

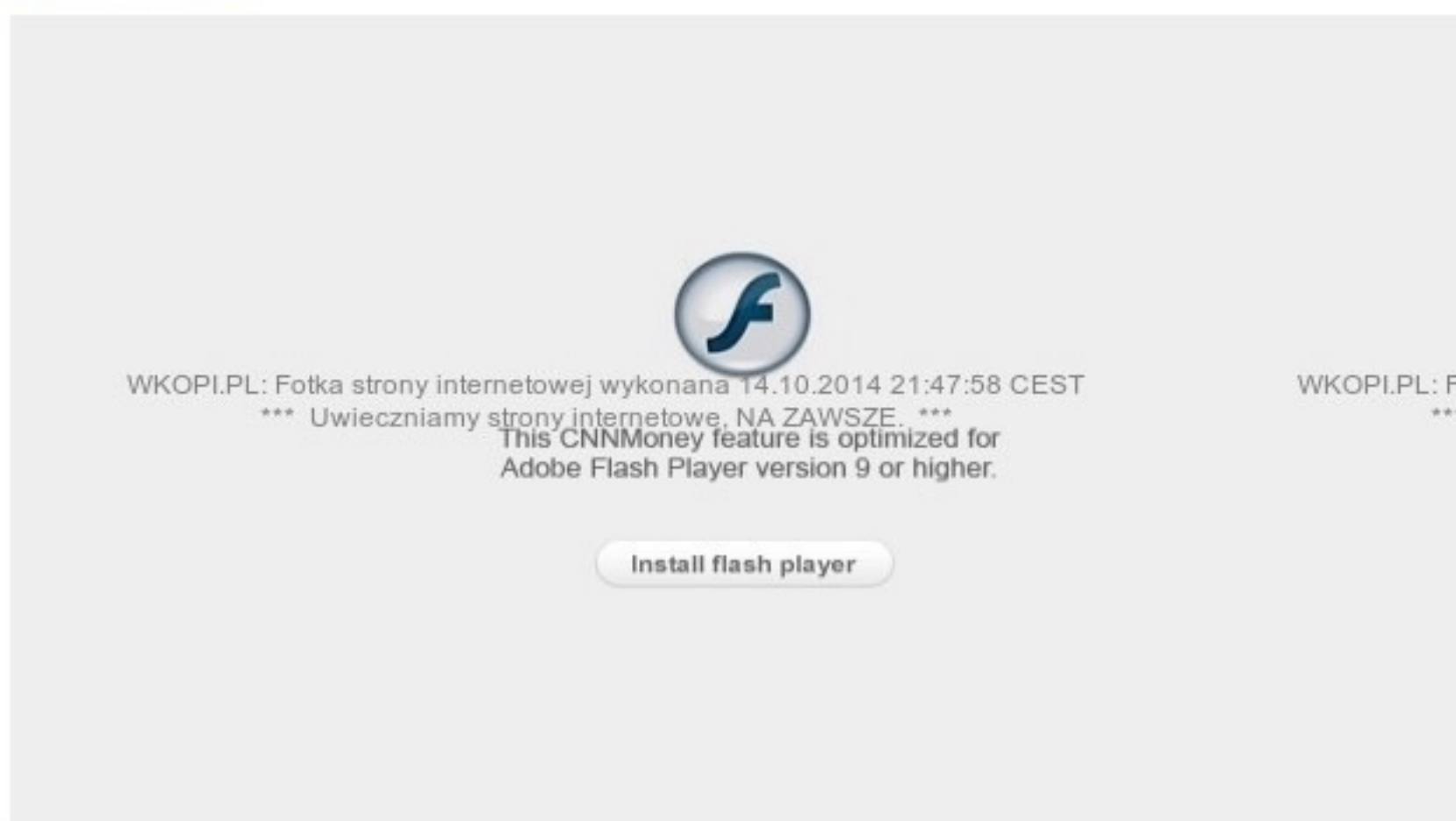
The Cybercrime Economy

# Russian hackers exploit Windows to spy on West

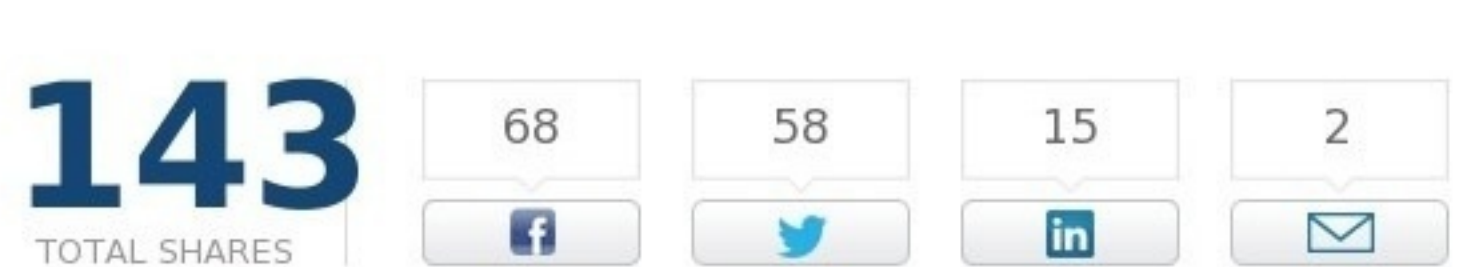
By Jose Pagliery @Jose\_Pagliery October 14, 2014: 1:36 PM ET

Recommend 90

Facebook Twitter LinkedIn Email



## 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

## You May Also Like

Sponsored Links by Taboola

 <b>BlackBerry Passport – Review</b> DrPrem.com	 <b>How anyone can make 70% profits on any amount in 60 Seconds</b> Business Observer	 <b>Are You Making These 7 Common Networking Mistakes?</b> GoWeLoveIt.info
---	--	---

## More from CNN Money

- People are now bending iPhones in Apple Stores**
- Taco Bell owner opens Asian fast food joint**
- RadioShack's CFO bails during cash crisis**
- German giants spend \$25 billion to buy U.S. rivals**
- GoPro angers investors with charity gift**
- The guy Newsweek called the 'inventor of Bitcoin plans to sue**

## Around the Web

- What Is "The Cloud" Anyway? Turns Out It's The Secret To Optimizing Performance.** FICO
- Windows tech tip of the week #1** Spiraling into control
- 10 Tricks to Instantly Look More Attractive in Photos** Learnist
- Why Do Fake Phone Numbers Start With 555?** Fake Number

## Join the Conversation



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

## Most Popular

-  Sorry ABC - you didn't win (yet)
-  Russian hackers exploit Windows to spy on West
-  Pricey Hermès bags 'reek like a skunk'

CNN Money | Portfolio

### How risky is your portfolio?



Find out with our **Portfolio Tracker.** [Try it now!](#)

## Technology Jobs




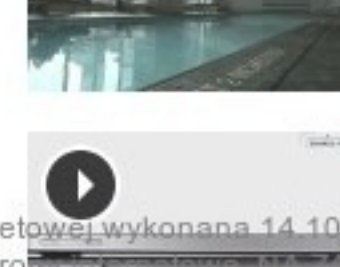

**Technolog HAYS Manufacturing** – Gdańsk

Search millions of jobs





Job title Location [Search](#)

See more Technology Jobs 

## Hot List

-  Neiman Marcus: 7 fantasy gifts for 2014
-  Most Innovative Cities in America
-  New earbuds take aim at Apple's Beats
-  NYC's first 5 star hotel in a decade
-  iPhone 6 vs. Galaxy Alpha: Cost to make WSZE. \*\*\*

## Most Popular Videos

-  Billionaire Saudi prince on ISIS and ...
-  Say Aloha to Larry Ellison's Hawaiian i...
-  Ukraine's booming wedding business
-  GE is dead in the water