Threat Alert

Malware Analysis – Mouse Hovering

Malware Analysis—Mouse Hovering Can Cause Infection

During the last few months, we've been watching an interesting twist in malware analysis. Cybercriminals recently developed a technique where, in some cases, malware can infect a device when the victim simply hovers their mouse over a malicious link.

The dangers of *clicking* on a link are well understood, but in this attack, merely *hovering* over the link can trigger the malware to load. Since mouse hovering is generally considered to be a safe method to view the URL associated with a given link, this attack vector, if fully exploited, presents cybercriminals with a powerful weapon. Fortunately, at this time, the attack appears to be limited to Microsoft PowerPoint files and requires user interaction to work.

Hovering

Currently, the attack starts when the victim receives a Microsoft PowerPoint file, usually as an email attachment (see the Lastline blog: Malicious Email Attachments – Protection from Infected PDF Files to learn more about dangerous emails). If the user opens the PowerPoint file and hovers over text or a photo in the PowerPoint slide deck that includes a malicious link, the hovering will trigger a mouseover action that installs the malware.

By default, current versions of Microsoft Office, including PowerPoint, launch in Protected View, which prevents the malicious content from executing. However, if the user has enabled the content by exiting Protected View, their machine will be infected.

Attack Methodology

The implications of this attack vector are quite threatening. Mouse hovering has legitimate uses, and if cybercriminals successfully expand the attack methodology to applications beyond PowerPoint, it will be difficult for system defenders to detect and thwart these attacks. The development also demonstrates that cybercriminals are experimenting with different techniques. While that's not a surprise, the approach is somewhat unique in that it doesn't rely on well-known hacking techniques that are largely understood and well defended by the security community.

Social Engineering

It's somewhat surprising that we haven't already seen this attack in other Microsoft Office files since they support similar functionality. It may also start showing up in non-Microsoft environments. As a precaution, network defenders should begin now to be on the lookout for this type of malware and deploy tools that can detect it via comprehensive static analysis and mouse-hovering simulation.

Since the attack depends on social engineering to dupe users into downloading the file and enabling content, organizations should also perform appropriate user training

 |