드포인트 수량** |
| windows | 874 |

## 2. 버전별 엔드포인트

|  |  |
| --- | --- |
| **에이전트 버전** | **엔드포인트 수량** |
| 22.3.2.373 | 121 |
| 23.2.3.358 | 444 |
| 22.2.4.558 | 84 |
| 22.1.4.10010 | 48 |
| 21.5.3.235 | 75 |
| 4.0.3.53 | 88 |
| 22.3.5.887 | 2 |
| 22.1.5.11025 | 1 |
| 21.7.2.1038 | 11 |

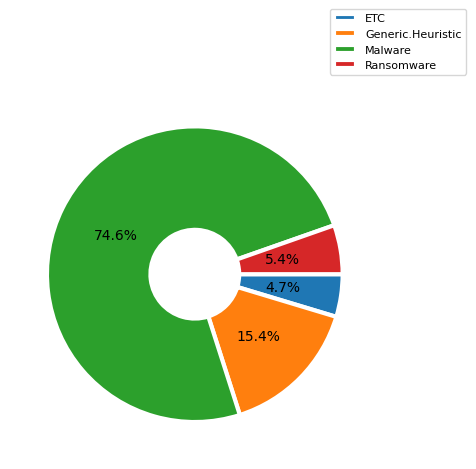
## 3. 보호되고 있는 엔드포인트

|  |  |
| --- | --- |
| **감염여부** | **엔드포인트 수량** |
| Healthy | 873 |
| Infected | 1 |

## 4. 기간내 Top20 탐지 Endpoints

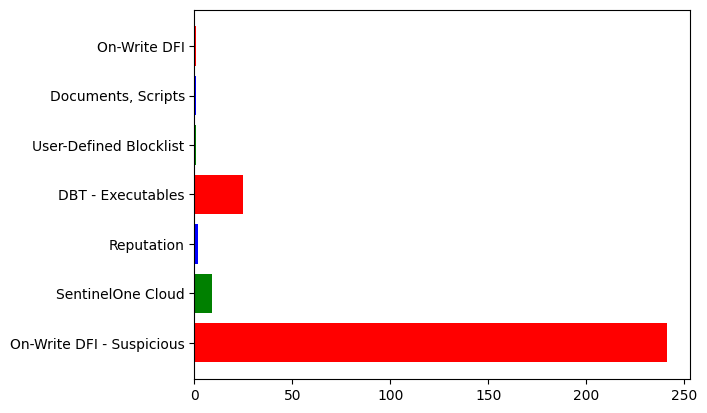
|  |  |  |
| --- | --- | --- |
| **No.** | **Endpoint** | **탐지건수** |
| 1 | ITN20-0083 | 112 |
| 2 | ITD17-00007 | 26 |
| 3 | ITD18-0018 | 15 |
| 4 | DESKTOP-OMIN4R5 | 15 |
| 5 | ITN23-0219 | 8 |
| 6 | ITN21-0132 | 7 |
| 7 | ITN23-0191 | 7 |
| 8 | ITN20-0052 | 6 |
| 9 | ITN23-0181 | 5 |
| 10 | ITN23-0210 | 5 |
| 11 | ITN21-0106 | 5 |
| 12 | ITN20-0146 | 4 |
| 13 | ITN23-0117 | 4 |
| 14 | user-PC | 3 |
| 15 | ITN23-B202 | 3 |
| 16 | ITN22-0020 | 2 |
| 17 | ITN22-0143 | 2 |
| 18 | ITN23-0167 | 2 |
| 19 | ITD22-B170 | 2 |
| 20 | ITN23-0188 | 2 |

## 5. 위협별 탐지



|  |  |
| --- | --- |
| **탐지내역** | **탐지수** |
| etc(Adware, Infostealer, PUA, Virus, ) | 13 |
| Generic.Heuristic | 43 |
| Malware | 208 |
| Ransomware | 15 |

## 6. 엔진별 탐지



|  |  |
| --- | --- |
| **엔진명** | **탐지수** |
| On-Write DFI - Suspicious | 241 |
| SentinelOne Cloud | 9 |
| Reputation | 2 |
| DBT - Executables | 25 |
| User-Defined Blocklist | 1 |
| Documents, Scripts | 1 |
| On-Write DFI | 1 |

## 7. 해결된 위협 정보

|  |  |
| --- | --- |
| **해결 상태** | **엔드포인트 수량** |
| mitigated | 108 |
| marked\_as\_benign | 37 |

## 8. 주요 탐지 내역 세부 사항

|  |  |
| --- | --- |
| 파일명 | delfino.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\Wizvera\Delfino-G3\delfino.exe |
| Originator Process | None |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 2회 |
| 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  Abnormalities This binary has an RWX section. It might contain self-modifying code  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  Abnormalities This binary has an RWX section. It might contain self-modifying code |

|  |  |
| --- | --- |
| 파일명 | veraport-g3-x64.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\npSecureDisk\npSecureDisk230143\veraport-g3-x64.exe |
| Originator Process | msedge.exe |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Direct Syscall Attempt to evade monitoring with a syscall directly from a library  MITRE : Defense Evasion [T1562.001] Malware Detected attempt to evade monitors with a direct syscall execution  MITRE : Defense Evasion [T1562.001] Direct Syscall Attempt to evade monitoring with a syscall directly from the main process binary  MITRE : Defense Evasion [T1562.001] Packer A UPX packed process was detected  MITRE : Defense Evasion [T1027][T1480.001] Evasion Application added firewall rules to allow network traffic  MITRE : Exfiltration [T1041][T1048][T1020][T1030][T1029] MITRE : Defense Evasion [T1562.004] Reconnaissance A known network sniffing executable was run  MITRE : Credential Access [T1040] MITRE : Discovery [T1040] General Detected by the Static Engine  Persistence Application registered itself to become persistent via an autorun  MITRE : Persistence [T1547.001] MITRE : Privilege Escalation [T1547.001] Evasion A new root certificate was added  MITRE : Defense Evasion [T1553.004] Persistence Application registered itself to become persistent via COM object  MITRE : Persistence [T1546.015] MITRE : Privilege Escalation [T1546.015] 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] Infostealer Microsoft Edge's private memory was accessed  MITRE : Credential Access [T1555.003] Evasion Anti-debug technique was used  MITRE : Defense Evasion  Evasion Anti-VM technique was used  MITRE : Defense Evasion  Privilege Escalation Execution of privileged instruction was identified  MITRE : Privilege Escalation  Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Persistence Detected loading of native DLLs from SysWow64 directory into native processes (Sunburst masquerading technique)  MITRE : Persistence [T1574.001] MITRE : Privilege Escalation [T1574.001] MITRE : Defense Evasion [T1574.001] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] |

|  |  |
| --- | --- |
| 파일명 | wizcertutil.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\00534\AppData\Local\Temp\is-7Q3DM.tmp\wizcertutil.exe |
| Originator Process | delfino-g3-setup-x86.tmp |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 2회 |
| 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  General This binary uses Dinkumware libraries which are commonly used by malware  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  General This binary uses Dinkumware libraries which are commonly used by malware |

|  |  |
| --- | --- |
| 파일명 | wizcertutil.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\00560\AppData\Local\Temp\is-T2AG3.tmp\wizcertutil.exe |
| Originator Process | delfino-g3-setup-x86.tmp |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 2회 |
| 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  General This binary uses Dinkumware libraries which are commonly used by malware  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  General This binary uses Dinkumware libraries which are commonly used by malware |

|  |  |
| --- | --- |
| 파일명 | n6agent.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume2\Program Files\NetClient6\n6agent.exe |
| Originator Process | services.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Attempt to evade monitoring using the Process hollowing technique  MITRE : Privilege Escalation [T1055.012] MITRE : Defense Evasion [T1055.012] Evasion Anti-VM technique was used  MITRE : Defense Evasion  Persistence Application registered itself to become persistent via service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] Evasion Application added firewall rules to allow network traffic  MITRE : Exfiltration [T1041][T1048][T1020][T1030][T1029] MITRE : Defense Evasion [T1562.004] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] |

|  |  |
| --- | --- |
| 파일명 | BMSScreenSaver.scr |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume2\windows\System32\BMSScreenSaver.scr |
| Originator Process | winlogon.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Attempt to evade monitoring using the Process hollowing technique  MITRE : Privilege Escalation [T1055.012] MITRE : Defense Evasion [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | WavesSvc64.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Waves\MaxxAudio\WavesSvc64.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Attempt to evade monitoring using the Process hollowing technique  MITRE : Privilege Escalation [T1055.012] MITRE : Defense Evasion [T1055.012] Infostealer Keylogger Installation  MITRE : Credential Access [T1056.001] MITRE : Collection [T1056.001] |

|  |  |
| --- | --- |
| 파일명 | IDAT.Win.InputPanel.exe |
| 분류 | PUA |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\ID Information System\IDAT.Win.InputPanel\IDAT.Win.InputPanel.exe |
| Originator Process | None |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 1회 |
| 구조/행위분석 |  |

|  |  |
| --- | --- |
| 파일명 | Uninstall.exe |
| 분류 | Virus |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\PROGRAM FILES (X86)\MeeSoft\ImageAnalyzer\Uninstall.exe |
| Originator Process | None |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | General This binary imports functions used to raise kernel exceptions |

|  |  |
| --- | --- |
| 파일명 | I3GMainSvc.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\IPinside\_LWS\I3GMainSvc.exe |
| Originator Process | services.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Attempt to evade monitoring using the Process hollowing technique  MITRE : Privilege Escalation [T1055.012] MITRE : Defense Evasion [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | DelfinoUAC.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\Wizvera\Delfino-G3\DelfinoUAC.exe |
| Originator Process | None |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 2회 |
| 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  Abnormalities This binary has an RWX section. It might contain self-modifying code  General This binary uses Dinkumware libraries which are commonly used by malware  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  Abnormalities This binary has an RWX section. It might contain self-modifying code  General This binary uses Dinkumware libraries which are commonly used by malware |

|  |  |
| --- | --- |
| 파일명 | whale.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Naver\Naver Whale\Application\whale.exe |
| Originator Process | None |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | General Detected by the Static Engine  Evasion Application added firewall rules to allow network traffic  MITRE : Exfiltration [T1041][T1048][T1020][T1030][T1029] MITRE : Defense Evasion [T1562.004] 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] Persistence Application registered itself to become persistent via service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] Privilege Escalation Execution of privileged instruction was identified  MITRE : Privilege Escalation  Evasion A new root certificate was added  MITRE : Defense Evasion [T1553.004] Evasion Anti-VM technique was used  MITRE : Defense Evasion  Persistence Application registered itself to become persistent via COM object  MITRE : Persistence [T1546.015] MITRE : Privilege Escalation [T1546.015] Persistence Application registered itself to become persistent via an autorun  MITRE : Persistence [T1547.001] MITRE : Privilege Escalation [T1547.001] Evasion Anti-debug technique was used  MITRE : Defense Evasion  Evasion Process wrote to a hidden file section  MITRE : Defense Evasion [T1564.004][T1027][T1480.001] Exploitation Detected suspicious shellcode API call  MITRE : Execution [T1106][T1059] MITRE : Defense Evasion [T1140] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |