해킹진단도구 활용 방안,
취약한 MS-SQL 서버를 통한 랜섬웨어 감염

한국인터넷진흥원 사고분석1팀

KISA 한국인터넷진흥원

목 차

1. 침해사고 사례를 통한 도구 활용 방안 개요

1.1. 개요

해당 침해사고 사례는 2020년부터 현재까지 기업 환경에서 빈번하게 발생하는 MS-SQL 기반의 랜섬웨어 및 데이터 유출 공격 사례입니다. 이러한 유형의 공격은 MS-SQL 서버의 취약점 또는 패스워드 관리 부재(ERP 와 같은 애플리케이션 설치 시 기본 계정/패스워드 사용) 등의 미흡한 계정 관리 환경을 악용하고 있습니다. 일반적으로 공격 자동화 도구를 사용해 대량의 MS-SQL 서버 스캔, 취약한 서버를 대상으로 랜섬웨어 배포, 데이터 탈취 후 금전 요구하는 방식으로 수행되며, 원격 접근 도구(RAT: Remote Access Tool)인 AnyDesk 와 같은 프로그램을 악용해 원격으로 접근한 후 공격을 수행하는 패턴도 보이고 있습니다. 해당 시나리오는 최근에 발생하는 공격 트랜드를 반영해 랜섬웨어 공격과 데이터 탈취를 결합한 복합적인 공격 방식이 반영되어 있으며, 해킹진단도구에서 진단한 결과를 바탕으로 대응할 수 있는 방안을 공유합니다.

1.2. 분석 대상

분석 대상은 2 대입니다. 아래 표는 분석 대상의 상세 정보입니다.

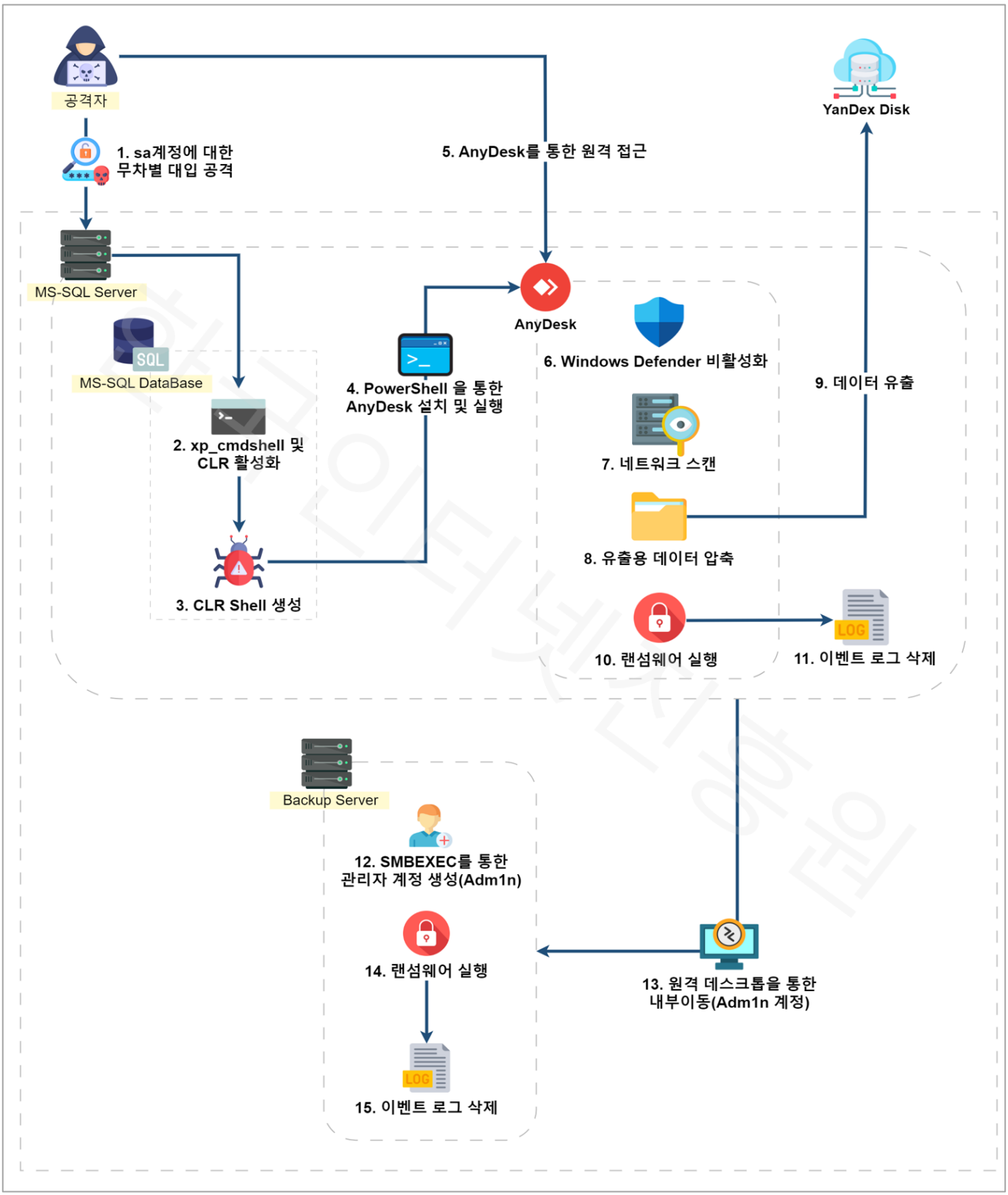
[표 1] 분석 대상 정보

번호	호스트명	용도	IP	운영체제
1	WIN-KD9PAVT710C	DataBase	192.168.0.67	Windows Server 2019
2	WIN-I518OE88C5M	Backup	192.168.0.68	Windows Server 2019

2. 주요 요약

2.1. 전체 요약

아래 그림은 실제 중소기업 대상으로 많이 발생하는 침해사고 시나리오로, 공격자가 원격으로 서버에 접근해 데이터를 유출 및 랜섬웨어 감염을 시도하는 과정을 단계적으로 표현한 개요도입니다.



[그림 1] 침해사고 개요도

3. 해킹진단도구를 통한 침해사고 진단

3.1. 해킹진단도구 진단 결과 보고서

해당 침해사고 케이스의 해킹진단도구 진단 결과 보고서는 다음과 같습니다.

✓ MS-SQL 데이터베이스 서버

WIN-KD9PAVT710C_192.168.0.67

■ 일반정보

IP주소	호스트명	OS정보	설치일자	로그인 계정
192.168.0.67	WIN-KD9PAVT710C	Microsoft Windows Server 2019 Standard (x64)	2024-09-24 19:19:07	Administrator

수집시간	분석시간	타임존
2024-09-25 16:02:46	2024-09-25 16:10:42	대한민국 표준시 UTC+9

■ 계정정보

계정	그룹	SID	계정생성일	최종로그인	설명
Administrator	Administrators	S-1-5-21-2381407900-1702101972-3354340170-500	2024-09-24 19:17:03	2024-09-24 20:00:03	컴퓨터 도메인을 관리하도록 기본 제공된 계정
DefaultAccount	System Managed Accounts Group	S-1-5-21-2381407900-1702101972-3354340170-503	2024-09-24 19:17:03		시스템에서 관리하는 사용자 계정입니다.
Guest	Guests	S-1-5-21-2381407900-1702101972-3354340170-501	2024-09-24 19:17:03		게스트가 컴퓨터 도메인을 액세스하도록 기본 제공된 계정
WDAGUtilityAccount		S-1-5-21-2381407900-1702101972-3354340170-504	2024-09-24 19:17:03		Windows Defender Application Guard 시나리오용으로 시스템에서 관리 및 사용하는 사용자 계정입니다.
SQLServer2005SQLBrowserUser$WIN-KD9PAVT710C		S-1-5-21-2381407900-1702101972-3354340170-1000	2024-09-24 19:56:26		해당 그룹의 멤버에게 SQL Server Browser 관련 인스턴스의 로그온 계정으로 지정되는 데 필요한 액세스와 권한이 있습니다.

■ 진단결과 : 심각 (26개 탐지룰 점검결과)

Level	정상	관심	주의	경계	심각
● 심각	21	0	2	3	0

[그림 2] 해킹진단도구 진단 결과 – 데이터베이스 서버

■ 검출결과

경계 (3개)

No	탐지명	설명	시간 (UTC+9)	내용
1	[EVT]_06_윈도우 명령어 셸 활성화 탐지(xp_cmdshell)	xp_cmdshell 활성화 변경 여부	2024-09-25 15:07:35	xp_cmdshell 0 1
2	[EVT]_14_윈도우 디펜더 백신의 실시간 감시 기능 비활성화 탐지	윈도우 디펜더 실시간 탐지 비활성화	2024-09-24 19:54:46	윈도우 디펜더 실시간 감시 비활성 설정 시간 : 2024-09-24 19:54:46
			2024-09-25 15:43:46	윈도우 디펜더 실시간 감시 비활성 설정 시간 : 2024-09-25 15:43:46
3	[EVT]_21_윈도우 명령어 셸 활성화 탐지(clr enabled)	MSSQL clr enabled 옵션 활성화 변경 여부	2024-09-25 15:07:35	clr enabled 0 1

주의 (2개)

No	탐지명	설명	시간 (UTC+9)	내용
1	[EVT]_08_사용자(관리자) 계정 생성 탐지	계정 생성	2024-09-24 19:16:23	생성된 계정 : WDAGUtilityAccount SID : S-1-5-21-2381407900-1702101972-3354340170-504 주체 : MINWINPC$
2	[EVT]_10_해킹이나 취약점 공격 등으로 관리자 권한 해킹 탐지	권한 상승	2024-09-25 15:41:54	내용 : Secondary Logon 실행

[그림 3] 해킹진단도구 검출 결과 – 데이터베이스 서버

✓ 백업 서버

WIN-I518OE88C5M_192.168.0.68

■ 일반정보

IP주소	호스트명	OS정보	설치일자	로그인 계정
192.168.0.68	WIN-I518OE88C5M	Microsoft Windows Server 2019 Standard (x64)	2024-09-24 19:19:14	Administrator

수집시간	분석시간	타임존
2024-09-25 16:03:19	2024-09-25 16:10:39	대한민국 표준시 UTC+9

■ 계정정보

계정	그룹	SID	계정생성일	최종로그인	설명
adm1n	Administrators	S-1-5-21-2814179269-961089793-1192736692-1000	2024-09-25 15:58:23	2024-09-25 15:59:13	
Administrator	Administrators	S-1-5-21-2814179269-961089793-1192736692-500	2024-09-24 19:17:01	2024-09-25 13:44:15	컴퓨터 도메인을 관리하도록 기본 제공된 계정
DefaultAccount	System Managed Accounts Group	S-1-5-21-2814179269-961089793-1192736692-503	2024-09-24 19:17:01		시스템에서 관리하는 사용자 계정입니다.
Guest	Guests	S-1-5-21-2814179269-961089793-1192736692-501	2024-09-24 19:17:01		게스트가 컴퓨터 도메인을 액세스하도록 기본 제공된 계정
WDAGUtilityAccount		S-1-5-21-2814179269-961089793-1192736692-504	2024-09-24 19:17:01		Windows Defender Application Guard 시나리오용으로 시스템에서 관리 및 사용하는 사용자 계정입니다.

■ 진단결과 : 심각 (26개 탐지룰 점검결과)

Level	정상	관심	주의	경계	심각
● 심각	24	0	1	1	0

[그림 4] 해킹진단도구 진단 결과 – 백업 서버(1)

■ 검출결과

경계 (1개)

No	탐지명	설명	시간 (UTC+9)	내용
1	[EVT]_14_윈도우 디펜더 백신의 실시간 감시 기능 비활성화 탐지	윈도우 디펜더 실시간 탐지 비활성화	2024-09-24 19:37:38	윈도우 디펜더 실시간 감시 비활성 설정 시간 : 2024-09-24 19:37:38

주의 (1개)

No	탐지명	설명	시간 (UTC+9)	내용
1	[EVT]_08_사용자(관리자) 계정 생성 탐지	계정 생성	2024-09-24 19:16:23	생성된 계정 : WDAGUtilityAccount SID : S-1-5-21-2814179269-961089793-1192736692-504 주체 : MINWINPC$
			2024-09-25 15:58:23	생성된 계정 : adm1n SID : S-1-5-21-2814179269-961089793-1192736692-1000 주체 : WIN-I518OE88C5M$

[그림 5] 해킹진단도구 검출 결과 – 백업 서버(2)

4. 해킹진단도구 검출 결과

각 탐지 결과에 대한 설명은 다음과 같으며, 공격자가 수행한 행위, 탐지 결과, 탐지 결과 대응 방안으로 구성되어 있습니다.

4.1. 데이터베이스 서버

1) [EVT]_06_윈도우 명령어 셸 활성화 탐지(xp_cmdshell)

해당 룰은 MS-SQL 서버에서 윈도우 명령 실행이 가능한 저장 프로시저인 xp_cmdshell 활성화 여부에 대해 진단합니다. xp_cmdshell은 SQL Server에서 **데이터베이스 명령으로 운영체제 명령을 실행할 수 있게 해주는 기능으로, 이 기능이 악용되면 해커가 시스템 명령을 실행해 서버를 제어**할 수 있습니다.

✓ **공격자 수행 행위**

공격자는 원격 명령을 호스트 시스템에서 실행하기 위해 xp_cmdshell을 활성화하며, 아래 명령어를 주로 사용합니다. 또한, **마스터 데이터베이스가 신뢰할 수 있는 상태로 설정**되도록 만듭니다. 이렇게 되면 데이터베이스 내에서 **외부 코드나 프로세스가 실행**될 수 있습니다.

```
EXEC sp_configure 'show advanced options', 1;
EXEC sp_configure 'xp_cmdshell', 1;
RECONFIGURE;
ALTER DATABASE master SET TRUSTWORTHY ON;
```

[그림 6] xp_cmdshell 활성화 명령어

✓ **검출 결과**

해킹진단도구에서는 공격자가 실행한 **EXEC sp_configure 'xp_cmdshell', 1;** 명령을 탐지합니다.

No	탐지명	설명	시간 (UTC+9)	내용
1	[EVT]_06_윈도우 명령어 셸 활성화 탐지(xp_cmdshell)	xp_cmdshell 활성화 변경 여부	2024-09-25 15:07:35	xp_cmdshell 0 1

[그림 7] 해킹진단도구 검출 결과 – xp_cmdshell

✓ **탐지 결과 대응 방안**

- xp_cmdshell 옵션을 활성화하면 **공격자가 시스템에서 외부 명령과 악성 코드를 직접 실행**할 수 있습니다.
- 관리자가 실행한 명령이 아닐 경우, 즉시 해당 프로시저를 비활성화하고 **백신 정밀 검사**를 수행해야 합니다.
- 공격자는 xp_cmdshell 을 활용해 시스템에 추가적인 악성코드를 설치하는 경우가 많기 때문에 정밀 검사를 통한 탐지 및 치료가 필요합니다.

침해사고로 확인된 경우, 24시간 이내 한국인터넷진흥원으로 신고해야 합니다.

2) [EVT]_08_사용자(관리자) 계정 생성 탐지

해당 룰은 시스템에서 사용자(관리자) 계정이 생성된 이벤트가 존재하는지 진단합니다. 공격자가 시스템에 침투한 후, 공격을 지속적으로 수행하기 위해 공격 전용 계정을 생성해 악성 행위를 수행합니다. 조직 내부에서 생성하지 않은 계정이 탐지되면 해당 시점에 공격자가 침투했을 가능성을 있어 추가 조사가 필요합니다.

✓ **공격자 수행 행위**

공격자가 계정을 생성하는 것은 시스템에 **장기적으로 머물기 위한 전략**입니다. 계정을 생성한 후에는 공격자가 **시스템을 자유롭게 조작하고 더 많은 공격을 수행**할 수 있게 되며, 공격의 탐지를 회피하고 흔적을 지우기 위한 중요한 수단으로 활용됩니다.

```
net user [user] [password] /add
```

[그림 8] 사용자 계정 추가 명령어

✓ **검출 결과**

해킹진단도구에서는 사용자(관리자) 계정이 생성될 경우, 아래 화면처럼 생성된 계정의 이름, 생성 시간 등을 확인할 수 있습니다.

1	[EVT]_08_사용자(관리자) 계정 생성 탐지	계정 생성	2024-09-24 19:16:23	생성된 계정 : WDAGUtilityAccount SID : S-1-5-21-2381407900-1702101972-3354340170-504 주체 : MINWINPC$

[그림 9] 해킹진단도구 검출 결과 – 사용자 계정 생성

✓ **탐지 결과 대응 방안**

- 사용자(관리자) 계정이 임의로 생성된 경우에는 **실제 사용자(관리자)가 수행한 행위인지 확인**해야 합니다.
- 사용자(관리자)가 수행한 행위가 아닐 경우, **즉시 해당 계정을 삭제**하고 진단 도구 탐지 결과에서 **추가 이상 행위가 식별됐는지 확인하고 조치**해야 합니다.

침해사고로 확인된 경우, 24시간 이내 한국인터넷진흥원으로 신고해야 합니다.

3) [EVT]_10_해킹이나 취약점 공격 등으로 관리자 권한 해킹 탐지

해당 룰은 Secondary Logon 서비스를 모니터링해 **정상적인 작업 이외의 권한 상승**이 이루어졌는지 탐지합니다. **Windows Defender 비활성화나 이벤트 로그 삭제**와 같은 다른 이상 징후와 함께 감지된다면, 이는 시스템이 권한 상승 공격에 노출되었을 가능성을 의미하며, 추가적인 확인이 필요할 수 있습니다.

✓ **공격자 수행 행위**

공격자가 **권한 상승(Privilege Escalation)**을 시도하는 주된 이유는 **더 높은 권한을 확보**해 시스템을 **자유롭게 조작**하고 **제한 없이 다양한 악성 행위를 수행**하기 위함입니다. 일반 사용자 권한만으로는 시스템의 핵심 자원에 접근하거나 중요한 설정을 변경할 수 없기 때문에, 공격자는 관리자 권한을 얻어야 시스템을 완전히 장악할 수 있습니다. 이를 통해 보안 소프트웨어를 비활성화하거나, 데이터 유출, 악성 코드 실행, 로그 삭제 등의 공격을 보다 쉽게 수행할 수 있습니다. 해당 시나리오에서는 '**BadPotato**'라 명명된 권한 상승 도구를 활용해 **Powershell 로 난독화된 명령(Whoami)을 실행**했습니다.

```
BadPotato.exe "powershell -NoP -NoL -sta -NonI -Exec Bypass -Enc dwBoAG8AYQBtAGkA"";
```

[그림 10] 난독화된 PowerShell 명령 실행

✓ **검출 결과**

해킹진단도구에서는 Secondary Logon 서비스의 실행 여부를 탐지하고 있습니다.

2	[EVT]_10_해킹이나 취약점 공격 등으로 관리자 권한 해킹 탐지	권한 상승	2024-09-25 15:41:54	내용 : Secondary Logon 실행

[그림 11] 해킹진단도구 검출 결과 – Secondary Logon 서비스 실행

✓ **탐지 결과 대응 방안**

- Secondary Logon 서비스는 정상 서비스이므로 실제 해킹 및 취약점 공격에 악용됐는지 여부는 **해킹진단도구에서 다른 이벤트가 탐지된 이력이 있는지 추가 확인**이 필요합니다.

4) [EVT]_14_윈도우 디펜더 백신의 실시간 감시 기능 비활성화 탐지

해당 룰은 Windows Defender 실시간 보호 기능이 비활성화**된 이벤트를 탐지**합니다. 일반적으로, 사용자가 업무 편의성을 위해 백신의 실시간 보호 기능을 비활성화 하기도 하지만 공격자가 공격의 탐지를 회피하기 위해 백신을 무력화하기도 합니다. 따라서, 사용자가 비활성화한 이력이 없는 경우에는 백신의 실시간 보호 기능이 비활성화된 시점에 공격자가 침투했을 가능성이 있어 추가 조사가 필요합니다.

✓ **공격자 수행 행위**

공격자가 **Windows Defender 실시간 보호 기능 비활성화**를 하는 주된 이유는 **보안 소프트웨어가 악성 행위를 탐지하거나 차단하지 못하게 하기 위함**입니다. Windows Defender 가 비활성화되면 공격자는 악성 코드 실행, 데이터 유출, 시스템 장악 등을 더 쉽게 수행할 수 있습니다.

✓ **검출 결과**

해킹진단도구에서는 Windows Defender 실시간 보호 기능 비활성화 행위를 탐지하고 있습니다.

2	[EVT]_14_윈도우 디펜더 백신의 실시간 감시 기능 비활성화 탐지	윈도우 디펜더 실시간 탐지 비활성화	2024-09-24 19:54:46	윈도우 디펜더 실시간 감시 비활성 설정 시간 : 2024-09-24 19:54:46
			2024-09-25 15:43:46	윈도우 디펜더 실시간 감시 비활성 설정 시간 : 2024-09-25 15:43:46

[그림 12] 해킹진단도구 검출 결과 – Windows Defender 실시간 감시 비활성화

✓ **탐지 결과 대응 방안**

- **Windows Defender 비활성화**와 같은 행위는 공격자가 **실시간 보호 기능을 무력화해 시스템을 무방비 상태로 만들어** 악성 행위를 자유롭게 할 수 있도록 합니다.
- 만약, 사용자(관리자)의 행위가 아니라면 해킹진단도구에서 다른 이벤트가 탐지된 이력이 있는지 확인하고, Windows Defender를 포함한 **백신 소프트웨어를 활용해 정밀 검사**를 수행해야 합니다.

5) [EVT]_21_윈도우 명령어 셸 활성화 탐지(clr_enabled)

해당 룰은 MS-SQL 서버에서 .NET Framework(Common Language Runtime, CLR) 기능의 활성화 여부를 진단합니다. clr enabled 옵션이 활성화되면 SQL Server 에서 외부 코드나 프로그램을 실행할 수 있는 환경이 마련됩니다. **이는 해커가 악성 코드를 직접 실행해 시스템을 제어할 수 있는 위험을 초래**할 수 있습니다.

✓ **공격자 수행 행위**

공격자는 원격 명령 실행을 위해 저장 프로시저를 활성화합니다. xp_cmdshell 과의 차이점은, **xp_cmdshell 은 운영체제 명령어를 SQL 명령으로 실행**할 수 있게 하는 반면, clr enabled 는 **.NET 기반의 코드를 실행**할 수 있도록 하기 때문에 더 복잡한 외부 프로그램이나 스크립트를 구동할 수 있는 광범위한 기능을 제공합니다.

```
EXEC sp_configure 'show advanced options', 1;
EXEC sp_configure 'clr enabled', 1;
RECONFIGURE;
```

[그림 13] clr enabled 활성화 명령어

✓ **검출 결과**

해킹진단도구에서는 clr enabled 활성화 행위를 탐지하고 있습니다.

3	[EVT]_21_윈도우 명령어 셸 활성화 탐지(clr enabled)	MSSQL clr enabled 옵션 활성화 변경 여부	2024-09-25 15:07:35	clr enabled 0 1

[그림 14] 해킹진단도구 검출 결과 – clr enabled 활성화

✓ **탐지 결과 대응 방안**

- clr enabled 옵션의 활성화는 **공격자가 시스템에서 외부 명령과 악성 코드를 직접 실행**할 수 있게 됩니다.
- 관리자가 실행한 명령이 아닌 경우, 즉시 해당 프로시저를 비활성화하고 **백신 소프트웨어를 활용해 정밀 검사**를 수행해야 합니다.
- 공격자는 **clr shell** 을 활용해 시스템에 추가적인 악성코드를 설치하는 경우가 많기 때문에 정밀 검사가 필요합니다.

4.2. 백업 서버

1) [EVT]_08_사용자(관리자) 계정 생성 탐지

해당 룰은 시스템에서 사용자(관리자) 계정이 생성된 이벤트가 존재하는지 진단합니다. 공격자가 시스템에 침투한 후, 공격을 지속적으로 수행하기 위해 공격 전용 계정을 생성해 악성 행위를 수행합니다. 조직 내부에서 생성하지 않은 계정이 탐지되면 해당 시점에 공격자가 침투했을 가능성을 있어 추가 조사가 필요합니다.

✓ **공격자 수행 행위**

공격자가 계정을 생성하는 것은 시스템에 **장기적으로 머물기 위한 전략**입니다. 계정을 생성한 후에는 공격자가 **시스템을 자유롭게 조작하고 더 많은 공격을 수행**할 수 있게 되며, 공격의 탐지를 회피하고 흔적을 지우기 위한 중요한 수단으로 활용됩니다.

```
smbexec.exe [username]:[password]@ip share "net user adm1n adm1n1! /add"
```

[그림 15] SMBEXEC를 통한 원격 명령 실행 – 계정 생성

✓ **검출 결과**

해킹진단도구에서는 사용자(관리자) 계정이 생성될 경우, 아래 화면처럼 생성된 계정의 이름, 생성 시간 등을 확인할 수 있습니다.

해당 시나리오에서는 **adm1n** 계정을 생성했으며, ***타이포스쿼팅(Typosquatting)**을 활용해 교묘하게 자주 사용되는 **admin 계정**으로 위장한 행위가 포함되어 있습니다. 공격자는 시스템에 존재하는 계정을 교묘하게 바꿔 사용자(관리자)의 탐지를 회피하기 위해 노력하기 때문에 주의가 필요합니다.

***타이포스쿼팅(Typosquatting)** : '단어우월' 효과의 영향으로 사람은 글자 하나하나를 인식하기 보다는 단어 하나를 전체로 인식하는 경향이 있습니다. 그러한 인간의 자연스러운 행동을 노려, URL 등의 철자를 속여서 교묘하게 사이트를 위장하는 사이버 공격이 타이포스쿼팅입니다.

No	탐지명	설명	시간 (UTC+9)	내용
1	[EVT]_08_사용자(관리자) 계정 생성 탐지	계정 생성	2024-09-24 19:16:23	생성된 계정 : WDAGUtilityAccount SID : S-1-5-21-2814179269-961089793-119273692-504 주체 : MINWINPC$
			2024-09-25 15:58:23	생성된 계정 : adm1n SID : S-1-5-21-2814179269-961089793-119273692-1000 주체 : WIN-I518OE88C5M$

[그림 16] 해킹진단도구 검출 결과 – 사용자 계정 생성

✓ **탐지 결과 대응 방안**

- 사용자(관리자) 계정이 임의로 생성된 경우에는 실제 사용자(관리자)가 수행한 행위인지 확인해야 합니다.
- 사용자(관리자)가 수행한 행위가 아닐 경우, 즉시 해당 계정을 삭제하고 진단 도구 탐지 결과에서 추가 이상 행위가 식별됐는지 확인하고 조치해야 합니다.

2) [EVT]_14_윈도우 디펜더 백신의 실시간 감시 기능 비활성화 탐지

해당 룰은 Windows Defender 실시간 보호 기능이 비활성화**된 이벤트를 탐지**합니다. 일반적으로, 사용자가 업무 편의성을 위해 백신의 실시간 보호 기능을 비활성화 하기도 하지만 공격자가 공격의 탐지를 회피하기 위해 백신을 무력화하기도 합니다. 따라서, 사용자가 비활성화한 이력이 없는 경우에는 백신의 실시간 보호 기능이 비활성화된 시점에 공격자가 침투했을 가능성이 있어 추가 조사가 필요합니다.

✓ **공격자 수행 행위**

공격자가 **Windows Defender 실시간 보호 기능 비활성화**를 하는 주된 이유는 **보안 소프트웨어가 악성 행위를 탐지하거나 차단하지 못하게 하기 위함**입니다. Windows Defender 가 비활성화되면 공격자는 악성 코드 실행, 데이터 유출, 시스템 장악 등을 더 쉽게 수행할 수 있습니다.

✓ **검출 결과**

해킹진단도구에서는 Windows Defender 실시간 보호 기능 비활성화 행위를 탐지하고 있습니다.

No	탐지명	설명	시간 (UTC+9)	내용
1	[EVT]_14_윈도우 디펜더 백신의 실시간 감시 기능 비활성화 탐지	윈도우 디펜더 실시간 탐지 비활성화	2024-09-24 19:37:38	윈도우 디펜더 실시간 감시 비활성 설정 시간 : 2024-09-24 19:37:38

[그림 17] 해킹진단도구 검출 결과 – Windows Defender 실시간 감시 비활성화

✓ **탐지 결과 대응 방안**

- **Windows Defender 비활성화**와 같은 행위는 공격자가 **실시간 보호 기능을 무력화해 시스템을 무방비 상태로 만들어** 악성 행위를 자유롭게 할 수 있도록 합니다.
- 만약, 사용자(관리자)의 행위가 아니라면 해킹진단도구에서 다른 이벤트가 탐지된 이력이 있는지 확인하고, Windows Defender를 포함한 **백신 소프트웨어를 활용해 정밀 검사**를 수행해야 합니다.