# Truecut Security News Letter
# 23년 3월 간추린 보안 이슈
Truecut Security, LAB

## 이달의 보안 동향 및 대응

- '탈옥'한 챗GPT, 멀웨어·랜섬웨어 제작 방법 술술…. 사이버 범죄 우려
- 러-우 전쟁 1년간 사이버 공격 3배 증가, 우리나라는 안전할까?
- 우려가 현실로…삼성전자, 챗GPT 빗장 풀자마자 '오남용' 속출
- HP "사이버 위협 진화로 엔드포인트 보안 솔루션 필요성 커져"
- 락빗 랜섬웨어 조직, "한국 국세청 해킹했다…해킹 파일 공개 예정" 주장

## 보안뉴스 요약

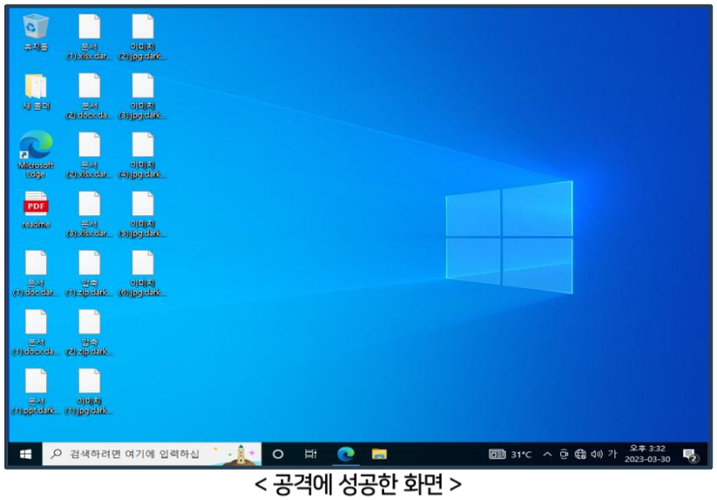
보안뉴스 23.03.05
**GlobeImposter 랜섬웨어, RDP 통해 재확산 중…**

보안뉴스 23.03.20
**미국, 유럽, 호주 노리는 새로운 랜섬웨어, 트리고나**

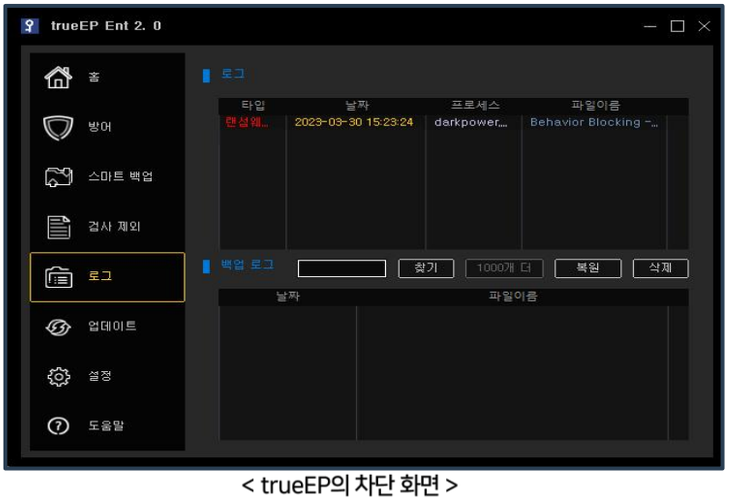
CCTV뉴스 23.03.22
**페라리, 랜섬웨어 공격 받아 일부 고객 정보 유출**

보안뉴스 23.03.27
**새로 나타난 다크파워 랜섬웨어, 한 달 만에 10개 조직 침해**

## 이달의 랜섬웨어 Dark power



< 공격에 성공한 화면 >




< trueEP의 차단 화면 >

### 침투

**피싱 메일에 악성파일을 첨부하여 유포**

- 피싱 메일 유포
- 메일 첨부 파일에 포함된 악성 스크립트 파일 실행

**» 침투단계에서 trueEP의 대응**

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

### 공격준비

**드라이브 순차 탐색**

- 특정 서비스 및 프로세스가 식별되면 종료 시도(악성코드 행위 모니터링 목적 프로세스)
- VSS(Volume Shadow Copy Service), 데이터 백업 서비스 및 맬웨어 방지 제품 중지

**» 공격준비단계에서 trueEP의 대응**

- 공격대상 폴더 및 파일 목록 식별행위 차단
- 백신 무력화 행위 차단(옵션)

### 공격

**유포된 악성코드 실행**

- 공격 대상 폴더 및 파일 목록 식별
- 특정 경로와 확장자를 제외한 모든 파일을 대상으로 암호화
- '*.dark_power' 파일명으로 변경

**» 공격단계에서 trueEP의 대응**

- 사용자행위 없는 자료 유출 행위 차단
- 해당 프로세스를 중단시켜 악성행위 차단


## 랜섬웨어 상세 분석

### Dark power

| 단계 | 사용된 기법 | trueEP의 대응 |
|---|---|---|
| 침투(유포) | 1) 피싱 메일에 악성파일을 첨부하여 유포<br>2) 익스플로잇 또는 RDP(Remote Desktop Protocol)접근 방식으로 시스템에 침투 | **trueEP는 인바운드 영역에는 개입하지 않음**<br>• 시그니처기반 제품들의 방어 영역<br>• 악성코드가 파일형태로 존재하는 실공격 이전의 단계<br><br>trueEP는 악성코드가 프로세스로 실행되어 실공격 행위를 하는 단계에서 탐지하고 차단하는 원리임. |
| 공격준비 | 1) 특정 서비스 및 프로세스가 식별되면 종료 시도<br>- (악성코드 행위 모니터링 목적 프로세스)<br>2) VSS(Volume Shadow Copy Service), 데이터 백업 서비스 및 맬웨어 방지 제품 중지<br>3) 백그라운드에서 악성행위 동작 (공격 대상 폴더 및 파일 목록 식별) | **trueEP는 사용자 행위 없는 레지스트리 접근 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위 차단**<br><br>1) 공격대상 폴더 및 파일 목록 식별행위 차단<br>2) 백신 무력화 행위 차단(옵션) |
| 공격 | 1) 특정 경로와 확장자를 제외한 모든 파일을 대상으로 암호화<br>2) WMI 쿼리 "Select * from Win32_NTEventLogFile" 및 "ClearEventLog()"를 사용하여 시스템 로그 삭제<br>3) '*.dark_power' 파일명으로 변경 | **trueEP 사용자 입력이 없는 파일 암호화 행위를 탐지하는 순간에 프로세스를 중단시켜 악성행위를 차단**<br><br>1) 사용자행위 없는 자료 유출 행위 차단<br>2) 해당 프로세스를 중단시켜 악성행위 차단 |

### Motalkombat

| 단계 | 사용된 기법 | trueEP의 대응 |
|---|---|---|
| 침투(유포) | 1) 원격 제어(RDP) 접근 방식으로 시스템에 침투하여 랜섬웨어를 실행<br>2) 메일 첨부 파일에 포함된 악성 스크립트 파일 실행 시 외부 서버로부터 추가 다운로드를 통해 랜섬웨어 감염이 이루어지는 방식<br>3) 한국에서 널리 사용되는 한글 워드 프로세서에서 발견된 오래된 EPS 취약점(CVE-2017-8291)을 악용 | **trueEP는 인바운드 영역에는 개입하지 않음**<br>• 시그니처기반 제품들의 방어 영역<br>• 악성코드가 파일형태로 존재하는 실공격 이전의 단계<br><br>trueEP는 악성코드가 프로세스로 실행되어 실공격 행위를 하는 단계에서 탐지하고 차단하는 원리임. |
| 공격준비 | 1) 'cmd.exe'를 통해 PowerShell 스크립트를 실행하는 '실행' 레지스트리 키에 새 값('RyPO')을 추가<br>2) Windows컴퓨터에 연결된 장치 검색 후 감염PC에 파일 복사 | **trueEP는 사용자 행위 없는 레지스트리 접근 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위 차단**<br><br>1) 시스템 레지스트리 접근 시 차단<br>2) 매체제어 로그 설정(옵션) |
| 공격 | 1) 특정 경로와 확장자를 제외한 모든 파일을 대상으로 암호화<br>2) '*.Remember_you_got_only_24_hours_to_make_the_payment_if_you_dont_pay_prize_will_triple_Mortal_Kombat_Ransomware' 파일명으로 변경<br>3) 파일이 암호화된 모든 폴더에 "HOW TO DECRYPT FILES.txt" 랜섬 노트 파일이 생성 | **trueEP는 사용자 입력이 없는 파일 암호화 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위를 차단**<br><br>1) 공격대상 폴더 및 파일 목록 식별 행위 차단<br>2) 사용자입력 없는 파일 암호화 행위 차단 |