The Cybercrime Economy

Russian hackers exploit Windows to spy on West

By Jose Pagliery @Jose_Pagliery October 14, 2014: 1:36 PM ET

This CNNMoney feature is optimized for Adobe Flash Player version 9 or higher.

Install flash player

28 years of Windows in :75

NEW YORK (CNNMoney)

Russian hackers have taken advantage of a bug in Microsoft Windows to spy on the Ukrainian government and a scholar living in the United States.

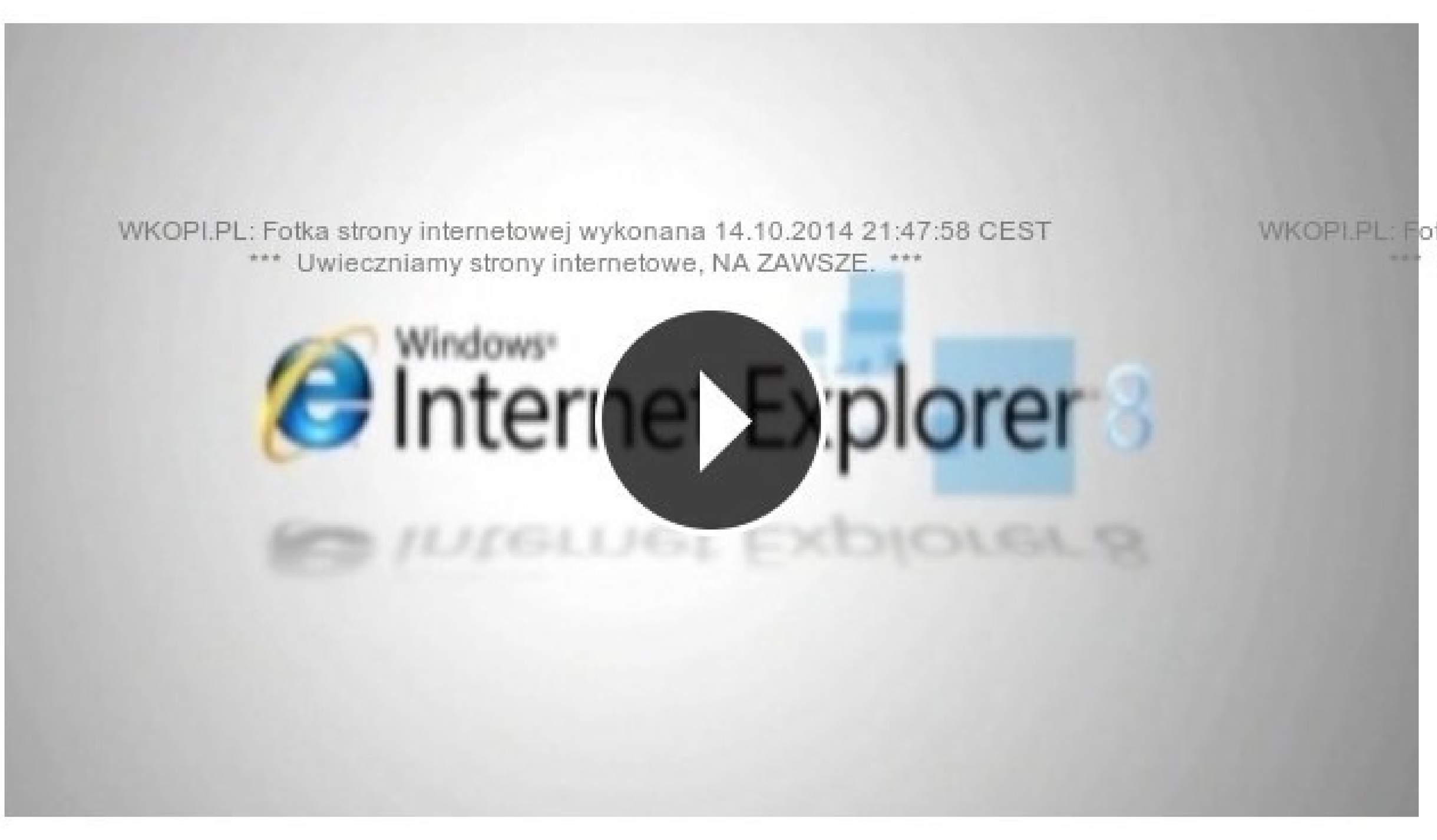
That's according to **iSight Partners**, a cybersecurity intelligence firm that contracts with governments. In **a report** Tuesday, the firm said it discovered the never-before-seen attack, which has been used by hackers in recent months.

The bug the hackers used exists in all modern versions of the Windows operating system: Vista, 7, 8 and 8.1. It's also present in 2008 and 2012 versions of Windows used by company servers. That means the vast majority of the world's computers -- nearly 68%, according to **NetMarketShare** -- are vulnerable to this unique type of attack.

Microsoft (**MSFT**, **Tech30**), which first learned of the bug from iSight Partners, released **a patch** at 1 p.m. EST.

Related: Dropbox says it wasn't hacked!

The Russian government did not respond to requests for comment. The Ukrainian government said it could not provide an immediate statement.



Internet Explorer bug worst for Windows XP

ISight, a Dallas-based intelligence firm, first spotted hackers using this attack in mid-August, sending phishing emails to Ukrainian government officials. The emails included a malware-laced PowerPoint attachment that claimed to be a terrorist watch list of pro-Russian separatists.

The malware had been tailored to spy on computers by quietly stealing emails and documents.

Related: FBI director says iPhones shield pedophiles from cops

The complexity and uniqueness of the attack led iSight to believe Russian hackers with government ties were responsible. Zero-day attacks (identified that way because they are brand new) are costly to develop, making them "typically the domain of cyber espionage teams and nation-states," said Stephen Ward, an executive at iSight Partners.

"The types of targets they were after relate to military, foreign policy and critical elements of the Russian GDP," Ward said.

That included a university researcher in the American Midwest who specializes in Russian culture, Ward said.

Investigators at iSight Partners were able to partially trace the attack, because hackers had made a mistake: A computer server sending messages to victimized computers was left openly visible on the Internet. On it were documents written in Russian language -- including instructions on how to use the malware.

The investigators believe the hackers are also responsible for spying attacks on a European government agency, a French telecom company and a Polish energy firm.

ISight dubbed the hacking group the "SandWorm Team," because the code it used was littered with references to the science fiction classic **Dune**. Sandworms are massive monsters that play a primary role in the novel.

This is only the latest cyberattack blamed on hackers in Russia. In the last year alone, Russia has been accused of **attacking U.S. oil and gas companies**, as well as **placing a digital bomb in the Nasdaq** and **hacking JPMorgan** and **several other financial institutions**.

CNNMoney is investigating recent hacks. Have you had money stolen from your bank account? Has someone stolen your identity? ***Share your story***.

Related: Snapchat isn't private. Period.

Related: How safe are you? CNNMoney's cybersecurity Flipboard magazine ■

First Published: October 14, 2014: 1:15 PM ET

Join the Conversation

DISQUS

We were unable to load Disqus. If you are a moderator please see our troubleshooting guide.

Google Spy-Tronix
At least the Russians hacks are spying on large and high value **foreign** targets....whereas our

WKOPI.PL: Fotka strony internetowej wykonana 14.10.2014 21:47:58 CEST *** Uwieczniamy strony internetowe, NA ZAWSZE. ***