STUXNET

krebsonsecurity.com/2010/09/stuxnet-worm-far-more-sophisticated-than-previously-thought/

KrebsonSecurity
In-depth security news and investigation

BLOG ADVERTISING | ABOUT THE AUTHOR

14 'Stuxnet' Worm Far More Sophisticated Than Previously Thought

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.

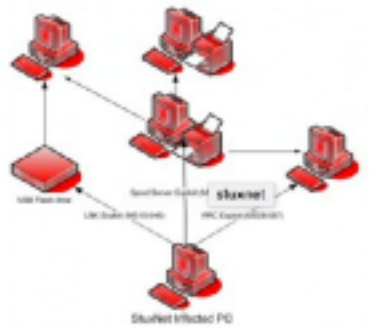

Image courtesy Kaspersky Lab

krebsonsecurity.com/wp-content/uploads/2010/09/stuxnet.jpg

Advertisement
ENFORCE YOUR NO CELL PHONE POLICY
Covert
75' Range
Only $499
Use Coupon Code KREBSSHIP for FREE shipping
www.pockethound.com

My New Book!

STUXNET – The target

- Disrupt the production of enriched uranium in Iran,
- Preventing them to achieve "atom power" status
- Demonstrated and observed:
  - production didn't reach expected goals and has even to be stopped for several weeks.