센티넬원 리포트

# 기간 : 2023-08-21 ~ 2023-11-21

# scope : KohYoung>1. 국내>Default Group

## 1. OS별 엔드포인트

|  |  |
| --- | --- |
| **OS 유형** | **엔드포인트 수량** |
| windows | 459 |
| linux | 7 |

## 2. 버전별 엔드포인트

|  |  |
| --- | --- |
| **에이전트 버전** | **엔드포인트 수량** |
| 22.1.2.217 | 157 |
| 21.7.2.1038 | 197 |
| 3.7.2.45 | 14 |
| 22.1.4.10010 | 60 |
| 3.7.3.53 | 10 |
| 21.6.4.423 | 1 |
| 21.7.5.1080 | 1 |
| 4.5.12.216 | 10 |
| 21.10.3.3 | 1 |
| 22.3.4.612 | 3 |
| 22.1.2.7 | 6 |
| 22.3.2.373 | 1 |
| 23.1.4.650 | 2 |
| 4.0.4.81 | 1 |
| 23.1.1.140 | 1 |
| 21.6.5.1072 | 1 |

## 3. 보호되고 있는 엔드포인트

|  |  |
| --- | --- |
| **감염여부** | **엔드포인트 수량** |
| Healthy | 456 |
| Infected | 10 |

## 4. 기간내 Top20 탐지 Endpoints

|  |  |  |
| --- | --- | --- |
| **No.** | **Endpoint** | **탐지건수** |
| 1 | KR-L2211C0021 | 137 |
| 2 | KR-L2306C0005 | 66 |
| 3 | KR-L2306C0006 | 49 |
| 4 | KR-L2209C0025 | 47 |
| 5 | KR-L2203C0015 | 46 |
| 6 | KR-D2210C0004 | 44 |
| 7 | KR-L2302C0008 | 44 |
| 8 | KR-L2205C0002 | 38 |
| 9 | KR-L2303C0031 | 34 |
| 10 | KR-L2306C0002 | 34 |
| 11 | DESKTOP-JYPARK | 27 |
| 12 | KR-L2212C0014 | 24 |
| 13 | KR-L2101C0007 | 22 |
| 14 | KR-L2303C0043 | 20 |
| 15 | KR-D2303C0014 | 20 |
| 16 | KR-L2306C0016 | 20 |
| 17 | KR-D2208C0055 | 18 |
| 18 | KR-L2303C0078 | 17 |
| 19 | KR-L2207C0112 | 16 |
| 20 | DESKTOP-Q3P6QAR | 16 |

## 7. 해결된 위협 정보

|  |  |
| --- | --- |
| **해결 상태** | **엔드포인트 수량** |
| mitigated | 103 |
| marked\_as\_benign | 79 |

## 8. 주요 탐지 내역 세부 사항

|  |  |
| --- | --- |
| 파일명 | HASPUserSetup.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\ws.kim\Downloads\DER\_1000수송환경기록계\HASPUserSetup\HASPUserSetup\HASPUserSetup.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to a remote process  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion User process created a process solely used by the system  MITRE : Execution  Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to a remote process  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion User process created a process solely used by the system  MITRE : Execution  Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | I3GProc.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume4\Program Files (x86)\IPinside\_LWS\I3GProc.exe |
| Originator Process | None |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Anti-VM technique was used  MITRE : Defense Evasion  General Detected by the Static Engine  Evasion Anti-VM technique was used  MITRE : Defense Evasion  General Detected by the Static Engine |

|  |  |
| --- | --- |
| 파일명 | NHCAAgent.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\IZEX\NetHelper Client V7.0 x64\NHCAAgent.exe |
| Originator Process | services.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Prevented the Task Manager from starting  MITRE : Defense Evasion  Evasion Process tampered with Windows user interface  Infostealer Keylogger Installation  MITRE : Credential Access [T1056.001] MITRE : Collection [T1056.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] 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] 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] Evasion Prevented the Task Manager from starting  MITRE : Defense Evasion  Evasion Process tampered with Windows user interface  Infostealer Keylogger Installation  MITRE : Credential Access [T1056.001] MITRE : Collection [T1056.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] 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] 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] |

|  |  |
| --- | --- |
| 파일명 | bdcam.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Bandicam\bdcam.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Injection attempt via Instrumentation Callback API  MITRE : Defense Evasion [T1055][T1562.001] MITRE : Privilege Escalation [T1055] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] General Process started from shortcut file  MITRE : Execution [T1204] Evasion Injection attempt via Instrumentation Callback API  MITRE : Defense Evasion [T1055][T1562.001] MITRE : Privilege Escalation [T1055] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | 4504FCDADC1E34DBEBBF22C9DE4D3CB08E525A50.sys |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\ProgramData\Dell\SARemediation\SystemRepair\Snapshots\Backup\4504FCDADC1E34DBEBBF22C9DE4D3CB08E525A50.sys |
| Originator Process | DellSupportAssistRemedationService.exe |
| 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 | tsrvctlEx.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\tcostream\client\tsrvctlEx.exe |
| Originator Process | services.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Evasion Application added firewall rules to allow network traffic  MITRE : Exfiltration [T1041][T1048][T1020][T1030][T1029] MITRE : Defense Evasion [T1562.004] 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] 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] Evasion Anti-VM technique was used  MITRE : Defense Evasion  Evasion Anti-debug technique was used  MITRE : Defense Evasion  Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Evasion Application added firewall rules to allow network traffic  MITRE : Exfiltration [T1041][T1048][T1020][T1030][T1029] MITRE : Defense Evasion [T1562.004] 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] 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] Evasion Anti-VM technique was used  MITRE : Defense Evasion  Evasion Anti-debug technique was used  MITRE : Defense Evasion  Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] |

|  |  |
| --- | --- |
| 파일명 | callGigabytefusionshortcutService.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume5\Program Files (x86)\Gigabyte Fusion\callGigabytefusionshortcutService.exe |
| Originator Process | runonce.exe |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | General Detected by the Static Engine  General Detected by the Static Engine |

|  |  |
| --- | --- |
| 파일명 | wpmsvc.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\Wizvera\Common\wpmsvc\wpmsvc.exe |
| Originator Process | services.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] 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] 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  Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] 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] 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  Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] |

|  |  |
| --- | --- |
| 파일명 | CRM\_Launcher2.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\PROGRAM FILES (X86)\CRM Launcher\CRM\_Launcher2.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Process wrote to a hidden file section  MITRE : Defense Evasion [T1564.004][T1027][T1480.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Exploitation Detected suspicious shellcode API call from vulnerable content  MITRE : Execution [T1106][T1059] MITRE : Defense Evasion [T1140] 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] General Process started from shortcut file  MITRE : Execution [T1204] General Detected by the Static Engine  Evasion Process wrote to a hidden file section  MITRE : Defense Evasion [T1564.004][T1027][T1480.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Exploitation Detected suspicious shellcode API call from vulnerable content  MITRE : Execution [T1106][T1059] MITRE : Defense Evasion [T1140] 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] General Process started from shortcut file  MITRE : Execution [T1204] General Detected by the Static Engine |

|  |  |
| --- | --- |
| 파일명 | SafeConnect.Entry.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\McAfee\McAfee Safe Connect\SafeConnect.Entry.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] |

|  |  |
| --- | --- |
| 파일명 | RexpertPrintStartup.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\clipsoft\Rexpert30PrintService\RexpertPrintStartup.exe |
| Originator Process | runonce.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | Hoax Eliminator.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume5\USERS\SEONYONG\Desktop\x64\Hoax Eliminator.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | 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] Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] 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] 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 A known network sniffing executable was run  MITRE : Credential Access [T1040] MITRE : Discovery [T1040] Evasion Detected Heaven's Gate technique in manipulated code execution  MITRE : Execution  Injection Suspicious library loaded into the process memory  Evasion Anti-debug technique was used  MITRE : Defense Evasion  Direct Syscall Attempt to evade monitoring with a syscall directly from the main process binary  MITRE : Defense Evasion [T1562.001] Evasion Anti-VM technique was used  MITRE : Defense Evasion  Privilege Escalation Execution of privileged instruction was identified  MITRE : Privilege Escalation  Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] 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 service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] |

|  |  |
| --- | --- |
| 파일명 | delfinounloader-g3.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume5\PROGRAM FILES (X86)\Wizvera\Delfino-G3\delfinounloader-g3.exe |
| Originator Process | \_iu14D2N.tmp |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | 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  Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] General Detected by the Static Engine  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  Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] General Detected by the Static Engine |

|  |  |
| --- | --- |
| 파일명 | parametric.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume4\PROGRAM FILES\PTC\Creo 4.0\M150\Parametric\bin\parametric.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] General Process started from shortcut file  MITRE : Execution [T1204] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | WavesSvc64.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\WINDOWS\System32\DriverStore\FileRepository\wavesapo11de.inf\_amd64\_246e3e0cc5d717fa\WavesSvc64.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | DCMApp.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\ws.kim\AppData\Local\EMC\ContentXfer\dcm\DCMApp.exe |
| Originator Process | chrome.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Detected in-memory hooks on AMSI DLL  MITRE : Defense Evasion [T1562.001][T1574] MITRE : Privilege Escalation [T1574] MITRE : Persistence [T1574] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Detected in-memory hooks on AMSI DLL  MITRE : Defense Evasion [T1562.001][T1574] MITRE : Privilege Escalation [T1574] MITRE : Persistence [T1574] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution |

|  |  |
| --- | --- |
| 파일명 | Bandizip.exe |
| 분류 | Ransomware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Bandizip\Bandizip.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | WavesSvc64.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\WINDOWS\System32\DriverStore\FileRepository\wavesapo11de.inf\_amd64\_d4eabf4492fbb4d5\WavesSvc64.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion The original filename is different from its actual name  MITRE : Defense Evasion [T1036.003][T1036.005][T1574.008] MITRE : Persistence [T1574.008] MITRE : Privilege Escalation [T1574.008] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion The original filename is different from its actual name  MITRE : Defense Evasion [T1036.003][T1036.005][T1574.008] MITRE : Persistence [T1574.008] MITRE : Privilege Escalation [T1574.008] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | X2.EXE |
| 분류 | Ransomware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Altium\AD22\X2.EXE |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Office program loaded vbe dll, might indicate macro execution  MITRE : Execution [T1059.005][T1204] MITRE : Initial Access [T1566.001] Evasion Detected in-memory hooks on AMSI DLL  MITRE : Defense Evasion [T1562.001][T1574] MITRE : Privilege Escalation [T1574] MITRE : Persistence [T1574] Privilege Escalation Suspicious Kerberoasting attack. Too many SPN tickets requests  MITRE : Credential Access [T1558.003] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] General Process started from shortcut file  MITRE : Execution [T1204] Evasion Office program loaded vbe dll, might indicate macro execution  MITRE : Execution [T1059.005][T1204] MITRE : Initial Access [T1566.001] Evasion Detected in-memory hooks on AMSI DLL  MITRE : Defense Evasion [T1562.001][T1574] MITRE : Privilege Escalation [T1574] MITRE : Persistence [T1574] Privilege Escalation Suspicious Kerberoasting attack. Too many SPN tickets requests  MITRE : Credential Access [T1558.003] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | innoSysChecker.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\innoFDS\innoSysChecker.exe |
| Originator Process | hrdLMS\_Setup.exe |
| 엔진 | On-Write DFI - Suspicious |
| 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  Hiding/Stealthiness The majority of sections in this PE have high entropy, a sign of obfuscation or packing  General This binary imports functions used to raise kernel exceptions  Infostealer This binary has keylogging capabilities  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | Typora.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Typora\Typora.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | SourceTree.exe |
| 분류 | Ransomware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\soowon.yang\AppData\Local\SourceTree\SourceTree.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Ransomware Ransomware activity that uses EFS  MITRE : Impact [T1485][T1486] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  General Process started from shortcut file  MITRE : Execution [T1204] Ransomware Ransomware activity that uses EFS  MITRE : Impact [T1485][T1486] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | CRM\_Launcher2.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\PROGRAM FILES (X86)\CRM Launcher\CRM\_Launcher2.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Process wrote to a hidden file section  MITRE : Defense Evasion [T1564.004][T1027][T1480.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Exploitation Detected suspicious shellcode API call from vulnerable content  MITRE : Execution [T1106][T1059] MITRE : Defense Evasion [T1140] Privilege Escalation Suspicious Kerberoasting attack. Too many SPN tickets requests  MITRE : Credential Access [T1558.003] General Process started from shortcut file  MITRE : Execution [T1204] General Detected by the Static Engine  Evasion Process wrote to a hidden file section  MITRE : Defense Evasion [T1564.004][T1027][T1480.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Exploitation Detected suspicious shellcode API call from vulnerable content  MITRE : Execution [T1106][T1059] MITRE : Defense Evasion [T1140] Privilege Escalation Suspicious Kerberoasting attack. Too many SPN tickets requests  MITRE : Credential Access [T1558.003] General Process started from shortcut file  MITRE : Execution [T1204] General Detected by the Static Engine |

|  |  |
| --- | --- |
| 파일명 | CRM Launcher Setup 4.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\hs.shin.KOHYOUNG\Downloads\CRM Launcher Setup 4.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Process wrote to a hidden file section  MITRE : Defense Evasion [T1564.004][T1027][T1480.001] General User logged on  MITRE : Persistence [T1078] MITRE : Defense Evasion [T1078] MITRE : Privilege Escalation [T1078] MITRE : Initial Access [T1078] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Exploitation Detected suspicious shellcode API call from vulnerable content  MITRE : Execution [T1106][T1059] MITRE : Defense Evasion [T1140] Privilege Escalation Suspicious Kerberoasting attack. Too many SPN tickets requests  MITRE : Credential Access [T1558.003] General Detected by the Static Engine  Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] Evasion Process wrote to a hidden file section  MITRE : Defense Evasion [T1564.004][T1027][T1480.001] General User logged on  MITRE : Persistence [T1078] MITRE : Defense Evasion [T1078] MITRE : Privilege Escalation [T1078] MITRE : Initial Access [T1078] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Exploitation Detected suspicious shellcode API call from vulnerable content  MITRE : Execution [T1106][T1059] MITRE : Defense Evasion [T1140] Privilege Escalation Suspicious Kerberoasting attack. Too many SPN tickets requests  MITRE : Credential Access [T1558.003] General Detected by the Static Engine  Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] |

|  |  |
| --- | --- |
| 파일명 | git-bash.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Git\git-bash.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | makensis.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\NSIS\Bin\makensis.exe |
| Originator Process | OpenWith.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | NSIS.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\NSIS\NSIS.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | uninst-nsis.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\NSIS\uninst-nsis.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | nsis-3.0-setup.exe |
| 분류 | Ransomware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\[000].GIT\KYI\_V3\KYI\_V3\_12fix\Installer\NSIS Lib\nsis-3.0-setup.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Ransomware Ransomware activity that uses EFS  MITRE : Impact [T1485][T1486] |

|  |  |
| --- | --- |
| 파일명 | nsis-3.09-setup.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\soowon.yang\Downloads\nsis-3.09-setup.exe |
| Originator Process | Everything.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | Bandizip.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Bandizip\Bandizip.exe |
| Originator Process | chrome.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | makensis.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\NSIS\Bin\makensis.exe |
| Originator Process | OpenWith.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | makensisw.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\NSIS\makensisw.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | KYI.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\source\Develop-KYI\KYI\Bin\KYI.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] General Process started from shortcut file  MITRE : Execution [T1204] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | WindowsSecuService.exe |
| 분류 | Generic.Heuristic |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Windows\System32\WindowsSecuService.exe |
| Originator Process | services.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Prevented the Task Manager from starting  MITRE : Defense Evasion  Evasion Process tampered with Windows user interface  Infostealer Keylogger Installation  MITRE : Credential Access [T1056.001] MITRE : Collection [T1056.001] 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] 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] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Prevented the Task Manager from starting  MITRE : Defense Evasion  Evasion Process tampered with Windows user interface  Infostealer Keylogger Installation  MITRE : Credential Access [T1056.001] MITRE : Collection [T1056.001] 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] 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] |

|  |  |
| --- | --- |
| 파일명 | uv\_x64.exe |
| 분류 | Generic.Heuristic |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume6\PROGRAM FILES (X86)\UltraViewer\uv\_x64.exe |
| Originator Process | UltraViewer\_Service.exe |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Infostealer Keylogger Installation  MITRE : Credential Access [T1056.001] MITRE : Collection [T1056.001] Injection Library was injected to a remote process  MITRE : Defense Evasion [T1055] MITRE : Privilege Escalation [T1055] Exploitation Detected suspicious shellcode API call  MITRE : Execution [T1106][T1059] MITRE : Defense Evasion [T1140] General Detected by the Static Engine  Infostealer Keylogger Installation  MITRE : Credential Access [T1056.001] MITRE : Collection [T1056.001] Injection Library was injected to a remote process  MITRE : Defense Evasion [T1055] MITRE : Privilege Escalation [T1055] Exploitation Detected suspicious shellcode API call  MITRE : Execution [T1106][T1059] MITRE : Defense Evasion [T1140] General Detected by the Static Engine |

|  |  |
| --- | --- |
| 파일명 | SourceTree.exe |
| 분류 | Ransomware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume8\Users\이승현\_SeunghyunLee\AppData\Local\SourceTree\SourceTree.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] General Process started from shortcut file  MITRE : Execution [T1204] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\soowon.yang\OneDrive - 고영테크놀러지\문서\Vault\[ NAS ]\[ 02. 제어실 Daily Meeting ]\제어2팀 CTM1파트\[ 2023 ]\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | eBUS SDK 64-bit for JAI.6.3.1.6545.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\jungho.kwon\Downloads\eBUS-SDK-for-JAI\_64-bit\_6.3.1\eBUS SDK 64-bit for JAI.6.3.1.6545.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Anti-VM technique was used  MITRE : Defense Evasion  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  General User logged on  MITRE : Persistence [T1078] MITRE : Defense Evasion [T1078] MITRE : Privilege Escalation [T1078] MITRE : Initial Access [T1078] |

|  |  |
| --- | --- |
| 파일명 | ttermpro.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\teraterm\ttermpro.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | Brainstorming\_20231114\_TGR 장착 상태에서 구동 방안.pptx |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\soowon.yang\Downloads\Brainstorming\_20231114\_TGR 장착 상태에서 구동 방안.pptx |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Process wrote to a hidden file section  MITRE : Defense Evasion [T1564.004][T1027][T1480.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Detected in-memory hooks on AMSI DLL  MITRE : Defense Evasion [T1562.001][T1574] MITRE : Privilege Escalation [T1574] MITRE : Persistence [T1574] |

|  |  |
| --- | --- |
| 파일명 | git-bash.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Git\git-bash.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | KY\_KYI\_Setup\_Medical\_x64\_1.1.12.0.3.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume21\KY\_KYI\_Setup\_Medical\_x64\_1.1.12.0.3.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution |

|  |  |
| --- | --- |
| 파일명 | KY\_KYI\_Setup\_Medical\_x64\_1.1.12.0.3\_Log.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\KY\_KYI\_Setup\_Medical\_x64\_1.1.12.0.3\_Log.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution |

|  |  |
| --- | --- |
| 파일명 | git-gui.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Git\cmd\git-gui.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | NAudio.dll |
| 분류 | PUA |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume2\JY\overwolf\0.234.0.8\NAudio.dll |
| Originator Process | OverwolfSetup.exe |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 2회 |
| 구조/행위분석 |  |

|  |  |
| --- | --- |
| 파일명 | UVUpdater.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\UltraViewer\Update\UVUpdater.exe |
| Originator Process | UltraViewer\_Service.exe |
| 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  Hiding/Stealthiness The majority of sections in this PE have high entropy, a sign of obfuscation or packing  Hiding/Stealthiness This binary may contain encrypted or compressed data as measured by high entropy of the sections (greater than 6.8)  Abnormalities This binary contains abnormal section names which could be an indication that it was created with non-standard development tools  Hiding/Stealthiness The majority of sections in this PE have high entropy, a sign of obfuscation or packing  Hiding/Stealthiness This binary may contain encrypted or compressed data as measured by high entropy of the sections (greater than 6.8) |

|  |  |
| --- | --- |
| 파일명 | Bandizip.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Bandizip\Bandizip.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | npp.8.5.8.Installer.x64.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\mh.han\Downloads\npp.8.5.8.Installer.x64.exe |
| Originator Process | msedge.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion A new root certificate was added  MITRE : Defense Evasion [T1553.004] Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Persistence Application registered itself to become persistent via COM object  MITRE : Persistence [T1546.015] MITRE : Privilege Escalation [T1546.015] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Injection Suspicious library loaded into the process memory  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | UVUpdater.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\UltraViewer\Update\UVUpdater.exe |
| Originator Process | UltraViewer\_Service.exe |
| 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  Hiding/Stealthiness The majority of sections in this PE have high entropy, a sign of obfuscation or packing  Hiding/Stealthiness This binary may contain encrypted or compressed data as measured by high entropy of the sections (greater than 6.8)  Abnormalities This binary contains abnormal section names which could be an indication that it was created with non-standard development tools  Hiding/Stealthiness The majority of sections in this PE have high entropy, a sign of obfuscation or packing  Hiding/Stealthiness This binary may contain encrypted or compressed data as measured by high entropy of the sections (greater than 6.8) |

|  |  |
| --- | --- |
| 파일명 | Bandizip.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Bandizip\Bandizip.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | bdcam.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Bandicam\bdcam.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Injection attempt via Instrumentation Callback API  MITRE : Defense Evasion [T1055][T1562.001] MITRE : Privilege Escalation [T1055] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] General Process started from shortcut file  MITRE : Execution [T1204] Evasion Injection attempt via Instrumentation Callback API  MITRE : Defense Evasion [T1055][T1562.001] MITRE : Privilege Escalation [T1055] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | git-gui.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Git\cmd\git-gui.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | test2.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\USERS\ds.park.KOHYOUNG\OneDrive - 고영테크놀러지\Python\MQA\_AV\AutoVerificationTool\dist\test2.exe |
| Originator Process | python.exe (pyinstaller.exe) |
| 엔진 | On-Write DFI - Suspicious |
| 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  Hiding/Stealthiness The majority of sections in this PE have high entropy, a sign of obfuscation or packing  General This is a compiled Python executable  General This binary imports functions used to raise kernel exceptions  Hiding/Stealthiness This binary may contain encrypted or compressed data as measured by high entropy of the sections (greater than 6.8)  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | test2.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\USERS\ds.park.KOHYOUNG\OneDrive - 고영테크놀러지\Python\MQA\_AV\AutoVerificationTool\dist\test2.exe |
| Originator Process | python.exe (pyinstaller.exe) |
| 엔진 | On-Write DFI - Suspicious |
| 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  Hiding/Stealthiness The majority of sections in this PE have high entropy, a sign of obfuscation or packing  General This is a compiled Python executable  General This binary imports functions used to raise kernel exceptions  Hiding/Stealthiness This binary may contain encrypted or compressed data as measured by high entropy of the sections (greater than 6.8)  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | 연구소.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume7\기본 SW\03. DRM 03. DRM 연구소 금고영역 확인후 사용자가 직접 설치\연구소.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Persistence Application registered itself to become persistent via COM object  MITRE : Persistence [T1546.015] MITRE : Privilege Escalation [T1546.015] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Persistence Application registered itself to become persistent via an autorun  MITRE : Persistence [T1547.001] MITRE : Privilege Escalation [T1547.001] Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] General User logged on  MITRE : Persistence [T1078] MITRE : Defense Evasion [T1078] MITRE : Privilege Escalation [T1078] MITRE : Initial Access [T1078] |

|  |  |
| --- | --- |
| 파일명 | AutodeskDesktopApp.exe |
| 분류 | Generic.Heuristic |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\Autodesk\Autodesk Desktop App\AutodeskDesktopApp.exe |
| Originator Process | runonce.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | QNAPNetBakWindows-4.5.12.1108.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\user\Downloads\QNAPNetBakWindows-4.5.12.1108.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Persistence Application registered itself to become persistent via scheduled task  MITRE : Persistence [T1053.005] MITRE : Execution [T1053.005] MITRE : Privilege Escalation [T1053.005] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Persistence Application registered itself to become persistent via service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Persistence Application registered itself to become persistent via scheduled task  MITRE : Persistence [T1053.005] MITRE : Execution [T1053.005] MITRE : Privilege Escalation [T1053.005] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Persistence Application registered itself to become persistent via service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | Q-Dir.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\Q-Dir\Q-Dir.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | General User logged on  MITRE : Persistence [T1078] MITRE : Defense Evasion [T1078] MITRE : Privilege Escalation [T1078] MITRE : Initial Access [T1078] Evasion Office program loaded vbe dll, might indicate macro execution  MITRE : Execution [T1059.005][T1204] MITRE : Initial Access [T1566.001] Evasion Process wrote to a hidden file section  MITRE : Defense Evasion [T1564.004][T1027][T1480.001] Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Detected in-memory hooks on AMSI DLL  MITRE : Defense Evasion [T1562.001][T1574] MITRE : Privilege Escalation [T1574] MITRE : Persistence [T1574] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | Bizentro.App.MAIN.Shell.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\Public\Documents\Bizentro\SmartClientViewer\10.10.0.81\Bizentro.App.MAIN.Shell.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] General Process started from shortcut file  MITRE : Execution [T1204] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | KalmuriSetup.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\jinsub.kim\Desktop\KalmuriSetup.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | understand.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\SciTools\bin\pc-win64\understand.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] General Process started from shortcut file  MITRE : Execution [T1204] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | git-bash.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Git\git-bash.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | Everything.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Everything\Everything.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\soowon.yang\OneDrive - 고영테크놀러지\문서\Vault\[ NAS ]\[ 02. 제어실 Daily Meeting ]\제어2팀 CTM1파트\[ 2023 ]\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Command line changed between process execution and main thread resumption |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\soowon.yang\OneDrive - 고영테크놀러지\문서\Vault\[ NAS ]\[ 02. 제어실 Daily Meeting ]\제어2팀 CTM1파트\[ 2023 ]\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Command line changed between process execution and main thread resumption |

|  |  |
| --- | --- |
| 파일명 | cov-analysis-win64-2022.12.1.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume7\[002]\_개발 SW\cov-analysis-win64-2022.12.1.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Detected loading 'fake' AMSI DLL to a process  MITRE : Defense Evasion [T1574.001][T1562.001][T1055.001] MITRE : Persistence [T1574.001] MITRE : Privilege Escalation [T1574.001][T1055.001] Evasion Command line changed between process execution and main thread resumption  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Detected loading 'fake' AMSI DLL to a process  MITRE : Defense Evasion [T1574.001][T1562.001][T1055.001] MITRE : Persistence [T1574.001] MITRE : Privilege Escalation [T1574.001][T1055.001] Evasion Command line changed between process execution and main thread resumption  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | TouchEn\_nxKey\_32bit.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\jihyun.song\Downloads\TouchEn\_nxKey\_32bit.exe |
| Originator Process | chrome.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Anti-debug technique was used  MITRE : Defense Evasion  Evasion Anti-VM technique was used  MITRE : Defense Evasion  Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] 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] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] 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] 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] 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] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | Minitab 16.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume7\Neptune\Minitab\Minitab16.1.1.0\_English\_Full\_Portable\_by sylar\Minitab16.1.1.0\_English\_Full\_Portable\Minitab 16.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Infostealer Keylogger Installation  MITRE : Credential Access [T1056.001] MITRE : Collection [T1056.001] Injection Library was injected to a remote process  MITRE : Defense Evasion [T1055] MITRE : Privilege Escalation [T1055] Privilege Escalation Execution of privileged instruction was identified  MITRE : Privilege Escalation  Evasion Anti-VM technique was used  MITRE : Defense Evasion  Evasion Command line changed between process execution and main thread resumption  Evasion Attempt to evade monitoring using the Process hollowing technique  MITRE : Privilege Escalation [T1055.012] MITRE : Defense Evasion [T1055.012] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to a remote process  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Exploitation Detected suspicious shellcode API call  MITRE : Execution [T1106][T1059] MITRE : Defense Evasion [T1140] Infostealer Keylogger Installation  MITRE : Credential Access [T1056.001] MITRE : Collection [T1056.001] Injection Library was injected to a remote process  MITRE : Defense Evasion [T1055] MITRE : Privilege Escalation [T1055] Privilege Escalation Execution of privileged instruction was identified  MITRE : Privilege Escalation  Evasion Anti-VM technique was used  MITRE : Defense Evasion  Evasion Command line changed between process execution and main thread resumption  Evasion Attempt to evade monitoring using the Process hollowing technique  MITRE : Privilege Escalation [T1055.012] MITRE : Defense Evasion [T1055.012] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to a remote process  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Exploitation Detected suspicious shellcode API call  MITRE : Execution [T1106][T1059] MITRE : Defense Evasion [T1140] |

|  |  |
| --- | --- |
| 파일명 | Coverity Point and Scan.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Coverity\Coverity Static Analysis\bin\Coverity Point and Scan.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | Review\_Setup\_x64\_3.2.0.0\_H01(62e9e4f09).exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\jihyun.song\Downloads\Review\_Setup\_x64\_3.2.0.0\_H01(62e9e4f09).exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | Local\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\Local\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | Local\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\Local\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | Skype.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\WindowsApps\Microsoft.SkypeApp\_15.107.3215.0\_x64\_\_kzf8qxf38zg5c\Skype\Skype.exe |
| Originator Process | dllhost.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Command line changed between process execution and main thread resumption  Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | Si3586Setup.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\D\Disk D\Project\installation\_program\SWDevTool\SourceInsight3\Si3586Setup.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | Fork.exe |
| 분류 | Ransomware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\sprite.kim\AppData\Local\Fork\Fork.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  General Process started from shortcut file  MITRE : Execution [T1204] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | codecompare.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\D\Disk D\Project\installation\_program\codecompare.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | git-bash.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Git\git-bash.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | GTEST\_KYIIF.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Bitbucket\KYI\_Medical\_v3.0\Installer\KYI\Bin\GTEST\_KYIIF.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_2.0.1.0.0\_231107\_5.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_2.0.1.0.0\_231107\_5.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_2.0.1.0.0\_231120.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_2.0.1.0.0\_231120.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6\_231120.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6\_231120.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6\_231120\_1.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6\_231120\_1.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6\_231120\_2.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6\_231120\_2.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6\_231120\_3.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6\_231120\_3.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | Git-2.34.1-64-bit.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume7\installation\_program\SWDevTool\Git-2.34.1-64-bit.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] |

|  |  |
| --- | --- |
| 파일명 | TSpcScan2.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\tcostream\client\TSpcScan2.exe |
| Originator Process | None |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution |

|  |  |
| --- | --- |
| 파일명 | VPWalletService.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\VP\VPWalletService\VPWalletService.exe |
| Originator Process | services.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | 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] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Detected loading 'fake' AMSI DLL to a process  MITRE : Defense Evasion [T1574.001][T1562.001][T1055.001] MITRE : Persistence [T1574.001] MITRE : Privilege Escalation [T1574.001][T1055.001] Infostealer Keylogger Installation  MITRE : Credential Access [T1056.001] MITRE : Collection [T1056.001] Injection Code injection to other process memory space via Reflection  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  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Command line changed between process execution and main thread resumption |

|  |  |
| --- | --- |
| 파일명 | npp.8.1.9.3.Installer.x64.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume7\installation\_program\npp.8.1.9.3.Installer.x64.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion A new root certificate was added  MITRE : Defense Evasion [T1553.004] 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 Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Injection Suspicious library loaded into the process memory  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | git-bash.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Git\git-bash.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to a remote process  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Injection Code injection to a remote process  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | test2.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\USERS\ds.park.KOHYOUNG\OneDrive - 고영테크놀러지\Python\MQA\_AV\AutoVerificationTool\dist\test2.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | General Detected by the Static Engine  General Detected by the Static Engine |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Reconnaissance Suspicious WMI query was identified  MITRE : Execution [T1047] MITRE : Discovery [T1518.001] MITRE : Collection [T1119] MITRE : Defense Evasion [T1480.001] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Reconnaissance Suspicious WMI query was identified  MITRE : Execution [T1047] MITRE : Discovery [T1518.001] MITRE : Collection [T1119] MITRE : Defense Evasion [T1480.001] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | SerialCom\_Static\_Analysis.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\vs\SYShare\Coverity\SerialCom\_Static\_Analysis.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | captura.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\WindowsApps\38526MediaLife.CoolScreenRecorder\_1.0.3.0\_x86\_\_1crh1k73ty8mg\captura.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Infostealer Keylogger Installation  MITRE : Credential Access [T1056.001] MITRE : Collection [T1056.001] Injection Library was injected to a remote process  MITRE : Defense Evasion [T1055] MITRE : Privilege Escalation [T1055] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Infostealer Keylogger Installation  MITRE : Credential Access [T1056.001] MITRE : Collection [T1056.001] Injection Library was injected to a remote process  MITRE : Defense Evasion [T1055] MITRE : Privilege Escalation [T1055] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution |

|  |  |
| --- | --- |
| 파일명 | KY\_KYI\_Setup\_Medical\_x64\_1.2.0.2.17.exe |
| 분류 | Ransomware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\[000].GIT\KYI\_V3\KYI\_V3\_12fix\Installer\KY\_KYI\_Setup\_Medical\_x64\_1.2.0.2.17.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Ransomware Ransomware activity that uses EFS  MITRE : Impact [T1485][T1486] Evasion Process wrote to a hidden file section  MITRE : Defense Evasion [T1564.004][T1027][T1480.001] |

|  |  |
| --- | --- |
| 파일명 | makensisw.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\NSIS\makensisw.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | KY\_KYI\_Setup\_Medical\_x64\_1.2.0.2.17.exe |
| 분류 | Ransomware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\[000].GIT\KYI\_V3\KYI\_V3\_12fix\Installer\KY\_KYI\_Setup\_Medical\_x64\_1.2.0.2.17.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Ransomware Ransomware activity that uses EFS  MITRE : Impact [T1485][T1486] Evasion Process wrote to a hidden file section  MITRE : Defense Evasion [T1564.004][T1027][T1480.001] |

|  |  |
| --- | --- |
| 파일명 | KY\_KYI\_Setup\_Medical\_x64\_1.2.0.2.17.exe |
| 분류 | Ransomware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\[000].GIT\KYI\_V3\KYI\_V3\_12fix\Installer\KY\_KYI\_Setup\_Medical\_x64\_1.2.0.2.17.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Ransomware Ransomware activity that uses EFS  MITRE : Impact [T1485][T1486] Evasion Process wrote to a hidden file section  MITRE : Defense Evasion [T1564.004][T1027][T1480.001] |

|  |  |
| --- | --- |
| 파일명 | cmd.exe (CLI 19b6) |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\WINDOWS\System32\cmd.exe (CLI 19b6) |
| Originator Process | explorer.exe |
| 엔진 | Anti Exploitation / Fileless |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Library was injected to a remote process  MITRE : Defense Evasion [T1055] MITRE : Privilege Escalation [T1055] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] General Process started from shortcut file  MITRE : Execution [T1204] Injection Library was injected to a remote process  MITRE : Defense Evasion [T1055] MITRE : Privilege Escalation [T1055] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | DS-EQCO125X40-60001467L.pdf |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\im.bae\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\TJLVT5NW\DS-EQCO125X40-60001467L.pdf |
| Originator Process | Q-Dir.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | EA.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume7\EA\EA.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Infostealer Behaves like a keylogger  MITRE : Credential Access [T1056.001] MITRE : Collection [T1056.001] Injection Library was injected to a remote process  MITRE : Defense Evasion [T1055] MITRE : Privilege Escalation [T1055] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | TortoiseGitProc.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\TortoiseGit\bin\TortoiseGitProc.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | Q-Dir.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\Local\C\Users\sprite.kim\AppData\Roaming\Q-Dir\Q-Dir.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  General Process started from shortcut file  MITRE : Execution [T1204] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | BDCAMSETUP\_KOR.EXE |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\sy.moon\Downloads\BDCAMSETUP\_KOR.EXE |
| Originator Process | msedge.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Injection attempt via Instrumentation Callback API  MITRE : Defense Evasion [T1055][T1562.001] MITRE : Privilege Escalation [T1055] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] 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] Injection Suspicious library loaded into the process memory  Evasion Injection attempt via Instrumentation Callback API  MITRE : Defense Evasion [T1055][T1562.001] MITRE : Privilege Escalation [T1055] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] 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] Injection Suspicious library loaded into the process memory |

|  |  |
| --- | --- |
| 파일명 | bdcam.exe |
| 분류 | Generic.Heuristic |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume6\PROGRAM FILES\Bandicam\bdcam.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Injection attempt via Instrumentation Callback API  MITRE : Defense Evasion [T1055][T1562.001] MITRE : Privilege Escalation [T1055] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | uninstall.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files (x86)\com0com\uninstall.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | Anaconda Powershell Prompt.lnk |
| 분류 | PUA |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\dk.cho\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Anaconda3 (64-bit)\Anaconda Powershell Prompt.lnk |
| Originator Process | \_conda.exe |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 1회 |
| 구조/행위분석 |  |

|  |  |
| --- | --- |
| 파일명 | quartus\_pgmw.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\intelFPGA\21.1\qprogrammer\bin64\quartus\_pgmw.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] General Process started from shortcut file  MITRE : Execution [T1204] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | Anaconda Powershell Prompt.lnk |
| 분류 | PUA |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\jake.yoon\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Anaconda3 (64-bit)\Anaconda Powershell Prompt.lnk |
| Originator Process | \_conda.exe |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 1회 |
| 구조/행위분석 |  |

|  |  |
| --- | --- |
| 파일명 | Review\_Setup\_x64\_3.2.0.0(4b91ebc70).exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\jy.park\Downloads\Review\_Setup\_x64\_3.2.0.0(4b91ebc70).exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | Review\_Setup\_x64\_3.2.0.0(4dd244f07).exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\jy.park\Downloads\Review\_Setup\_x64\_3.2.0.0(4dd244f07).exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | Anaconda Powershell Prompt.lnk |
| 분류 | PUA |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\ProgramData\Microsoft\Windows\Start Menu\Programs\Anaconda3 (64-bit)\Anaconda Powershell Prompt.lnk |
| Originator Process | \_conda.exe |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 1회 |
| 구조/행위분석 |  |

|  |  |
| --- | --- |
| 파일명 | printTest.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\다운로드\[멘토씨리즈] C언어(개정판)\멘토씨리즈 C언어(개정판)\day02\_c\day02\Debug\printTest.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 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 This binary has an RWX section. It might contain self-modifying code  General This binary imports functions used to raise kernel exceptions  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | casting.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\다운로드\[멘토씨리즈] C언어(개정판)\멘토씨리즈 C언어(개정판)\day07\_c\Debug\casting.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 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 This binary has an RWX section. It might contain self-modifying code  General This binary imports functions used to raise kernel exceptions  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | arTest2.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\다운로드\[멘토씨리즈] C언어(개정판)\멘토씨리즈 C언어(개정판)\day23\_c\Debug\arTest2.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 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 This binary has an RWX section. It might contain self-modifying code  General This binary imports functions used to raise kernel exceptions  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | stringTest.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\다운로드\[멘토씨리즈] C언어(개정판)\멘토씨리즈 C언어(개정판)\day25\_c\day25\Debug\stringTest.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 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 This binary has an RWX section. It might contain self-modifying code  General This binary imports functions used to raise kernel exceptions  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | arrTest.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\다운로드\[멘토씨리즈] C언어(개정판)\멘토씨리즈 C언어(개정판)\day27\_c\day27\Debug\arrTest.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 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 This binary has an RWX section. It might contain self-modifying code  General This binary imports functions used to raise kernel exceptions  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | arrTest.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\다운로드\[멘토씨리즈] C언어(개정판)\멘토씨리즈 C언어(개정판)\day26\_c\day26\Debug\arrTest.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 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 This binary has an RWX section. It might contain self-modifying code  General This binary imports functions used to raise kernel exceptions  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | cafe.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\다운로드\[멘토씨리즈] C언어(개정판)\멘토씨리즈 C언어(개정판)\day28\_c\Debug\cafe.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 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 This binary has an RWX section. It might contain self-modifying code  General This binary imports functions used to raise kernel exceptions  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | task.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\다운로드\[멘토씨리즈] C언어(개정판)\멘토씨리즈 C언어(개정판)\day35\_c\Debug\task.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 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 This binary has an RWX section. It might contain self-modifying code  General This binary imports functions used to raise kernel exceptions  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | task.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\다운로드\[멘토씨리즈] C언어(개정판)\멘토씨리즈 C언어(개정판)\day36\_c\Debug\task.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 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 This binary has an RWX section. It might contain self-modifying code  General This binary imports functions used to raise kernel exceptions  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | task.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\다운로드\[멘토씨리즈] C언어(개정판)\멘토씨리즈 C언어(개정판)\day37\_c\Debug\task.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 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 This binary has an RWX section. It might contain self-modifying code  General This binary imports functions used to raise kernel exceptions  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | task.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\다운로드\[멘토씨리즈] C언어(개정판)\멘토씨리즈 C언어(개정판)\day38\_c\Debug\task.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 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 This binary has an RWX section. It might contain self-modifying code  General This binary imports functions used to raise kernel exceptions  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | test.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\다운로드\[멘토씨리즈] C언어(개정판)\멘토씨리즈 C언어(개정판)\day40\_c\Debug\test.exe |
| Originator Process | explorer.exe |
| 엔진 | On-Write DFI - Suspicious |
| 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 This binary has an RWX section. It might contain self-modifying code  General This binary imports functions used to raise kernel exceptions  General This binary imports debugger functions |

|  |  |
| --- | --- |
| 파일명 | Kalmuri.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume4\Users\jinsub.kim\Desktop\Kalmuri.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] |

|  |  |
| --- | --- |
| 파일명 | FD-FFOCT\_Wojtkowski\_2019.pdf |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume7\Project\25. Task-FFOCT\20231031\_FFOCT\20231031\_FFOCT\FD-FFOCT\_Wojtkowski\_2019.pdf |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Detected in-memory hooks on AMSI DLL  MITRE : Defense Evasion [T1562.001][T1574] MITRE : Privilege Escalation [T1574] MITRE : Persistence [T1574] |

|  |  |
| --- | --- |
| 파일명 | bdcam.exe |
| 분류 | Generic.Heuristic |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\PROGRAM FILES\Bandicam\bdcam.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Injection attempt via Instrumentation Callback API  MITRE : Defense Evasion [T1055][T1562.001] MITRE : Privilege Escalation [T1055] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | veraport-g3-x64-sha2.exe |
| 분류 | Ransomware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\yg.jeong.KOHYOUNG\Downloads\veraport-g3-x64-sha2.exe |
| Originator Process | msedge.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Persistence Application registered itself to become persistent via service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Reconnaissance Network sniffing API DLL loaded  MITRE : Credential Access [T1040] MITRE : Discovery [T1040] Evasion Application added firewall rules to allow network traffic  MITRE : Exfiltration [T1041][T1048][T1020][T1030][T1029] MITRE : Defense Evasion [T1562.004] Persistence Application registered itself to become persistent via an autorun  MITRE : Persistence [T1547.001] MITRE : Privilege Escalation [T1547.001] Ransomware Suspicious file manipulation behavior - possibly Ransomware  MITRE : Impact [T1485][T1486] 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] Direct Syscall Attempt to evade monitoring with a syscall directly from the main process binary  MITRE : Defense Evasion [T1562.001] Reconnaissance A known network sniffing executable was run  MITRE : Credential Access [T1040] MITRE : Discovery [T1040] 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] 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 Detected Heaven's Gate technique in manipulated code execution  MITRE : Execution  Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] |

|  |  |
| --- | --- |
| 파일명 | LookoSmartUpdate\_Installer.exe |
| 분류 | Ransomware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\ws.kim\Downloads\LookoSmartUpdate\_Installer.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Application manipulated safe mode configuration:  MITRE : Persistence  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Injection Code was executed in a remote process  MITRE : Defense Evasion [T1055] MITRE : Privilege Escalation [T1055] Injection Process injected a DLL to another process using CreateRemoteThread/SetThreadContext  MITRE : Defense Evasion [T1055.001] MITRE : Privilege Escalation [T1055.001] Injection Process attempted to inject a DLL to another process using CreateRemoteThread/SetThreadContext  MITRE : Defense Evasion [T1055.001] MITRE : Privilege Escalation [T1055.001] Injection Code injection to a remote process  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] 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 in safe mode  MITRE : Persistence  Persistence Application registered itself to become persistent via service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Application manipulated safe mode configuration:  MITRE : Persistence  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Injection Code was executed in a remote process  MITRE : Defense Evasion [T1055] MITRE : Privilege Escalation [T1055] Injection Process injected a DLL to another process using CreateRemoteThread/SetThreadContext  MITRE : Defense Evasion [T1055.001] MITRE : Privilege Escalation [T1055.001] Injection Process attempted to inject a DLL to another process using CreateRemoteThread/SetThreadContext  MITRE : Defense Evasion [T1055.001] MITRE : Privilege Escalation [T1055.001] Injection Code injection to a remote process  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] 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 in safe mode  MITRE : Persistence  Persistence Application registered itself to become persistent via service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] |

|  |  |
| --- | --- |
| 파일명 | GCC.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume1\Program Files\GIGABYTE\Control Center\GCC.exe |
| Originator Process | None |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Suspicious library loaded into the process memory |

|  |  |
| --- | --- |
| 파일명 | GBT\_MB\_Update\_23.10.25.01.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume1\Users\백승주\_SeungjuBaek\AppData\Local\Temp\7zSB190.tmp\GBT\_MB\_Update\_23.10.25.01.exe |
| Originator Process | None |
| 엔진 | On-Write DFI - Suspicious |
| 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  General This is a Nullsoft Installer  Hiding/Stealthiness This binary may contain encrypted or compressed data as measured by high entropy of the sections (greater than 6.8) |

|  |  |
| --- | --- |
| 파일명 | AnySupportClient.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\b.seong\Downloads\AnySupportClient.exe |
| Originator Process | msedge.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | 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 an autorun  MITRE : Persistence [T1547.001] MITRE : Privilege Escalation [T1547.001] Persistence Application registered itself to become persistent via service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] 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 an autorun  MITRE : Persistence [T1547.001] MITRE : Privilege Escalation [T1547.001] Persistence Application registered itself to become persistent via service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | setup.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\b.seong\Desktop\ANSYSLICMAN\_2032R2\_WINX64\setup.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Persistence Application registered itself to become persistent via service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Persistence Application registered itself to become persistent via service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | SecureConnector.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\ForeScout SecureConnector\SecureConnector.exe |
| Originator Process | services.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion The original filename is different from its actual name  MITRE : Defense Evasion [T1036.003][T1036.005][T1574.008] MITRE : Persistence [T1574.008] MITRE : Privilege Escalation [T1574.008] General User logged on  MITRE : Persistence [T1078] MITRE : Defense Evasion [T1078] MITRE : Privilege Escalation [T1078] MITRE : Initial Access [T1078] |

|  |  |
| --- | --- |
| 파일명 | OPTICSTUDIO\_2023R2.01\_WINX64.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\b.seong\Desktop\OPTICSTUDIO\_2023R2.01\_WINX64\OPTICSTUDIO\_2023R2.01\_WINX64.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Application added firewall rules to allow network traffic  MITRE : Exfiltration [T1041][T1048][T1020][T1030][T1029] MITRE : Defense Evasion [T1562.004] Injection Suspicious library loaded into the process memory  General User logged on  MITRE : Persistence [T1078] MITRE : Defense Evasion [T1078] MITRE : Privilege Escalation [T1078] MITRE : Initial Access [T1078] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Persistence Application registered itself to become persistent via an autorun  MITRE : Persistence [T1547.001] MITRE : Privilege Escalation [T1547.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | ansyslmcenter.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\ANSYS Inc\Shared Files\licensing\winx64\ansyslmcenter.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] General Process started from shortcut file  MITRE : Execution [T1204] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | OpticStudio.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Program Files\Ansys Zemax OpticStudio 2023 R2.01\OpticStudio.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] General Process started from shortcut file  MITRE : Execution [T1204] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] General Process started from shortcut file  MITRE : Execution [T1204] |

|  |  |
| --- | --- |
| 파일명 | OPTICSBUILDERCREO4\_2023R2.01\_WINX64.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\b.seong\Desktop\OPTICSBUILDERCREO\_2023R2.01\_WINX64\OPTICSBUILDERCREO4\_2023R2.01\_WINX64.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Application added firewall rules to allow network traffic  MITRE : Exfiltration [T1041][T1048][T1020][T1030][T1029] MITRE : Defense Evasion [T1562.004] 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] Injection Suspicious library loaded into the process memory  General User logged on  MITRE : Persistence [T1078] MITRE : Defense Evasion [T1078] MITRE : Privilege Escalation [T1078] MITRE : Initial Access [T1078] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] |

|  |  |
| --- | --- |
| 파일명 | RazerInstaller.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Windows\Installer\Razer\Installer\RazerInstaller.exe |
| Originator Process | None |
| 엔진 | On-Write DFI - Suspicious |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Hiding/Stealthiness The majority of sections in this PE have high entropy, a sign of obfuscation or packing  Hiding/Stealthiness This binary may contain encrypted or compressed data as measured by high entropy of the sections (greater than 6.8)  Hiding/Stealthiness The majority of sections in this PE have high entropy, a sign of obfuscation or packing  Hiding/Stealthiness This binary may contain encrypted or compressed data as measured by high entropy of the sections (greater than 6.8) |

|  |  |
| --- | --- |
| 파일명 | NMPA\_권장임상평가경로사용지침(220714)\_원문.doc |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\sj.shin\Downloads\NMPA\_권장임상평가경로사용지침(220714)\_원문.doc |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Exploitation Document behaves abnormally  MITRE : Execution [T1059][T1203][T1204.002] MITRE : Initial Access [T1566.001] Evasion Office program loaded vbe dll, might indicate macro execution  MITRE : Execution [T1059.005][T1204] MITRE : Initial Access [T1566.001] Evasion Detected in-memory hooks on AMSI DLL  MITRE : Defense Evasion [T1562.001][T1574] MITRE : Privilege Escalation [T1574] MITRE : Persistence [T1574] |

|  |  |
| --- | --- |
| 파일명 | Microsoft Office Visio 2007.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume8\06. Util\03 Portable SW\Portable\_Microsoft Visio 2007\Microsoft Office Visio 2007.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Command line changed between process execution and main thread resumption  Evasion Attempt to evade monitoring using the Process hollowing technique  MITRE : Privilege Escalation [T1055.012] MITRE : Defense Evasion [T1055.012] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to a remote process  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Exploitation Detected suspicious shellcode API call  MITRE : Execution [T1106][T1059] MITRE : Defense Evasion [T1140] Evasion Command line changed between process execution and main thread resumption  Evasion Attempt to evade monitoring using the Process hollowing technique  MITRE : Privilege Escalation [T1055.012] MITRE : Defense Evasion [T1055.012] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to a remote process  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Exploitation Detected suspicious shellcode API call  MITRE : Execution [T1106][T1059] MITRE : Defense Evasion [T1140] |

|  |  |
| --- | --- |
| 파일명 | LookoDevTool.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\ws.kim\Desktop\LookoDevTool.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | creosvcs\_64.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\ws.kim\Downloads\MED-100WIN-CD-410\_M110\_Win64\install\addon\creosvcs\_64.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Persistence Application registered itself to become persistent via an autorun  MITRE : Persistence [T1547.001] MITRE : Privilege Escalation [T1547.001] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Persistence Application registered itself to become persistent via an autorun  MITRE : Persistence [T1547.001] MITRE : Privilege Escalation [T1547.001] |

|  |  |
| --- | --- |
| 파일명 | ALCapture310.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\ws.kim\Downloads\ALCapture310.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Injection Library was injected to a remote process  MITRE : Defense Evasion [T1055] MITRE : Privilege Escalation [T1055] 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 scheduled task  MITRE : Persistence [T1053.005] MITRE : Execution [T1053.005] MITRE : Privilege Escalation [T1053.005] Persistence Application registered itself to become persistent via service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion A new root certificate was added  MITRE : Defense Evasion [T1553.004] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Packer Process suspicious as packed  MITRE : Defense Evasion [T1027][T1480.001] |

|  |  |
| --- | --- |
| 파일명 | DCMAppInstaller.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\ws.kim\Downloads\DCMAppInstaller.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion A new root certificate was added  MITRE : Defense Evasion [T1553.004] Evasion Indirect command was executed  MITRE : Defense Evasion [T1218][T1202] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | BANDIZIP-SETUP-STD-X64.EXE |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume3\Users\ws.kim\Downloads\BANDIZIP-SETUP-STD-X64.EXE |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] 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] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.5.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.5.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.5.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.5.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Persistence Application registered itself to become persistent via an autorun  MITRE : Persistence [T1547.001] MITRE : Privilege Escalation [T1547.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | ffac7070pcl6230410w646iml.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume6\기본 SW\ffac7070pcl6230410w646iml.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Injection Suspicious library loaded into the process memory  Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.5.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.5.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.5.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.5.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.5.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.5.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.5.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.5.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.5.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.5.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | Copy\_Release.bat |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\PTVDiskVolumeZ\[000].GIT\WinIST\_V3\_Working2\Install\Copy\_Release.bat |
| Originator Process | explorer.exe |
| 엔진 | Documents, Scripts |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | HASPUserSetup.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\CdRom0\USB key for win10\HASPUserSetup.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 1회 |
| 구조/행위분석 | Persistence Application registered itself to become persistent via service  MITRE : Privilege Escalation [T1543.003][T1547.001] MITRE : Persistence [T1543.003][T1547.001] 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] 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] Evasion Manipulated code execution flow using the Heaven's Gate technique  MITRE : Execution  General User logged on  MITRE : Persistence [T1078] MITRE : Defense Evasion [T1078] MITRE : Privilege Escalation [T1078] MITRE : Initial Access [T1078] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Suspicious registry key was created  MITRE : Defense Evasion [T1112][T1027][T1564.005][T1480.001] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |

|  |  |
| --- | --- |
| 파일명 | WinIST\_3.0.1.1.6.exe |
| 분류 | Malware |
| 조치여부 | not\_mitigated |
| 탐지경로 | \Device\HarddiskVolume10\WinIST\_3.0.1.1.6.exe |
| Originator Process | explorer.exe |
| 엔진 | Behavioral AI Engine |
| 탐지 횟수 | 2회 |
| 구조/행위분석 | Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] Evasion Code injection to other process memory space during the target process' initialization  MITRE : Defense Evasion [T1055.012] MITRE : Privilege Escalation [T1055.012] Injection Code injection to other process memory space via Reflection  MITRE : Defense Evasion [T1055][T1055.002] MITRE : Privilege Escalation [T1055][T1055.002] |