Issued 6/15/17

Hovering Over Links Can Install New Malware

The weakest link in computer security is often the user, which is why so many online attacks involve social engineering. If someone can trick you into opening an email attachment or visiting a malware website, they can own your system. Even when you think you're being careful, clever online villains might still be able to hack you. Security firm Trend Micro says a new method of delivering malware has popped up that doesn't require you to even click on anything. All you need to do is hover your mouse over the wrong link.

The danger users are exposed to depends on how old the version of PowerPoint happens to be. On older versions of PowerPoint, hovering over a link would load a preview. These versions of the software could be instructed to run a PowerShell script, which is how the malware reaches out to a server to install a trojan. Starting with Office 2010, Microsoft enabled a feature called Office Protected View that prevents scripts from running. Anyone using an older version of PowerPoint or a new one with Protected View disabled is vulnerable.

Of course, this attack also relies upon email currently. People should know better than to download an attachment and open in, even if it looks like an invoice. Trend Micro suggests people consider all emailed files from unknown sources to be dangerous, not just executables.