



Checkpoint Washington

Reporting on diplomacy, intelligence and military affairs



On Twitter | E-Mail Checkpoint | More national security news | RSS Feed

ABOUT THIS BLOG

Checkpoint Washington is produced by the national security staff of The Washington Post.

E-mail us Follow us on Twitter: @checkpointwash

SUBSCRIBE

Select ...

SEARCH THIS BLOG

Go

RECENT POST STORIES

More from the Post's national security team

- Clinton lands in Kabul for talks with Karzai, other Afghan leaders
- U.S. appoints new special envoy to North Korea
- Pentagon lawyer warns of militarized approach to counterterrorism

WHO WE ARE

- Jason Ukman
- Rajiv Chandrasekaran
- Karen DeYoung
- Peter Finn
- Greg Jaffe
- Glenn Kessler
- Colum Lynch
- Greg Miller
- Ellen Nakashima
- Walter Pincus
- Mary Beth Sheridan
- Julie Tate
- William Wan
- Joby Warrick
- Craig Whitlock

Posted at 08:35 AM ET, 10/19/2011

New Stuxnet-like code is discovered

By Ellen Nakashima

Cybersecurity researchers have found a piece of malware on computer systems in Europe that bears startling similarities to Stuxnet, the mysterious virus that was used to sabotage Iran's nuclear program, and it appears to have been designed to secretly gather intelligence.

In a new paper, U.S.-based researchers at Symantec say that the code — dubbed Duqu — was written by whoever unleashed Stuxnet, or perhaps by someone who had access to the computer language underlying it. The new code was written to capture information that can help "mount a future attack on an industrial control facility."

"Duqu is essentially the precursor to a future Stuxnet-like attack," the paper said.

Although the codes share similar traits, they differ in significant ways. Stuxnet's payload was designed specifically to disrupt the machines that controlled the speed of centrifuges in a uranium enrichment plant in Iran. Duqu is designed to capture data such as computer keystrokes (including, say, passwords) and system information.

The discovery of the code by a lab in Europe is a reminder, said Kevin Haley, security response director for Symantec, that "the groups or organizations behind these attacks are not going to stop at one. They are going to do another."

Other researchers are expressing caution.

"This is all typical computer network espionage, which Stuxnet clearly was not," said Dmitri Alperovitch, an independent security researcher.

The new code — dubbed Duqu because it creates files with the prefix ~DQ — has been found so far in a handful of European manufacturers of industrial control systems. Security experts are continuing to analyze new variants.

Symantec's technical paper can be found here.

By Ellen Nakashima | 08:35 AM ET, 10/19/2011

Recommend 8 Share

Previous: Intel panel warns against cutting too deep

The Post Most: Nation

Most Popular

- Dangerous exotic animals turned loose, hunted down in Ohio
- Sirte fall; rumors swirl of Gaddafi capture, but all unconfirmed
- Desperation, abuse emerge as police investigate alleged scheme to collect disabi
- Judge hammers Lindsay Lohan, revokes probation, actress could face more jail tim
- Yueyue, Chinese toddler struck in hit-and-run, reported brain dead

Top Videos

Top Galleries

RECOMMENDS







Clinton pokes fun at...
 The Best Defense...
 Patients drove VA costs...
 Danger Room...
 Inter panel warns against...
 Dot Buzz...
 The Envoy...
 New Stuxnet-like code is...
 discovered Eye

Fact-checking the CNN/WRLC debate
 Live Q&A, 1 p.m. ET
 Glenn Kessler fact checks the Republican presidential candidates in the Oct. 18 CNN GOP debate.

11:00 AM Tracee Hamilton Q&A
 1:00 PM Got Plans? Discuss great ideas for local entertainment, dates and family fun.

[Weekly schedule, past shows](#)

Connect with the Post

Facebook: Become a fan of the Washington Post

Today's Paper

The Washington Post



[Full Paper](#) | [Metro](#) | [Style](#) | [Sports](#)

[Updated newspaper stories](#)

National Newsletters

Sign-up for e-mail newsletters and alerts and get the news you need delivered directly to your inbox.

Economy & Business News Alerts
 The Most


Behind the Government Showdown
 Today's Headlines & Columnists

National News Alerts

Enter your e-mail address [Subscribe](#)

[See all Washington Post Newsletters](#)

Featured Reads


[Federal Diary](#)

jckdumb symantec hyping. Stuxnet was a very complex multi payload program developed by intelligence agencies...the only similarities to Duqu being they target industrial control systems. That may be significant, but it shouldn't be equated with a true stuxnet like virus unleashed on an industrial facility...which may or not be so devastating as we don't know the true effects of Stuxnet on it's intended targets...iran's nuke facilities

10/19/2011 11:56:00 AM EDT

Recommended by 1 reader

Reply



spamsux1

Right jck. Stuxnet was an actual attack program. Worlds apart.

10/19/2011 12:09:44 PM EDT



laurelphoto

After the sword was invented, the TWO EDGED Sword became common.

10/19/2011 1:48:11 PM EDT

Recommended by 1 reader

Write reply here...



Bhawk1

Is there someone out there ready to blackmail governments and corps with this potential? Perhaps the US/Israel didn't do it to Iran. The ability to control all the bozoputers in the world is the stuff of movies but maybe its real.

10/19/2011 9:43:51 AM EDT

Reply



laurelphoto

Well, the US POWER GRID is very VULNERABLE.

10/19/2011 1:48:55 PM EDT

Write reply here...



spamsux1

Jeez. A bit of sensationalism, don't you think? Stuxnet and a keystroke logger are hardly in the same league.

10/19/2011 9:39:21 AM EDT

Recommended by 1 reader

Reply

Sponsored Links

OBJE - Stock Jump!
Money in Social Media View Ticker and Invest Today
www.ObsceneInteractive.com

EMBA Hot Penny Stock
EMBA may prove to be the hottest penny stock going this year. Read now
<http://www.TechStockWire.com/>

53 Year Old Mom Looks 25
The Shocking Results of Her \$4 Wrinkle Trick Has Botox Docs Worried
www.LifestylesAlert.com/MUST-SEE

[Buy a link here](#)

[RSS Feed](#) [Subscribe to The Post](#)

© 2011 The Washington Post Company

Columnist Joe Davidson delves into the issues and happenings in the federal workforce.



2Chambers

Join Felicia Sonmez and she explores the events taking place in the 112th Congress.



Classical Beat

Anne Midgette takes the measure of the classical music scene.

[See more featured items](#)

WP Social Reader

Hide this

Friends' Activity **Most Popular In National**

Your Friends' Most Recent Activity

Login

You need to be logged into Facebook to see your friends' recent activity.



An injured toddler is ignored, and Chinese ask why

298 people recommend this.



Witnesses: Libyan fighters overrun last positions of Gadhafi loyalists in Sirte, city falls

133 people recommend this.



Exotic animals escape Ohio preserve - The Washington Post

232 people recommend this.



Reports: Moammar Gaddafi killed

61 people recommend this.



Amnesty: Arms from the US, Europe used against protesters in Middle East, North Africa

499 people recommend this.



Rick Perry, Ron Paul have mixed record on energy subsidies

85 people recommend this.

Facebook social plugin

[Tell me more](#)

Featured Advertiser Links

Oil Spill, Mesothelioma Class Action, Fosamax Fracture, Asbestos & Veterans , Actos Bladder Cancer

Topamax Side Effects, Mesothelioma Treatment, Yaz Blood Clot, Asbestos cancer, Actos, Mesothelioma Symptoms

Join Pres. Obama. It's time to do it again.

Looking to buy a home? Visit TWP Real Estate section for the latest open houses.

Make Your Vanguard Investing More Profitable - Free Research Report Reveals Best & Worst Funds

Ways you can get us

- Mobile
- Apps
- Newsletter & alerts
- RSS
- Post Store
- Facebook
- Photo Store
- Twitter
- Washington Post Live

The Washington Post

- About Us
- Work for us
- Community Relations
- PostPoints
- Corrections/Suggestions
- Archive
- Contact the Ombudsman
- Report a problem

Web site

- Make us your homepage
- Digital Guidelines
- Ask The Post

Newspaper

- Subscribe
- Home delivery service
- e-Replica
- Reprints

Advertise

- In the newspaper
- On the web site
- Mobile
- Events

The Washington Post Company

- Post Company web sites

Partners