Written by Marco Attard
21 April 2017

According to Kaspersky exploits remain a serious security threat-- an old vulnerability related to the Stuxnet worm still poses as an open door for hackers targeting Windows computers.

Known as CVE-2010-2568, the flaw was initially patched out back in 2010, but Kaspersky says it is still one of the most widespread software exploits. Used by the Stuxnet worm to remotely execute code without user knowledge, between 2015 and 2016 it was used to target around 25% of Kaspersky users who encountered an exploit.

The vulnerability only affects Windows XP, Windows Server 2008 and Windows 7 systems, but hackers are on the hunt for susceptible systems through malware able to self-replicate over a network and remain in affected computers.

Other pieces of out-of-date software carry similar vulnerabilities, including Microsoft Office, Android and Java.

The moral of the story? One has to ensure their software is up to date. After all, the hacker group named Sofacy (aka APT28 and or Fancy Bear) has made use of 25 vulnerabilities during the 2010-2016 period, including 6 zero-days. Following it is the Equation group with 17 vulnerabilities, of which 8 are zero-days. Vulnerabilities can become more dangerous if made public, since big threat hours can grab and repurpose them "within hours."

As such, one should enable auto-update features if available, and select software vendors with a responsible approach to security. Network management should use patch management

solutions for centralised software updates, and personnel must be educated on social engineering making victims open documents or links infected with exploits.

Go Exploits: How Great is the Threat?