Dubious security vulnerability: Code execution via LNK file

devblogs.microsoft.com/oldnewthing/20190403-00

April 3, 2019

Raymond Chen

A security vulnerability report arrived that claimed to have achieved code execution via a shortcut (LNK) file. The report was somewhat convoluted, but it went something like this:

1. Start with this pre-fabricated shortcut file.
2. Copy it to a folder of your choosing.
3. Edit the shortcut file in this very special way, substituting the full path to the shortcut file where specified.
4. Double-click the shortcut file.
5. Code execution is achieved!

If you can trick the user into double-clicking an arbitrary shortcut file of your choosing, then you don't have to do all this weird special editing nonsense.

1. Create a shortcut that runs `pwnzor.exe` directly from an Internet-accessible file share.
2. Double-click the shortcut file.
3. Code execution is achieved!

When phrased this way, it's clear that the attack is really a social engineering attack: If you can convince a user to do anything you tell them to, then you can get them to do anything.

This in itself is not particularly interesting.

Upon closer inspection, what the finder was actually reporting was that they found a clever way to make a file both a legal LNK file and a legal script file. The "Edit the shortcut file in this very special way" was setting things up so that the LNK file could feed itself to the script engine.

This was an interesting discovery, the ability to polyglot a LNK file with a script file. But it's not a security vulnerability. It's just a curiosity.

Because you still have to convince the user to run it.

Raymond Chen

Follow