「기술문서」

스피어피싱 공격 타깃별 피해 시나리오 분석

악성행위에 사용되는 도구를 중심으로

인터넷침해대응센터 KrCERT/CC KOREA INTERNET SECURITY CENTER

과학기술정보통신부 KISA 한국인터넷진흥원

CONTENTS

집　　필 : 침해사고분석단 종합분석팀
이슬기 선임, 이재광 팀장

감　　수 : 신대규 본부장, 이동근 단장

KISC KrCERT/CC KOREA INTERNET SECURITY CENTER
인터넷침해대응센터
KrCERT/CC
KOREA INTERNET SECURITY CENTER

1. 서론

o 최근 대형 침해사고로 이어지는 공격들은 특정 타깃을 오랜 기간 관찰(Reconnaissance)하여 정보를 획득하고, 스피어 피싱과 같은 타깃형 공격을 이용해 내부 네트워크로 침투하는 전략이 주로 사용된다.

o 타깃형 공격에 대응하기 위해서 공격 타깃의 업무특성 및 보유자산으로 인한 피해 분석과 추가 발생 가능한 공격에 대한 예측이 필요하다. 하지만, 특정 타깃별로 어떠한 침해사고가 발생할 수 있는지 모호하다는 문제점이 존재한다. 따라서 자사의 위협 노출에 대하여 구체적으로 문제점을 파악하고 관리적/기술적 대응방안을 마련하기 위해서는, **공격 타깃과 공격 기법에 따른 기존 사고 사례 분석이 수반되어야 한다.**

o 최근 TTPs(Tactics, Techniques, Procedures) 단위로 공격자 혹은 공격그룹을 프로파일링하는 트렌드가 유행하고 있는데, 이는 IoCs(Indicators of Compromise) 단위의 단발성 대응이 아니라, TTPs 분석을 통해 지속적으로 공격을 대응할 수 있기 때문이다. 하지만 공격자 중심의 분석과는 다른 관점, 방어자 관점에서 피해 발생 가능한 유형을 구분하고, 방어 전략을 마련할 수 있는 연구는 미진한 실정이다. 위의 문제점을 해결하기 위하여, **'한국인터넷진흥원'은 방어자가 구체적인 방어 전략을 수립할 수 있도록 공격 타깃별 발생할 수 있는 침해사고 시나리오 분석과 공격도구가 어떠한 기능을 사용하는지 소개한다.**

o 구체적으로 설명하면, 본 보고서에서는 **타깃이 보유하고 있는 자산으로 인하여 기업에게 미치는 피해를 분석하고, 최종적으로 감염된 악성코드가 어떠한 행위를 할 수 있는지 설명한다.** 이를 위하여 침해사고에서 보편적으로 이용되는 악성코드가 어떠한 기능을 갖추고 있으며, 손쉽게 이용가능한지 소개한다. 또한, 시나리오를 구현 및 검증함으로써, 제안하는 시나리오가 실제로 발생할 수 있는 현실이고, 자사에 발생할 수 있는 실질적 위협임을 인식시키고자 한다.

o 본 보고서를 통해 얻고자 하는 기대효과는, 각 기업에서 **자사의 보안현황을 점검**하고 **구체적인 방어 전략을 수립**하는 등의 보안활동이 수반되어, 기업의 전체적인 대응 수준을 제고하게 되기를 희망한다.

< 참고 >

o 공격자가 최초 침투(Initial Access)를 위해 채택하는 보편적인 전략이 스피어 피싱이다. 공격 타깃을 오랜 기간 관찰(Reconnaissance)하여 타깃 정보를 획득하고, 스피어 피싱을 통해 내부 네트워크로 침투하는 것이 최근 침해사고에서 많이 나타나므로 스피어 피싱을 기반으로 시나리오를 선정하였다.

o 또한, 스피어 피싱은 **타깃 별로 피해 범위와 위험수준**이 다르기 때문에, 방어자는 직무 특성으로 인한 위협요인(보유자산 등)을 고려하여 방어전략을 마련할 수 있다.

2. 스피어피싱 타깃별 피해 시나리오

o 이하 시나리오(2건)에서는 IT 환경에서 주요 역할을 수행하는 개발자와 서버관리자에게 직접적인 침투 시도가 발생하고, 각 타깃이 보유한 자산과 역할로 인해 침해사고가 어떻게 특화되는지 서술한다.

시나리오 1	(개발자) 소스코드 저장소 계정 탈취 → 전사 소스코드 유출

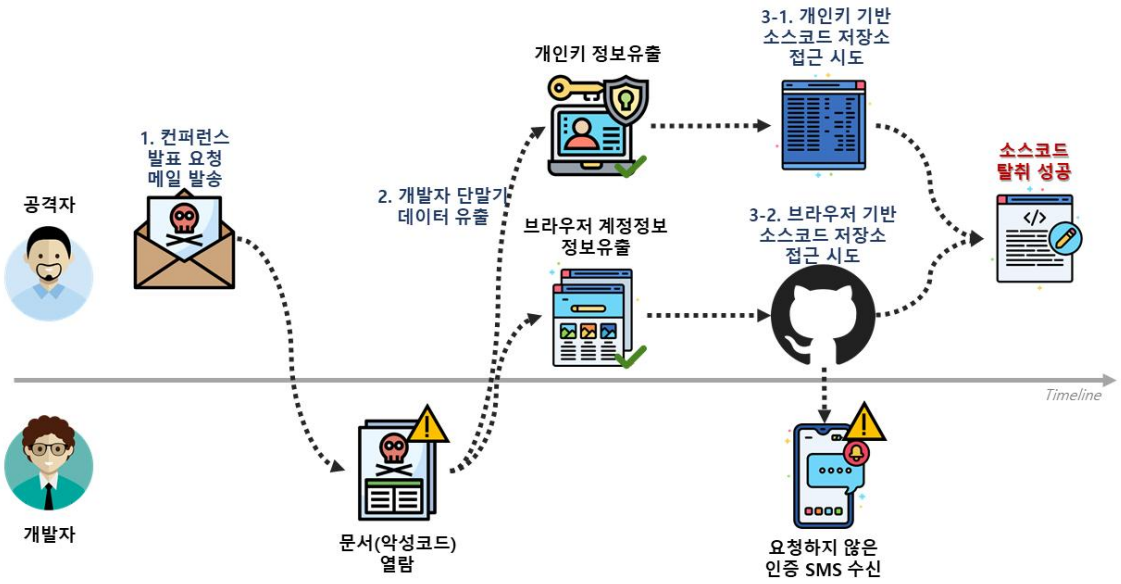
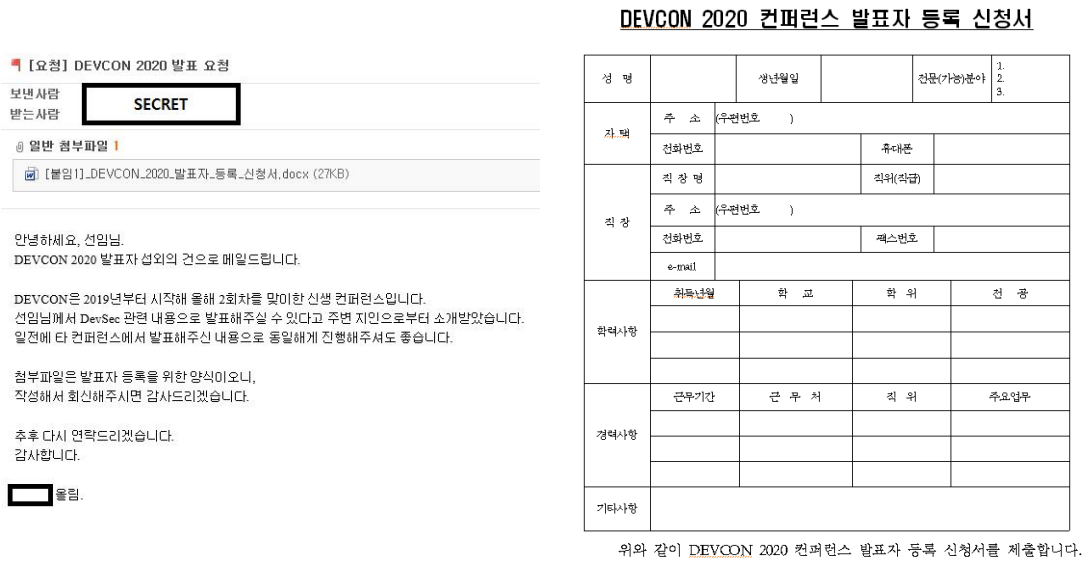


그림 2-1. 개발자 단말기 감염으로 인한 소스코드 탈취 시나리오

1. 스피어 피싱 메일(개발자 컨퍼런스 발표요청, 정보유출 기능-문서형 악성코드 첨부) 발송



[요청] DEVCON 2020 발표 요청

보낸사람 SECRET
받는사람

일반 첨부파일 1

[붙임1]_DEVCON_2020_발표자_등록_신청서.docx (27KB)

안녕하세요, 선임님.
DEVCON 2020 발표자 섭외의 건으로 메일드립니다.

DEVCON은 2019년부터 시작해 올해 2회차를 맞이한 신생 컨퍼런스입니다.
선임님께서 DevSec 관련 내용으로 발표해주실 수 있다고 주변 지인으로부터 소개받았습니다.
일전에 타 컨퍼런스에서 발표해주신 내용으로 동일해게 진행해주셔도 좋습니다.

첨부파일은 발표자 등록을 위한 양식이오니,
작성해서 회신해주시면 감사드리겠습니다.

추후 다시 연락드리겠습니다.
감사합니다.

[redacted] 올림.

DEVCON 2020 컨퍼런스 발표자 등록 신청서

성 명		생년월일		전문(가능)분야	1. 2. 3.
자택	주 소 (우편번호)				
	전화번호		휴대폰		
직 장	직 장 명		직위(직급)		
	주 소 (우편번호)				
	전화번호		팩스번호		
	e-mail				
학력사항	취득년월	학 교	학 위	전 공	
경력사항	근무기간	근 무 처	직 위	주요업무	
기타사항					

위와 같이 DEVCON 2020 컨퍼런스 발표자 등록 신청서를 제출합니다.

그림 2-2. 스피어 피싱 메일 본문 및 신청서 양식으로 위장한 문서형 악성코드(예시)

2. 감염된 개발자 컴퓨터 데이터(자격증명, 인증서, 작업 이력 등) 유출

o 개발자 컴퓨터의 계정정보는 OS 혹은 서드파티 애플리케이션(웹브라우저, 비밀번호 관리 프로그램 등)에 저장되는 경향이 있다. 또한, 그 외에도 개발 편의성을 위하여 아래와 같이 평문으로 노출된 아이디, 비밀번호를 파일로 저장하는 경우가 많다.

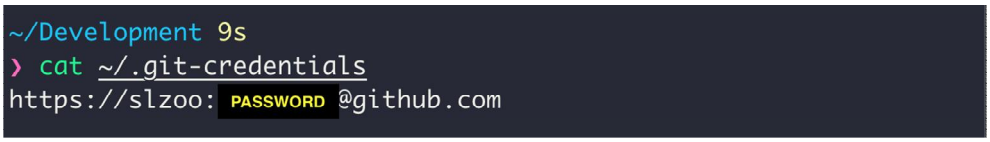


그림 2-3. 자격증명 정보를 포함한 파일기반 저장소 접근 및 소스코드 유출

o 웹브라우저에 자격증명을 저장하는 경우, 아래 그림 2-4와 같이 간단한 스크립트를 통해 저장된 자격증명 평문과 방문이력 등을 확인할 수 있다. 따라서 로컬 컴퓨터에서 아래 코드가 실행되지 않도록 방지해야 하며, 무엇보다 핵심적인 자격증명 정보를 웹 브라우저에 저장하지 않는 것이 중요하다.

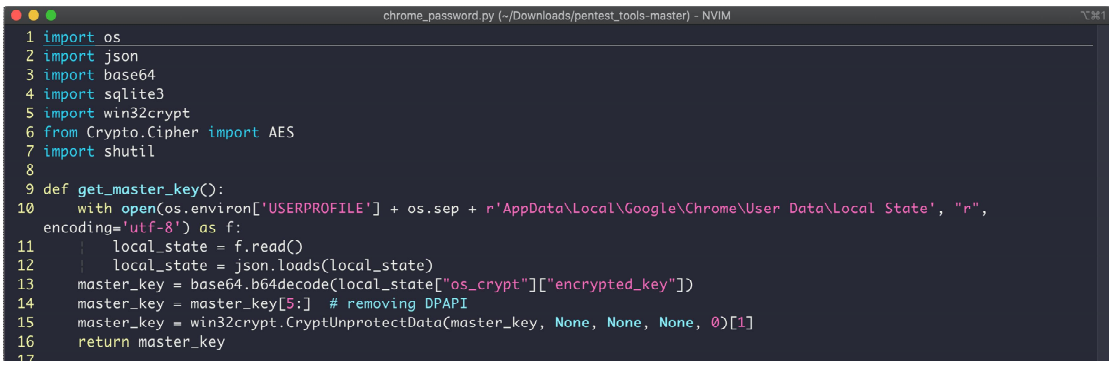


그림 2-4. Google Chrome에 저장된 자격증명 평문 추출코드(Windows)

3-1. 개발자 작업 기록을 검색하여 저장소 주소 획득 → ssh 개인키를 이용한 소스코드 유출

o 내·외부 소스코드 저장소에 접근할 때, 보편적으로 많이 사용되는 방식이 공개키 알고리즘을 이용한 인증 방식이다. 소스코드 저장소에는 공개키를 저장해두고, 접근하려는 단말기의 개인키를 이용해 인증하는 방식으로 데이터를 교환한다.

o 로컬 컴퓨터가 장악되었을 때, 공격자는 방어자의 작업 히스토리(~/.zsh_history)와 개인키(~/.ssh/id_rsa) 등에도 접근할 수 있다. 두 개의 파일이 공격자에게 전달되었을 경우 공격자는 작업 히스토리를 확인하여 소스코드 저장소 대상을 알 수 있다.

그림 2-5. 작업 히스토리 내 외부 소스코드 저장소 타겟 확인

o 위의 확인된 소스코드 저장소를 대상으로 등록된 공개키에 매칭되는 개인키를 확보한 공격자는 소스코드를 다운로드 할 수 있다. 아래 그림 2-6는 개인키가 없었을 때는 권한이 없어 저장소로 접근하지 못하지만, 개인키 확보 후 인증에 성공, 소스코드를 다운로드한 결과이다.

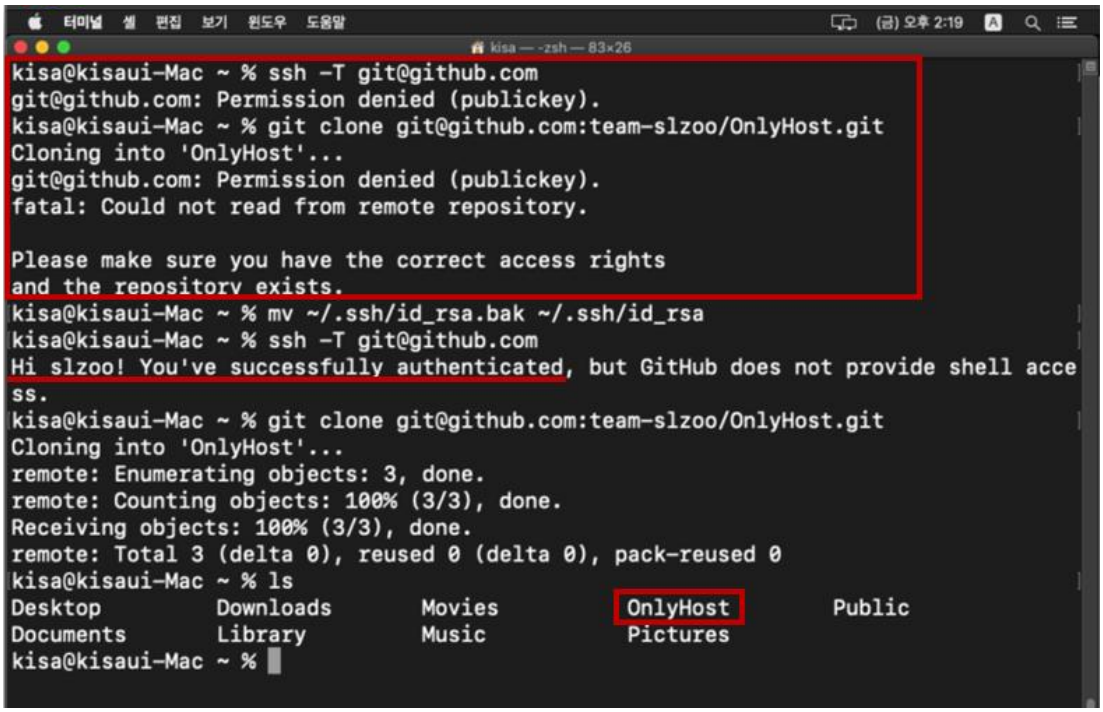


그림 2-6. ssh 개인키 기반의 저장소 접근 및 소스코드 유출

o 정리하면, 공격자는 개발자 로컬 컴퓨터에 저장된 개인키와 소스코드 저장소 주소만을 이용하여 개발자에게 허용된 소스코드를 확보할 수 있다.

3-2. 탈취한 자격증명을 이용하여 브라우저를 통한 소스코드 저장소 접근 시도

o 정보유출 시도를 통해 브라우저에 저장된 소스코드 저장소 자격증명을 획득하면, 공격자는 웹을 통해 직접 접근을 시도할 수 있다. 이 때, 사용자에게 부여된 저장소 별 권한에 따라 유출되는 정보범위가 결정되며, 전체 저장소를 관리하는 사용자가 공격받은 경우에는 모든 소스코드가 유출될 수 있다.

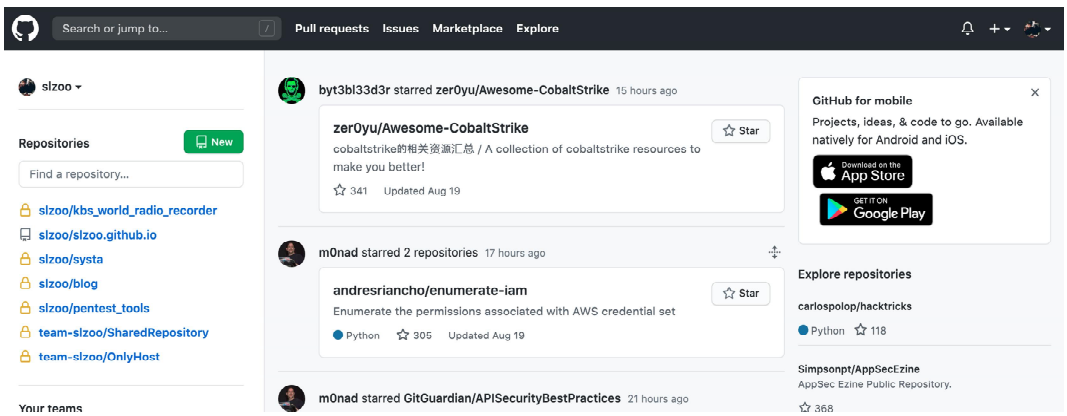


그림 2-7. 소스코드 저장소 접속 성공

o 하지만, 아래 그림 2-8처럼 2단계 인증이 설정되어 있다면 웹을 통한 소스코드 유출을 방지할 수 있다. 이 때, 수신하는 2단계 인증문자는 외부침투를 인지할 수 있는 마지막 시점이다.

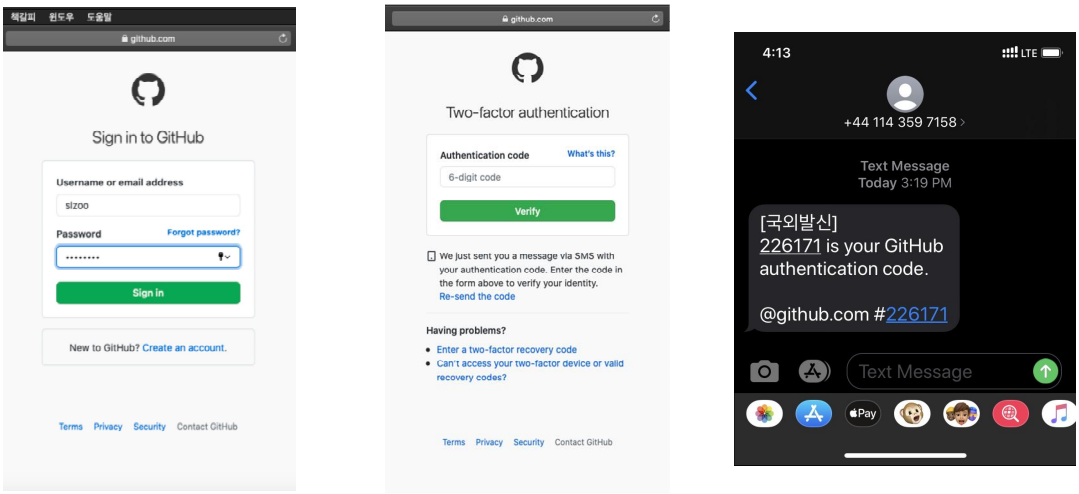


그림 2-8. 자격증명 기반의 로그인 시도 및 2단계 인증문자 수신

o 위와 같이 조직 내 소스코드 저장소에 접근하는 모든 계정에 대하여 2단계 인증을 요구할 수 있다. 그 외에도 접근하는 IP에 대한 설정 등을 통해 보다 높은 보안성을 갖출 수 있다. 하지만, 이러한 보안 설정에도 불구하고 절차 3을 통해 소스코드가 탈취될 수 있다.

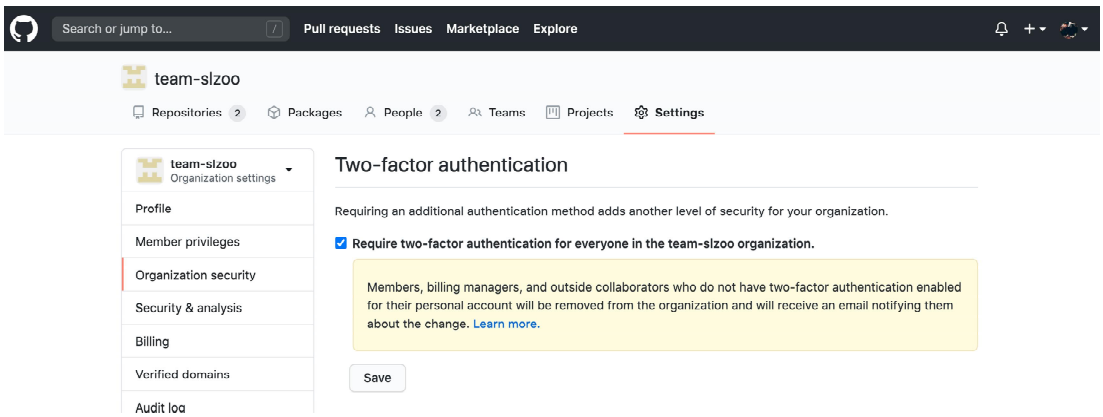


그림 2-9. 외부 소스코드 저장소의 조직 보안설정(2단계 인증 설정)

o 이에 추가하여 고려해야할 사항으로는 조직에 속한 저장소 권한이다. 본 사례를 구성하기 위해 참고한 GitHub의 경우, 모든 조직원이 저장소에 접근할 수 있는 READ 권한으로 초기 값이 설정되어 있다. 이에 해당하는 경우, 모든 저장소에 접근하여 소스코드를 확인, 복제할 수 있기 때문에 전사 소스코드가 유출될 수 있는 우려가 존재한다.

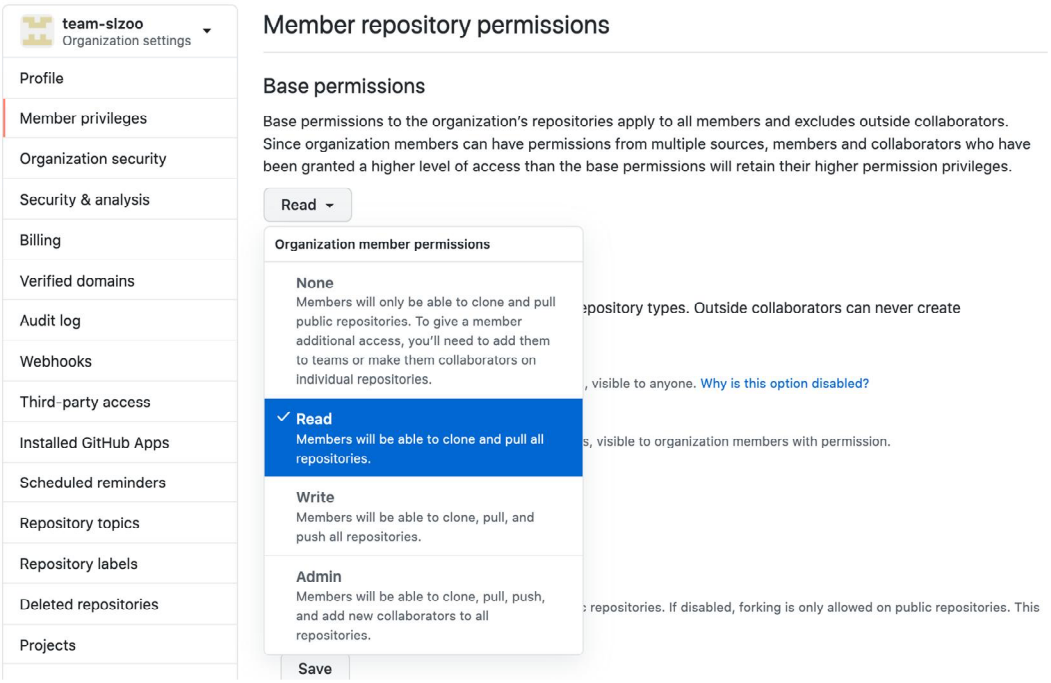


그림 2-10. 조직원에 대한 소스코드 저장소 디폴트 권한 설정

시나리오 2	(서버관리자) Active Directory 장악 → 전사 데이터 랜섬웨어 감염

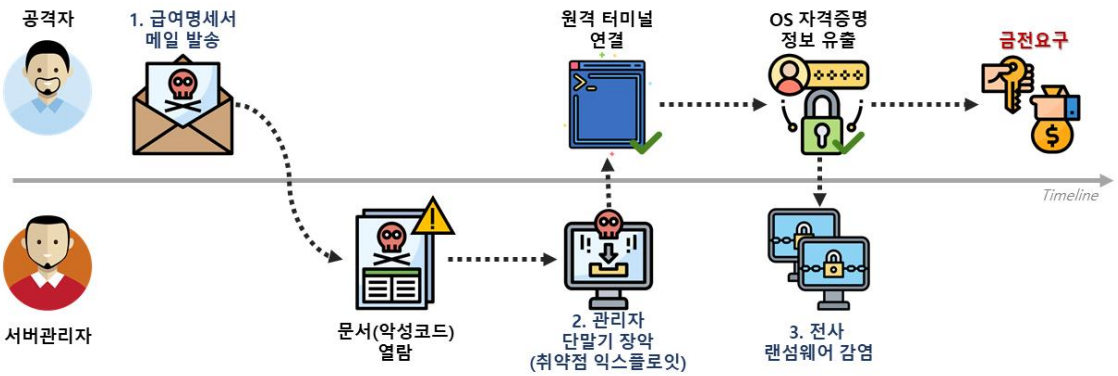


그림 2-11. 서버관리자 단말기 침투로 인한 전사 네트워크 랜섬웨어 감염 시나리오

o 시나리오 환경을 구성하는 핵심 요소인 Active Directory는 다수의 단말기를 관리하기 위해 사용되는 중앙집중형 관리체계이다. 서버 관리자는 도메인 컨트롤러(a.k.a. AD서버)에 접근하여 통일된 보안정책 적용 및 소프트웨어 배포 등 관리 작업을 수행한다. 아래 그림 2-12와 같이 네트워크가 구성되어 있을 때, 외부로부터 서버관리자의 단말기가 감염되는 경우, 저장되어 있는 OS 자격증명정보가 유출되고 전사 네트워크가 장악되어 치명적인 피해로 이어질 수 있다.

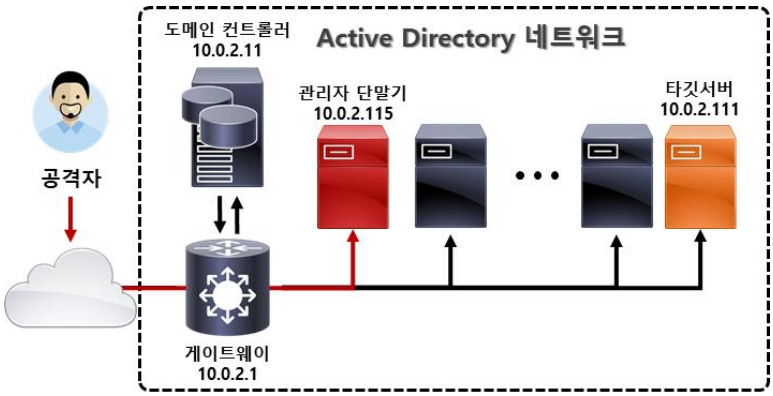
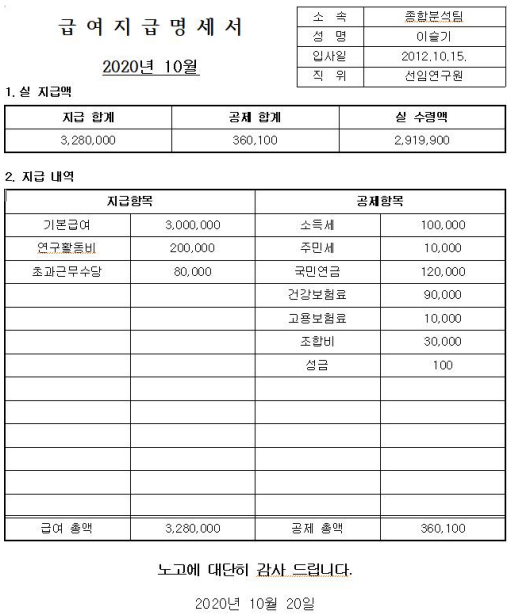


그림 2-12. Active Directory 네트워크 구성도

1. 스피어 피싱 메일(급여명세서, 취약점 발현 및 원격제어 악성코드 첨부) 송신



급 여 지 급 명 세 서

2020년 10월

소 속	종합분석팀
성 명	이슬기
입사일	2012.10.15.
직 위	선임연구원

1. 실 지급액

지급 합계	공제 합계	실 수령액
3,280,000	360,100	2,919,900

2. 지급 내역

지급항목		공제항목	
기본급여	3,000,000	소득세	100,000
연구활동비	200,000	주민세	10,000
초과근무수당	80,000	국민연금	120,000
		건강보험료	90,000
		고용보험료	10,000
		조합비	30,000
		성금	100
급여 총액	3,280,000	공제 총액	360,100

노고에 대단히 감사 드립니다.

2020년 10월 20일

그림 2-13. 스피어 피싱 메일 본문 및 급여명세서로 위장한 문서형 악성코드(예시)

2. 감염된 단말기에서 AD 서버 장악을 위한 취약점 익스플로잇

o 서버관리자를 직접적으로 공격하는 스피어 피싱 메일의 경우, 관리자 PC에 저장되어 있는 자격증명 정보로 인해, 공격자는 보다 손쉽게 공격이 가능하다. 하지만, 측면이동(Lateral Movement)을 통해서 서버관리자 단말기로 침투할 수 있다.

o 공격자가 장시간에 걸쳐 타겟을 수집·분석하여 정교하게 구성한 스피어 피싱은 직접적으로 서버관리자를 노릴 수 있다. 하지만 최근, Zerologon으로 명명된 고위험 취약점은 서버관리자 단말기 뿐 아니라, 도메인에 연결된 단말기가 공격에 노출되었을 때, AD 서버에 접근하여 관리자 계정을 획득할 수 있다[1, 2].

※ 본 시나리오에서는 Zerologon을 이용하여 AD 서버 관리자 권한을 획득하며, 시나리오 진행의 편의성을 위하여 Kali Linux를 이용하여 테스트를 수행한다.

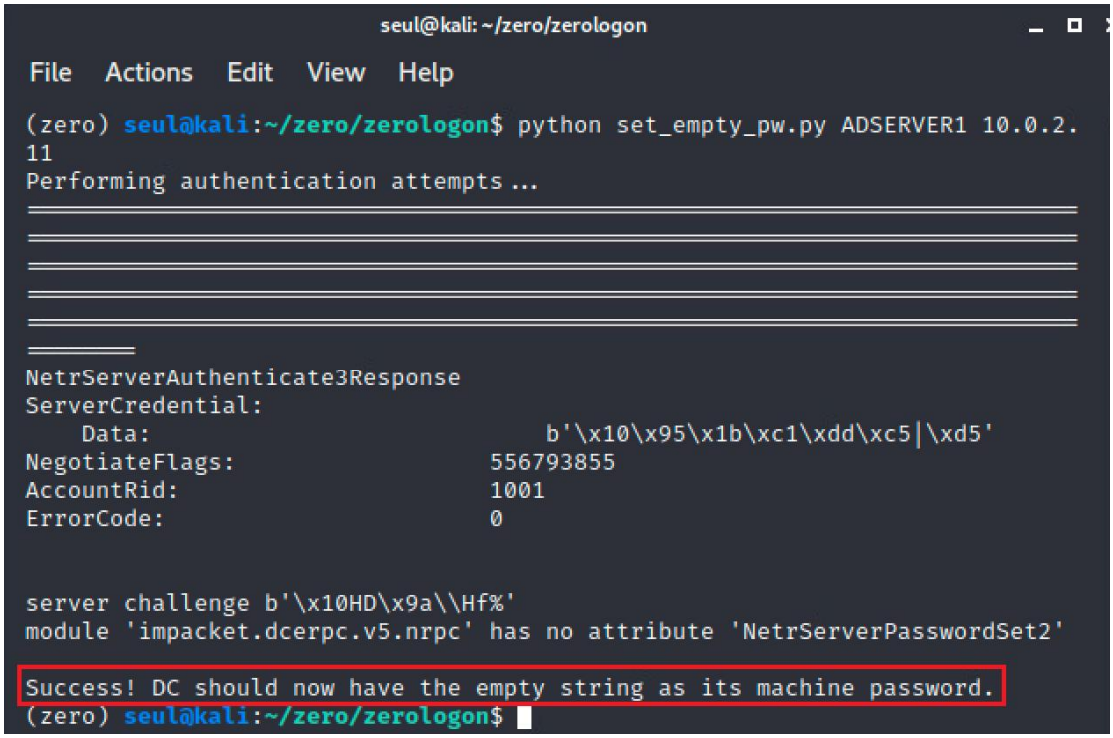


그림 2-14. Zerologon 익스플로잇 결과

o 위의 익스플로잇을 통해 취약점이 발현되었고, AD 서버가 장악되었다고 판단할 수 있다. 아래 그림 2-15와 2-16는 Impacket 프레임워크에 포함된 도구(secretsdump, wmiexec)를 이용, 관리자 권한의 원격 터미널 연결 결과를 보여준다.

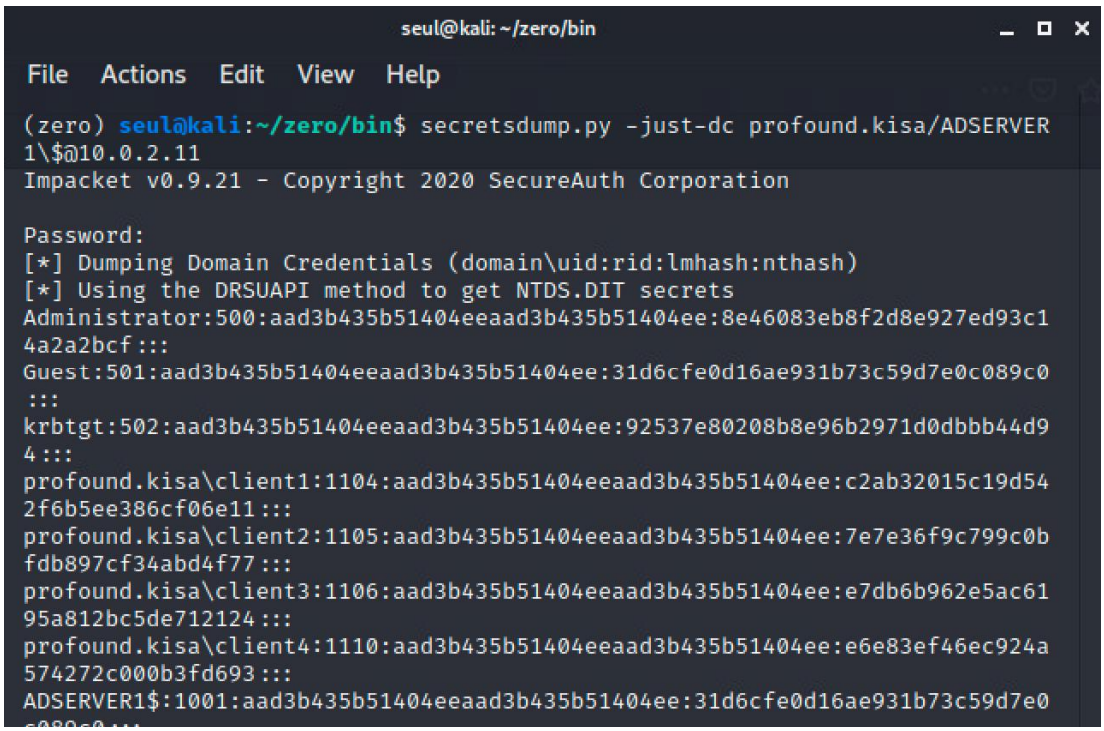


그림 2-15. 사용자의 NTLM 해시 수집 결과(DCSync)

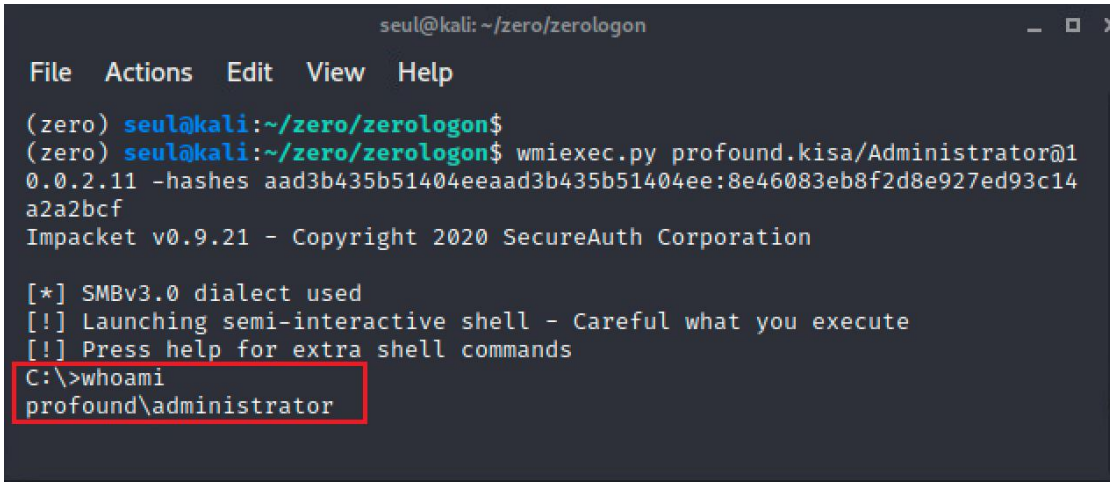


그림 2-16. 원격 터미널 연결 결과

o 공격자는 AD 서버를 장악한 이후, 내부 네트워크에 포함된 정보와 정책 등을 수집 할 수 있으며, 이를 위한 스크립트는 오픈소스로 공개되어 있다. 파일 업로드/다운로드, AD 서버에 연결된 단말기로의 정책 배포, 악성코드 삽입 등 관리자로서의 권한을 악용한 모든 행위를 수행할 수 있다.

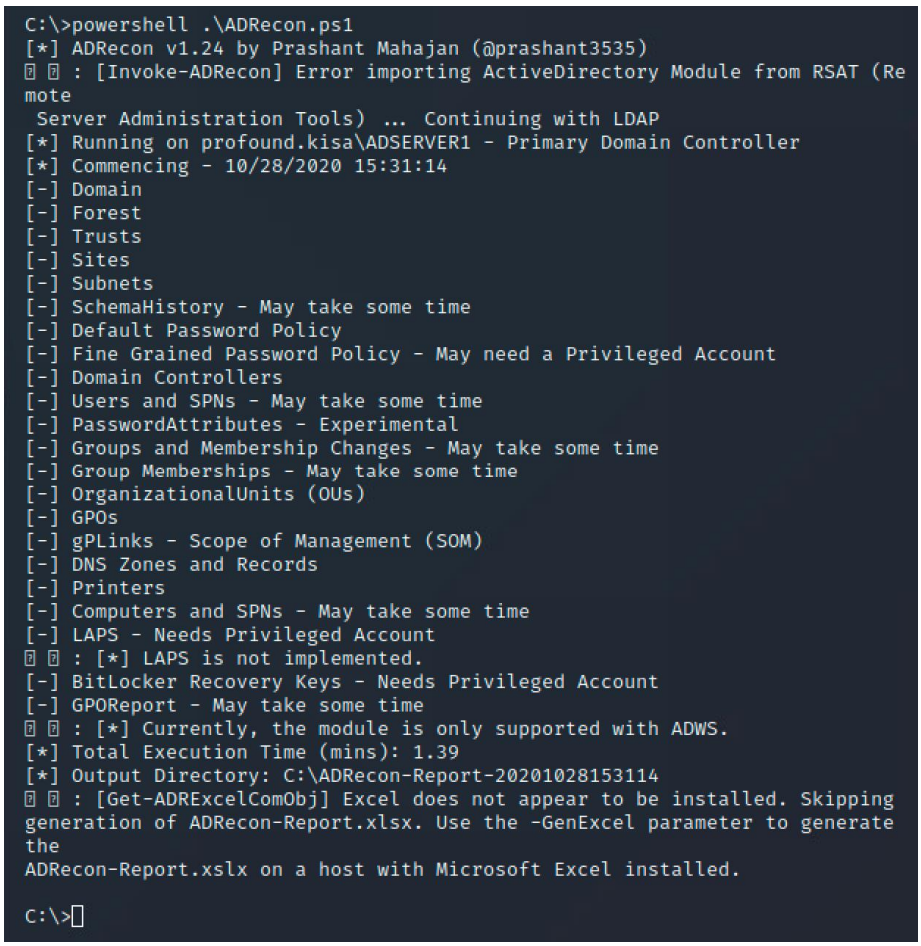


그림 2-17. ADRecon: Active Directory Recon 스크립트 실행결과[3]

3. AD 서버 관리자 권한을 악용한 랜섬웨어 유포 및 실행

o 금전적인 목적을 달성하기 위하여 공격자는 AD 서버에 연결된 단말기 및 서버 등을 대상으로 랜섬웨어를 유포, 감염하는 행위를 수행한다. 이를 위한 다양한 방법 중 아래 그림 2-18은 AD 서버의 시작 프로그램에 랜섬웨어 유포·실행 스크립트를 삽입한 화면이다.

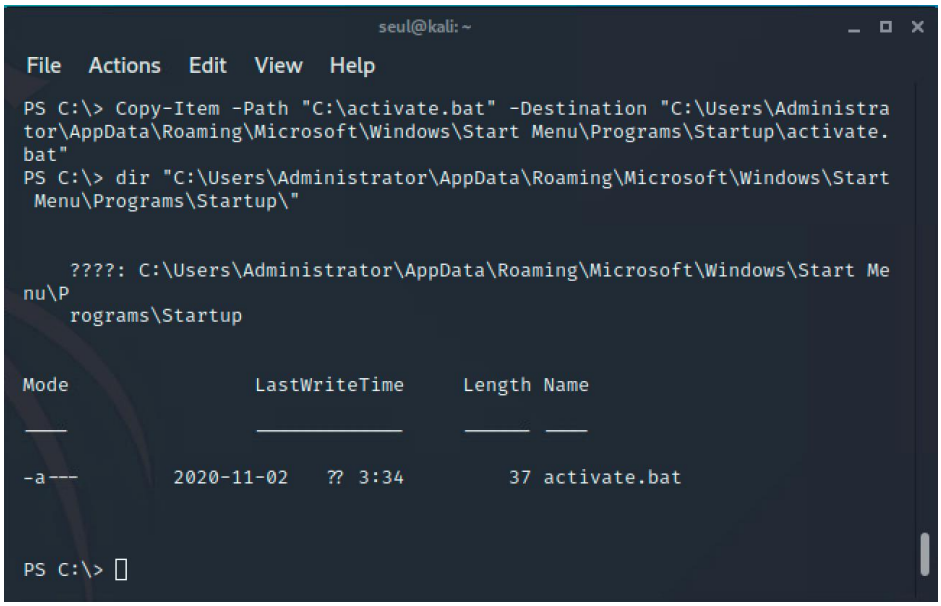


그림 2-18. 랜섬웨어 유포 스크립트 등록(AD 서버 시작 프로그램)

o 랜섬웨어 유포·실행 스크립트로 인해 AD 네트워크에 연결된 모든 단말기로 랜섬웨어(ransomware.ps1)가 전파될 수 있으며, 감염파일(ransomware_infected.txt)이 생성될 수 있으며 랜섬웨어 유형에 따라 복구가 불가능할 수 있다.

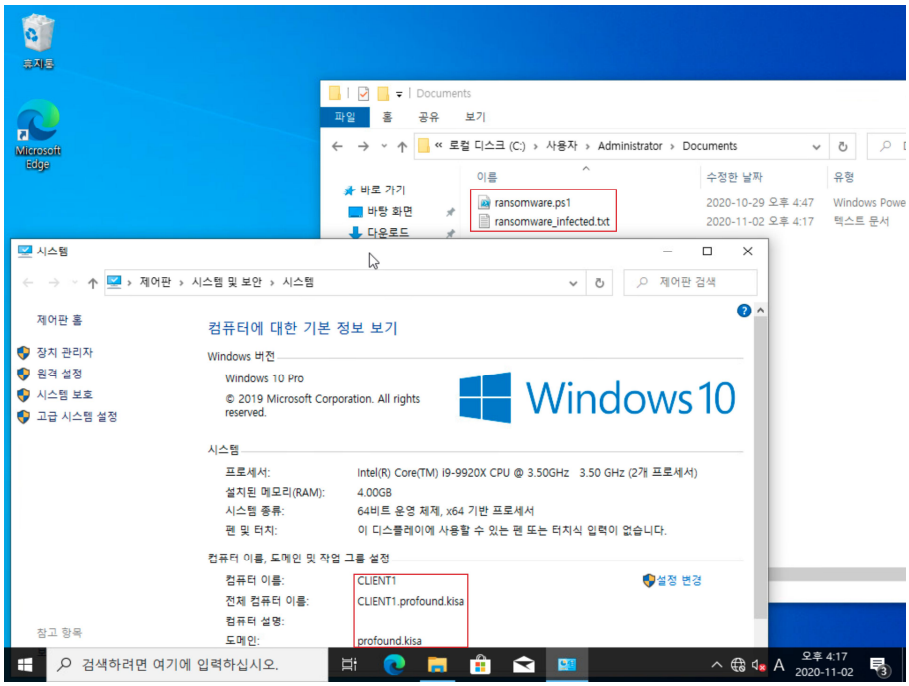


그림 2-19. 타겟 시스템의 랜섬웨어 감염결과(예시)

3. 시나리오에 사용되는 도구 분석

그림 3-1. 시나리오에 사용되는 도구 및 주요 기능

o 최근 탐지되는 악성코드는 특정 기능으로 국한되는 것이 아니라 복합적으로 구성되어 있거나 다양한 기능의 악성코드를 조합하여 공격자의 최종 목적을 달성하는 방식으로 침해사고가 전개되기 때문에 최종목적을 달성하기 위해 수행되는 악성행위 기준으로 도구를 소개한다.

o 스피어 피싱을 통해 내부로 침투한 경우, 모든 파일(문서, 그림, DB 등)에 접근하여 정보를 탈취할 수 있으므로, 침투 이후에는 모든 자료를 가져갈 수 있다고 판단해야 한다. 이에 대한 피해 확산을 경감시키기 위하여 **주요한 정보에 접근할 수 있는 계정과 권한에 대한 철저한 접근제어**가 우선이다.

o 스피어 피싱을 통해 내부로 침투한 공격자는 공개된 소프트웨어를 통해 공격에 필요한 데이터를 수집하거나 측면이동(Lateral Movement)을 할 수 있다. 대표적으로 Mimikatz, PsExec 등이 있으며, 지속적인 업데이트를 통해, 최신버전의 윈도우 환경에서도 주요 정보에 접근가능하다. 또한, **윈도우 계정정보, 원격 접속정보 뿐 아니라 브라우저에 저장된 정보를 평문수준까지 해독**하여 확인할 수 있기 때문에 더 위험하다고 볼 수 있다. 아래는 Mimikatz를 통해 어떠한 정보가 탈취될 수 있는지와 Google Chrome에 저장되어 정보가 탈취된 결과, 그 외 공격에 사용되는 도구의 시연이다.

o Mimikatz는 **로컬 PC의 계정이름과 패스워드, 원격으로 접속한 PC의 계정이름과 패스워드**를 확인할 수 있다. 특히 윈도우 7의 경우, 평문으로 해당 패스워드를 확인할 수 있다. 윈도우 10에서는 NTLM 해시값으로 저장되나, 이를 재사용(Pass the Hash)해서, 권한을 획득할 수 있다. 따라서 마찬가지로 계정이 도용될 수 있다고 확인할 수 있다. 또한, 윈도우 7에서 추출된 ID/PW를 확인해보면, 원격으로 접속한 PC의 계정과 패스워드를 그대로 확인할 수 있어, 크리덴셜 스터핑(Credential Stuffing) 기법과 연계하면 그 피해는 더 확산될 수 있다.

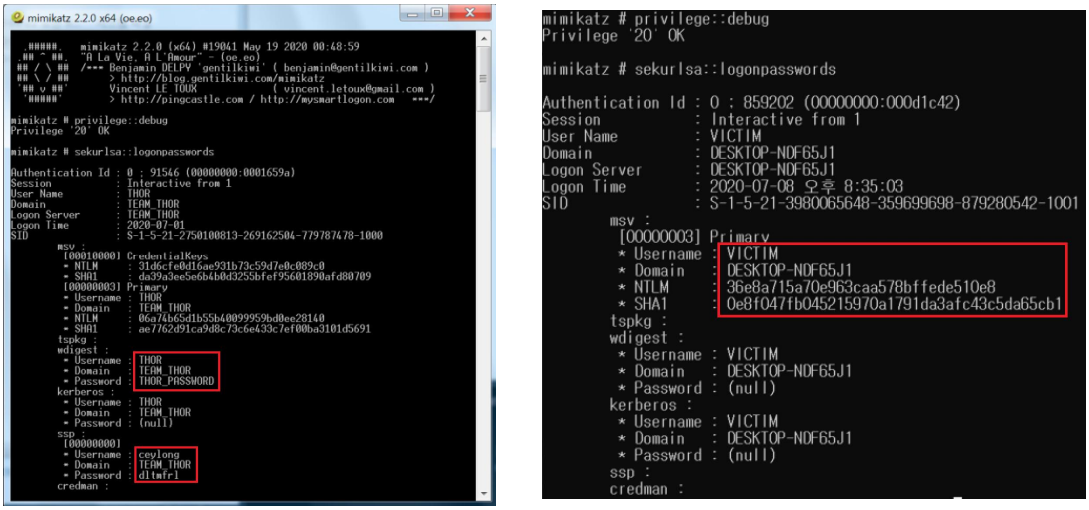


그림 3-2. Mimikatz를 이용한 ID/PW 추출결과(Windows 7/Windows 10)

o Mimikatz를 이용하여 윈도우 자격 증명 관리자에 저장된 정보 또한 추출 가능하다.

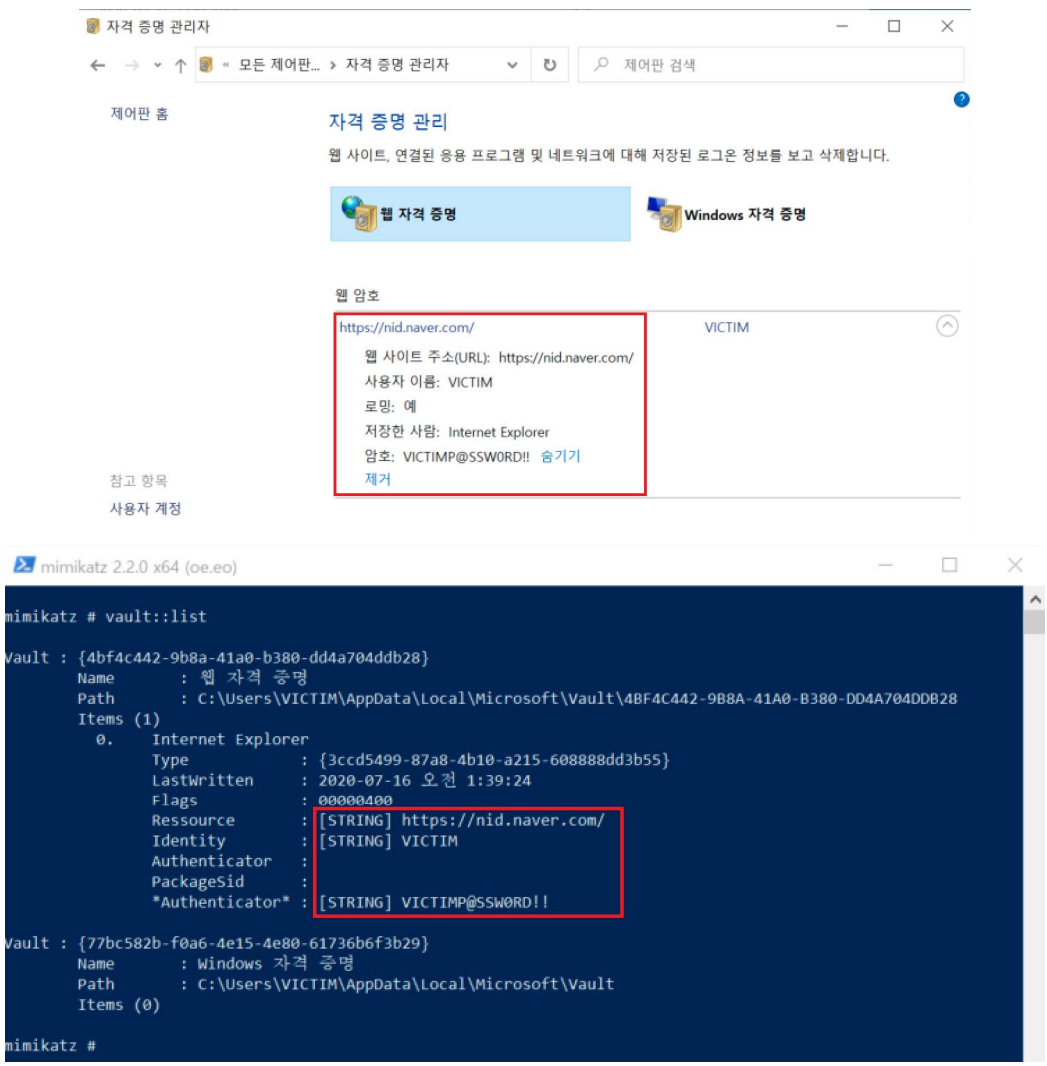


그림 3-3. 윈도우 자격 증명 관리자 정보 탈취

o 원격 데스크톱을 이용한 원격접속(RDP)의 경우에는 자격 증명정보가 접속하는 원격 서버 내에 저장되고, 접속을 시도하는 단말기에는 저장되지 않는다. 하지만 Restricted Admin mode를 설정하고 접속하는 경우, 접속 단말기 내에 NTLM 해시 등을 저장하기 때문에 이를 이용하여 Pass The Hash 공격이 가능하다.

※ Windows 10의 경우 디폴트 해제되어 있으나, 특권 로그인 계정의 수를 경감시키기 위하여 대규모 조직의 경우 이를 설정하여 사용하기도 한다.

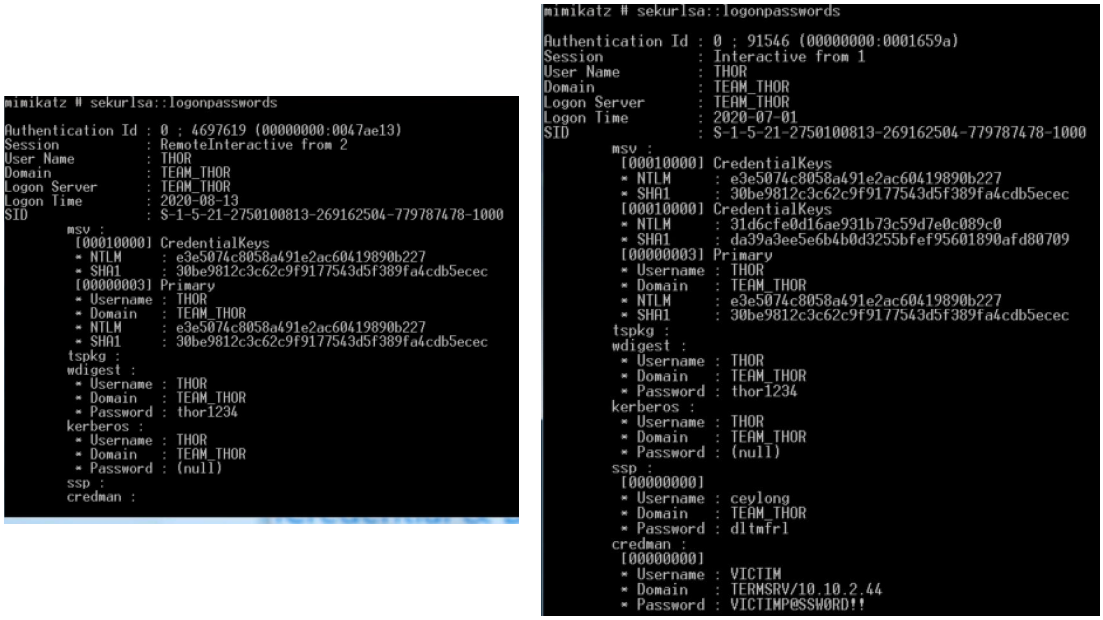


그림 3-4. 원격데스크톱으로 접속했던 계정 정보

o **브라우저(Chrome, Firefox, IE, Edge 등)에 저장되어 있는 자격증명(Credential), 히스토리, 쿠키, 즐겨찾기** 또한 탈취될 수 있다. 언급한 브라우저 모두 자동완성 기능을 위해 사용자 정보를 DPAPI(Data Protection Application Programming Interface)로 저장하고 활용한다. 악성코드 또한 DPAPI를 호출하여 평문 값을 획득할 수 있으므로, **자격증명 정보가 유출되었더라도 이를 보완할 수 있는 2채널 인증 등이 필요하다.**

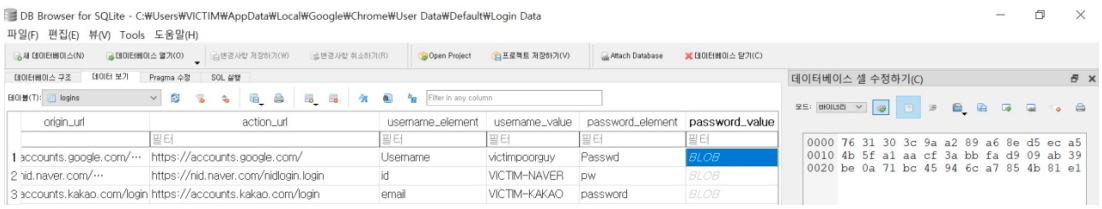


그림 3-5. Google Chrome에 저장된 계정정보

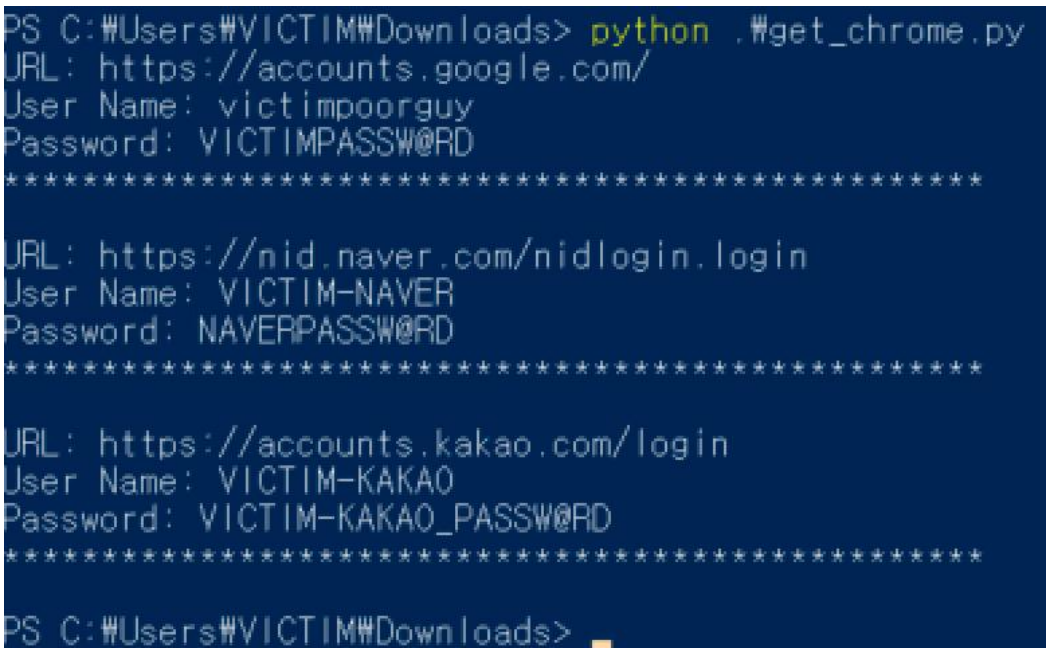


그림 3-6. Google Chrome에 저장된 계정정보(비밀번호 해독)

o 자격증명을 탈취하는 것이 아니라, 도메인 내부에 존재하는 문서파일이나, 실행파일 등을 탈취하는 악성코드 또한 존재한다. 따라서 **내부 침투가 성공적으로 이루어졌다면, 내/외부로 접근할 수 있는 모든 데이터가 탈취**되었다고 의심하고 대응해야 한다.

o 그 외 Mimikatz를 통해 사용자/시스템 인증서가 탈취 가능하며, Mimikatz가 아니더라도 와이파이 패스워드 등도 탈취가 손쉽게 가능하다. NAC(Network Access Control) 장비와 같이 내부 네트워크에서 발생하는 트래픽을 관리하지 않는다면, 치명적인 위협으로 이어질 수 있다.

그림 3-7. 와이파이 패스워드 탈취

o 특히, 개발자의 경우, 편의성을 위하여 Git 자격증명을 평문으로 저장하고 이용하기도 하여 개발자 PC로 침투했다고 가정할 경우, 자격증명을 손쉽게 탈취당할 수 있으며 소스코드 저장소로 접근도 용이하다.

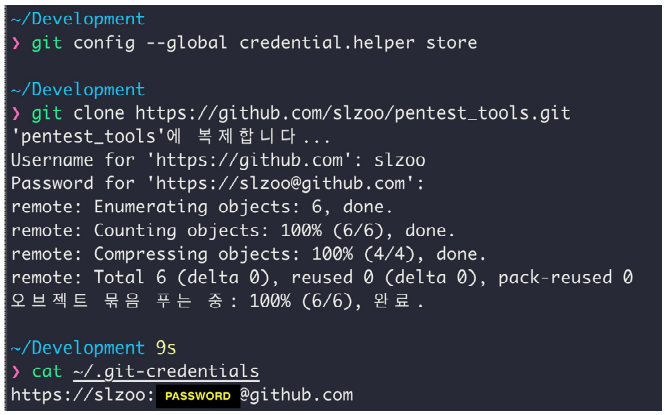


그림 3-8. git-credential store 옵션으로 노출된 계정

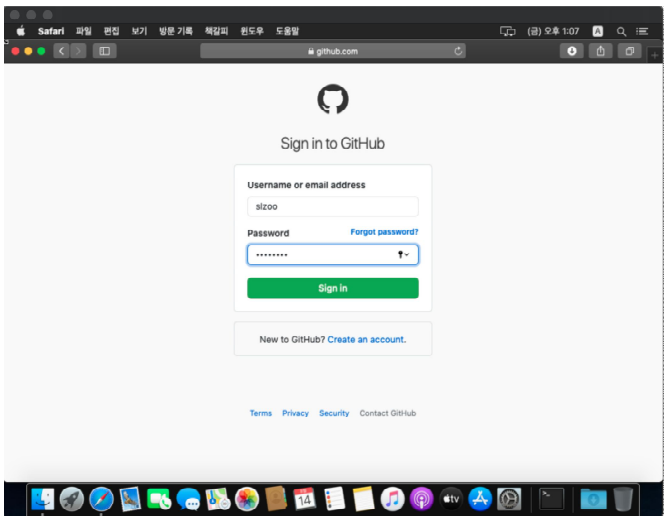


그림 3-9. 소스코드 관리서버 접근(GitHub)

- 하지만, 개발 보안을 유의하는 기업은 특정 인증서에서만 동작하도록 등록해두고 이용한다. 예를 들어 GitHub의 설정에 ssh 공개키를 등록하여, 개인키를 가지고 있는 경우에만 접근 가능하도록 설정할 수 있다. 하지만 내부의 저장소(Repository) 별로 접근권한 설정을 해두지 않고 타 부서의 소스코드까지 열람할 권한이 부여된다면 전사 관리 중인 소스코드가 유출될 우려가 있다.

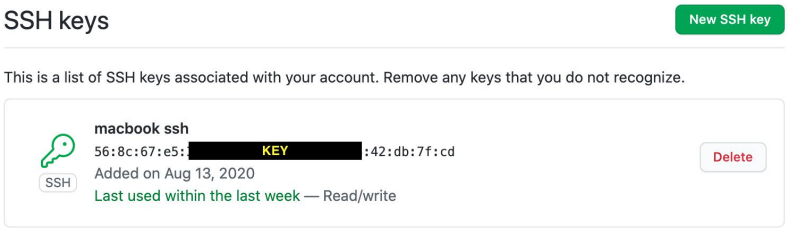


그림 3-10. 계정으로의 접근을 관리하기 위한 ssh 키 등록(GitHub)

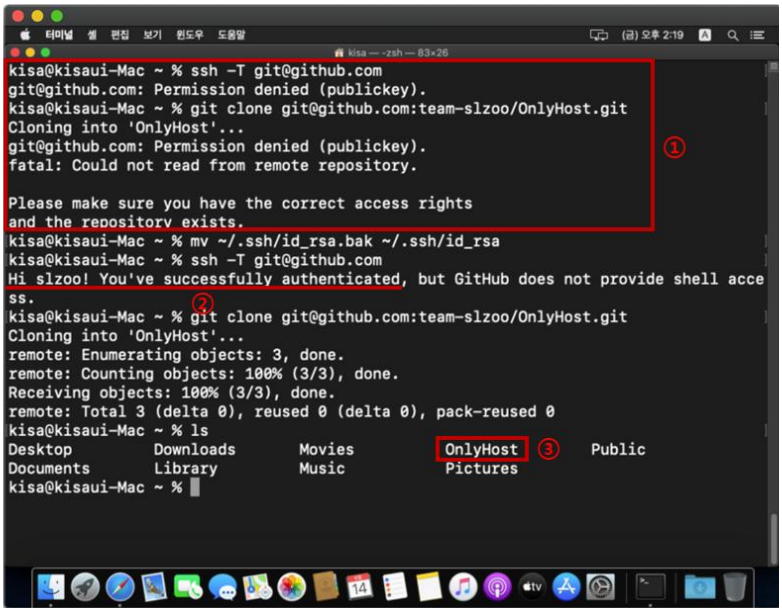


그림 3-11. ssh 개인키 탈취로 인한 소스코드 유출

o PsExec는 Sysinternals에서 공식적으로 지원하는 유틸리티로서, 원격에서 타깃 시스템의 프로세스를 실행하고 그 출력을 로컬로 전달하는 방식으로 구현한 시스템 관리 도구이다[4]. 이와 동일한 기능을 파이썬으로 구현한 소프트웨어도 존재한다. 이러한 관리도구는 시스템 운영을 위해 널리 이용되지만, 공격자로부터 악용될 수 있는 여지 또한 남아있다. 추가로, psexec.py가 포함되어 있는 Impacket 프레임워크의 secretsdump와 wmiexec 또한 마찬가지로 공격자에게 빈번하게 악용되는 도구이다[5, 6].

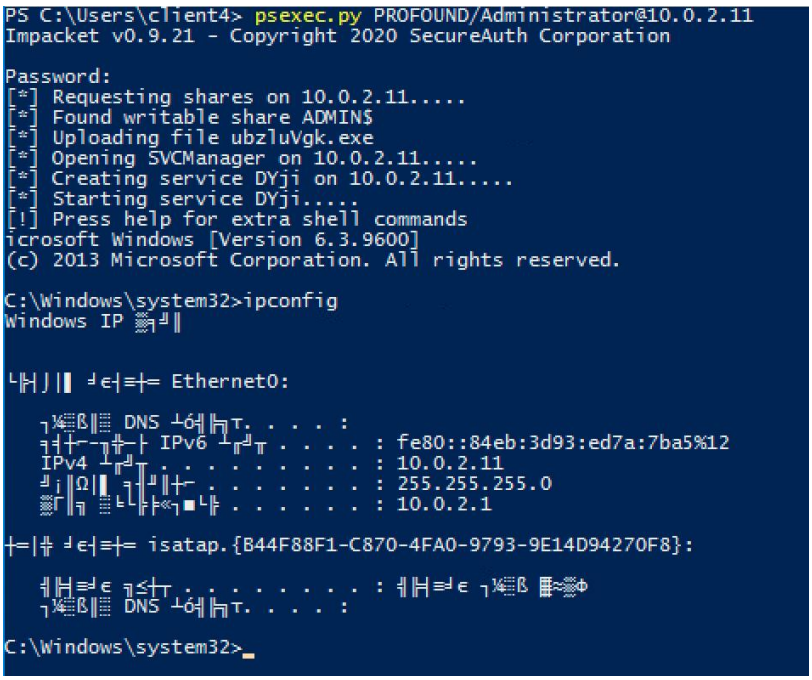


그림 3-12. 원격 터미널(PsExec) 실행

4. 결론

【Defender's Insight】

타깃형 공격을 통해 공격자가 임직원의 단말기로 침투하면, 감염된 단말기는 추가 공격에 활용되거나 내부문서 암호화 등의 피해가 발생할 수 있다. 이러한 랜섬웨어 감염 피해를 경감하기 위하여 주기적인 백업과 업데이트가 요구된다. 또한, 공격자에 의해 개발자 PC가 감염되면 단말기 내 소스코드가 유출되고 기업 내부 개발 환경으로 침투가 가능하다. 제품 업데이트 서버의 추가 감염을 통해 피해 범위가 크게 확산될 가능성이 존재하기 때문에, 개발자 PC 등 개발 환경에 대한 주기적인 점검이 필요하다. 서버관리자도 마찬가지로 기업 네트워크의 중앙거점으로 활용하는 AD 서버 계정을 잘 관리하고 있는지 점검이 필요하다. 단말기별 용도 분리를 통해 안전한 환경에서 서버를 관리하고, 비정상 접근을 모니터링 하는 사전예방 활동이 필요하다.

정교하게 구성된 타깃형 공격은 일시적으로 차단할 수 있지만, 결국 내부로의 침입을 막을 수 없다. 이는 보안 솔루션과 이용자 교육이 불필요하다는 이야기가 아니며, APT(Advanced Persistent Attack)의 정의에 따라, 공격자는 시스템 내부로 침투하고야 말 것이라는 사실을 의미한다. 따라서 Post-Exploitation 단계에서 발생하는 징후를 이용하여 신속히 대응하거나, 피해 확산을 방지하기 위한 기본적인 접근제어 수준부터 재점검하는 보안 활동이 필요하다.

보안담당자는 주기적인 침투 테스트 수행과 발생하는 징후(이벤트 로그 등)를 분석하고 내부 네트워크에 공격자가 침투한 상태에서의 방어전략 마련도 필요하다. 이 방어 전략은 외부에서 내부로의 침입차단이 아니라, 내부에서의 피해확산 혹은 유출차단을 목적으로 한다. 따라서 기존의 '성공' 아니면 '실패'라는 이분법적인 접근을 넘어서서, 피해 감소의 측면을 고려한 보안사고 대응전략이 필요하다. 사고발생시점과 사고인지시점 사이의 피해 감소 노력이 전체적인 침해사고 피해를 줄일 수 있을 것으로 기대한다.

5. 참고문헌

[1] Tom Tervoort, Secura, "Zerologon: Unauthenticated domain controller compromise by subverting Netlogon cryptography (CVE-2020-1472), Sep. 2020.

[2] risksense, "ZeroLogon exploitation script," https://github.com/risksense/zerologon/

[3] adrecon, "ADRecon: Active Directory Recon," https://github.com/adrecon/ADRecon

[4] Microsoft, "PsExec v2.2," https://docs.microsoft.com/en-us/sysinternals/downloads/psexec/

[5] SecureAuthCorp, "Impacket," https://github.com/SecureAuthCorp/impacket/

[6] Riccardo, F-Secure Consulting, "Hunting for Impacket," https://riccardoancarani.github.io/2020-05-10-hunting-for-impacket/

Icon made by Freepik, Eucalyp, monkik, surang from www.flaticon.com