Malwarebytes LABS

Ransomware targets Edge users

Posted: January 12, 2022 by Mark Stockley

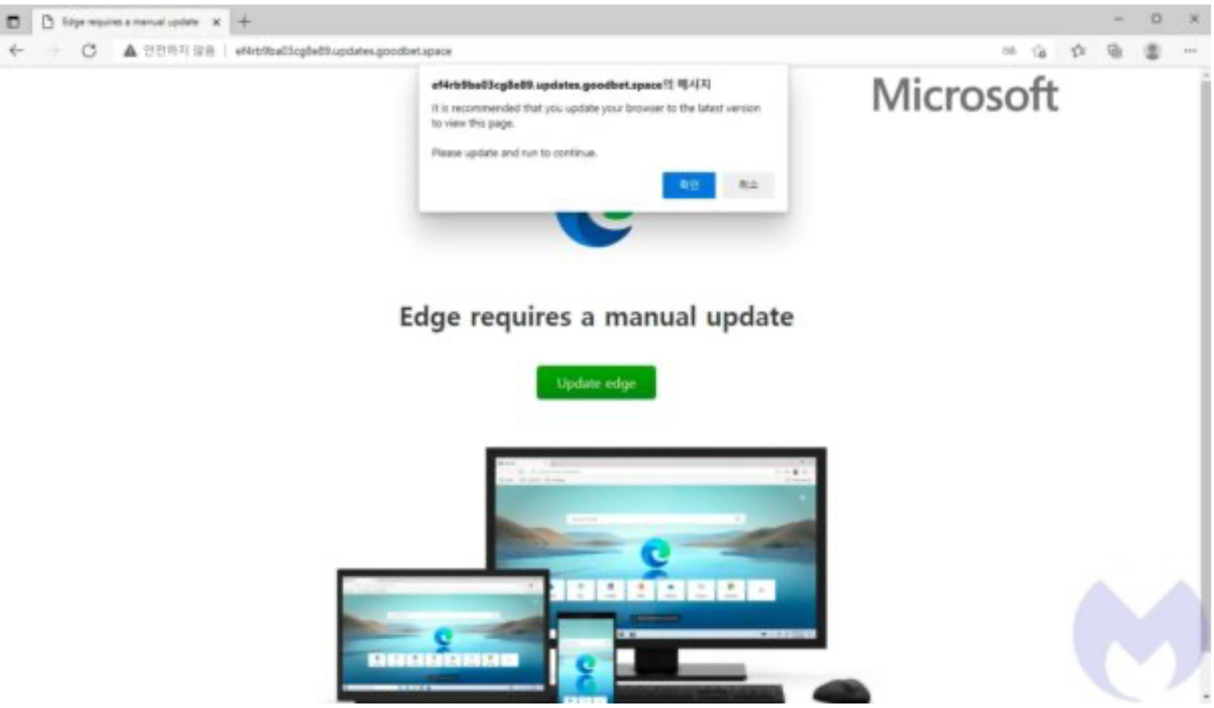
Unless you've been hiding under a rock for the last twenty years, you've probably heard the one about "keeping your software up to date". Applying software updates promptly is arguably the single most useful thing you can do to keep yourself secure online, and vendors, experts, pundits, and blogs like ours, never let users forget it!

And because it's good advice that's easy to follow, cybercriminals like to use fake software updates to con users.

Fake software updates have been a go-to tactic for getting users to download malware for many years. A convincingly-branded message that tells users they need to update their out of date software taps into all the good security messaging users have soaked up, it gives them a reason to install strange software from the Internet, and it carries exactly the right mixture of implied threat and urgency that social engineers like.

For years, fake Flash updates were a fixture of web-based malware campaigns. Flash provided just the right kind of patsy: It was famous for its security holes, and new updates were released almost every month. But with Adobe's media player a year into its long overdue retirement, criminals have had to look elsewhere for a convincing cover story, and where better than perhaps the most frequently updated software of them all, the web browser? Browsers have an almost frenetic update schedule, and many users understand that installing regular updates is a normal and important part of their everyday use.

Last week, Malwarebytes' Threat Intelligence worked with nao_sec researchers to investigate a recently-discovered update to the Magnitude Exploit Kit that was duping users with a fake Microsoft Edge browser update.


Edge requires a manual update
안전하지 않음 | ef4rb9ba03cg8e89.updates.goodbet.space
Microsoft
Edge requires a manual update
Update edge

ef4rb9ba03cg8e89.updates.goodbet.space의 메시지

It is recommended that you update your browser to the latest version to view this page.

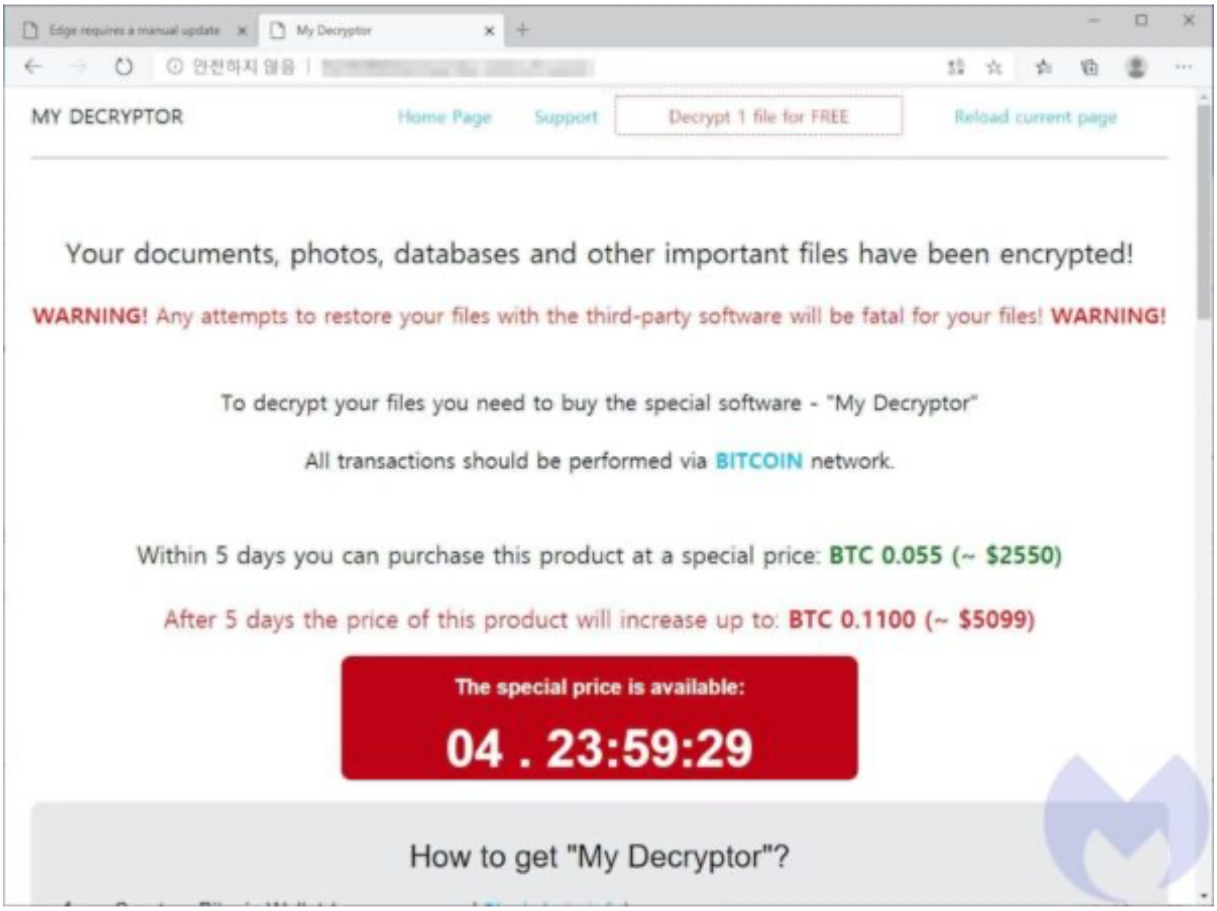
Please update and run to continue.

The Magnitude exploit kit offers users ransomware dressed up as Microsoft Edge

The Magnitude exploit kit uses a grab-bag of social engineering lures and exploits to attack web users and install ransomware on their computers. Although Magnitude has been used to target different geographies and deliver different kinds of ransomware in the past, these days it is strictly focussed on installing Magniber ransomware on targets in South Korea.

The fake Edge update attack flows like this:

1. A user visits an ad-heavy website and encounters a malicious ad.
2. The malicious advert redirects them to a “gate”, known as Magnigate.
3. Magnigate runs IP address and browser checks to determine if the user will be attacked.
4. If the user fits the attackers’ criteria, Magnigate redirects them to the Magnitude exploit kit landing page.
5. Based on information from Magnigate, the exploit kit chooses an attack from its collection.
6. In this case, the exploit determines the best attack is a fake Microsoft Edge update.
7. The “update” is actually a malicious Windows Application package (.appx) file.
8. The .appx file downloads Magniber ransomware from the Internet.
9. Magniber encrypts the user’s files and demands a ransom.



Your documents, photos, databases and other important files have been encrypted!

WARNING! Any attempts to restore your files with the third-party software will be fatal for your files! WARNING!

To decrypt your files you need to buy the special software - "My Decryptor"

All transactions should be performed via BITCOIN network.

Within 5 days you can purchase this product at a special price: BTC 0.055 (~ $2550)

After 5 days the price of this product will increase up to: BTC 0.1100 (~ $5099)

The special price is available:

04 . 23:59:29

How to get "My Decryptor"?

A Magniber ransom demand

Magnitude is regularly updated with fresh attacks, and the fake Edge update appears to have been added in the last few weeks. In the past, Magnitude has made extensive use of Flash and Internet Explorer vulnerabilities, but as the software landscape has changed it has had to adapt. In late 2021, it was seen targeting a sandbox escape vulnerability in the Chrome browser family, for example. That should be no surprise, Chrome is the most popular web browser by far and it suffered from an unprecedented glut of zero-days in 2021.

The number of problems affecting Chrome's V8 JavaScript engine suggest there may be underlying problems in that part of the browser, and we fully expect that the near-term future of exploit kits will be Chrome exploits. However, that won't stop exploit kits from taking advantage of other tactics, like fake updates, where they're more likely to succeed.

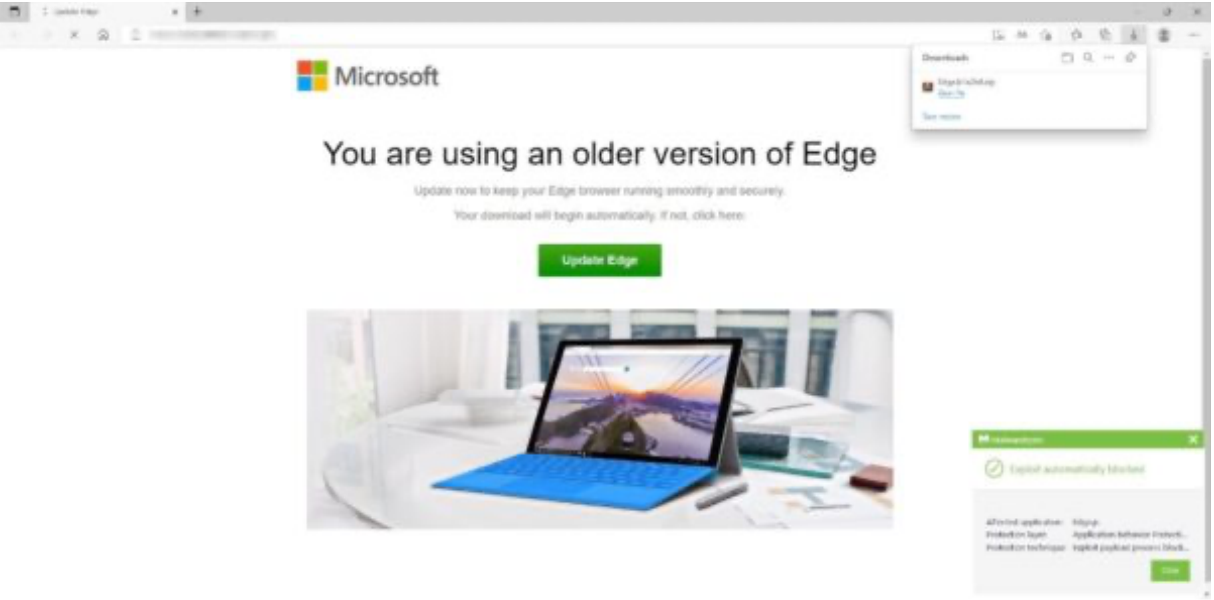
Although Edge is based on the same browser as Chrome, uses the same V8 JavaScript engine, and is vulnerable to the same exploits, those exploits will only work on browsers that are out of date. And since browsers are pretty good at installing updates, Magnitude also needs attacks that work against fully updated browsers.

The irony is that the users most likely to run into an attack telling them they need to update their browser are the ones who already have.

If you want to know what version of Edge you’re running and if there are updates available, we suggest you follow the official guidance from Microsoft:

1. Open Edge, select **Settings and more**, and then select **Settings**.
2. Scroll down and select **About Microsoft Edge**.

Malwarebytes blocks Magniber ransomware.



You are using an older version of Edge

Update now to keep your Edge browser running smoothly and securely.

Your download will begin automatically. If not, click here.

Exploit automatically blocked

Affected application: [illegible]
Protection layer: Application behavior Protecti...
Protection technique: Exploit payload process block...

Malwarebytes blocks a Magniber ransomware download