The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russian Cyber Attackers Used 2 Unknown Flaws — U.S. Security Firm

By The Moscow Times

April 19, 2015

The same hackers are also believed to have broken into White House machines containing unclassified but sensitive information such as the president's travel schedule.

SAN FRANCISCO — A widely reported Russian cyber-spying campaign against diplomatic targets in the United States and elsewhere has been using two previously unknown flaws in software to penetrate target machines, a security company investigating the matter said on Saturday.

FireEye Inc, a prominent U.S. security company, said the espionage effort took advantage of holes in Adobe Systems Inc's Flash software for viewing active content and Microsoft Corp's ubiquitous Windows operating system.

The campaign has been tied by other firms to a serious breach at U.S. State Department computers. The same hackers are also believed to have broken into White House machines containing unclassified but sensitive information such as the president's travel schedule.

FireEye has been assisting the agencies probing those attacks, but it said it could not comment on whether the spies are the same ones who penetrated the White House because that would be classified as secret.

FireEye said that Adobe had issued a fix for the security weakness on Tuesday, so that users with the most current versions should be protected. The Microsoft problem by itself is less dangerous, since it involves enhanced powers on a computer from those of an ordinary user.

A Microsoft spokesman said the company was working on a patch.

In October, FireEye said the group it calls APT28 had been at work since 2007 and had targeted U.S. defense attaches and military contractors, NATO alliance offices and government officials in Georgia and other countries of special interest to the Kremlin.

Days before that report, security firm Trend Micro Inc described a campaign it called "Pawn Storm" against computers in the State Department, Russian dissidents, NATO and other Eastern European nations. Because Pawn Storm and APT28 used some of the same tools and hit the same targets, other information security professionals concluded they were the same hackers.

On Thursday, Trend Micro said that the Pawn Storm hackers had increased their activity recently and had targeted bloggers who had interviewed President Barack Obama. It also said the group had "probably" stolen online credentials of a military correspondent at an unnamed major U.S. newspaper.

Though the security flaws APT28 used are new, it had been well established that the group was highly skilled. Saturday's report is one in a flurry generated by rival firms ahead of the RSA Conference this week in San Francisco, the largest annual technology security gathering in the country.

Original url:
https://www.themoscowtimes.com/2015/04/19/russian-cyber-attackers-used-2-unknown-flaws-us-security-firm-a45886