Windows flaws let Russian hackers spy on NATO

WASHINGTON, USA: Hackers based in Russia used a flaw in Microsoft Windows to spy on NATO, European governments and other organisations as far back as 2009, security researchers have found.

A flaw in Windows software allowed Russian hackers to spy on NATO, various European governments, energy and telecommunications companies and US academic institutions according to researchers at iSight Partners. A patch for the flaw will be released by Microsoft this week. Image: Popmatters

A report by the cybersecurity firm iSight Partners said the flaw dubbed "Sandworm" allowed the cyber spies to gain access to computers using all versions of Windows for PCs and servers over the past five years.

The researchers said Microsoft was notified of the vulnerability and was making a patch available.

The report said the team exploiting this flaw began operating in 2009, and stepped up its efforts in late 2013, after the crisis in Ukraine.

The researchers said the targets included NATO, Ukrainian government organisations, Western European governments, energy and telecommunications companies in Europe and US academic institutions, but added that visibility is limited and that there is a potential for broader targeting from this group.

They noted that many of the attacks have been specific to the Ukrainian conflict with Russia and to broader geopolitical issues related to Russia.

According to a blog post by iSight, it's not clear what data may have been stolen but that the broad range of attacks virtually guarantees that all of those entities targeted fell victim to some degree.

"We immediately notified targeted entities, our clients across multiple government and private sector domains and began working with Microsoft to track this campaign and develop a patch for the vulnerability," iSight added.

It noted that NATO was targeted as early as December 2013, and that other attacks hit a Polish energy firm and French telecommunications company.

According to iSight the cyberspying effort was referred to as Quedach by another security firm F-Secure, which described some elements of the campaign last month but only captured a small component of the activities and failed to identify use of the security flaw.