Real attacks

threatpost Podcasts / Malware / Vulnerabilities / InfoSec Insiders / Webinars

← Study: Password Security Improves with Age Researchers Find Methods fo

Flame Malware Uses Forged Microsoft Certificate to Validate Components

Author:
Dennis Fisher

June 4, 2012 / 12:00 pm

2 minute read

Share this article:

Microsoft has found that some components of the Flame malware were signed using a forged digital certificate that the attackers were able to create by exploiting a weakness in the way that Microsoft's Terminal Services allows customers to sign code with Microsoft certificates. The company has sent out an update that will remove three untrusted certificates from the Microsoft Trusted Certificate Store and has made a change to the way Terminal Services handles code signing.

Microsoft Security Response Center Report an iss

Flame malware collision attack explained

Security Research & Defense / By swiat / June 6, 2012 / malware, PKI

Since our last MSRC blog post, we've received questions on the nature of the cryptographic attack we saw in the complex, targeted malware known as Flame. This blog summarizes what our research revealed and why we made the decision to release Security Advisory 2718704 on Sunday night PDT. In short, by default the attacker's certificate would not work on Windows Vista or more recent versions of Windows. They had to perform a collision attack to forge a certificate that would be valid for code signing on Windows Vista or more recent versions of Windows. On systems that pre-date Windows Vista, an attack is possible without an MD5 hash collision. This certificate and all certificates from the involved certificate authorities were invalidated in Security Advisory 2718704. We continue to encourage all customers who are not installing updates automatically to do so immediately.

Mysterious Missing Extensions

Limitation of secure channels