



FRIDAY, AUGUST 12, 2011

8M Web pages hacked, mined

Go to infected site, risk stolen identity

By Byron Acohido
USA TODAY

Some 8 million Web pages, published mostly by smaller merchants and professional firms, have been hijacked this summer and set up to usurp control of the PCs of unsuspecting site visitors.

That's the latest development in a new style of hacking sweeping across the Internet, according to research by website security firm Armorize.

"The misuse of numerous small sites is making the Internet a much more dangerous place," says Alena Varkockova, lab analyst at anti-virus firm Avast. "Even the unimportant sites can do big harm when misused."

A single criminal gang using computer servers located in Ukraine is responsible for the latest twist in converting legitimate websites into delivery mechanisms for "drive-by downloads," according to Wayne Huang, chief technical officer at Armorize.

In a drive-by download, malicious software gets inserted into the Web browser of any unsuspecting Internet user who simply has navigated to a hacked Web page.

With control of the visitor's browser, the attacker can easily install malicious software that silently harvests all account log-ons, identity data and payment card data. The PC is usually also slotted into a botnet, a network of infected "robot" PCs controlled by the bad guys, who then use it on an ongoing basis to spread spam, carry out hacktivist attacks and do other criminal activities.

Google and Microsoft say they continually scan for Web pages conducting malicious activities and issue warning pages in search results and via Google's Chrome and Microsoft's Internet Explorer browsers. They also provide free guidance and tools for website owners to diagnose and clean up problems.

But many of the infected Web pages won't get cleaned up anytime soon, as these wrongdoers use "myriad techniques to ensure their malicious software goes undetected," says Jon Clay, product manager at anti-virus firm Trend Micro. Use of polymorphic infections that constantly change has become commonplace, says Clay.

Internet users can reduce their risk by keeping Web browser and anti-virus updates current and avoiding use of Internet Explorer, since Microsoft's dominant browser is also the most intensively probed for security holes, says Adam Wosotowsky, senior analyst at anti-virus firm McAfee.

"I suggest using Firefox or Chrome," he says.