22년 07월 간추린 보안 이슈

2022. 07. 31

트루컷시큐리티 기술연구소

이 달의 보안 동향 및 대응

●랜섬웨어 공격자들이 자료까지 탈취하는 경우가 크게 증가함.
> 복구비를 지불하지 않는 경우에 대비한 이중압박 목적으로, 자료유출 공격에 대한 대비의 필요성이 크게 대두됨.

●침투 및 방어제품 우회 단계에서 진화된 기법을 보임.
> 반면 실제 암호화하는 단계에서는 이전과 크게 달라진 것이 없어, 트루이피 알고리즘의 방어 범주를 벗어나지 못하는 것을 확인.

●버그바운티를 통해 랜섬웨어 완성도를 높이려는 시도가 나타남.

●특정 대상을 공격하는 타겟형 랜섬웨어가 주류를 이루었음.
> 불특정 다수를 대상으로 하는 공격은 줄어드는 추세임.

간추린 보안 뉴스

매일경제 22.07.19
삼성전자까지 털렸다...재택 근무 PC도 해킹 표적

PC·노트북·휴대폰 포함한 `엔드포인트` 보안 중요해져
신종 악성코드 계속 생겨서 기존 백신으론 대응 불가능

매일경제 22.07.21
방화벽으로도 못 막는 클라우드 해킹 급증

랜섬웨어 감염 후 비용을 지불하고도 데이터 복구에 실패하는 기업이 늘고 있다는 조사결과가 나왔다.

동아경제 22.07.22
기업들, 랜섬웨어 비용 지불하고 복구 못해

랜섬웨어 감염 후 비용을 지불하고도 데이터 복구에 실패하는 기업이 늘고 있다는 조사결과가 나왔다.

보안뉴스 22.07.22
정보 탈취 악성코드 '에이전트 테슬라' 국내서 기승

인포스틸러 악성코드 AgentTesla(1위)와 Formbook(3위),
다운로더 악성코드 'GuLoader' 등 유포

한경닷컴 22.07.25
비즈니스로 진화하는 랜섬웨어...

작년 랜섬웨어 피해 76% 증가, KISA, 올 1분기 70종 탐지, 이 중 50종은 변종

한국일보 22.07.26
국내 대형 제약사도 '랜섬웨어' 공격당했다

대형제약사 A사, "25일 랜섬웨어 공격받아"
"오프라인으로 업무 보고, 구두 보고로 진행"

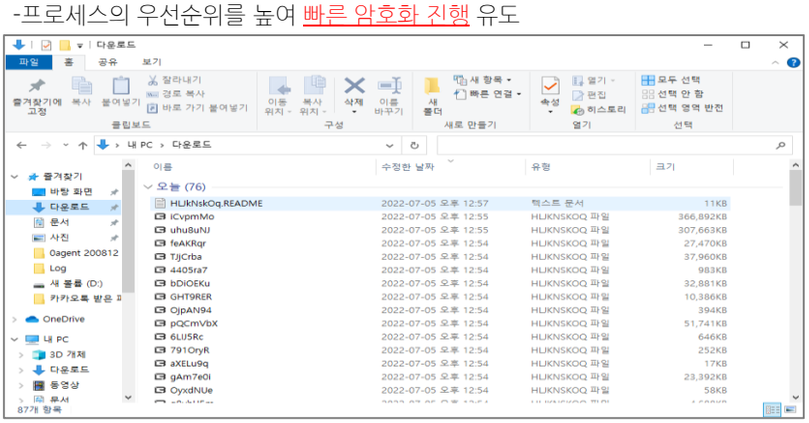
이달의 랜섬웨어 차단보고

Lockbit 3.0 - 최근 가장 활동량이 높은 랜섬웨어

랜섬웨어 유형
-악명 높은 비너스락커(VenusLocker) 조직에 의한 RaaS 유형
-랜섬웨어가 직접 유포되는 것이 아니고 피싱메일 클릭 시 다운로드되는 유형

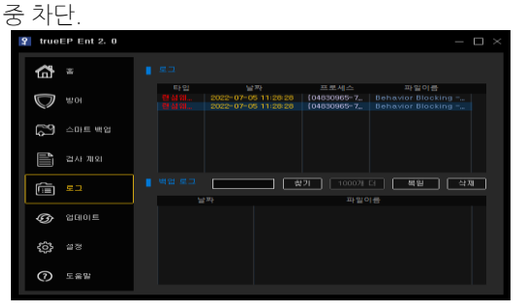
유포 방식
-입사지원서로 위장한 피싱 메일로 유포
-아래한글(hwp) 아이콘으로 위장한 실행파일(exe)을 유포
-랜섬웨어 완성도를 높이기 위한 버그바운티도 병행

동작 방식
-자료탈취 및 파일 암호화 공격을 동시에 진행하는 방식으로 공격
-파일명과 확장자를 [랜덤한 6자리].[랜덤한 9자리] 문자열 형식으로 변경
-기존 파일이 어떤 것이었는지 식별 불가
-보안서비스 및 특정 서비스를 무력화한 후에 공격
(sppsvc-MS 소프트웨어 보호 플랫폼 서비스,WinDefend-윈도우디펜더,
wscsvc-보안센터 알림,vmvss-VMWare서비스,VSS-Volume Shadowcopy)
-프로세스의 우선순위를 높여 빠른 암호화 진행 유도



〈 공격에 성공한 화면 〉

트루이피에 의한 공격 방어
-LockBit 3.0은 "일부 서비스"를 무력화시키고 침투하는 진화된 형태를 보이고 있으나, 공격단계에서는 트루이피 행위기반 방어알고리즘의 방어 범주를 벗어나지 못하고 있는 것으로 확인되었음.
-자료탈취공격을 선행할 경우, 트루이피의 유출차단 알고리즘에 의해 자료유출 및 암호화 이중 차단.



〈 트루이피가 LockBit 3.0을 차단한 화면 〉

랜섬웨어 상세 분석

LockBit 3.0

단계	사용된 기법(빨간색은 새롭게 적용된 기법)	트루이피의 대응
침투(유포)	1) 피싱 메일로 유포(국내에서는 저작권 위반, 입사지원서 등을 사칭) 2) 불특정 다수가 아닌 기업을 타겟팅하여 유포 3) 버그바운티 도입(제품의 문제에 신속하게 대응하고 계속해서 발전하겠다는 의지 표명) 4) 분석을 회피하기 위해 다양한 분석 방지 기술 사용 -코드 패킹, 난독화 및 함수 주소의 동적 해결, 함수 트램폴린 및 안티 디버깅 기술 등 세계에서 가장 빠르고 안정적인 랜섬웨어라고 주장	트루이피는 인바운드 영역에는 개입하지 않음 -시그니처기반 제품들의 영역 -이 단계에선 파일형태로 존재하며, 공격행위가 존재하지 않음 트루이피는 프로세스 형태로 실행되어 행위가 발생하는 단계에서 보안기능을 수행
공격준비	1) 복구를 막기 위해 볼륨 섀도우 복사본을 삭제 2) 특정 서비스 및 프로세스가 식별되면 종료 시도 3) 자신의 복사본을 %programdata% 디렉터리에 쓴 다음 이 프로세스에서 시작 4) 실행 시 특정 암호를 요구하며, 암호는 샘플 혹은 캠페인 마다 고유 - 암호를 복구하지 못하면 동적 및 샌드박스 분석을 불가능하게 함 5) 공격 중 절전모드 전환이나 화면 꺼짐을 막기 위해 SetThreadExecutionState 함수 사용 6) 관리자 권한으로 실행되며, 권한이 없는 경우 UAC 우회 시도	트루이피는 아래 각 행위 탐지시 차단 -행위 차단시 프로세스 킬 1) 볼륨 섀도우 복사본 삭제행위 차단(옵션) 2) 백신서비스 종료 행위 차단 3) %programdata% 디렉토리 선감시
공격	1) 공격 대상 폴더 및 파일 목록 식별 2) 자료 탈취와 암호화 공격을 동시에 실행 3) 여러 작업을 병렬로 수행하기 위해 다양한 스레드를 생성하여 빠르게 암호화 진행 4) 암호화 후 이전 파일명을 알아 볼 수 없도록 파일명을 임의의 문자열로 바꿈. 5) 확장자는 캠페인 또는 샘플마다 다르게 변경("HLJkNskOq" 및 "futRjC7nx" 확인)	트루이피는 아래 각 행위 탐지시 차단 -행위 차단시 프로세스 킬 1) 공격대상 폴더 및 파일 목록 식별행위 차단 2) 사용자입력없는 자료유출 행위 차단 3) 사용자입력없는 암호화 행위 차단

☞ 세계에서 가장 빠르고 안정적이라고 주장하는 랜섬웨어지만, 트루이피의 방어 알고리즘에 의해 선제적으로 차단됨을 확인함

Gwisin(귀신)

단계	사용된 기법(빨간색은 새롭게 적용된 기법)	트루이피의 대응
침투(유포)	1) 국내 특정 기업을 대상으로 제작 유포 - 해외 사례는 발견되지 않음 2) 국내 사정에 능통한 해커가 가담했거나 북한 해커일 것으로 추정 3) MSI 설치 파일 형태로 유포(매그니베로와 동일-단 매그니베르는 불특정 다수에게 유포) 4) 윈도우 및 리눅스, VMware 가상머신까지 모두 공격 대상 5) 서버를 장악하여 내부 시스템에 전파하는 것으로 추정 사례가 많지 않고, 실행 조건을 찾기 어려움(분석을 하지 못하도록 방어)	트루이피는 인바운드 영역에는 개입하지 않음 -시그니처기반 제품들의 영역 -이 단계에선 파일형태로 존재하며, 공격행위가 존재하지 않음 트루이피는 프로세스 형태로 실행되어 행위가 발생하는 단계에서 보안기능을 수행
공격	1) 공격 대상 폴더 및 파일 목록 식별 2) 자료 탈취와 암호화 공격을 동시에 실행 3) 백신 프로그램을 무력화 하고 공격 4) 실행 시 특별한 인자값을 요구 - 보안제품의 탐지 미 디버깅 방해 목적 5) 윈도우 정상 프로세스에 인젝션하여 공격 - 리스크가 크지만, 백신 회피를 위한 목적으로 추정 6) DLL 내부에 피해 기업정보 존재(랜섬노트에도 표시) 7) 안전모드로 강제 재부팅한 후 암호화 공격 8) 파일 확장자를 피해기업의 이름으로 변경	트루이피는 아래 각 행위 탐지시 차단 -행위 차단시 프로세스 킬 1) 공격대상 폴더 및 파일 목록 식별행위 차단 2) 사용자입력없는 자료유출 행위 차단 3) 사용자입력없는 암호화행위 차단 4) 백신서비스 종료 행위 차단 5) 안전모드 방어 활성화

☞ 실행을 위한 인자값을 요구하고, 윈도우 프로세스에 인젝션하는 등 상당한 기술력을 갖춘 랜섬웨어로 추정되고 있지만,
트루이피 행위차단 알고리즘의 차단 조건에 해당하는 행위가 포함 (5가지 이상) 되므로 방어가 가능할 것으로 추정.