# USB Webkey Threat

Aaron Hiltgen, Associate of (ISC)$^2$

a_hiltgen@cox.net

# Traditional USB Device Protection

- Disable Autorun and/or Autoplay!
  - Most previous threats involving USB devices relied on this feature.

- Sadly, this is not true any more.

# USB Webkey

- This particular webkey is distributed by a local hospital to expecting mothers.
- Webkeys are also used in advertising campaigns by pharmaceutical companies, major credit card companies, major cities, etc.

- Demonstration

# The Device

- This is not a typical USB storage device
- When inserted into a computer, the device acts like a USB keyboard
  - Sends keystrokes invoking the run command then directs the user to a website owned by the makers of the key which redirects to the hospital website

# The Threat

- The device uses a rewritable EEPROM to store the necessary commands
- There have already been articles posted online discussing ways that the device has successfully been compromised
- Similar devices have also been created and inserted inside of other USB devices.
  - A USB mouse was rewired with a USB hub inside so that it would function as a mouse but could also include a USB webkey to exploit the targeted computer.

# The Threat (cont.)

- These devices are not recognized by Windows as a USB device but as a peripheral.
  - There are ways to protect against this threat in Windows, one of which involves changing several registry key values
  - I have included an article in the references section which discusses this method of securing Windows XP and 7

# Title (44-pt)

- Our limited testing included Linux and Mac machines as well
  - Both fared somewhat better since the commands that this particular device sent were oriented towards a Windows machine
  - The webkey was identified as a keyboard by the Mac
  - The webkey did send keystrokes to the boxes, which were ignored, but the device also interfered with keyboard function since it sent repeated keystrokes to the box.

# References

- Companies that make USB Webkeys
  - www.kyp.com
  - webkey.com
- Protecting Windows Machines
  - http://www.irongeek.com/i.php?page=security/locking-down-windows-vista-and-windows-7-against-malicious-usb-devices
- Attack system that includes Webkey programming option
  - http://www.offensive-security.com/metasploit-unleashed/SET_Menu_Based_Driving

# References

- Article on creating your own Webkeys
  - https://www.infosecisland.com/blogview/10658-USB-Attack-Vectors-move-Beyond-Flash-Drives.html
- Articles on hiding Webkeys inside other devices
  - http://news.cnet.com/8301-27080_3-20028919-245.html?tag=TOCmoreStories.0
  - http://www.theregister.co.uk/2011/06/27/mission_impossible_mouse_attack/

# References

- Cached article on hacking a Webkey
- (Cannot guarantee availability, so a copy is provided with these slides)
  - http://webcache.googleusercontent.com/search?q=cache:tQOruQVA-xQJ:blog.skot9000.com/post/810488123/american-express-webkey-hack+webkey+hack&cd=6&hl=en&ct=clnk&gl=us&source=www.google.com