Dubious security vulnerability: Once I have tricked the user into running a malicious shortcut, I can install malware

devblogs.microsoft.com/oldnewthing/20250414-00/?p=111072

April 14, 2025

A security vulnerability report arrived in the form of a ten-page PDF, formatted like a term paper, purporting to have found a way to leverage shortcut files to install malware. It begins with a 300-word abstract that opens “Computer security is of growing importance in today’s connected world,” followed by a 400-word introduction that similarly focuses on the importance of keeping your computer secure.

Now, I have experience with, and occasionally even enjoy, reading journal papers. But a security vulnerability report is not supposed to be a journal paper. Your goal is not to impress upon the reader the importance of computer security and therefore justify your avenue of research. By the time you get to the vulnerability report, it is already a given that computer security is important, and the research has already justified itself by the existence of the proof of concept. You don’t need to convince me that this is a worthwhile endeavor. You also don’t have to teach me what malware is, or pad your text with discussion of what sorts of bad things malware can do once it has become established.

Okay, finally I get to page five, when they finally lay out the attack. I’ll boil it down for you rather than making you suffer through five pages of text and screen shots.[1]

- Create a shortcut file that runs a command line which installs malware.
- Convince the user to launch the shortcut.
- Malware is now installed!

In the various screen shots included in the paper, one of them is a warning dialog from the system.

Open File – Security Warning

Do you want to open this file?

Name:	C:\Users\Victim\Downloads\Harmless.lnk
Publisher:	**Unknown Publisher**
Type:	Shortcut
From:	C:\Users\Victim\Downloads\Harmless.lnk

Open
Cancel

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software.

Windows displays this warning when you try to run a shortcut that was downloaded from the Internet, because shortcuts can execute any command line and therefore can perform any operation that you yourself have the power to do.

Which includes installing malware into your user profile.

The paper assumes that the user trusts the source from which the shortcut was downloaded and approved the dangerous operation.

So there is no technical security vulnerability here. It's a social engineering attack: You have to convince the user to run the shortcut even though the system told them it's not necessarily a great idea.

Maybe next time, they can cut to the chase and just say so, instead of wrapping it inside a ten-page term paper.

[1] Or the 250-word "conclusion."