asec.ahnlab.com /ko/90326/

MS-SQL 서버 공격 사례에서 확인된 XiebroC2

⋮ 9/28/2025

악성코드

- 2025년 09월 29일

AhnLab SEcurity intelligence Center(ASEC)에서는 부적절하게 관리되고 있는 MS-SQL 서버를 대상으로 하는 공격들을 모니터링하고 있으며 최근 XiebroC2를 이용한 공격 사례를 확인하였다. XiebroC2는 소스 코드가 공개된 C2 프레임워크로서 CobaltStrike와 유사하게 정보 수집, 원격 제어, 방어 회피와 같은 다양한 기능들을 지원한다. **[1]**

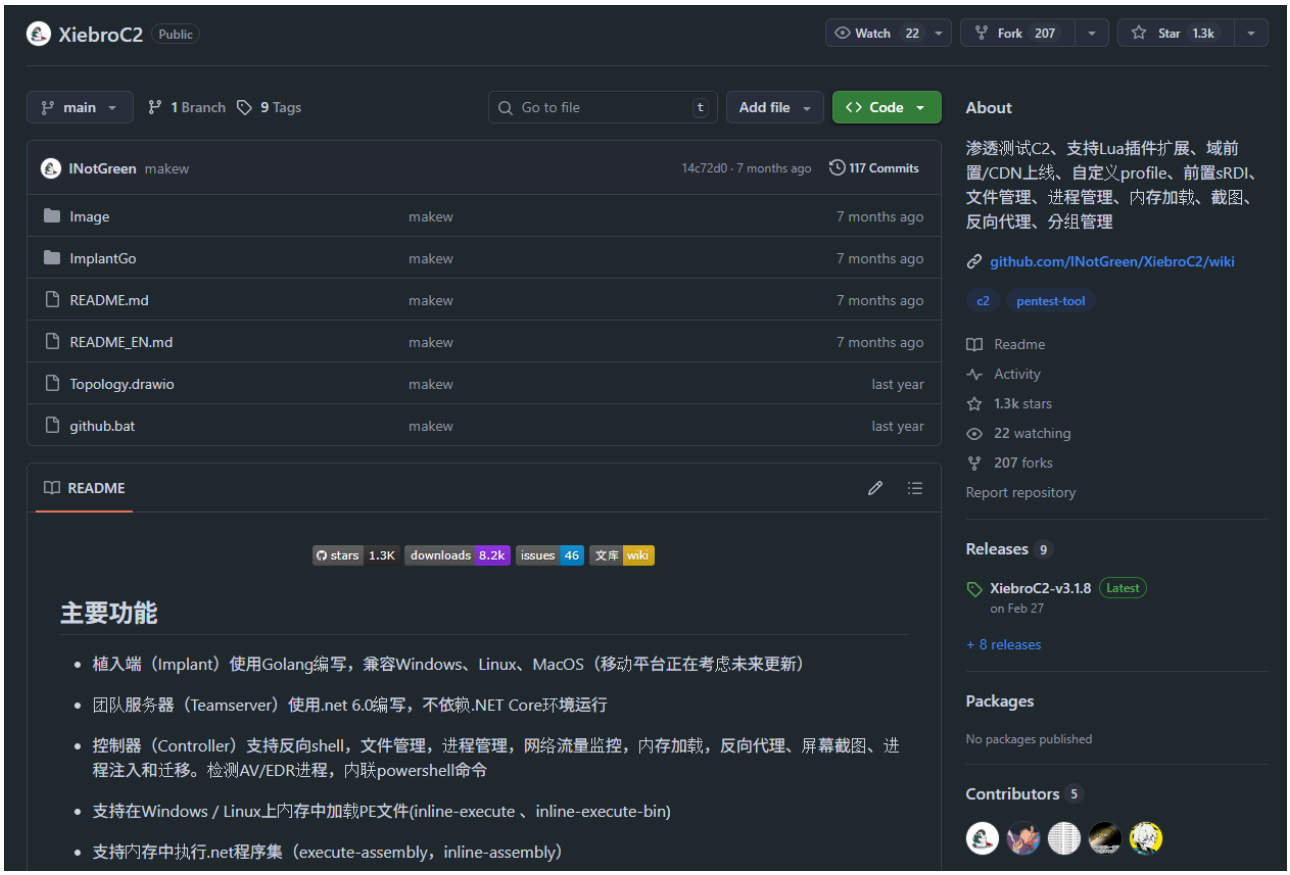

Figure 1. XiebroC2의 깃허브 페이지

1. 공격 사례

공격이 확인된 시스템은 외부에 공개되어 있으며 취약한 자격 증명 정보를 사용하는 것으로 추정된다. 해당 시스템은 이미 다양한 악성코드들의 설치 시도가 확인되었으며 일반적인 MS-SQL 서버 대상 공격 사례들처럼 주로 코인 마이너가 사용되었다.

공격자는 로그인에 성공한 이후 JuicyPotato를 설치하였다. 참고로 MS-SQL 서비스의 경우 이름 담당하는 프로세스들이 취약점이나 부적절한 설정에 의해 공격자의 명령을 실행할 수 있다고 하더라도 기본 설정에 의해 낮은 권한을 가지고 실행 중임에 따라 해당 프로세스의 권한으로 실행되는 악성코드 또한 추가적인 악성 행위를 수행하는 데 한계가 존재한다. 이에 따라 공격자들은 Potato 악성코드들을 주로 사용하는데 현재 실행 중인 프로세스 계정의 토큰들 중 특정 권한을 악용하는 방식으로 권한을 상승시켜 주기 때문이다.

JuicyPotato를 설치한 이후에는 파워쉘을 이용해 XiebroC2를 다운로드하였다.

Target Type	File Name	File Size	File Path
Target	tee.exe	5.58 MB	%ALLUSERSPROFILE%\tee.exe
Current	powershell.exe	445 KB	%SystemRoot%\system32\windowspowershell\v1.0\powershell.exe
Parent	cmd.exe	283 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	sqlservr.exe	610.01 KB	%ProgramFiles%\microsoft sql server\mssql15.sqlexpress\mssql\binn\sqlservr.exe

Process	Module	Target	Behavior	Data
powershell.exe	N/A	N/A	Downloads executable file	http://183.196.14.213/tee.exe tee.exe
sqlservr.exe	N/A	N/A	Deletes executable file	N/A
cmd.exe	N/A	update.exe	Creates process	N/A
powershell.exe	N/A	N/A	Connects to network	http://183.196.14.213:2780/tee.exe

Figure 2. XiebroC2를 다운로드하는 MS-SQL 서비스

2. XiebroC2

XiebroC2는 CobaltStrike와 유사한 C2 프레임워크로서 소스 코드가 공개되어 있다. 실제 백도어 기능을 담당하는 Implant는 Go 언어로 작성되었으며 멀티 플랫폼 즉 윈도우, 리눅스, macOS 운영체제를 지원한다. 공격자는 감염 시스템에 설치된 XiebroC2를 이용해 리버스 쉘, 파일 및 프로세스 관리, 네트워크 모니터링과 같은 원격 제어 및 리버스 프록시 그리고 스크린샷 등의 기능을 사용할 수 있다.

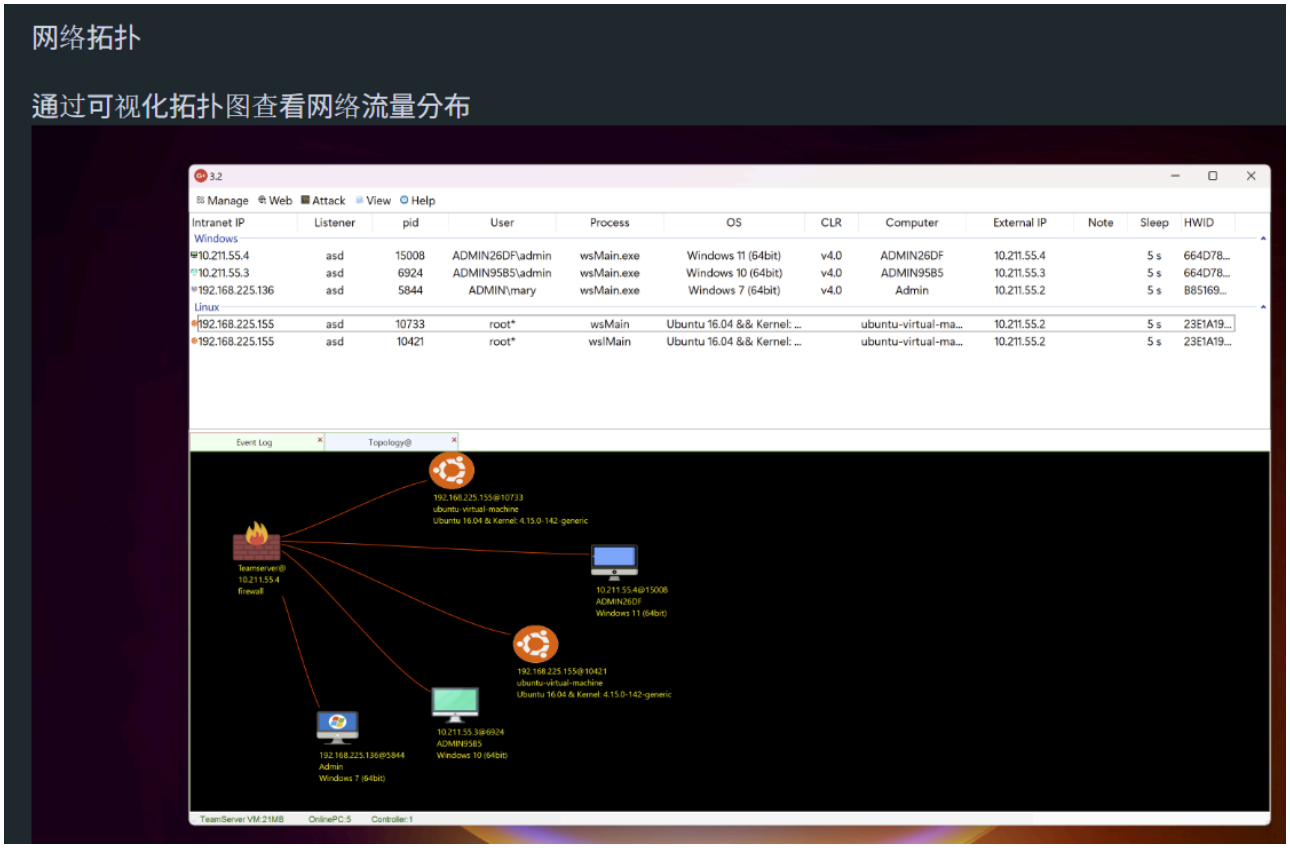

Figure 3. XiebroC2의 패널 (깃허브)

XiebroC2에는 다음과 같은 형태의 설정 정보가 존재한다. 실행 후에는 PID, HWID, 컴퓨터 이름, 사용자 이름과 같은 정보를 수집하고 C&C 서버와 연결 후 공격자의 명령을 수행할 수 있다.

- HostPort = “1.94.185[.]235:8433”
- Protocol = “Session/Reverse_Ws”
- ListenerName = “test2”
- AesKey = “QWERt_CSDMAHUATW”

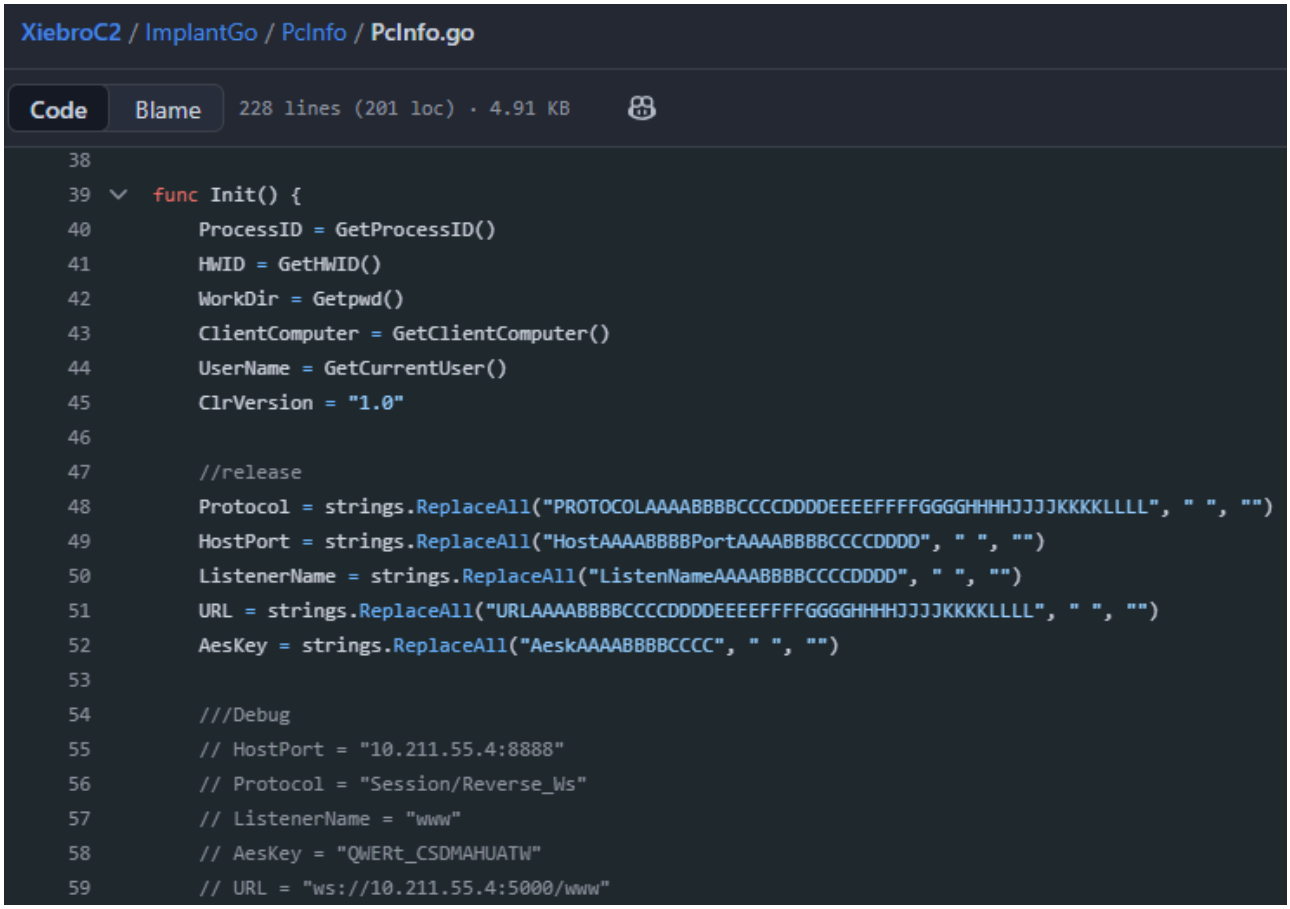

Figure 4. XiebroC2가 수집하는 정보

3. 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

4cfdd0ae14185e72a74e67717c23526c

7d28a709a6ca6eef5af40f48cf7e3d12

추가 IoC는 ATIP에서 제공됩니다.

URL

http[:]//183[.]196[.]14[.]213[:]2780/tee[.]exe

추가 IoC는 ATIP에서 제공됩니다.

IP

1[.]94[.]185[.]235

추가 IoC는 ATIP에서 제공됩니다.

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