



Fortinet threat landscape report highlights new zero-day vulnerabilities

1-15-April 2011



EC NEWS ANNIVERSARY SPECIAL



Fortinet threat landscape report highlights new zero-day vulnerabilities

Fortinet has announced its February 2011 Threat Landscape report, which details five zero-day vulnerabilities found in Cisco (FGA-2011-03), Adobe (FGA-2011-06) and Microsoft (FGA-2011-04) products. FortiGuard Labs worked diligently with these companies to address and disclose these vulnerabilities as part of its responsible disclosure program, which includes more than 125 zero-day vulnerability discoveries to date.

Microsoft also issued a zero-day security advisory regarding an information disclosure vulnerability with IE and MHTML, making it possible under certain conditions for attackers to inject a client-side script in the response of a Web request run in the context of the victim's Internet Explorer. The script could spoof content, disclose information or take any action that the user could take on the affected Web site on behalf of the targeted user.

SpyEye botnet activity surges

The SpyEye Botnet entered the Threat Landscape Report's Top 10 malware listing for the first time this month, signaling a possible shift of criminal organizations around the world that had previously employed the Zeus botnet. Historically, Zeus developers have made efforts to avoid detection and analysis on their configuration files by prepending garbage (red herrings) before data structures. Last year, FortiGuard Labs analyzed an emerging mobile component of Zeus, known as Zimo and recently noted that Zimo B has resurfaced with both a Symbian and Windows Mobile version that was actively in the wild.

"We're likely to see similar ongoing activity by the SpyEye group, such as routine obfuscation of their data and command and control transmissions," said Derek Manky, Senior Security Strategist at Fortinet. "SpyEye developers are also working to make their product more efficient in terms of management and automation, which is evidenced by the bot's new Automatic Transfer System."

New credit card phishing email

This month FortiGuard Labs observed a new credit card phishing email, which employs a scare tactic that says the account has been "in violation of policies." In the example discovered, the highlighted link pointed to a rogue domain that did not belong to the card vendor – however, streamed authentic content from card vendor's site.

"Always observe these types of trails before clicking on links," Manky said. "In this case, clicking the link would direct the victim to a landing site located at a data center in Bangkok. This landing site would then redirect the user to a server in China, which borrowed content from the legitimate credit card site using a proxy. This man-in-the-middle setup allowed the attackers to easily intercept login credentials along the way."

Once these credentials are obtained, it becomes very easy for criminals to launder stolen funds through the likes of anonymous transferring services and money mules.

FortiGuard Labs compiled threat statistics and trends for February based on data from FortiGate network security appliances and intelligence systems in production worldwide.

EXPRESS COMPUTER | WWW.EXPRESSCOMPUTERONLINE.COM | APRIL 1-15, 2011 | 77

