

15 April 2008



The webpage attempting to drop the infection
Cyveillance

By: Bogdan Popa, Security and Search Engines Editor

Sued? Antivirus Update Required!

Fake subpoenas send CEOs to infected website

A new and pretty dangerous phishing attack was launched a few days ago, targeting the CEOs of online companies. According to Cyveillance's official blog, the CEO of the company, Panos Anastassiadis, received a suspicious email, apparently a subpoena, which informed him that he had been sued, the message including a link supposed to allow the receiver to download court documents. What's interesting is that, in comparison with the traditional phishing scams, this "spear phishing" (as it's called) attack, includes all kinds of details such as the name of the receiver and even the phone number. This means that the spammer had to do a little bit of research work before he sent the message but, since we're talking about a CEO, hacking his computer is probably a thing to be proud of - for a phisher. "Like many other spear phishing attacks, the phisher performed research before launching his or her attack. Specifically, the individual was able to locate use our CEO's email address and the Cyveillance phone number in the email. This information was used to enable and build additional credibility for the attack," the security experts of Cyveillance wrote. As mentioned, the message came with an email which stated that it provided access to court documents. However, once the reader clicked on it, he was redirected to a page informing that the case was closed and no further action was required. But, without the user even knowing about it, the page attempted to drop and install a Trojan-Downloader which, according to Cyveillance, couldn't be detected by several antivirus technologies. According to the scanning information provided by VirusTotal and concerning the file uploaded by Cyveillance, Avast, AVG, BitDefender, Kaspersky, McAfee and several others didn't detect the infection. However, F-Secure, F-Prot, AntiVir, NOD32v2 and Microsoft's security tool found the Trojan-Downloader.