FireEye takes security firm to court over vulnerability disclosure

ERNW contends it thought it had responsibly cooperated with FireEye

By Jeremy Kirk   FOLLOW

IDG News Service | September 10, 2015

A spat between two security companies shows just how sensitive reporting software vulnerabilities can be, particularly when it involves a popular product.

The kerfuffle between FireEye and ERNW, a consultancy in Germany, started after an ERNW researcher found five software flaws in FireEye's Malware Protection System (MPS) earlier this year.

One of the flaws, found by researcher Felix Wilhelm, could be exploited to gain access to the host system, according to an advisory published by ERNW.

[Also on ITworld: Low and no-cost ways to learn about IT security. Don't miss a thing! Sign up for ITworld's daily newsletter.]

As is customary in the industry, ERNW contacted FireEye in early April with details of the problems.

ERNW planned to release an advisory after a 90-day disclosure period, wrote the company's founder, Enno Rey, in a blog post Thursday. But in the next few months, relations between the two companies became strained.

FireEye, which reviewed ERNW's proposed notification, contended it contained too much technical detail about the inner workings of its MPS product, Rey wrote.

Although ERNW felt the detail was needed to understand how the vulnerabilities posed a risk, the company removed them from its advisory, Rey wrote.

In a face-to-face meeting in Las Vegas on Aug. 5, Ray wrote that it appeared the two companies had reached a consensus on a draft of the disclosure document.

But about a day later, FireEye sent ERNW a cease-and-desist letter, which focused on the disclosure of the company's intellectual property, Rey wrote. The letter contended that no consensus had been reached between the parties the day before.

Before ERNW responded in writing, FireEye obtained an injunction on Aug. 13 from a district court in Hamburg.

Wilhelm presented his findings on Thursday at the 44CON conference in London. He has published his slide deck, but some information relating to FireEye's technology has been redacted in order to comply with the injunction.

A slide from ERNW researcher Felix Wilhelm's presentation for the 44CON conference in London was redacted in order to comply with a German court's injunction.

Escalating the matter to court was unexpected considering it appeared on Aug. 5 that the companies had reached a resolution, Rey wrote.

"We can only speculate what the intentions are from their side," he wrote. "In general, we consider it an inappropriate strategy to sue researchers responsibly reporting security vulnerabilities."

FireEye had no intention to block ERNW from discussing the vulnerabilities publicly, wrote the company's vice president for global communications, Vitor C. De Souza, in an email.

But "we were not willing to expose any of the proprietary information that would put our business and customers at risk," he wrote. "Under German law, they were also not allowed to release intellectual property that was not theirs."

FireEye issued a notification describing the vulnerabilities, which it patched some time ago, on Sept. 8. Although it is customary to include a timeline from when a vendor is notified to when patches were issued, FireEye's notice doesn't contain one.

Jeremy Kirk — *Australia Correspondent*

👤 ✉️ 📡

❯ **Free Course: JavaScript: The Good Parts**

💬 **View Comments**

YOU MIGHT LIKE

Android device makers to release monthly security fixes

How Secure Scrum can help you build better software

The Ultimate Way to Get Cheap Hotel Rooms
Hotel Bargains