이달의 보안 동향 및 대응

- '나눔로또' 판매 동행복권, 해킹으로 부정 로그인 시도... 개인정보 유출 가능성
- 전자세금계산서 솔루션 스마트빌, 해킹으로 개인정보 유출
- IBM "기업 데이터 유출 비용 사상 최고치 갱신"
- 北 해킹 조직 '킴수키'에 前장관 등 1468명 털렸다

보안뉴스 요약

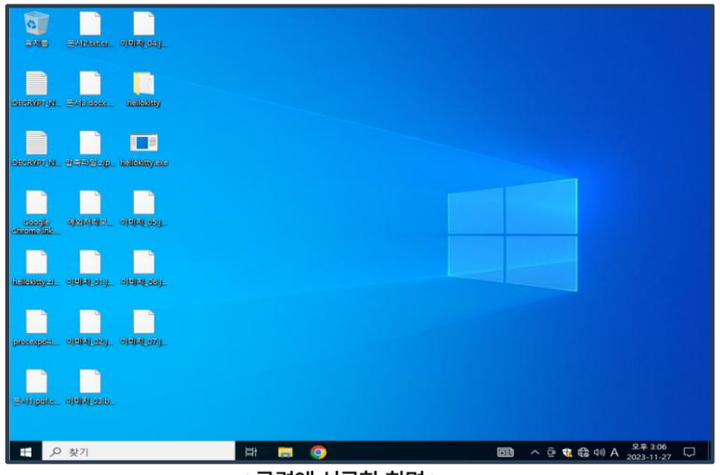
보안뉴스 23.11.03
아파치 액티브MQ에서 발견된 최고 등급 취약점, 헬로키티 랜섬웨어 단체가 공략 중

헬로T 23.11.08
3분기 신규 랜섬웨어 공격 비중 17.6%...능동적인 조치 필요

보안뉴스 23.11.14
로얄, 한 해 동안 350개 조직 침해해 2억 7500만 달러 요구

디지털데일리 23.11.25
랜섬웨어 당한 골프존, 작년 정보보호에 20억원 썼지만… 개인정보 유출은 없나?

이달의 랜섬웨어 HelloKitty



< 공격에 성공한 화면 >

< trueEP의 차단 화면 >

침투

원격 코드 실행 취약점을 통한 배포

1) 아파치 서버 원격 코드 취약점을 통한 익스플로잇 공격

» 침투단계에서 trueEP의 대응

- trueEP는 순수 행위기반 방어 원리로 프로세스가 행위를 하기 이전인 침투 단계에서는 대응하지 않음

공격준비

프로세스 및 서비스 강제 종료

- 원활한 감염을 위한 프로세스 강제 종료
- 시스템 백업 및 섀도우 복사본 삭제

» 공격준비단계에서 trueEP의 대응

- 사용자입력 없는 정보탈취 행위 차단
- 기타 준비 단계에서의 행위가 trueEP 행위기반 알고리즘에 위배될 경우 차단
- 공격대상 폴더 및 파일 목록 식별 행위 차단
- MS백업 무력화 공격 차단 (옵션)

공격

유포된 악성코드 실행

- "<filename>. Crypt"으로 데이터 암호화
- "DECRYPT-NOTE.txt" 랜섬노트 생성

» 공격단계에서 trueEP의 대응

- 사용자입력 없는 암호화 행위 차단
- 행위 차단 시 프로세스 킬

랜섬웨어 상세 분석

HelloKitty

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 아파치 액티브엠큐 서버(Apache ActiveMQ Server)의 취약점 CVE-2023-46604를 통한 침투	**trueEP는 인바운드 영역에는 개입하지 않음** • 시그니처 기반 제품들의 방어 영역 • 악성코드가 파일 상태로만 존재하며 행위는 없는 단계 **trueEP는 악성코드가 프로세스로 실행되어 실공격 행위를 하는 단계에서 탐지하고 차단하는 원리임.**
공격준비	1) 원활한 감염을 위한 약 1,500개 이상의 프로세스 및 서비스 강제 종료 • "C:₩Windows₩System32₩net.exe" stop MSSQLServerADHelper10 • "C:₩Windows₩System32₩taskkill.exe" /f /im mysql* 2) 시스템 백업 및 섀도우 복사본 삭제	**trueEP는 계정을 탈취하고, 권한을 상승 등 일련의 진행 과정에서 trueEP 행위기반 알고리즘에 위배될 경우, 이를 탐지하여 차단함** • 사용자입력 없는 정보탈취 행위 차단 • 기타 준비 단계에서의 행위가 trueEP 행위기반 알고리즘에 위배될 경우 차단 • MS백업 무력화 공격 차단 (옵션)
공격	1) 공격 대상 폴더 및 파일 목록 식별 2) "<filename>. Crypt"으로 데이터 암호화 3) "DECRYPT-NOTE.txt" 랜섬노트 생성	**trueEP는 사용자 입력이 없는 파일 암호화 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위를 차단** • 공격대상 폴더 및 파일 목록 식별 행위 차단 • 사용자입력 없는 암호화 행위 차단 • 행위 차단 시 프로세스 킬

Royal

단계	사용된 기법	trueEP의 대응
공격준비	1) Cobalt Strike를 배포하여 원격으로 시스템 액세스 및 권한 상승을 위한 공격 도구로 사용 2) "delete shadows /all /quiet" 명령줄과 함께 Vssadmin.exe 프로세스를 사용하여 섀도 복사본 백업을 삭제	**trueEP는 계정을 탈취하고, 권한을 상승 등 일련의 진행 과정에서 trueEP 행위기반 알고리즘에 위배될 경우, 이를 탐지하여 차단함** • 윈도우 백업 삭제 행위 차단(옵션) • MS백업 무력화 공격 차단 (옵션)
공격	1) 공격 대상 폴더 및 파일 목록 식별 2) "<filename>. royal"으로 데이터 암호화 3) "README.TXT" 랜섬노트 생성	**trueEP는 사용자 입력이 없는 파일 암호화 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위를 차단** • 공격대상 폴더 및 파일 목록 식별 행위 차단 • 사용자입력 없는 암호화 행위 차단 • 행위 차단 시 프로세스 킬