Issued 7/12/17

Adobe Flash Player users should update their software NOW

One of the favorite pieces of software for malicious hackers to target on users' computers is Adobe Flash Player. Why? Well, there are a few reasons.

First, Adobe Flash Player is on an awful lot of computers. Many users may have it installed it long ago in order to access Flash-based media content online, such as videos. Malicious hackers can rely upon a large number of people having Flash installed, making it a target for attack.

Second, the version of Adobe Flash Player installed on your computer may be out-of-date. Users may have failed to configure updates properly, or chosen to ignore reminders to update the software promptly when a new security update is released. There's only one thing more attractive to a malicious hacker than widely-used ubiquitous software, and that's widely-used ubiquitous software that hasn't been kept updated with the latest patches. It doesn't matter if a hacker doesn't have zero-day exploit to throw at your Adobe Flash Player if you haven't been bothering to keep it protected against known vulnerabilities.

Third, there has been a long history of malicious hackers finding critical security holes in Adobe Flash Player, and building their attacks into exploit kits for anyone to deploy. Flash is closed, proprietary software controlled by Adobe and it has been plagued with software vulnerabilities and serious flaws over many years. Quite why Flash has been targeted so often is open to some debate, but the mere fact that it has suggests that it will continue to be for some time to come.

The upshot of this is that when Adobe releases new security patches for Adobe Flash Player, it would be very sensible indeed for its users to sit up and take notice. Earlier today Adobe issued a security advisory detailing updates it has released for Adobe Flash Player for Windows, Macintosh, Linux and Chrome OS. The updates are said to address critical vulnerabilities that could potentially allow an attacker to take control of a vulnerable system, allowing a remote attacker to execute code on a victim's computer and take control over their device.