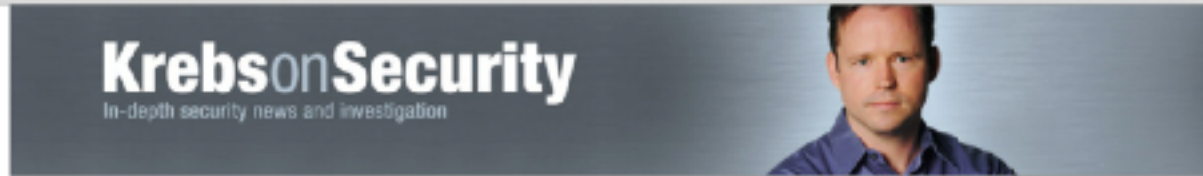
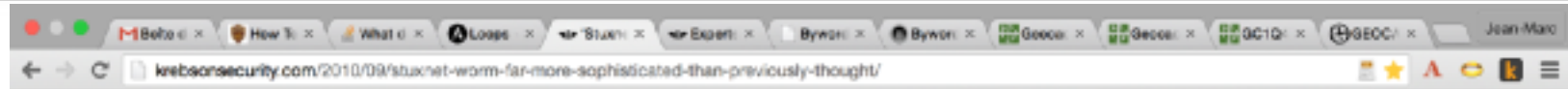


# 500 Kb of mystery...

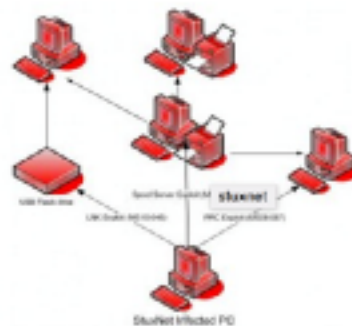


## 14 'Stuxnet' Worm Far More Sophisticated Than Previously Thought

SEP 10

The "Stuxnet" computer worm made international headlines in July, when security experts discovered that it was designed to exploit a previously unknown security hole in Microsoft Windows computers to steal industrial secrets and potentially disrupt operations of critical information networks. But new information about the worm shows that it leverages at least three other previously unknown security holes in Windows PCs, including a vulnerability that Redmond fixed in a software patch released today.

As first reported on July 15 by KrebsOnSecurity.com, Stuxnet uses a vulnerability in the way Windows handles shortcut files to spread to new systems. Experts say the worm was designed from the bottom up to attack so-called Supervisory Control and Data Acquisition (SCADA) systems, or those used to manage complex industrial networks, such as systems at power plants and chemical manufacturing facilities.



BLOG ADVERTISING ABOUT THE AUTHOR

Advertisement

**ENFORCE YOUR NO CELL PHONE POLICY**

**POCKET HOUND**

- Covert
- 75' Range
- Only \$499

Use Coupon Code **KREBSHIP** for FREE shipping

[www.pockethound.com](http://www.pockethound.com)

My New Book!



The source was reliable. The source is  
[krebsonsecurity.com/wp-content/uploads/2010/09/stuxnet.jpg](http://krebsonsecurity.com/wp-content/uploads/2010/09/stuxnet.jpg)

Image courtesy Kaspersky Lab