

**Marry with me**

**침해사고 상세 분석**

**보고서**

목차

[1 개요 4](#_Toc154429045)

[1.1 조사 배경 4](#_Toc154429046)

[1.2 조사 대상 4](#_Toc154429047)

[1.3 침해 사고조사 분석 Process 4](#_Toc154429048)

[2 총평 7](#_Toc154429049)

[2.1 사고 조사 총평 7](#_Toc154429050)

[2.2 침해 사고 타임라인 8](#_Toc154429051)

[3 상세 조사 결과 10](#_Toc154429052)

[3.1 Exchange Server (WIN-NNR40DDHJ75, 172.30.40.106) 10](#_Toc154429053)

[3.2 Active Directory (WIN-DGHQL8QFN54, 172.30.40.100) 27](#_Toc154429054)

[3.3 OU (DB 관리자, 172.30.40.123) 37](#_Toc154429055)

[4 권고사항 45](#_Toc154429056)

[4.1 WAF 솔루션 45](#_Toc154429057)

[4.2 Exchange 서버 (KB 패치, CU 패치) 45](#_Toc154429058)

[4.3 보안 관제 서비스 45](#_Toc154429059)

[4.3.1 원격 관제 서비스 45](#_Toc154429060)

[4.3.2 파견 관제 서비스 46](#_Toc154429061)

[4.4 취약점 진단 서비스 46](#_Toc154429062)

[4.5 웹쉘 탐지 솔루션 46](#_Toc154429063)

[4.6 EDR 솔루션 46](#_Toc154429064)

[4.7 OWA서버 외부 접근 차단 46](#_Toc154429065)

[4.8 자동 로그인 세션 만료 시간 설정 46](#_Toc154429066)

[4.9 2차인증 47](#_Toc154429067)

[4.10 아웃바운드 정책 실행 47](#_Toc154429068)

[4.11 웹 디렉토리 실행 권한 설정 47](#_Toc154429069)

[4.12 Trust to Trust 접근 정책 강화 47](#_Toc154429070)

[4.13 비밀번호 정책 강화 47](#_Toc154429071)

[4.14 DB 접근 제어 솔루션 47](#_Toc154429072)

[4.15 DLP (데이터 손실 방지) 47](#_Toc154429073)

[4.16 WDigest 비활성화 47](#_Toc154429074)

[4.17 백신 프로그램 48](#_Toc154429075)

[4.18 접근 통제 솔루션 48](#_Toc154429076)

[4.19 Zero Trust 기법 48](#_Toc154429077)

[5 악성코드 분석 49](#_Toc154429078)

[6 침해 지표 57](#_Toc154429079)

[6.1 공격 지표 57](#_Toc154429080)

[6.2 침해 도구 지표 57](#_Toc154429081)

[7 그림 목차 58](#_Toc154429082)

[8 표 목차 62](#_Toc154429083)

# 개요

## 조사 배경

"Marry with me" 결혼 정보 업체의 내부 PC들이 공격에 피해를 입어, 조직 내부의 시스템이 랜섬웨어에 감염되었고, 이로 인해 업체는 업무에 심각한 장애를 겪고 있으며, 조직 내 데이터 유출과 민감 정보 노출 가능성을 신속하고 효과적으로 식별하기위해 사고 원인 분석과 침해사고 조사에 착수함.

## 조사 대상

| **번호** | **IP** | **Host** | **역할** | **OS** |
| --- | --- | --- | --- | --- |
| 1 | 172.30.40.106 | WIN-NNR40DDHJ75 | Exchange Server | Window Server 2016 |
| 2 | 172.30.40.100 | WIN-DGHQL8QFN54 | Active  Directory Server | Window Server 2016 |
| 3 | 172.30.40.123 | Kim | DB 관리자 PC | Window Server 2016 |
| 4 | 172.30.40.104 | Kim | DB Server | Ubuntu 20.04 LTS |

[표 1‑1] 조사대상

## 침해 사고조사 분석 Process



[그림 1.1] 침해 사고 분석 Process

1. 관련정보 파악

| **No** | **항목** | **설명** |
| --- | --- | --- |
| 1 | 환경정보 파악 | 침해사고가 발생한 서버의 위치 및 내부 서비스 파악 등 인터뷰 내용 외적인 부분에 대한 확인 과정 |
| 2 | 이미지 가능여부 | 침해사고 대상 서버에 대한 격리 유무를 확인하고 이에 따른 효과적인 분석 방법을 선택. (현장 보존이 필요할 경우 디스크, 메모리에 대한 이미징 작업 수행) |
| 3 | 초기대응 | 침해 사고와 관련한 피해가 계속 발생할 경우 이에 대한 초기 대응 조치를 수행(공격자 IP차단, 서버 격리, 피해 증상에 대한 대응책 제시 등) |

[표 1‑2] 관련정보 파악

1. 사고 시스템 분석

| **No** | **항목** | **설명** |
| --- | --- | --- |
| 1 | 디스크 이미징 | 격리 유무를 확인한 디스크에 대한 이미징 작업 수행 |
| 2 | 시스템 로그 | 시스템 운영 중에 기록되는 로그 분석을 통해 공격자의 서버 침투 유무 및 행위에 대해 분석 |
| 3 | 보안장비 로그 | 보안장비 로그 분석을 통해 침해사고 분석 대상 이외의 피해를 분석 |
| 4 | 시스템 정보수집 | 운영 되는 시스템의 정보 수집 및 분석 |

[표 1‑3] 사고 시스템 분석 설명

1. 원인 분석

| **No** | **항목** | **설명** |
| --- | --- | --- |
| 1 | 디지털 포렌식 | 파일 삭제되었거나 공격자가 스스로의 흔적을 제거한 경우, 디지털 포렌식 도구(Encase, Forensic explorer 등)을 이용하여 복원 작업 수행 후 원인 분석 |
| 2 | 메모리 분석 | 메모리 내에 잔존하는 데이터 중 침해사고의 원인으로 추정되는 내용에 대한 분석 |
| 3 | 악성코드 분석 | 악성코드가 발견될 경우 악성코드의 기능, 피해 범위 등을 분석 |
| 4 | 취약점 분석 | 서비스 중인 Application의 취약점을 조사하여 로그를 남기지 않는 형태의 공격에 대한 원인 분석 |

[표 1‑4] 원인 분석 설명

1. 대응 방안

| **No** | **항목** | **설명** |
| --- | --- | --- |
| 1 | 사고대응보고 | 침해사고가 계속하여 발생되는 경우 이에 대한 초기 대응을 수행하고 결과에 대한 보고 |
| 2 | 사고원인규명 | 침해사고 대상에 대한 원인 분석 후 분석된 결과에 대한 보고 |
| 3 | 사고대책수립 | 발견된 침해사고 원인에 대한 적절한 대책 수립을 위한 회의 |
| 4 | 사고대책권고 | 침해사고 원인에 대한 적절한 조치사항 권고 |

[표 1‑5] 대응 방안 설명

1. 조사 수행 기간 및 인원

| **번호** | **기간** | **분석자** | **비고** |
| --- | --- | --- | --- |
| 1 | 2023-12-14 ~ 2023-12-19 | 민작은바위 | 조장 |
| 2 | 김민재 | 침해 흔적 분석 |
| 3 | 류태영 | 침해 흔적 분석 |
| 4 | 박종원 | 침해 흔적 분석 |
| 5 | 서경범 | 침해 흔적 분석 |
| 6 | 서민성 | 침해 흔적 분석 |
| 7 | 이석 | 침해 흔적 분석 |
| 8 | 이성제 | 침해 흔적 분석 |
| 9 | 장서현 | 침해 흔적 분석 |
|  | 정대로 | 침해 흔적 분석 |

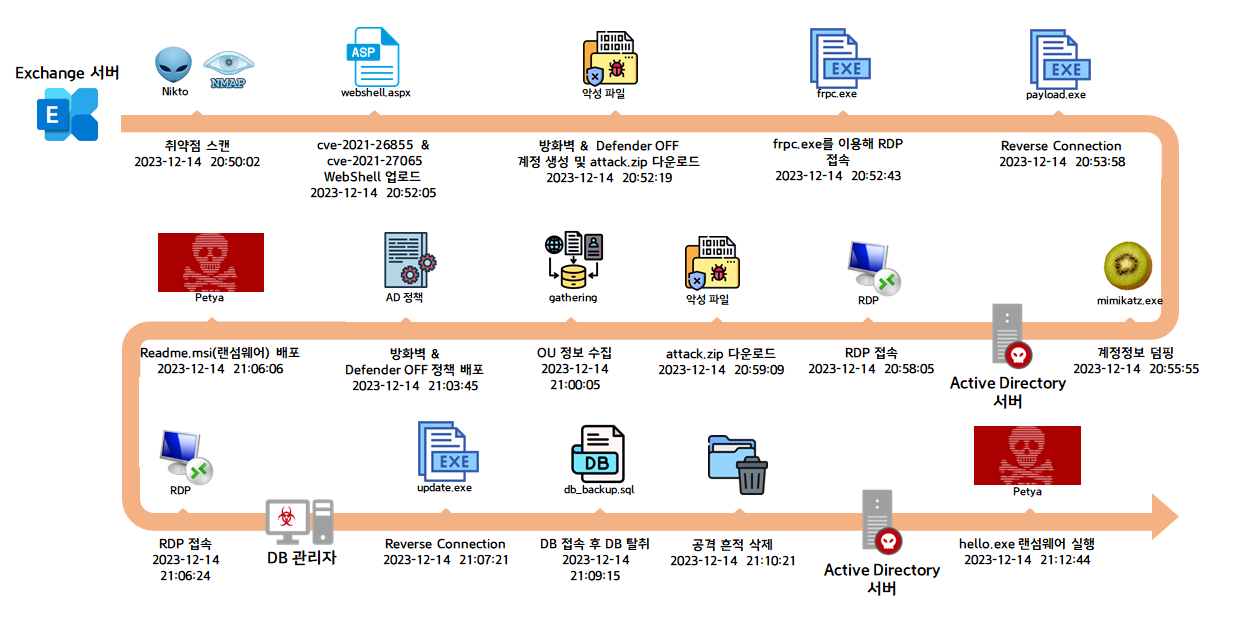
[표 1‑6] 조사 수행 기간 및 인원

# 총평

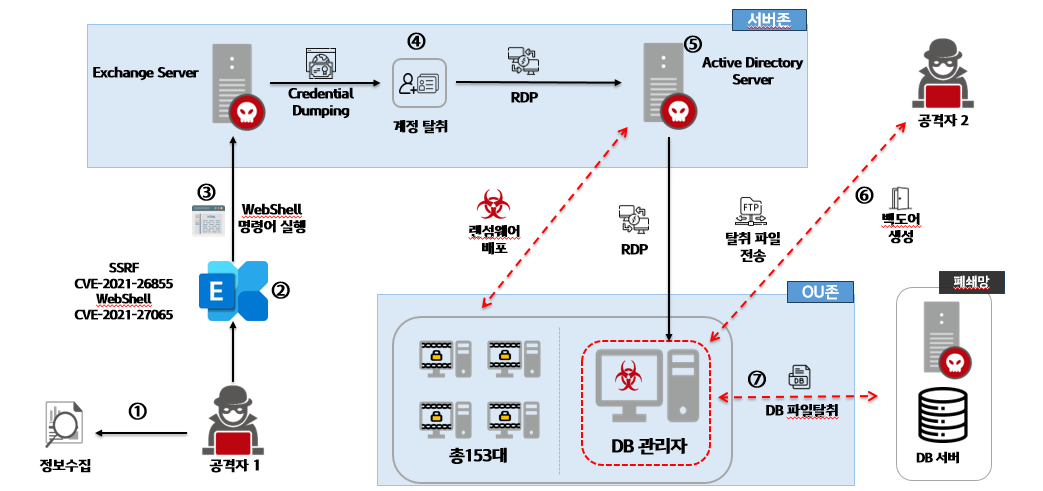
## 사고 조사 총평

|  |  |
| --- | --- |
| **결과** | 최초 신고 이후 분석을 진행한 결과Active Directory에 연결된 OU PC 총 153중 153대가 랜섬웨어에 감염된 것을 확인 그중 DB 관리자 PC를 통해 DB 서버에서 고객정보 약 100GB 정보 유출이 확인 |
| **원인**  **/**  **현상** | 1. Exchange Server 취약 버전 사용, 웹쉘 탐지 미흡 / CVE-2021-26855(인증 우회), CVE-2021-27065(웹쉘 업로드)  2. 악성코드 미 탐지 / 악성코드 실행  3. Outbound 통신 미 차단 / Reverse Connection  4. 암호화 되지 않은 DB파일, DB Server자동 로그인 / DB 파일 탈취  5. 랜섬웨어 행위 미 탐지 / 랜섬웨어 배포 |
| **개선**  **방안** | ∙ 사고 단계별 대응책   |  |  |  |  | | --- | --- | --- | --- | | **사고 단계** | **사고 주요 원인** | **대응방안** | **솔루션** | | **초기 정찰** | 불필요한 정보 노출 | 불필요한 포트 비활성 | WAF서비스  보안관제 서비스 | | **초기 침투** | 취약한 Exchange버전 | KB패치, CU패치  OWA 외부 접근 차단 | 취약점 진단 서비스 | | **거점 확보** | SSRF인한 웹쉘 업로드  및  악성파일 실행 | 웹 디렉토리 실행 권한 설정  아웃바운드 정책 설정 | 웹쉘 탐지 솔루션  백신 프로그램  EDR | | **내부 정찰**  **및**  **내부 확산** | 관리자 계정 획득 | WDigest 비활성화  비밀번호 정책 강화 | ㆍ | | 망 분리 미흡 | Trust To Trust 접근 정책 강화 | 접근 통제 솔루션 | | DB관리자 계정으로 DB접속 | 2차인증 사용  DB 암호화 | DB 접근제어 솔루션 | | **연결 유지** | 악성파일 실행 | 아웃바운드 정책 설정 | 백신 프로그램  EDR | | **목표 달성** | 암호화 되지 않은 DB 유출 | DB 암호화  아웃바운드 정책 설정 | DLP(정보유출방지솔루션) | | AD 배포 정책 이용하여  OU 랜섬웨어 배포 | ㆍ | 백신 프로그램  EDR | |

## 침해 사고 타임라인



[그림 2.1] 침해 사고 타임라인



[그림 2.2] 침해 사고 모식도

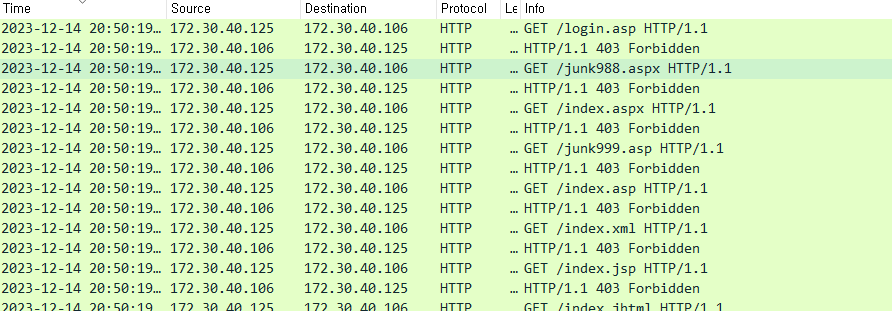
| **No** | **타임라인**  **(2023-12-14)** | **SRC** | **DST** | **설명** |
| --- | --- | --- | --- | --- |
| 1 | 20:50:02 | 공격자1 | EX서버 | 공격대상 취약점 스캔 |
| 2 | 20:52:05 | 공격자1 | EX서버 | CVE-2021-26855 & CVE-2021-27065 취약점을 활용한  웹쉘 업로드 |
| 3 | 20:52:19 | 공격자1 | EX서버 | 웹쉘을 통해 방화벽 & Defender OFF, 계정 생성 및 attack.zip 다운로드 |
| 4 | 20:52:43 | 공격자1 | EX서버 | frpc.exe를 이용해 Exchange서버 RDP 접속 |
| 5 | 20:53:58 | 공격자1 | EX서버 | Reverse Connection위해 payload.exe실행 |
| 6 | 20:55:55 | 공격자1 | EX서버 | mimikatz.exe를 이용해 AD관리자 계정정보 덤핑 |
| 7 | 20:58:05 | EX서버 | AD서버 | Exchange서버에서 AD서버로 RDP접속 |
| 8 | 20:59:09 | AD서버 | EX서버 | attack.zip 다운로드 |
| 9 | 21:00:05 | AD서버 | - | Gathering을 통해OU정보 수집 |
| 10 | 21:03:45 | AD서버 | OU | AD서버에서 방화벽 & Defender OFF 정책 배포 |
| 11 | 21:06:06 | AD서버 | OU | AD서버에서 Readme.msi(랜섬웨어)배포 |
| 12 | 21:06:24 | AD서버 | DB서버 | AD서버에서 DB관리자 RDP 접속 |
| 13 | 21:07:21 | DB서버 | 공격자2 | Reverse Connection 위해 update.exe 실행 |
| 14 | 21:09:15 | DB서버 | DB서버 | DB접속 후 고객정보 관련 DB탈취 |
| 15 | 21:10:21 | DB서버 | - | 공격자가 사용했던 도구 삭제 |
| 16 | 21:12:44 | AD서버 | - | hello.exe 랜섬웨어 실행 |

[표 2‑1] 타임라인 표

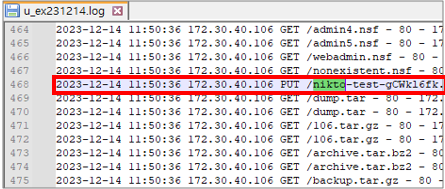
# 상세 조사 결과

## Exchange Server (WIN-NNR40DDHJ75, 172.30.40.106)

방화벽 로그 확인 결과, 2023-12-14 20:50:19부터 공격자 A (172.30.40.125) 로부터 스캔 공격이 들어온 것이 확인된다. 또한 2023-12-14 20:50:36부터 Exchange서버의 웹 로그에서 nikto 스캔 공격의 정황도 확인된다.

****

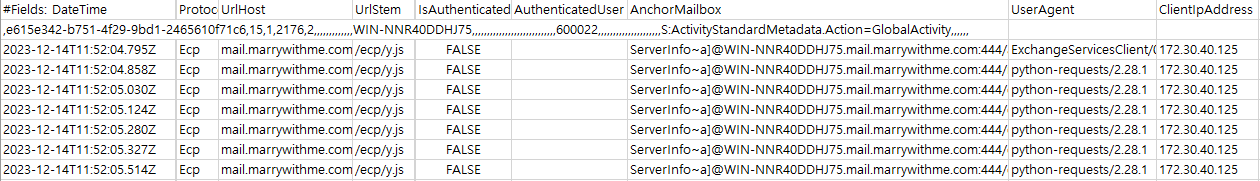
[그림 3.1] 방화벽 로그 확인



[그림 3.2] 스캔 공격 확인 (UTC+9) 적용 전

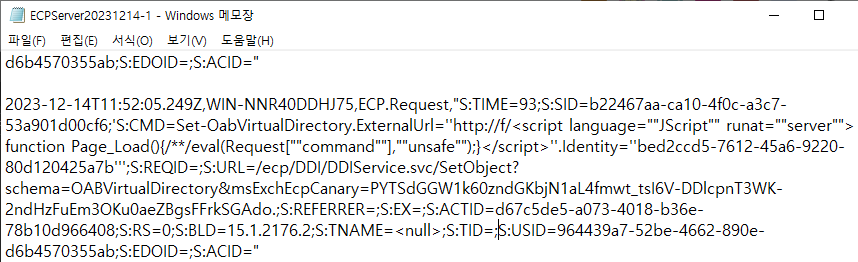
**CVE-2021-26855 + CVE-2021-27065**

현재 사용자의 Exchange 서버에는 /ECP 경로에 요청을 보낼 때 사용되는 쿠키인 X-BEResource를 이용하는 취약점(CVE-2021-26855)이 존재한다. 공격자는 2023-12-14 20:52:04부터 쿠키 값을 변조하여 인증 요청을 하고 취약점이 있는 Exchange 서버에서 정상적으로 인증 처리 되어 내부 리소스로 접근하였다. 이때 ECP에 변조된 인증 값을 사용하여 접근할 경우, Exchange 로그에서 AuthenticatedUser 부분이 공란이고 AnchorMailBox가 ServerInfo~\*/\*인 패턴이 확인된다.



[그림 3.3] Exchange의 HttpProxy 로그 중 ECP로그 확인 (UTC+9) 적용 전

아래 사진을 통해 script 태그를 사용하여 eval 함수를 서버 측에서 실행하는 코드가 삽입 되어 있는 것이 확인되며, 이를 통해 2023-12-14 20:52:05부터 공격자가 웹쉘을 생성한 것으로 확인된다.



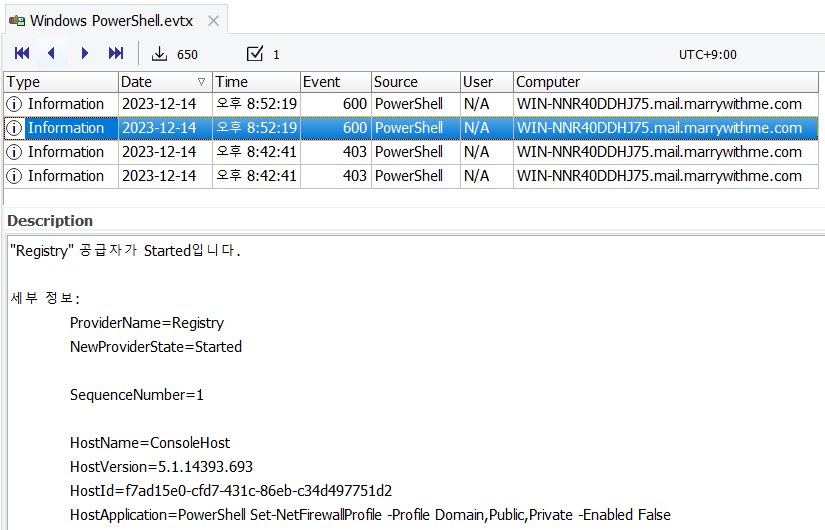
[그림 3.4] Exchange의 ECPServer 로그 (UTC+9) 적용 전

아래의 Exchange의 웹 로그에서 공격자가 2023-12-14 20:52:20 부터 실행한 웹쉘 명령어들을 볼 수 있다.



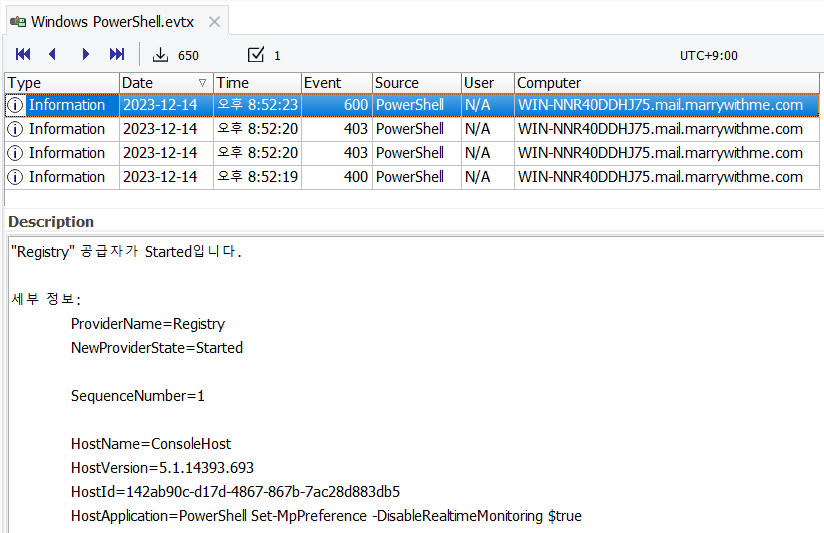
[그림 3.5] Exchange 웹 로그 - 웹쉘 실행 명령어

명령어들을 순서대로 분석해보면, 2023-12-14 20:52:19부터 공격자가 PowerShell 명령어를 사용하여 Windows 방화벽을 비활성화 한 로그가 확인되며, 이는 공격자가 공격을 수행하기 앞서 Windows 방화벽을 비활성화 한 것으로 확인된다.



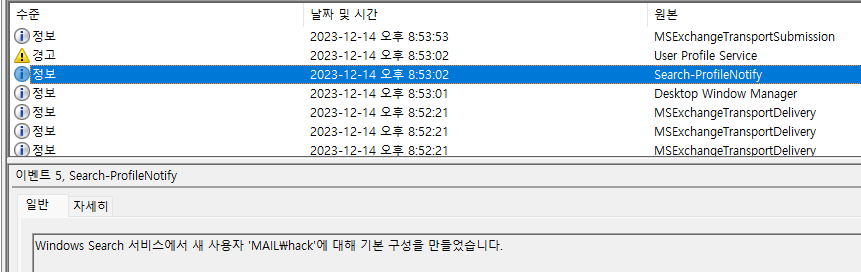
[그림 3.6] 이벤트 로그(PowerShell) - Windows Firewall Off

또한, 2023-12-14 20:52:23부터 공격자가 PowerShell 명령어를 통해 Windows Defender 설정을 수정한 이벤트 로그 확인도 가능하다. 아래 사진에 표시된 명령어는 실시간 보호 기능을 비활성화 하는데 사용된다.



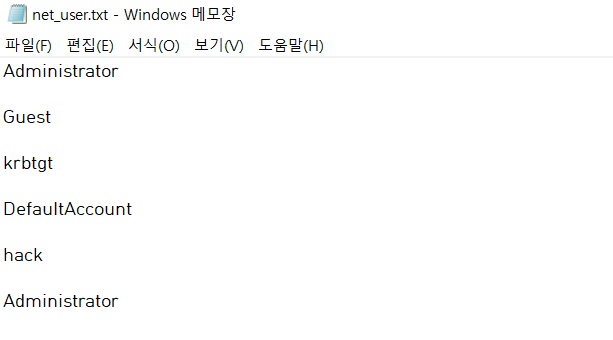
[그림 3.7] 이벤트 로그(PowerShell) - Windows Defender Off 확인

이벤트 뷰어의 Application 로그를 확인해 본 결과, 2023-12-14 20:53:02부터 hack이라는 계정이 생성된 것으로 확인된다.



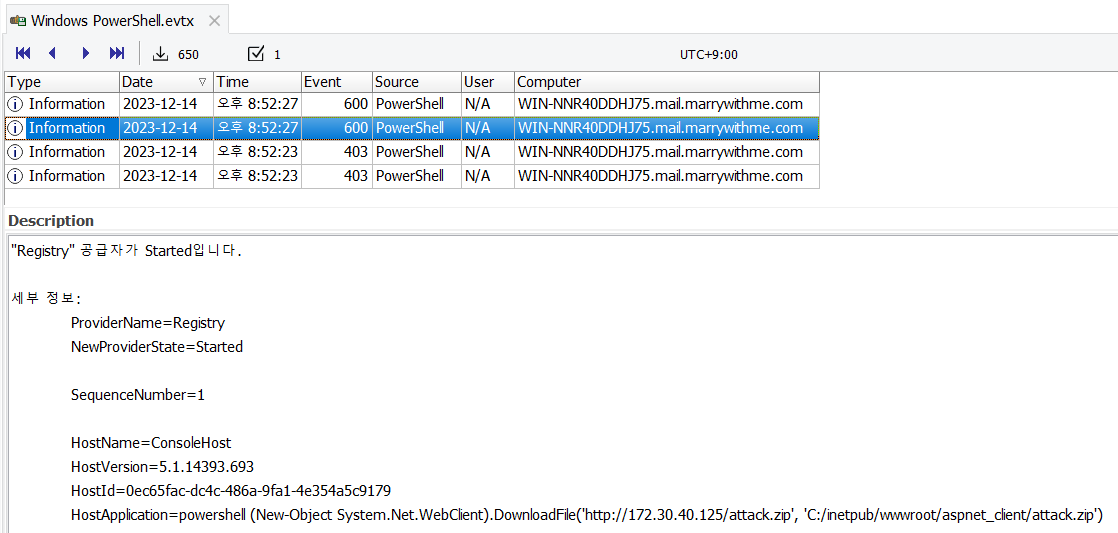
[그림 3.8] 이벤트 로그(Application) – hack 기본 구성 생성

또한 휘발성 데이터 수집 결과 중 하나인 net\_user.txt 와 [그림 3.5] Exchange 웹 로그 - 실행 명령어를 통해 hack이 생성되어 있는 것이 확인된다.



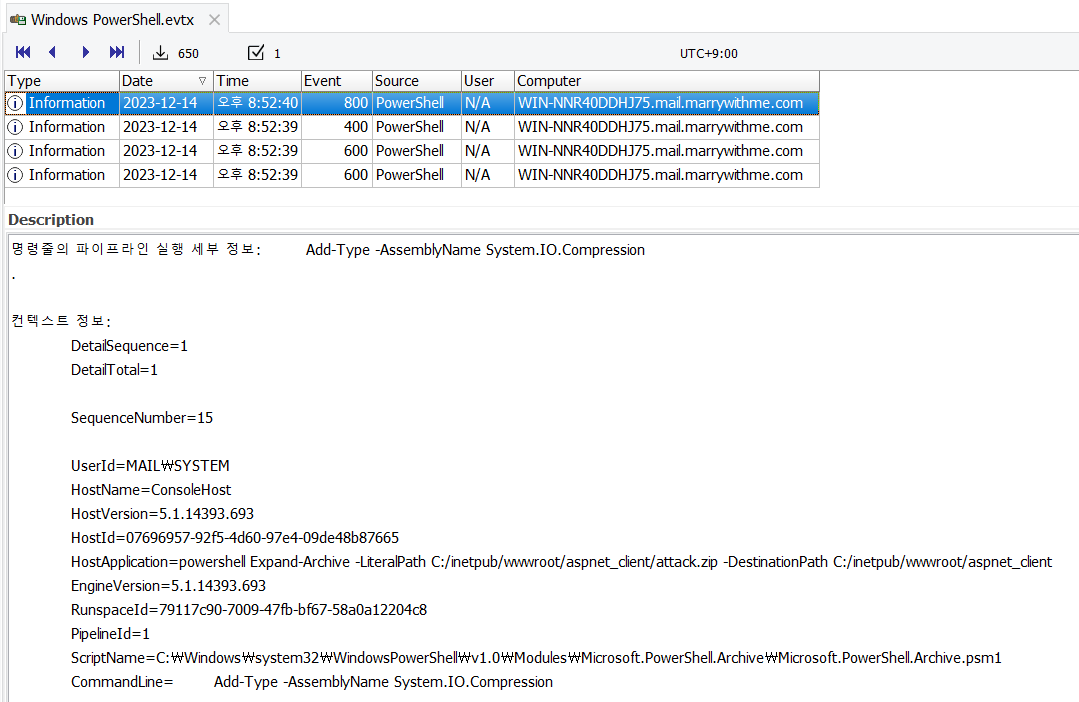
[그림 3.9] net\_user.txt - 계정 정보 확인

공격자는 2023-12-14 20:52:27부터 웹쉘을 이용하여 ‘http://172.30.40.125’ 에서 압축파일(attack.zip)을 다운로드하고, ‘C:/inetpub/wwwroot/aspnet\_client’에 저장하는 명령어를 실행한 흔적을 Powershell 이벤트 로그에서 확인 하였고. 이는 공격자가 [그림 3.6] 이벤트 로그(PowerShell) - Windows Firewall Off [그림 3.7] 이벤트 로그(PowerShell) - Windows Defender Off 확인 을 통해 Windows Defender 및 실시간 감시를 비활성화 후 악성 파일을 다운로드한 것으로 확인된다.



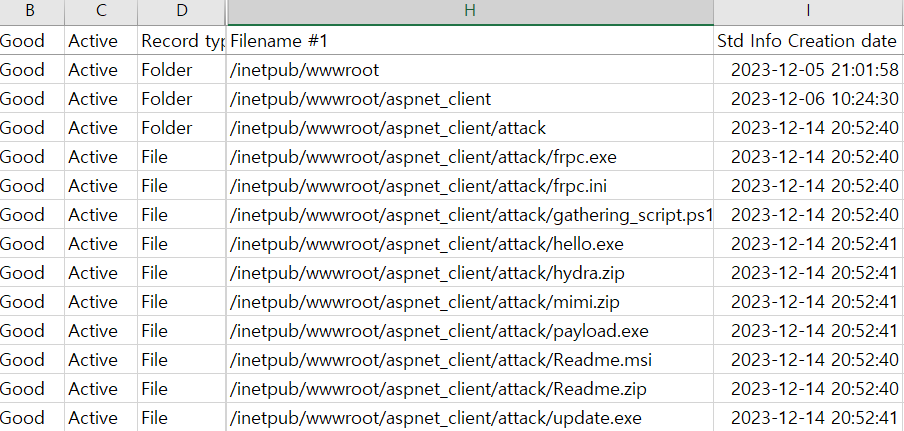
[그림 3.10] 이벤트 로그(PowerShell) - attack.zip 다운로드

공격자는 2023-12-14 20:52:40부터 웹쉘로 공격자가 다운로드한 압축파일(attack.zip)을 압축 해제한 것으로 확인 된다.



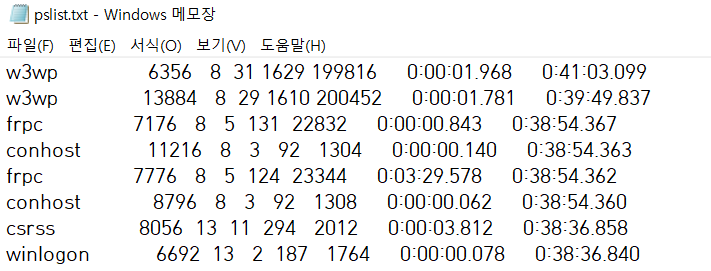
[그림 3.11] 이벤트 로그(PowerShell) - attack.zip 압축 해제

공격자가 2023-12-14 20:52:40부터 다운로드한 압축파일(attack.zip) 압축 해제 후 공격자가 사용할 공격 도구 및 실행 파일이 내부에 포함되어 있음을 아래 사진을 통해 알 수 있다.



[그림 3.12] MFT – attack.zip 내의 파일 확인

frpc는 Reverse Connection을 통해 원격으로 RDP에 접근이 가능하도록 한다. [그림 3.13] pslist.txt – frpc.exe 실행 확인을 보면 frpc가 실행 중임을 확인 하였고 frpc.ini를 확인한 결과, 공격자 A (172.30.40.125)의 7000번 포트로 RDP 연결 시키는 파일 인 것이 확인된다.

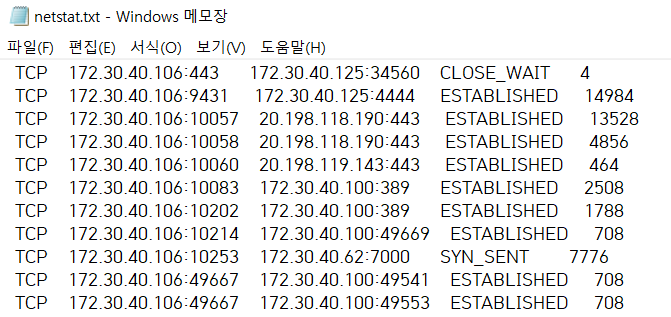


[그림 3.13] pslist.txt – frpc.exe 실행 확인



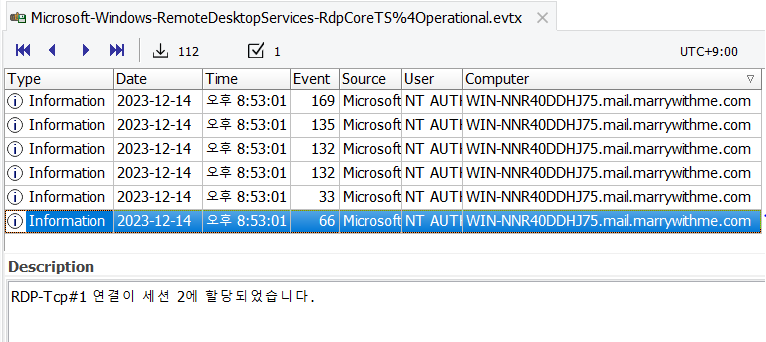
[그림 3.14] frpc.ini 파일 확인

아래 사진을 보면 Exchange 공격자 A (172.30.40.125) 의 7000포트와 연결된 기록이 존재한다. [그림 3.14] frpc.ini 파일 확인에서도 확인 할 수 있듯이 공격자 A (172.30.40.125) IP로 RDP 연결이 확인된다.



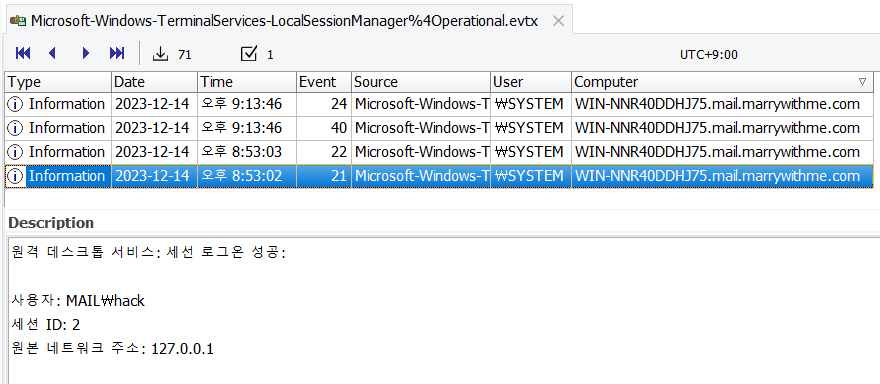
[그림 3.15] netstat.txt - 연결 IP 및 포트 확인

Event Log Explorer를 사용하여 원격 데스크톱 서비스 관련 이벤트 로그 확인 결과, 2023-12-14 20:53:01부터 공격자가 Exchange 서버인 WIN-NNR40DDHJ75.mail.marrywithme.com와 RDP 연결이 확인된다.



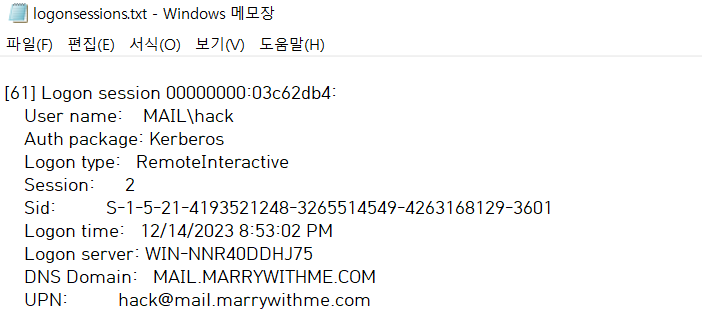
[그림 3.16] 이벤트 로그(RdpCore) - RDP 세션 연결 내역

Exchange 서버 WIN-NNR40DDHJ75.mail.marrywithme.com에 원격 데스크톱 서비스가 실행되어 세션 로그온 성공이 확인된다. 공격자는 2023-12-14 20:53:02부터 해당 시점에 거점 확보를 위하여 Exchange 서버에 침투한 것으로 확인된다.



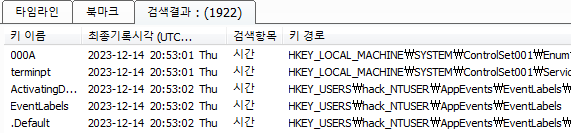
[그림 3.17] 이벤트 로그(LocalSession) - RDP 세션 로그온 성공 내역

휘발성 데이터 수집 결과 중 하나인 logonsessions.txt를 통해서 공격자는 새로 생성된 MAIL\hack 계정으로 Exchange 서버 mail.marrywithme.com에 세션 로그인 한 내역이 확인된다.



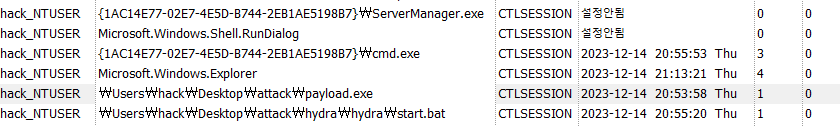
[그림 3.18] logonsessions.txt - 로그온 세션 정보

REGA를 사용하여 레지스트리를 분석한 결과, 2023-12-14 20:53:02부터 공격자가 Exchange 서버에 RDP로 접속한 후 최초 활동한 시간대를 알 수 있다.



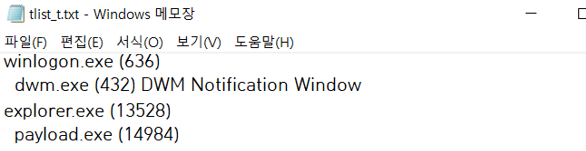
[그림 3.19] 레지스트리(REGA) - 공격자 최초 활동 내역

REGA를 통해 응용프로그램 사용 로그 확인 결과, 공격자는 2023-12-14 20:53:58부터 hack 계정으로 payload.exe(백도어)를 실행한 것이 확인된다. 공격자는 Exchange 서버로 최초 침투 후 연결 유지를 위해 payload.exe(백도어)를 실행한 것으로 보인다.



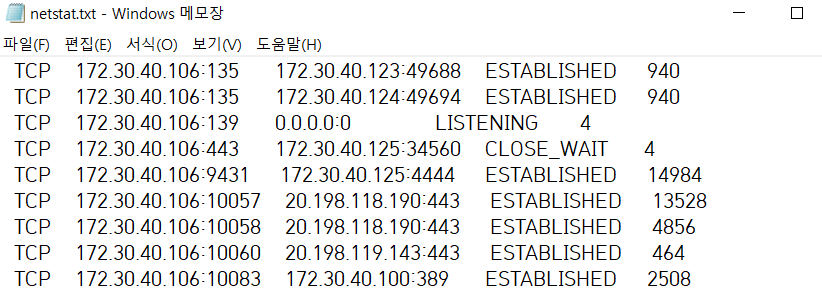
[그림 3.20] 레지스트리(REGA) - backdoor 흔적 확인

프로세스 트리 구조 확인 결과, explorer.exe 고객정보 DB 탈취, 악성코드 실행(백도어) 자식 프로세스로 payload.exe(백도어)가 실행된 것으로 보인다.



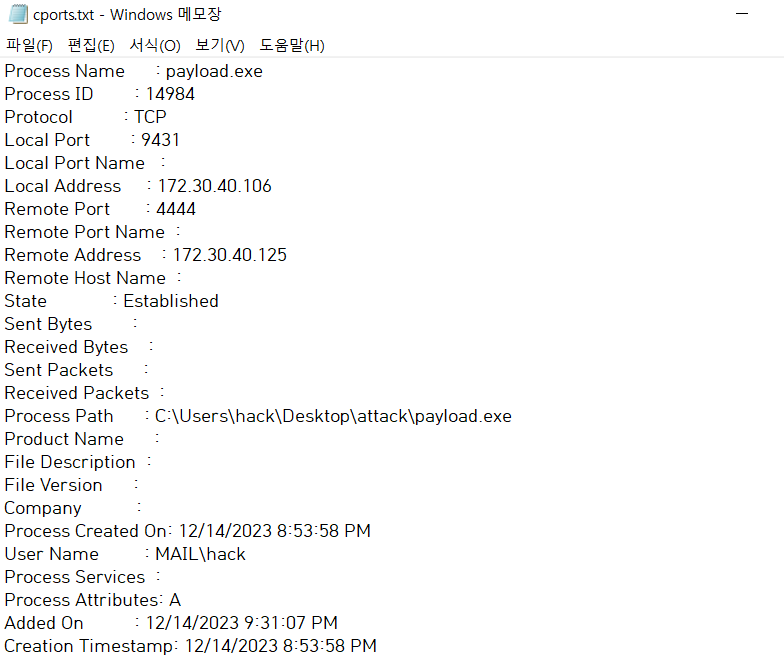
[그림 3.21] t\_list.txt - payload.exe 실행

네트워크 통신 내역 확인 결과, 최초 침투 지점인 Exchange 서버(172.30.40.106)와 TCP 통신한 IP 정보 리스트를 확인할 수 있다.[그림 3.10] 이벤트 로그(PowerShell) - attack.zip 다운로드에서 웹쉘을 통해 http://172.30.40.125로부터 공격자가 압축파일(attack.zip)을 다운로드한 로그를 보면 공격자 A (172.30.40.125) IP는 최초 침투를 위해 사용된 공격자 IP인 것으로 확인된다.



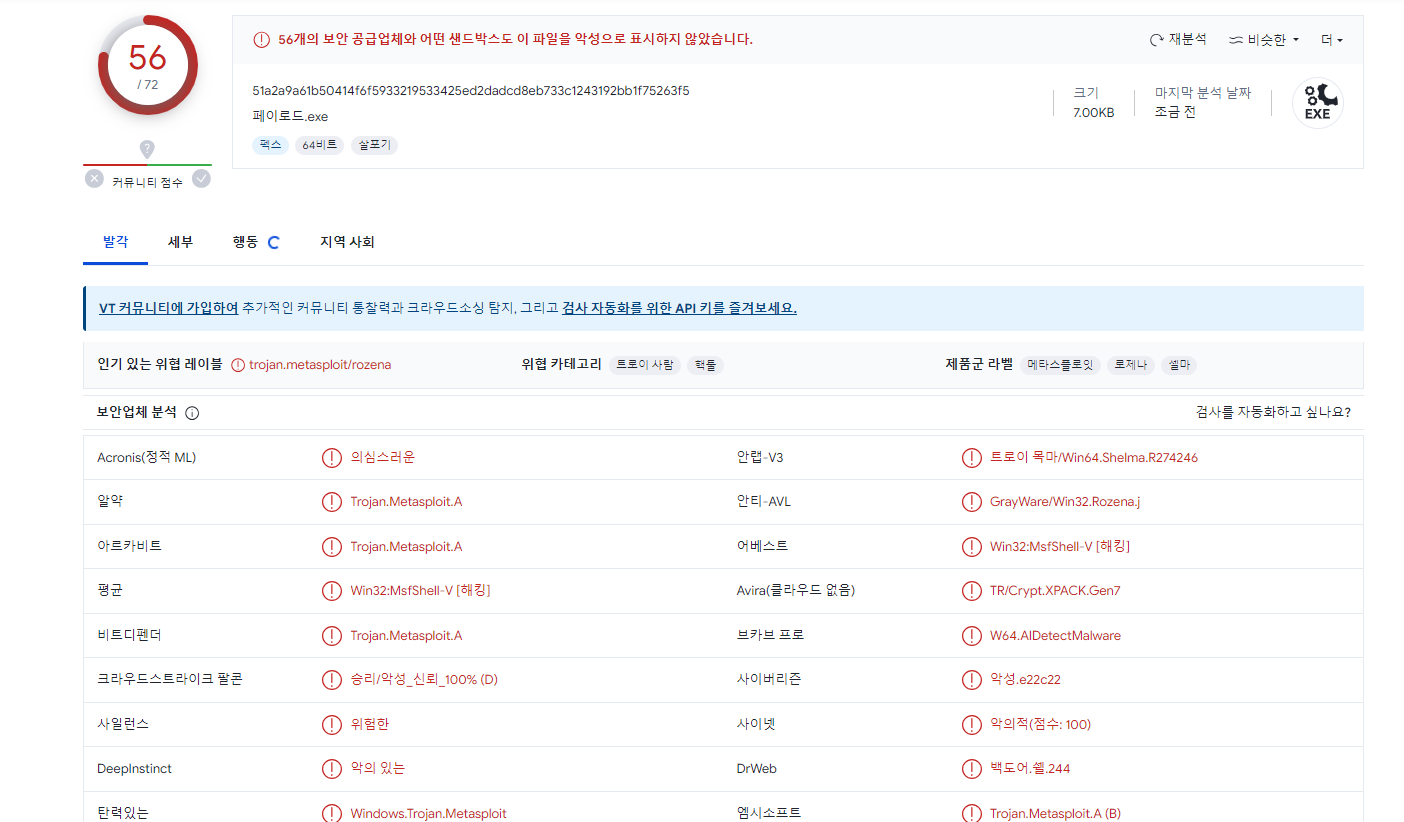
[그림 3.22] netstat.txt - backdoor 연결 공격자 IP 확인

cports.txt 통해서 payload.exe(백도어)를 실행하여 공격자로 추정된 IP 172.30.40.125가 Exchange 서버 172.30.40.106와 4444 포트를 통해 원격 통신한 것으로 확인된다.



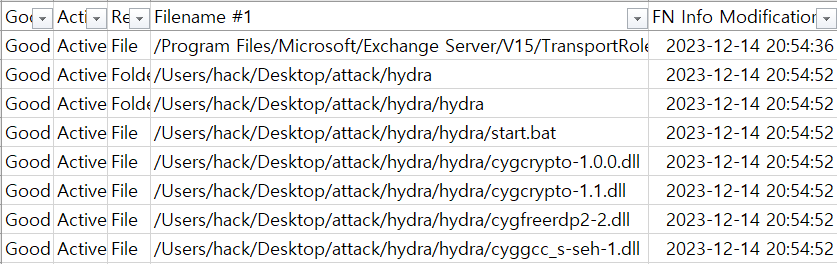
[그림 3.23] cports.txt - payload.exe 실행

Virus Total을 통해 분석을 진행한 결과 payload.exe(백도어) 파일은 외부와 Reverse 연결하는 악성 파일로 확인된다.



[그림 3.24] Virus Total – payload.exe 결과

MFT 확인 결과 공격자가 2023-12-14 20:54:52부터 /Users/hack/Desktop/attack/hydra/ 경로에 hydra 폴더가 생성된 기록이 확인 가능하다. 내부에 hydra 실행 파일이 존재하는 것으로 확인된다.



[그림 3.25] hydra 폴더 생성 확인

2023-12-14 20:55:20부터 hydra 실행 파일인 start.bat 파일을 실행한 로그가 확인된다.



[그림 3.26] 레지스트리(REGA) - hydra start.bat 실행 로그

start.bat 실행 후, 2023-12-14 20:55:28부터 hydra 하위 경로에 output.txt가 생성된 것을 확인 할 수 있고, 공격자는 hydra를 통해 내부 AD 관리자 계정 비밀번호 탈취 시도한 것으로 보이지만 이 행위를 통해 계정정보를 탈취하였는지는 확인 할 수 없었다.

텍스트, 폰트, 번호, 라인이(가) 표시된 사진

자동 생성된 설명

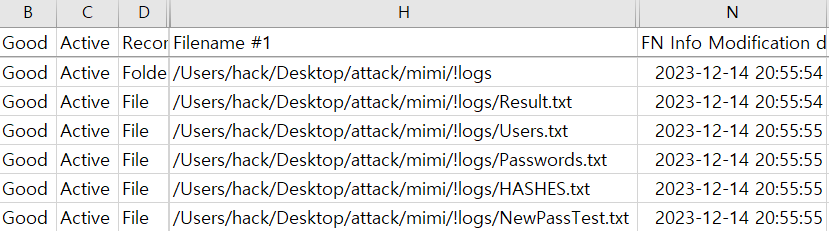
[그림 3.27] 레지스트리(REGA) - output.txt

MFT 확인 결과, 공격자가 2023-12-14 20:55:45부터 Users/hack/Desktop/attack/mimi/ 경로에 Mimi 폴더 생성이 확인되며 폴더 안 프로그램을 확인 해본 결과 암호 크래킹 도구인 mimikatz인 것을 확인 하였다.



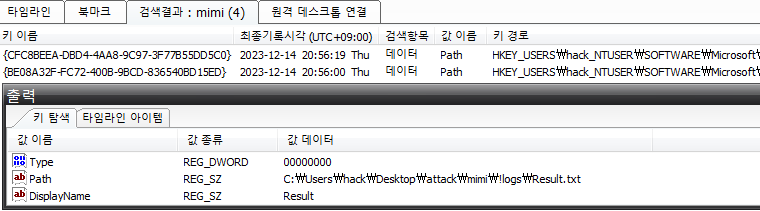
[그림 3.28] MFT - mimikatz 폴더 생성 확인

공격자가 2023-12-14 20:55:54부터 mimikatz를 실행한 결과인 !logs 폴더가 생성되었다. 생성된 파일(HASHES.txt)의 hash 값을 통해 공격자는 관리자 계정 비밀번호를 탈취한 것으로 보인다.

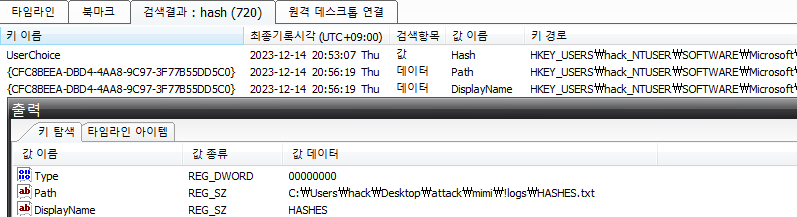


[그림 3.29] MFT - mimikatz 실행 결과

2023-12-14 20:56:00부터 \!log에 Result.txt 및 2023-12-14 20:56:19부터 hash.txt가 생성된 것이REGA를 통해서도 확인된다.

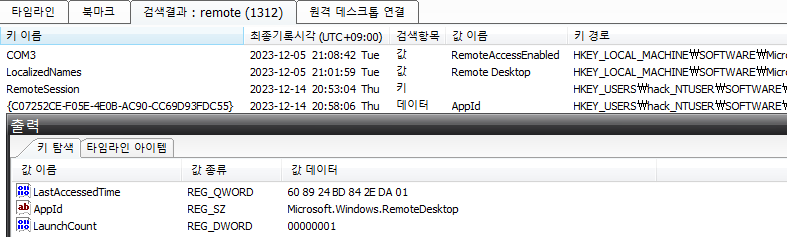


[그림 3.30] 레지스트리(REGA) - Result.txt

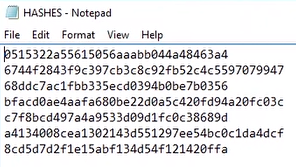


[그림 3.31] 레지스트리(REGA) - HASHES.txt

2023-12-14 20:53:04부터 공격자는 mimikatz를 통해 얻은 해시값을 복호화 하여 관리자 계정 비밀번호를 획득하고 AD에 RDP 접속한 것으로 확인된다.

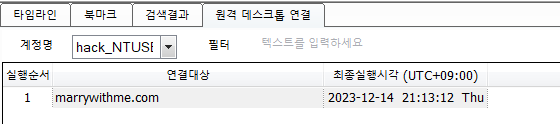


[그림 3.32] 레지스트리(REGA) - RemoteDesktop 실행



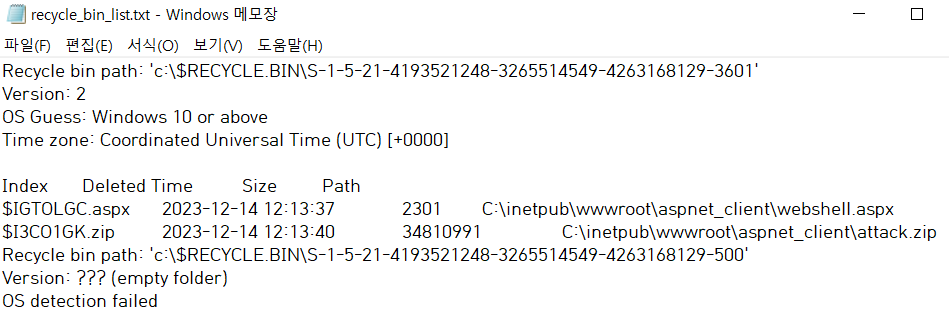
[그림 3.33] HASHES.txt 내용 확인

아래 그림을 통해 공격자가 Exchange 서버에서 AD에 연결된 RDP의 최종 실행 시각이 2023-12-14 21:13:12로, 이때 공격자는 Exchange 서버와 AD 간의 RDP 접속을 종료한 것으로 확인된다.



[그림 3.34] 레지스트리(REGA) - RDP 최종실행시각

recycle\_bin\_list.txt를 확인한 결과, 2023-12-14 21:13:47부터 webshell.aspx, attack.zip 파일이 삭제된 것으로 확인된다. 이는 공격자가 Exchange 서버에서 AD와의 RDP 접속 종료 후, Exchange 서버에서 수행한 공격 행위의 흔적을 지우기 위해 webshell.aspx와 attack.zip 파일을 삭제한 것으로 확인된다.



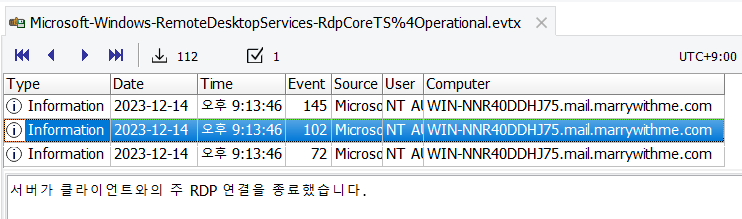
[그림 3.35] recycle\_bin\_list.txt - 휴지통 존재 파일 확인 (UTC+9) 적용 전

netusers\_local\_history.txt를 통해 공격자 소유 계정 hack으로 Exchange 서버에서의 마지막 로그온 시간대가 2023-12-14 21:13분 인 것으로 확인된다.



[그림 3.36] netusers\_local\_history.txt - 공격자 마지막 로그온 확인

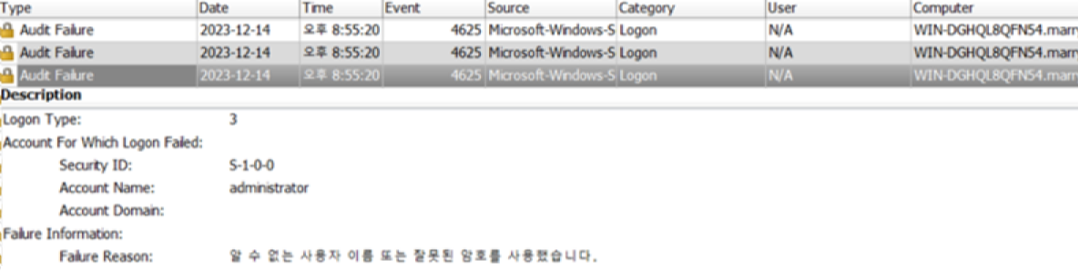
이벤트 로그(RdpCore)를 통해 RDP 관련 이벤트 로그 확인 결과, 공격자가 2023-12-14 21:13:46부터 모든 공격을 마치고 Exchange 서버와의 RDP 연결을 종료한 것이 확인된다.



[그림 3.37] 이벤트 로그(RdpCore) - RDP 연결 종료 시간 확인

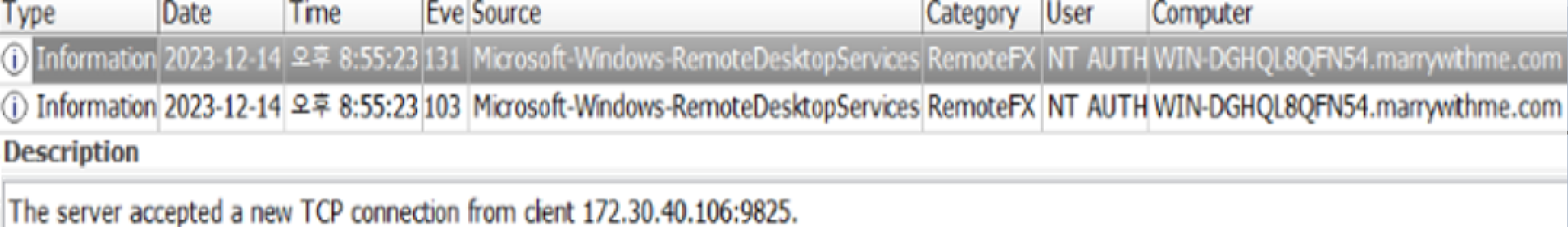
## Active Directory (WIN-DGHQL8QFN54, 172.30.40.100)

[그림 3.26] 레지스트리(REGA) - hydra start.bat 실행 로그 에서는 계정탈취 성공여부를 확인 할 수 없었지만 아래 로그가 같은 시간대에 아래 로그인 실패한 로그 기록이 대량으로 확인된 것으로 보아, hydra를 통해 2023-12-14 20:55:20부터 무차별 대입 공격이 이루어졌음이 확인된다.



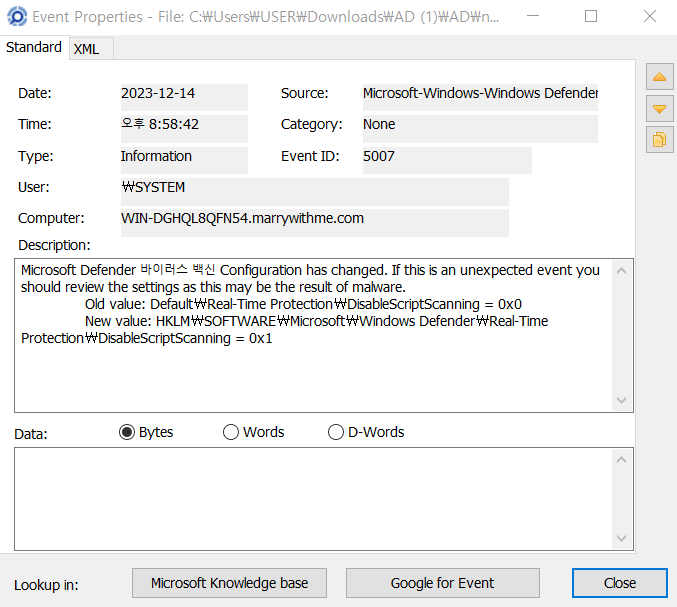
[그림 3.38] 이벤트 로그 (Security) – 로그인 실패

[그림 3.29] MFT - mimikatz 실행 결과와 [그림 3.33] HASHES.txt 내용 확인 에서 수집한 계정 정보로 2023-12-14 20:55:23부터 AD 서버에 원격 접속했다는 것이 확인된다.



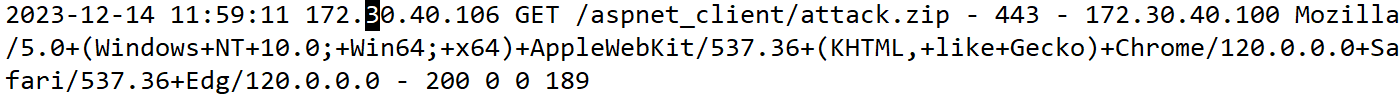
[그림 3.39] 이벤트 로그(RemoteDesktopServices) – 원격 접속

RDP로 접속한 공격자가 2023-12-14 20:58:42부터 Windows Defender의 Real-time Protection을 비활성화 한 것을 확인 할 수 있다.

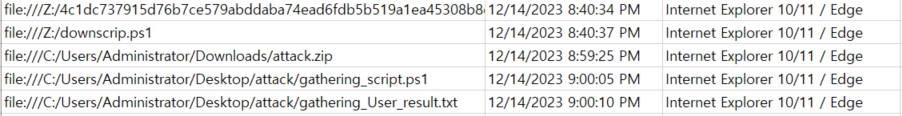


[그림 3.40] 이벤트 로그(Windows Defender) - Defender 비활성화

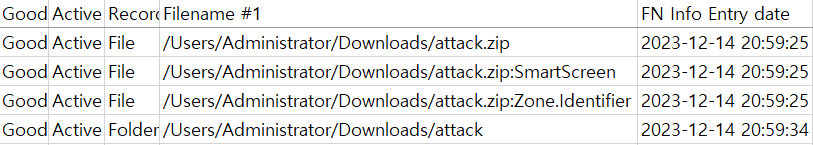
공격자가 2023-12-14 20:55:20부터 Exchange로부터 EDGE로 다운로드한 압축파일(attack.zip)을 웹 로그 에서 확인 할 수 있었고, 2023-12-14 20:59:25부터 MFT에서 attack 폴더 생성이 확인되었다.



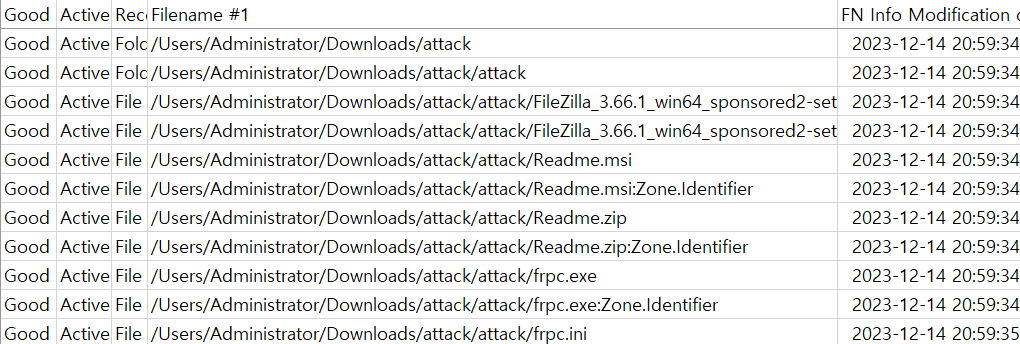
[그림 3.41] exchange 웹 로그 (UTC+9) 적용 전



[그림 3.42] browsinghistory - attack.zip EDGE 다운

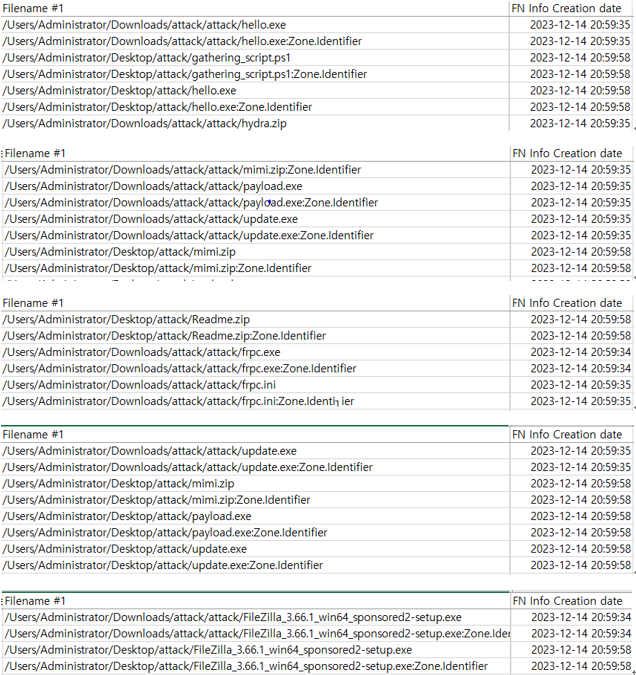


[그림 3.43] attack.zip 다운로드



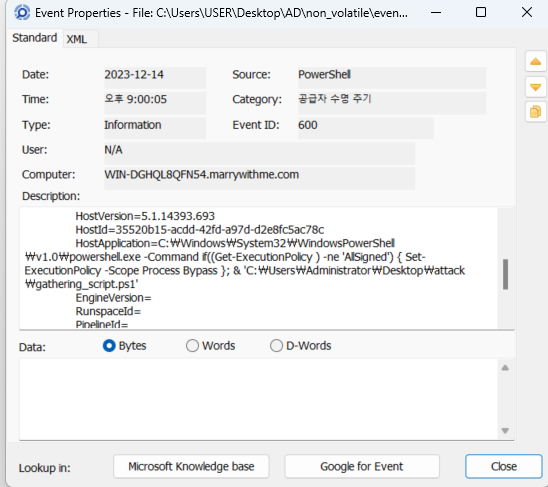
[그림 3.44] MFT – attack 폴더 생성

2023-12-14 20:59:35부터 attack 폴더 안에(hello.exe, payload.exe, frpc.exe, update.exe ,filezilla.setup.exe, gathering\_script.ps1) 생성이 확인되었다.

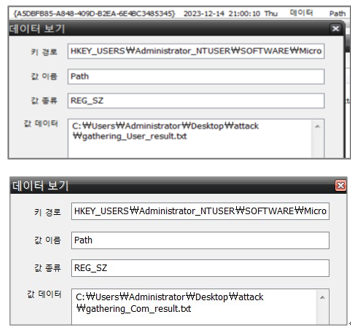


[그림 3.45] MFT – attack 폴더 내용 확인

[그림 3.44] MFT – attack 을 통해 다운받은 해당 폴더 목록 중 gathering\_script.ps1을 확인하였고 아래 그림을 통해 gathering\_script.ps1이 2023-12-14 21:00:05부터 실행된 것이 이벤트 로그(Powershell)에서 확인된다. 해당 파일 확인 결과 OU정보를 수집하여 gathering\_User\_result.txt와 gathering\_Computer\_result.txt로 저장한 것이 아래 사진으로 확인된다.



[그림 3.46] 이벤트 로그(Powershell) - gathering\_script.ps1 실행



[그림 3.47] gathering스크립트 실행결과

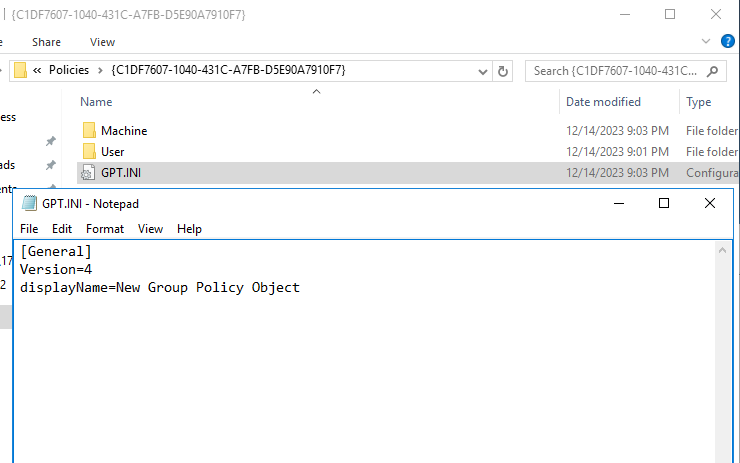
아래 그림을 통해 방화벽 및 Defender 비활성화 하는 정책이 확인된다.

.

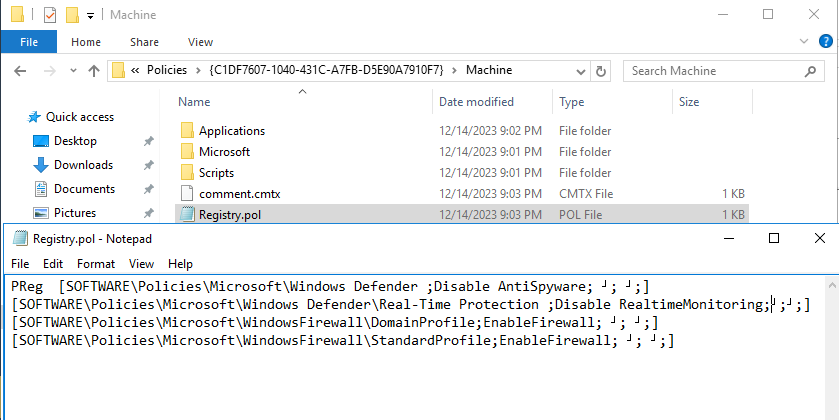


[그림 3.48] def 할당된 정책을 확인

아래 사진을 통해 2023-12-14 21:03부터 Registry.pol 파일에서 정책 추가한 것이 확인된다.

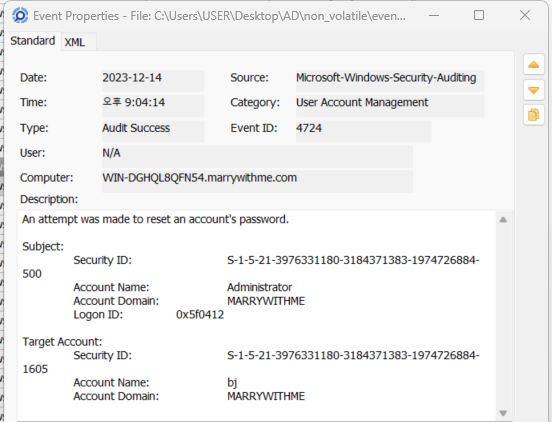


[그림 3.49] 정책 생성 및 생성시간

****

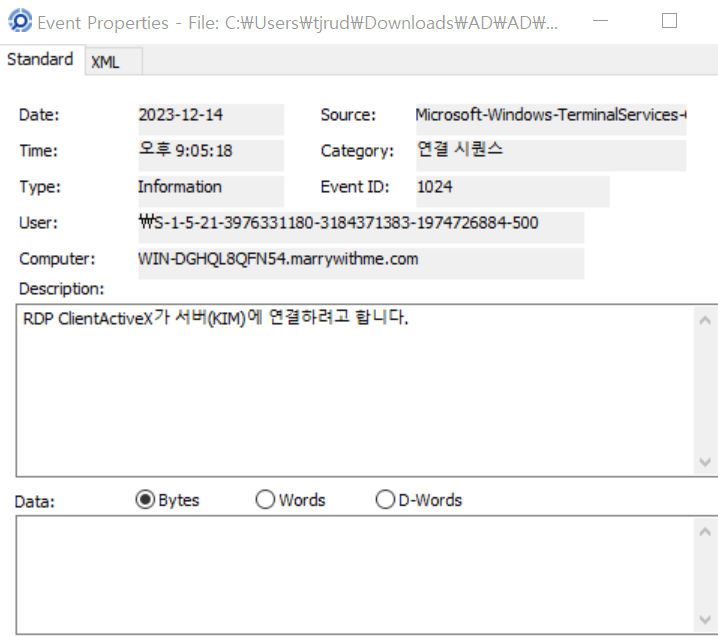
[그림 3.50] 정책 추가 및 설정파일

[그림 3.47] gathering스크립트 실행결과 통해 2023-12-14 21:04:14부터 얻은 OU PC의 계정 정보를 통해 침투할 OU PC의 비밀번호를 변경하였고, 아래 그림을 통해 확인된다.



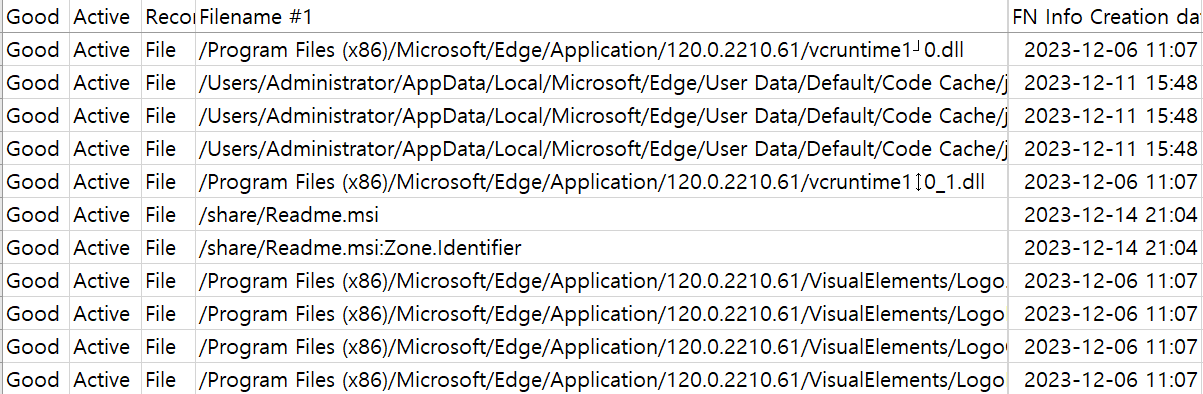
[그림 3.51] 이벤트 로그(security)

[그림 3.51] 이벤트 로그(security)으로 변경한 패스워드를 통해 침투할 DB관리자PC에 RDP 접속한 것을 아래 그림을 통해 확인할 수 있고, 초기 침투 단계부터 공격자는 2023-12-14 21:05:18부터 DB관리자(172.30.40.123) IP로 RDP 접속이 확인된다.

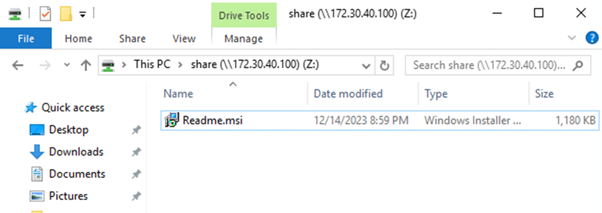


[그림 3.52] 이벤트 로그(TerminalServices) - DB관리자 RDP연결

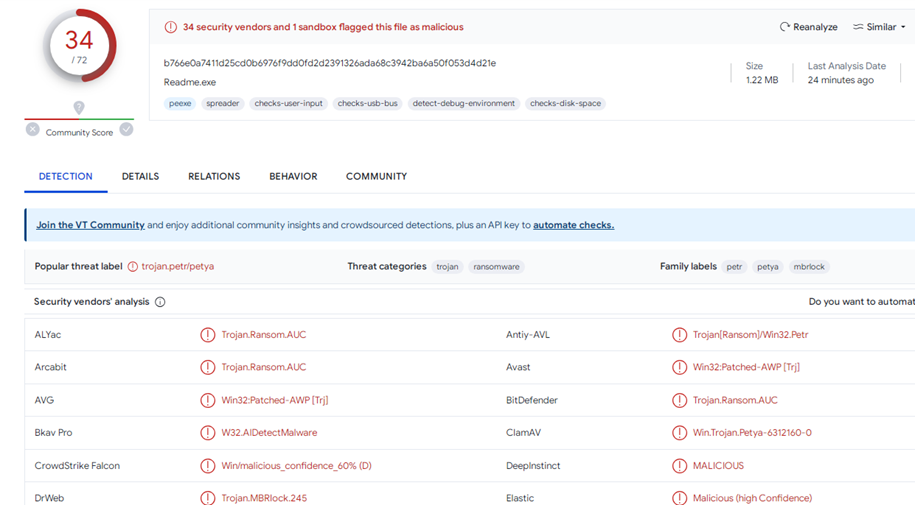
아래 그림을 통해 2023-12-14 21:04부터 Readme.msi 파일이 공유 폴더로 이동한 것을 확인할 수 있으며 Readme.msi파일을 Virus Total에 업로드하여 확인해본 결과 랜섬웨어 파일 인 것을 확인할 수 있었다. 그리고 AD서버에서 Readme.msi을 배포하는 정책이 설정되었다는 것이 확인된다.



[그림 3.53] msi 공유 폴더 이동



[그림 3.54] msi 파일 확인

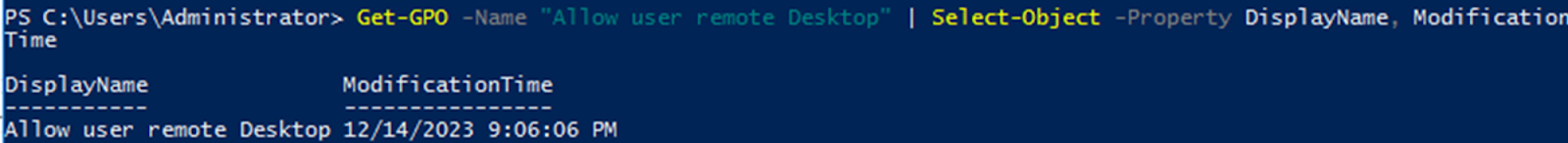


[그림 3.55] Readme.msi Virustotal 업로드

Readme.msi을 배포하는 정책 설정을 확인했고, 아래 사진을 통해 정책 업데이트 한 결과 또한 확인된다.

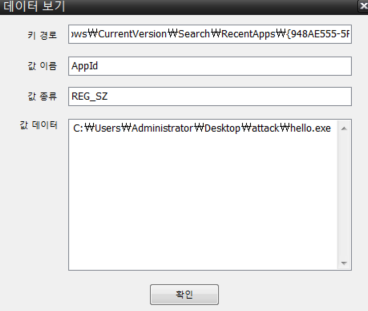


[그림 3.56] Allow user remote Desktop 정책 배포

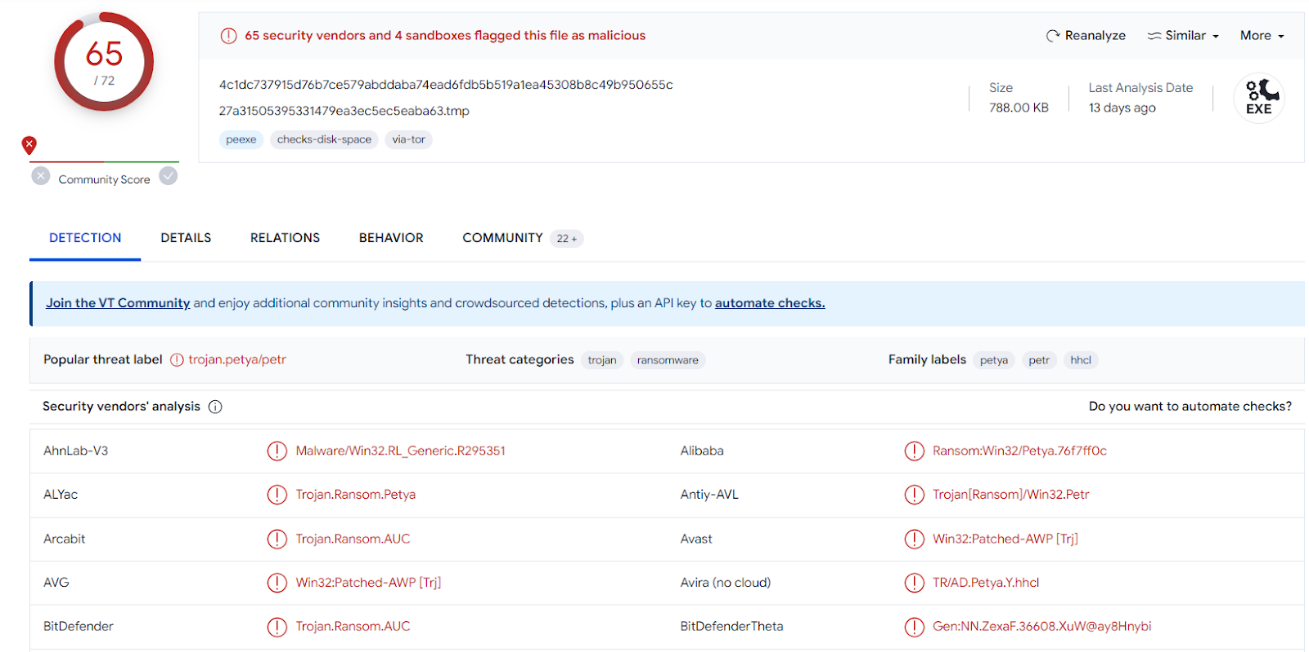


[그림 3.57] Allow user remote Desktop GPO 업데이트 확인 결과

hello.exe파일도 Virus Total에 통해 확인한 결과 [그림 3.55] Readme.msi Virustotal 업로드와 같은 랜섬웨어 파일임을 알 수 있다. 이를 바탕으로 AD 서버에서 랜섬웨어 파일이 실행되었다는 것을 알 수 있다.



[그림 3.58] 레지스트리(REGA) - hello.exe 실행

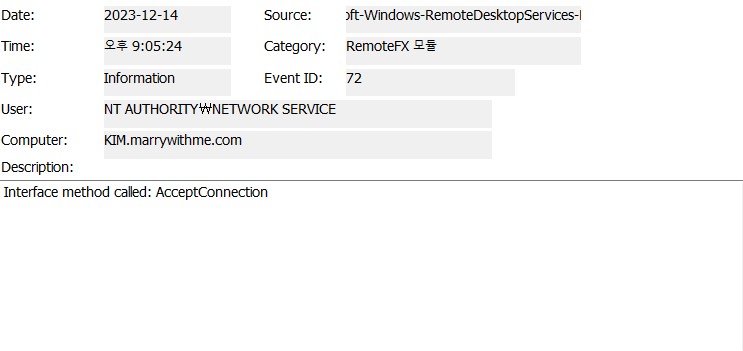


[그림 3.59] Virustotal - hello.exe 확인

`

## DB 관리자(KIM, 172.30.40.123)

[그림 3.51] 이벤트 로그(security)에서 2023-12-14 21:05:24부터 변경한 비밀번호로 DB관리자PC을 RDP로 접속한 로그가 확인된다.

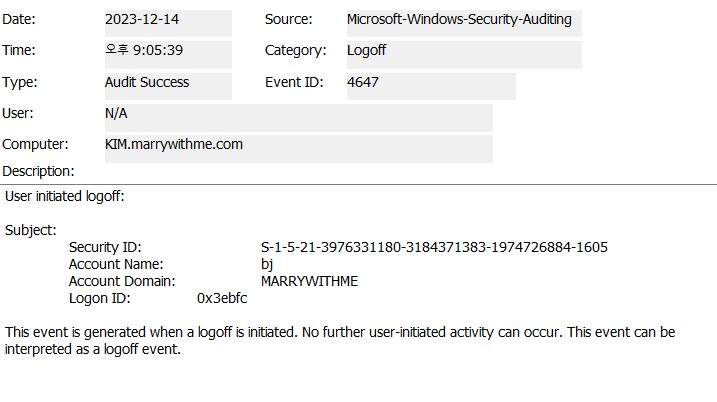
****

[그림 3.60] 이벤트 로그(RemoteDestopServices) - RDP



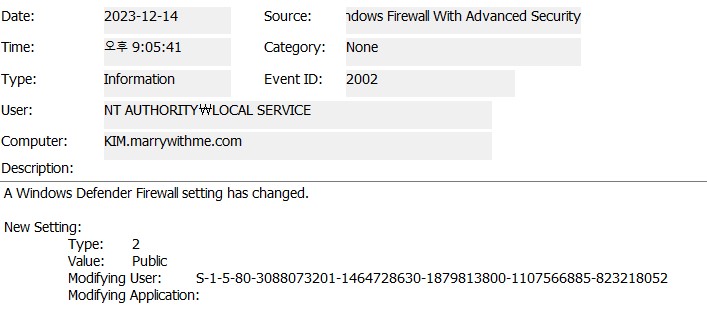
[그림 3.61] 이벤트 로그(Security) - logon

아래그림은 [그림 3.48] def 할당된 정책을 확인을 적용하기 위해서 2023-12-14 21:05:39부터 로그오프한 것으로 보인다.



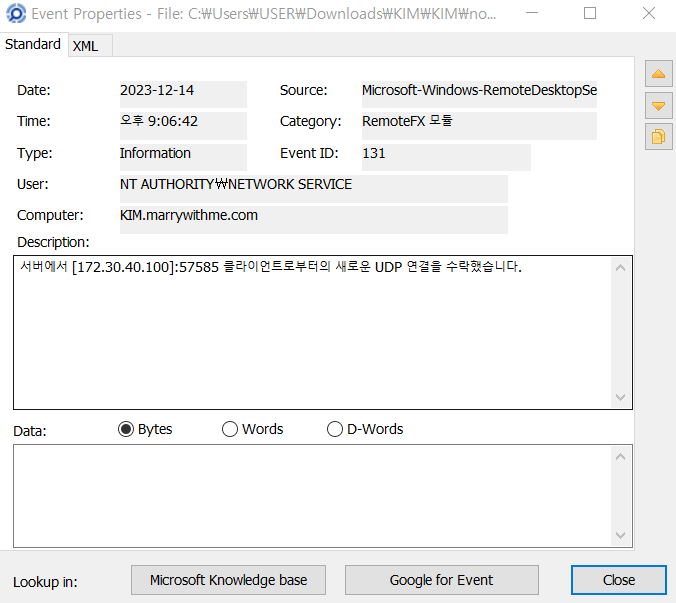
[그림 3.62] 이벤트 로그(Security) – logoff

아래 그림에서 2023-12-14 21:05:41부터 방화벽 정책이 바뀐 것이 확인된다.



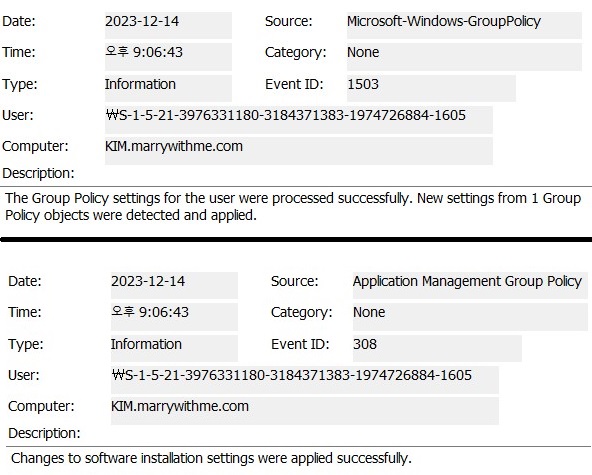
[그림 3.63] 이벤트 로그(Firewall) – Firewall change

아래 그림을 보면 2023-12-14 21:06:42부터 def 정책 적용이 끝난 뒤 다시 RDP 접속한 것으로 보인다.



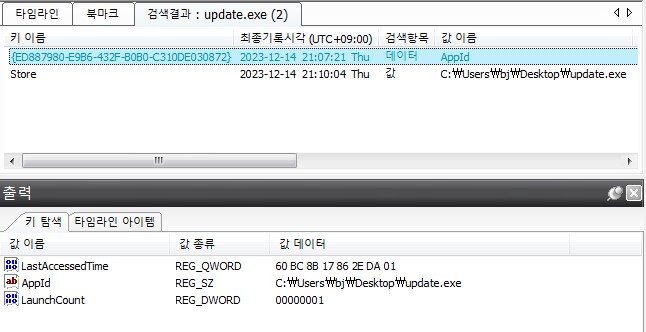
[그림 3.64] 이벤트 로그(RemoteDesktopservice) - RDP

[그림 3.56] Allow user remote Desktop 정책 배포 을 통해 2023-12-14 21:06:43부터 배포된 정책이 설정되었다는 것을 아래 그림을 통해 알 수 있다.



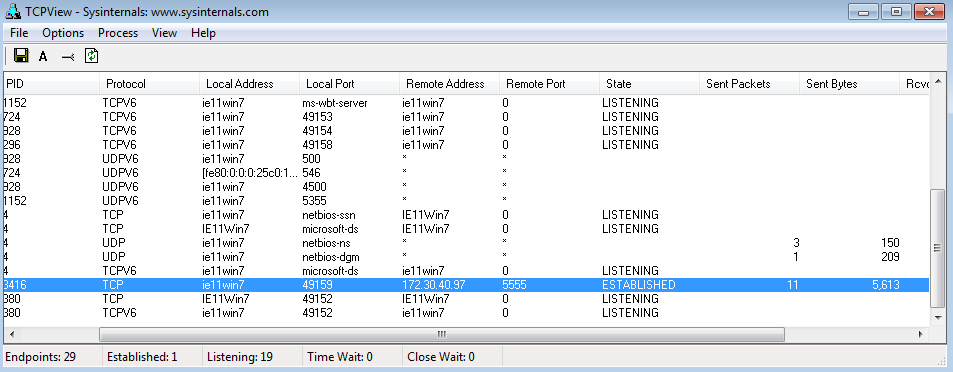
[그림 3.65] 이벤트 로그(Group Policy) – 정책배포

아래 그림을 보면 레지스트리 분석 도구(REGA)를 통해 2023-12-14 21:07:21부터 바탕화면에 있는 update.exe(백도어) 파일 실행된 흔적이 확인된다.



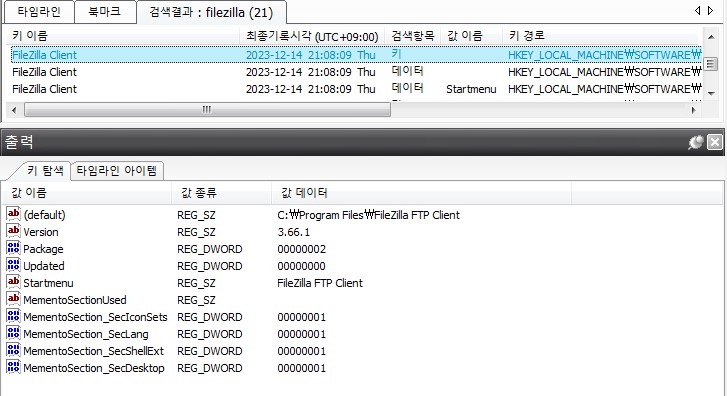
[그림 3.66] 레지스트리(REGA) - update.exe 실행

아래 그림은 update.exe(백도어)를 추출하여 샌드박스에서 동적 분석을 실행한 결과, 공격자 B (172.30.40.97)의 5555포트와 연결되는 것이 확인되고, 이를 통해 백도어를 생성하는 파일이라는 것을 알 수 있다.



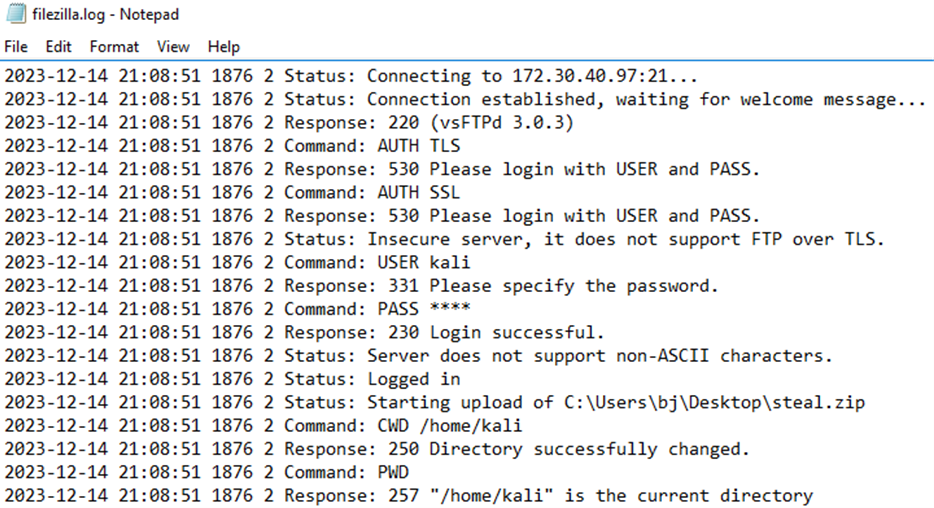
[그림 3.67] TcpView – update.exe 실행

2023-12-14 21:08:09부터 레지스트리(REGA)를 통해 filezilla가 실행되었다는 것이 확인된다.



[그림 3.68] 레지스트리(REGA) - filezilla 실행

filezilla 로그를 통해 확인한 결과, 2023-12-14 21:08:51부터 filezilla에 접속이 확인되었으며, DB 관리자 PC가 공격자 B (172.30.40.97) 에 연결한 것이 확인된다.

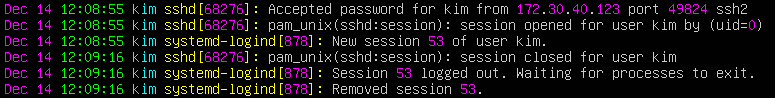


[그림 3.69] filezilla 로그

MFT파일을 통해 확인한 WinSCP.ini 실행 시간과, auth.log에서 확인한 DB관리자가 (172.30.40.123) 접속한 로그를 통해 공격자가2023-12-14 21:09:15부터 WinSCP를 이용해 DB에 접속한 것으로 보인다.

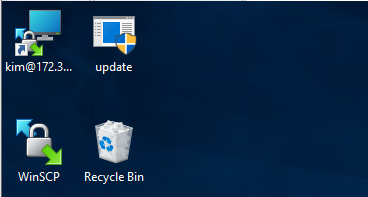


[그림 3.70] MFT – WinSCP



[그림 3.71] auth.log의 DB서버 접속

공격자는 바탕화면에 있는 WinSCP 자동 로그인 세션을 통해 DB에 접근한 것으로 보인다.



[그림 3.72] WinSCP DB 서버 자동 로그인

filezilla 로그를 통해 확인한 결과 공격자가 2023-12-14 21:09:57부터 steal.zip 파일을 공격자 B (172.30.40.97) 로 전송했다는 것을 알 수 있다.



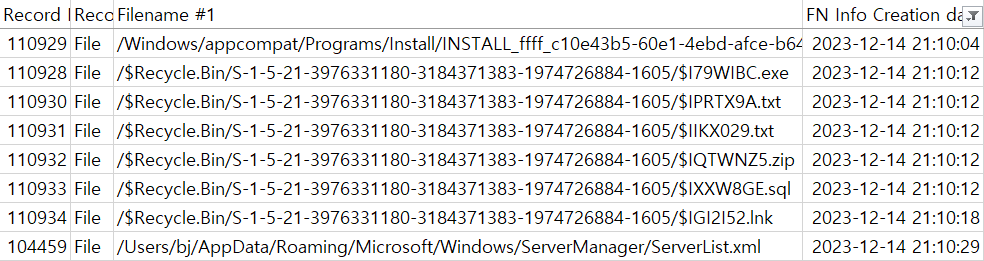
[그림 3.73] filezila.log - steal.zip탈취

 휴지통에서 복원한 steal.zip 내에 있는 db\_backup.sql 파일 내용을 확인해 본 결과, DB서버의 고객 정보를 확인할 수 있었고, 이는 공격자가 고객 정보를 탈취해서 유출시켰다는 것을 의미한다.

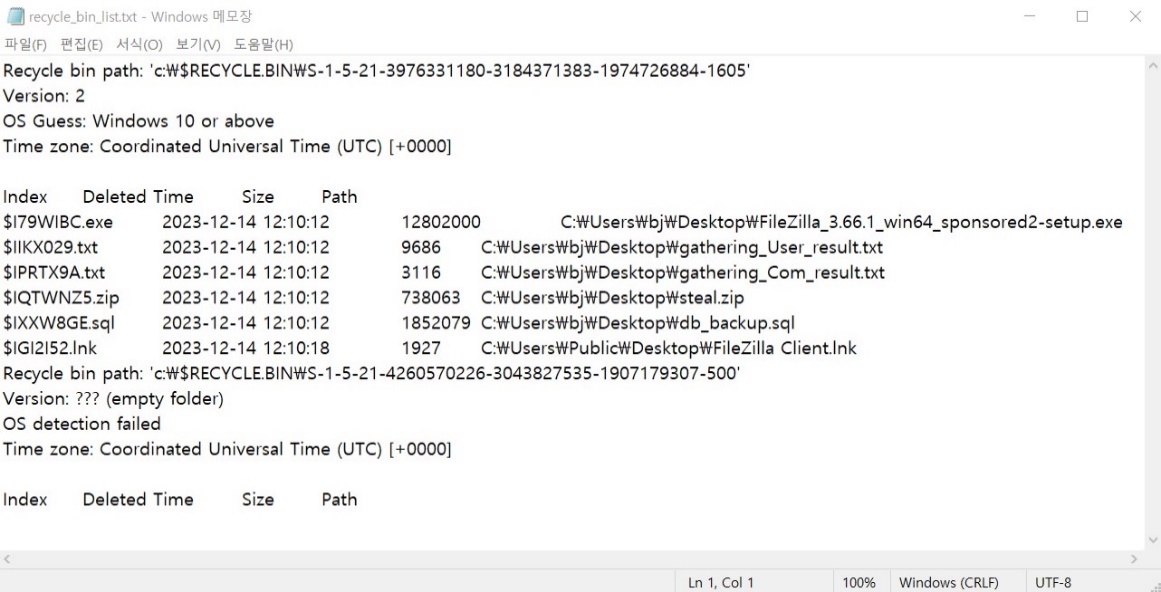


[그림 3.74] db\_backup.sql

MFT를 통해 공격자가 사용한 도구 및 탈취 파일들을 2023-12-14 21:10:12부터 삭제한 것을 확인하였고, 휴지통에서 삭제된 파일(filezlila.exe, gathering\_User\_result.txt, steal.zip)이 확인된다.

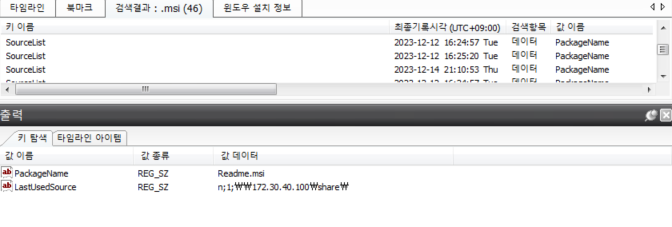
****

[그림 3.75] MFT – 도구 및 탈취 파일 삭제 확인



[그림 3.76] 삭제된 파일명 확인

레지스트리를 통해 (172.30.40.100)에서 공유 폴더[그림 3.54] msi 파일 확인 을 통해 Readme.msi가 2023-12-14 21:10:53부터 공유되어 있는 것을 확인할 수 있다.



[그림 3.77] 레지스트리(REGA) - Readme.msi 공유 기록

# 권고사항

|  |  |  |
| --- | --- | --- |
| **행위** | **개선 사항** | **솔루션** |
| OWA서버 노출 | OWA서버 외부 접근 차단 | WAF서비스, 보안관제 서비스 |
| 취약한 Exchange 버전 | KB패치, CU패치 |  |
| DB관리자와 DB서버 자동로그인 | 자동 로그인 세션 만료 시간 설정 | DB 접근 제어 솔루션 |
| 암호화 되지 않은 DB | 2차인증, DB 암호화 | DB 통합 솔루션, DLP |
| 아웃바운드 정책 미흡 | 아웃바운드 정책 설정 | 백신 프로그램 |
| 악성파일 설치 및 실행 | 아웃바운드 정책 설정 | 백신 프로그램, EDR |
| 웹쉘을 이용한 명령어 실행 | 웹 디렉토리 실행 권한 설정 | 웹쉘 탐지 솔루션 |
| 계정 정보 수집 도구 사용한  관리자 계정 획득 | 비밀번호 정책 강화  WDigest 비활성화 |  |
| 망 분리 미흡 | Trust To Trust 접근 정책 강화 | 접근 통제 솔루션 |

[표 4‑1] 권고사항

## WAF 솔루션

트래픽을 모니터링 및 필터링하고, 웹 어플리케이션으로 들어오는 악성 트래픽 또는 앱에서 보안 이벤트를 탐지한다.

## Exchange 서버 (KB 패치, CU 패치)

취약한 버전의 KB 패치와 CU 패치를 진행하면, 이전 버전에서 발견된 버그들이 수정되며, 새로운 패치에 따른 S/W나 운영 체제 성능이 개선되고 호환성 또한 향상된다.

## 보안 관제 서비스

조직의 정보 자원 및 보안 시스템을 운영하기 위해 사이버 공격 정보를 탐지 및 분석하여 즉시 대응하는 업무

### 원격 관제 서비스

자체 관제에 어려움이 있고, 전문 인력의 도움이 필요한 경우, 보안관제센터에서 원격으로 보안 관제 서비스를 제공하고 있다

<https://www.skshieldus.com/kor/service/information/remote/remote.do> (SK Shieldus 원격 관제 서비스)

### 파견 관제 서비스

현장에서 상주하며 보안 장비를 효율적으로 운영하며, 사고 발생 시 신속한 초기 대응 및 상황 전파가 가능하도록 하는 파견 관제 서비스를 제공한다.

<https://www.skshieldus.com/kor/service/information/remote/dispatch.do> (SK Shieldus 파견 관제 서비스)

## 취약점 진단 서비스

전자 금융감독 규정, 정보보호 기반 규정 등 국내 보안 컴플라이언스 규정을 충족하기 위해 취약점을 진단하는 원스톱 서비스

<https://www.skshieldus.com/kor/service/information/consulting/vulnerability.do> (SK Shieldus 취약점진단팀)

## 웹쉘 탐지 솔루션

웹쉘 코드 패턴을 탐지하는 프로그램을 통해 웹 디렉토리 권한 및 정보 탈취를 예방한다.

<https://www.skshieldus.com/kor/service/information/info-solution/solution.do> (SK Shieldus 웹쉘탐지/대응 솔루션)

## EDR 솔루션

엔드 포인트에서 탐지 및 대응, 실시간 분석 및 위협 탐지, 위협 대응 자동화, 위협 격리 및 해결, 위협 취적 지원을 핵심 기능으로 구성된다.

<https://www.skshieldus.com/kor/service/information/remote/remote.do> (SK Shieldus 원격관제팀 – EDR 서비스 제공)

## OWA서버 외부 접근 차단

VPN(내부망에서만 사용)이나 OutLook(프로그램)을 통해서만 메일 볼 수 있게 외부에서의 접근을 차단 한다.

## 자동 로그인 세션 만료 시간 설정

웹 애플리케이션 등에서 사용자가 로그인한 후에 일정 시간 동안 활동이 없을 경우 자동으로 로그인 세션을 만료 시키는 기능이 있다.

## 2차인증

사용자가 자신의 신원을 확인하는 과정에서 두 가지 이상의 다른 방법을 사용하는 보안 절차를 말하며 대표적으로 지문인식, OTP 등이 있다.

## 아웃바운드 정책 실행

화이트리스트 정책, 즉 허용되는 대외 서비스만 가능하고 사용하지 않는 서비스는 차단하여 불확실한 IP에 대해 예방한다.

## 웹 디렉토리 실행 권한 설정

웹 디렉토리 실행 권한 설정은 웹 서버에서 특정 디렉토리 내의 파일이나 스크립트를 실행할 수 있는 권한을 설정하는 것을 의미한다.

## Trust to Trust 접근 정책 강화

Trust to Trust 접근 정책 강화를 통해 신뢰 도메인 간에만 통신이 되고, 접근 권한을 최소화하며, 사용자 별 접근 권한에 대해 분리 설정해야 한다.

## 비밀번호 정책 강화

비밀번호 정책 강화는 조직이나 시스템에서 사용자들의 비밀번호를 관리하고 보호하기 위해 적용되는 보안 정책이다.

## DB 접근 제어 솔루션

데이터베이스 시스템에 대한 접근을 제한하고 모니터링하는 보안 솔루션을 제공한다.

## DLP (데이터 손실 방지)

문서 고유번호를 넣고 이동될 때마다 고유번호 식별 및 분류하여, 내부 기밀문서가 전송 되는 것을 방지한다.

## WDigest 비활성화

Registry에서 WDigest를 비활성화함에 따라 비밀번호를 메모리에 평문으로 저장하는 것을 방지한다. 또한 로그오프 후 일정 시간이 지나면 캐쉬 메모리에서 비밀번호 삭제까지 된다.

## 백신 프로그램

실시간 보호 및 행위 기반 침입 차단을 실시하여 악성프로그램을 탐지하고 치료한다.

## 접근 통제 솔루션

무단 출입을 방지하고 허가된 사용자만이 특정 영역이나 자원에 접근할 수 있도록 보장한다.

## Zero Trust 기법

회사 내부망 네트워크를 마이크로 세분화 후 접근 권한을 부여하여 내부 이동을 통한 DB 접근이 되지 않도록 한다.

# 악성코드 분석

|  |  |
| --- | --- |
| **update.exe** | |
| 샌드박스를 통한 upload.exe 악성파일 여부 판별 결과는 다음과 같다. 프로세스 트리 구조 확인 결과 explorer.exe 자식 프로세스로 update.exe 실행이 확인된다.  C:\Users\USER\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\TempState\ShareServiceTempFolder\1.jpeg  [그림 5.1] Process Explorer – 프로세스 확인  cmd창에 netstat 명령어 실행해 연결된 네트워크 결과 확인 결과, 공격자 B(172.30.40.97:5555) 세션 성립 상태 확인된다.  C:\Users\USER\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\TempState\ShareServiceTempFolder\2.jpeg  [그림 5.2] cmd – 네트워크 연결 확인  아래 그림 또한 update.exe 프로세스가 공격자 B (172.30.40.97)와 5555포트로 원격 통신하고 있음 확인된다.  C:\Users\USER\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\TempState\ShareServiceTempFolder\3.jpeg  [그림 5.3] TCPView - 원격 통신 확인  update.exe 프로세스 추출하여 Virus Total 사이트 통한 확인 결과 update.exe 파일이 악성 실행 파일인 것으로 확인된다.  C:\Users\USER\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\TempState\ShareServiceTempFolder\4.jpeg  [그림 5.4] Virus Total – 악성 파일 확인 | |
| update.exe 파일을 동적 분석한 결과 172.30.40.97의 5555포트를 통해 연결되어 있는 것을 확인 할 수 있다. | |
| **MD5** | 2f7287dc43b17359704391ecd9dd2c07 |
| **SHA1** | cbce8bf56e9b8eb6a2a5d47e073a043c03c91711 |
| **SHA256** | 3c34a778386a99658f039248f0222002eaa80183f61e698e63c86309683fd943 |

[표 5‑1] update.exe 분석

|  |  |
| --- | --- |
| **payload.exe** | |
| 샌드박스를 통한 payload.exe 악성파일 여부 판별 결과는 다음과 같다. 프로세스 트리 구조 확인 결과 explorer.exe 자식 프로세스로 payload.exe 실행이 확인된다.  C:\Users\USER\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\TempState\ShareServiceTempFolder\5.jpeg  [그림 5.5] Process Explorer – 프로세스 확인  cmd창에 netstat 명령어 실행해 연결된 네트워크 결과 확인 결과, IP 172.30.40.125:4444 세션 성립 상태 확인된다.  C:\Users\USER\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\TempState\ShareServiceTempFolder\6.jpeg  [그림 5.6] cmd – 네트워크 연결 확인  아래 그림 또한 payload.exe 프로세스가 IP 172.30.40.125와 4444포트로 원격 통신하고 있음 확인된다.  C:\Users\USER\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\TempState\ShareServiceTempFolder\7.jpeg  [그림 5.7] TCPView - 원격 통신 확인  payload.exe 프로세스 추출하여 Virus Total 사이트 통한 확인 결과 payload.exe 파일이 악성 실행 파일인 것으로 확인된다.  C:\Users\USER\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\TempState\ShareServiceTempFolder\8.jpeg  [그림 5.8] Virus Total – 악성 파일 확인 | |
| payload.exe 파일을 동적 분석한 결과 172.30.40.125의 4444포트를 통해 연결되어 있는 것을 확인 할 수 있다. | |
| **MD5** | ba4525fc6f78f04d321273dcc7eeae58 |
| **SHA1** | b3a420ae22c224f1911b2bb5535e5f5ca1f4843f |
| **SHA256** | 51a2a9a61b50414f6f5933219533425ed2dadcd8eb733c1243192bb1f75263f5 |

[표 5‑2] payload.exe 분석

|  |  |
| --- | --- |
| **Petya(랜섬웨어)** | |
| Petya는 MBR과 파일들을 암호화 변조하여 시스템 부팅을 방해하는 랜섬웨어 이며, 로컬 네트워크를 통해서만 감염된다. 감염된 시스템을 재부팅 하면 Petya의 시작 화면이 나타나고, 사용자는 키를 구매하여 복호화 할 수 있다.  C:\Users\USER\Desktop\새 폴더\8.jpg  [그림 5.9] Petya 감염 확인  피해 PC에서 발견된 Readme.msi를 추출하여 exe형태로 변환하였다.  C:\Users\USER\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\TempState\ShareServiceTempFolder\9.jpeg  [그림 5.10] Readme.msi를 추출하여 exe형태로 변환  해당 파일을 Virus Total 사이트 통한 확인 결과, Readme.exe 파일이 악성 파일인 것으로 확인 된다.  C:\Users\USER\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\TempState\ShareServiceTempFolder\10.jpeg  [그림 5.11] Virus Total – 악성 파일 확인 | |
| msi 파일을 exe 파일로 변환하여 확인한 결과 petya 랜섬웨어인 것을 확인 할 수 있었다. | |
| **MD5** | a92f13f3a1b3b39833d3cc336301b713 |
| **SHA1** | d1c62ac62e68875085b62fa651fb17d4d7313887 |
| **SHA256** | 4c1dc737915d76b7ce579abddaba74ead6fdb5b519a1ea45308b8c49b950655c |

[표 5‑3] Petya 분석

# 침해 지표

## 공격 지표

| **번호** | **IP** | **역할** | **행위** |
| --- | --- | --- | --- |
| 1 | 172.30.40.125 | 공격자IP | 웹쉘 업로드, 악성 명령어 실행, 악성코드 실행(백도어),  Reverse RDP |
| 2 | 172.30.40.97 | 공격자IP | 고객정보 DB 탈취, 악성코드 실행(백도어) |

[표 6‑1] 공격 지표

## 침해 도구 지표

| **번호** | **도구** | **구분** | **사이즈** | **Hash** |
| --- | --- | --- | --- | --- |
| 1 | mimikatz.exe | Credential 탈취 도구 | 1,309,448KB | a3cb3b02a683275f7e0a0f8a9a5c9e07 |
| 2 | !only Result.bat | Credential 탈취 도구 스크립트 | 1KB | 2fb3a09c38bad6deb69e78db99ce3f77 |
| 3 | filezilla.setup.exe | FTP 도구 | 12,802,000KB | 343cc8cffac4dc1140a27c76154c4639 |
| 4 | frpc.ini | Reverse Proxy 설정 파일 | 171KB | 838a93ffcefadb8440e18970e447f028 |
| 5 | frpc.exe | Reverse Proxy 도구 | 14,573,056KB | 4a79a8b1f6978862ecfa71b55066aadd |
| 6 | payload.exe | 백도어 | 7,168KB | ba4525fc6f78f04d321273dcc7eeae58 |
| 7 | update.exe | 백도어 | 73,802KB | 2f7287dc43b17359704391ecd9dd2c07 |
| 8 | Readme.msi | 랜섬웨어 | 1,208,320KB | f8ef92bbe534a588720eef47d1c87536 |
| 9 | hello.exe | 랜섬웨어 | 806,912KB | a92f13f3a1b3b39833d3cc336301b713 |
| 10 | hydra.exe | 비밀번호 크래킹 도구 | 442,880KB | 9b4fca18ba3df92ea7856b794da91889 |
| 11 | Password-list.txt | 비밀번호 사전 | 2,676KB | 52a38041908ef6ac1b0928db95d2af9e |
| 12 | start.bat | hydra 실행 스크립트 | 92KB | 85761586d3a904d7d1d497cd67da11ad |
| 13 | gathering\_script.ps1 | OU Credential수집 스크립트 | 290KB | 7506ec6b15eb9270b1f48ad69fee7a5d |

[표 6‑2] 침해 도구 지표

# 그림 목차

[[그림 1.1] 침해 사고 분석 Process 4](#_Toc154428941)

[[그림 2.1] 침해 사고 타임라인 8](#_Toc154428942)

[[그림 2.2] 침해 사고 8](#_Toc154428943)

[[그림 3.1] 방화벽 로그 확인 10](#_Toc154428944)

[[그림 3.2] 스캔 공격 확인 (UTC+9) 적용 전 10](#_Toc154428945)

[[그림 3.3] Exchange의 HttpProxy 로그 중 ECP로그 확인 (UTC+9) 적용 전 11](#_Toc154428946)

[[그림 3.4] Exchange의 ECPServer 로그 (UTC+9) 적용 전 11](#_Toc154428947)

[[그림 3.5] Exchange 웹 로그 - 웹쉘 실행 명령어 12](#_Toc154428948)

[[그림 3.6] 이벤트 로그(PowerShell) - Windows Firewall Off 12](#_Toc154428949)

[[그림 3.7] 이벤트 로그(PowerShell) - Windows Defender Off 확인 13](#_Toc154428950)

[[그림 3.8] 이벤트 로그(Application)– hack 기본 구성 생성 13](#_Toc154428951)

[[그림 3.9] net\_user.txt - 계정 정보 확인 14](#_Toc154428952)

[[그림 3.10] 이벤트 로그(PowerShell) - attack.zip 다운로드 14](#_Toc154428953)

[[그림 3.11] 이벤트 로그(PowerShell) - attack.zip 압축 해제 15](#_Toc154428954)

[[그림 3.12] MFT – attack.zip 내의 파일 확인 16](#_Toc154428955)

[[그림 3.13] pslist.txt – frpc.exe 실행 확인 16](#_Toc154428956)

[[그림 3.14] frpc.ini 파일 확인 16](#_Toc154428957)

[[그림 3.15] netstat.txt - 연결 IP 및 포트 확인 17](#_Toc154428958)

[[그림 3.16] 이벤트 로그(RdpCore) - RDP 세션 연결 내역 17](#_Toc154428959)

[[그림 3.17] 이벤트 로그(LocalSession) - RDP 세션 로그온 성공 내역 18](#_Toc154428960)

[[그림 3.18] logonsessions.txt - 로그온 세션 정보 18](#_Toc154428961)

[[그림 3.19] 레지스트리(REGA) - 공격자 최초 활동 내역 19](#_Toc154428962)

[[그림 3.20] 레지스트리(REGA) - backdoor 흔적 확인 19](#_Toc154428963)

[[그림 3.21] t\_list.txt - payload.exe 실행 19](#_Toc154428964)

[[그림 3.22] netstat.txt - backdoor 연결 공격자 IP 확인 20](#_Toc154428965)

[[그림 3.23] cports.txt - payload.exe 실행 20](#_Toc154428966)

[[그림 3.24] Virus Total – payload.exe 결과 21](#_Toc154428967)

[[그림 3.25] hydra 폴더 생성 확인 21](#_Toc154428968)

[[그림 3.26] 레지스트리(REGA) - hydra start.bat 실행 로그 22](#_Toc154428969)

[[그림 3.27] 레지스트리(REGA) - output.txt 22](#_Toc154428970)

[[그림 3.28] MFT - mimikatz 폴더 생성 확인 23](#_Toc154428971)

[[그림 3.29] MFT - mimikatz 실행 결과 23](#_Toc154428972)

[[그림 3.30] 레지스트리(REGA) - Result.txt 23](#_Toc154428973)

[[그림 3.31] 레지스트리(REGA) - HASHES.txt 24](#_Toc154428974)

[[그림 3.32] 레지스트리(REGA) - RemoteDesktop 실행 24](#_Toc154428975)

[[그림 3.33] HASHES.txt 내용 확인 24](#_Toc154428976)

[[그림 3.34] 레지스트리(REGA) - RDP 최종실행시각 25](#_Toc154428977)

[[그림 3.35] recycle\_bin\_list.txt - 휴지통 존재 파일 확인 (UTC+9) 적용 전 25](#_Toc154428978)

[[그림 3.36] netusers\_local\_history.txt - 공격자 마지막 로그온 확인 26](#_Toc154428979)

[[그림 3.37] 이벤트 로그(RdpCore) - RDP 연결 종료 시간 확인 26](#_Toc154428980)

[[그림 3.38] 이벤트 로그 (Security) – 로그인 실패 27](#_Toc154428981)

[[그림 3.39] 이벤트 로그(RemoteDesktopServices) – 원격 접속 27](#_Toc154428982)

[[그림 3.40] 이벤트 로그(Windows Defender) - Defender 비활성화 28](#_Toc154428983)

[[그림 3.41] exchange 웹 로그 (UTC+9) 적용 전 28](#_Toc154428984)

[[그림 3.42] browsinghistory - attack.zip EDGE 다운 28](#_Toc154428985)

[[그림 3.43] attack.zip 다운로드 28](#_Toc154428986)

[[그림 3.44] MFT – attack 폴더 생성 28](#_Toc154428987)

[[그림 3.45] MFT – attack 폴더 내용 확인 29](#_Toc154428988)

[[그림 3.46] 이벤트 로그(Powershell) - gathering\_script.ps1 실행 30](#_Toc154428989)

[[그림 3.47] gathering스크립트 실행결과 31](#_Toc154428990)

[[그림 3.48] def 할당된 정책을 확인 31](#_Toc154428991)

[[그림 3.49] 정책 생성 및 생성시간 31](#_Toc154428992)

[[그림 3.50] 정책 추가 및 설정파일 32](#_Toc154428993)

[[그림 3.51] 이벤트 로그(security) 32](#_Toc154428994)

[[그림 3.52] 이벤트 로그(TerminalServices) - DB관리자 RDP연결 33](#_Toc154428995)

[[그림 3.53] msi 공유 폴더 이동 33](#_Toc154428996)

[[그림 3.54] msi 파일 확인 34](#_Toc154428997)

[[그림 3.55] Readme.msi Virustotal 업로드 34](#_Toc154428998)

[[그림 3.56] Allow user remote Desktop 정책 배포 35](#_Toc154428999)

[[그림 3.57] Allow user remote Desktop GPO 업데이트 확인 결과 35](#_Toc154429000)

[[그림 3.58] 레지스트리(REGA) - hello.exe 실행 35](#_Toc154429001)

[[그림 3.59] Virustotal - hello.exe 확인 36](#_Toc154429002)

[[그림 3.60] 이벤트 로그(RemoteDestopServices) - RDP 37](#_Toc154429003)

[[그림 3.61] 이벤트 로그(Security) - logon 37](#_Toc154429004)

[[그림 3.62] 이벤트 로그(Security) – logoff 38](#_Toc154429005)

[[그림 3.63] 이벤트 로그(Firewall) – Firewall change 38](#_Toc154429006)

[[그림 3.64] 이벤트 로그(RemoteDesktopservice) - RDP 39](#_Toc154429007)

[[그림 3.65] 이벤트 로그(Group Policy) – 정책배포 40](#_Toc154429008)

[[그림 3.66] 레지스트리(REGA) - update.exe 실행 40](#_Toc154429009)

[[그림 3.67] TcpView – update.exe 실행 40](#_Toc154429010)

[[그림 3.68] 레지스트리(REGA) - filezilla 실행 41](#_Toc154429011)

[[그림 3.69] filezilla 로그 41](#_Toc154429012)

[[그림 3.70] MFT – WinSCP 42](#_Toc154429013)

[[그림 3.71] auth.log의 DB서버 접속 42](#_Toc154429014)

[[그림 3.72] WinSCP DB 서버 자동 로그인 42](#_Toc154429015)

[[그림 3.73] filezila.log - steal.zip탈취 43](#_Toc154429016)

[[그림 3.74] db\_backup.sql 43](#_Toc154429017)

[[그림 3.75] MFT – 도구 및 탈취 파일 삭제 확인 44](#_Toc154429018)

[[그림 3.76] 삭제된 파일명 확인 44](#_Toc154429019)

[[그림 3.77] 레지스트리(REGA) - Readme.msi 공유 기록 44](#_Toc154429020)

[[그림 5.1] Process Explorer – 프로세스 확인 49](#_Toc154429021)

[[그림 5.2] cmd – 네트워크 연결 확인 50](#_Toc154429022)

[[그림 5.3] TCPView - 원격 통신 확인 50](#_Toc154429023)

[[그림 5.4] Virus Total – 악성 파일 확인 51](#_Toc154429024)

[[그림 5.5] Process Explorer – 프로세스 확인 52](#_Toc154429025)

[[그림 5.6] cmd – 네트워크 연결 확인 52](#_Toc154429026)

[[그림 5.7] TCPView - 원격 통신 확인 53](#_Toc154429027)

[[그림 5.8] Virus Total – 악성 파일 확인 54](#_Toc154429028)

[[그림 5.9] Petya 감염 확인 55](#_Toc154429029)

[[그림 5.10] Readme.msi를 추출하여 exe형태로 변환 55](#_Toc154429030)

[[그림 5.11] Virus Total – 악성 파일 확인 56](#_Toc154429031)

# 표 목차

[[표 1‑1] 조사대상 4](#_Toc154429032)

[[표 1‑2] 관련정보 파악 5](#_Toc154429033)

[[표 1‑3] 사고 시스템 분석 설명 5](#_Toc154429034)

[[표 1‑4] 원인 분석 설명 5](#_Toc154429035)

[[표 1‑5] 대응 방안 설명 6](#_Toc154429036)

[[표 1‑6] 조사 수행 기간 및 인원 6](#_Toc154429037)

[[표 2‑1] 타임라인 표 9](#_Toc154429038)

[[표 4‑1] 권고사항 45](#_Toc154429039)

[[표 5‑1] update.exe 분석 51](#_Toc154429040)

[[표 5‑2] payload.exe 분석 54](#_Toc154429041)

[[표 5‑3] Petya 분석 56](#_Toc154429042)

[[표 6‑1] 공격 지표 57](#_Toc154429043)

[[표 6‑2] 침해 도구 지표 57](#_Toc154429044)