Security
April 8, 2009 12:01 AM PDT

Microsoft: Scareware, PDF exploits rise

by Elinor Mills

The use of scareware and exploits that take advantage of common file formats like PDF, Excel and Word rose in the second half of last year as online scammers realized people are getting smarter about recognizing spam and phishing e-mails, according to a **Microsoft security report** released on Wednesday.

There was a significant increase in rogue security software, which falsely informs people they need to buy security software and instead either does nothing or steals personal information, the **Microsoft Security Intelligence Report** found.

Two rogue malware families--Win32/FakeXPA and Win32/FakeSecSen-- were detected on more than 1.5 million computers, pushing them into the list of top 10 threats in the second half of 2008. One rogue application, dubbed Win32/Renos, was found on 4.4 million computers, showing growth of nearly 70 percent over the first half of the year, according to the report issued twice a year.

Microsoft and the Attorney General's office in Washington state filed a handful of lawsuits against alleged scareware companies **last year**.

Meanwhile, the total number of unique vulnerability disclosures dropped 3 percent during the second half of last year and was down 12 percent for the year from the prior year. The proportion of vulnerabilities disclosed in operating systems continued to decline, to 8.8 percent, while 4.5 percent affected browsers and 86.7 percent affected applications and other software.

During the second half of 2008, Microsoft released 42 security bulletins addressing 97

vulnerabilities, a 67 percent increase over the first half of the year. For the full year, the company released 78 security bulletins addressing 155 vulnerabilities, up nearly 17 percent from 2007.

Microsoft software accounted for 6 of the top 10 browser-based vulnerabilities attack on computers running Windows XP in the second half of last year, while there were none for computers running **Windows Vista**.

The most frequently exploited holes in Office were also some of the oldest, with more than 91 percent of attacks exploiting a single vulnerability for which a security fix had been available for more than two years.

Attacks targeting PDF files rose sharply, reaching twice as many in July as in all of the first half of 2008, the report said. Adobe **last month** released a security update to fix a critical vulnerability in Adobe Reader 9 and Acrobat 9 for which exploits had been reportedly found in the wild for nearly two months.

Corporate environments running Forefront Client Security are more likely to encounter worm infections than home computers running Windows Live OneCare, while home computers had more Trojans and Trojan downloaders, the report found.

As for e-mail, more than 97 percent of it is unwanted as either spam, phishing attacks or have malicious attachments, the report found.

Despite the seeming industry emphasis on malicious hacking and other Internet attacks, lost and stolen equipment remains the most common cause of security breaches resulting in data loss, representing half of all reported incidents, according to the **Open Security Foundation's OSF Data Loss Database**. Stolen **laptops**, for instance, represented 33.5 percent of all data loss incidents and combined with lost equipment represented half of all incidents reported. Hacking accounted or malware incidents accounted for less than 20 percent.

Updated 11:25 a.m. PDT with link to report.

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal