이달의 보안 동향 및 대응

- 보안 담당자들, 최근 불거진 '모압 사건'을 어떤 식으로 받아들여야 할까?
- 日 외무성 극비 전산망, 중국에 뚫렸었다... 日 언론 보도
- "中지원 해커에 군 전산망 뚫렸다"…네덜란드, 해킹 사실 공개
- 국내 대학 등 100곳 해킹… 中해커 소행인듯
- 방글라데시 해커, 이스라엘 지원 이유로 한국은행 등 디도스 공격 감행했다
- "北, 국내 '콜드론치' 기술 탈취해 SLBM 개발 단축"

보안뉴스 요약

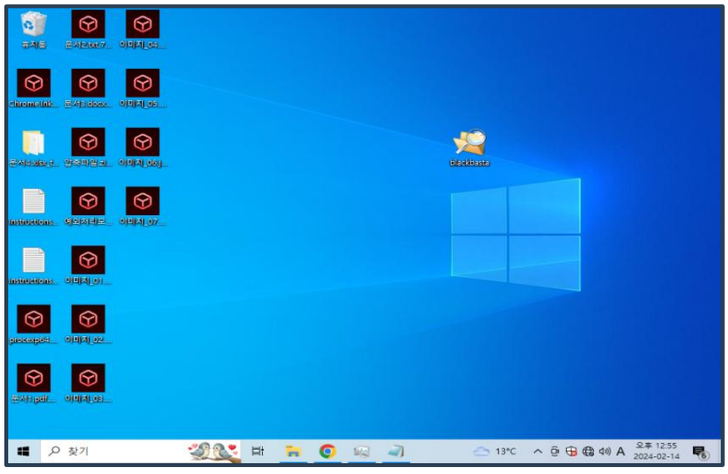
ITWORLD 24.02.07
"2023년 랜섬웨어 피해자 수 1년새 약 50% 증가"

보안뉴스 24.02.13
블랙바스타에 당한 현대자동차 유럽, 3TB 데이터 침해돼

동아일보 24.02.20
"AI 활용한 랜섬웨어-악성코드로 사이버 공격 늘어"

보안뉴스 24.02.21
국제 공조로 무력화 된 록빗 랜섬웨어, "공격 인프라부터 소스코드, 복호화 키까지"

이달의 랜섬웨어 Blackbasta



< 공격에 성공한 화면 >

< trueEP의 차단 화면 >

침투

취약점을 통한 시스템 접근

- Microsoft Exchange Server의 ProxyShell 취약점을 통해 피해자 시스템 접근

» 침투단계에서 trueEP의 대응

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

공격준비

네트워크 스캐닝 및 측면 이동

- 호스트에 대한 자격 증명 수집
- 네트워크를 통해 파일 암호화 멀웨어 배포
- 방화벽 정책 변경, 레지스트리 값 수정
- PsExec, RDP등을 사용하여 네트워크 확산 진행

» 공격준비단계에서 trueEP의 대응

- 준비 단계에서의 행위가 trueEP 행위기반 알고리즘에 위배될 경우 차단
- 시스템 레지스트리 접근 시 차단

공격

유포된 악성코드 실행

- "<filename>. [random]"으로 데이터 암호화
- 섀도우 복사본 삭제
- "instructions_read_me.txt" 랜섬노트 생성

» 공격단계에서 trueEP의 대응

- 사용자입력 없는 암호화 행위 차단
- 행위 차단 시 프로세스 킬

랜섬웨어 상세 분석

Blackbasta

단계	사용된 기법	trueEP의 대응
침투(유포)	1) Microsoft Exchange Server의 ProxyShell 취약점을 통해 피해자 시스템 접근	**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) Random-letters.ico 및 Random-letters.jpg 파일을 %TEMP% 디렉터리 쓴 후 바탕화면 변경 2) 호스트에 대한 자격 증명 수집 후 네트워크를 통해 파일 암호화 멀웨어 배포 3) Net.exe을 사용하여 권한 추가 및 변경, netsh.exe를 사용하여 방화벽 정책 변경, reg.exe를 사용하여 레지스트리 값 수정 4) PsExec, RDP등을 사용하여 네트워크 확산 진행	**trueEP는 계정을 탈취하고, 권한을 상승 등 일련의 진행 과정에서 trueEP 행위기반 알고리즘에 위배될 경우, 이를 탐지하여 차단함** 1) 시스템 레지스트리 접근 시 차단 2) 파일 유출진행 시 유출차단 알고리즘에 의한 이중방어 진행
공격	1) “<filename>. [random]”으로 데이터 암호화 2) 섀도우 복사본 삭제 3) “instructions_read_me.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

Crysis

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 원격 데스크톱 프로토콜(Remote Desktop Protocol, RDP) 및 터미널 서비스를 통해 원격 접근하여 공격자가 직접 랜섬웨어(Ransomware)악성 파일 실행	**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) 네트워크 스캐닝 및 계정 정보 수집 진행 2) Windows 방화벽에서 파일 및 프린터 공유 설정 3) 볼륨 섀도 복사본 제거	**trueEP는 사용자 행위 없는 레지스트리 접근 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위 차단** • MS백업 무력화 행위 차단(옵션) 1) %programdata% 디렉토리 선감시
공격	1) 공격 대상 폴더 및 파일 목록 식별 2) “<filename>. [random].[zohodzin@tuta.io].z1n.”으로 데이터 암호화	**trueEP 사용자 입력이 없는 파일 암호화 행위를 탐지하는 순간에 프로세스를 중단시켜 악성행위를 차단** • 사용자입력 없는 파일 암호화 행위 차단 • 행위 차단 시 프로세스 킬