May 7, 2009

UCSB researchers hijack Torpig botnet

Suggested articles & links

Good guys hijack evil botnet

NPR's *Future Tense*

May 6, 2009

Interview with Giovanni Vigna, Associate Professor of Computer Science and co-director of the Security Lab at UC Santa Barbara.

Computer science researchers at the University of California Santa Barbara earlier this year managed to infiltrate the Torpig botnet, a vast zombie network of infected Windows computers designed to steal identities and money from its victims. Torpig infects machines with malware, then monitors keystrokes to steal user names and passwords for logging into online banks and other sites.

Listen to the interview.

Botnet hijack: Inside the Torpig malware operation

ZD Net

May 4th, 2009

Security researchers at University of California, Santa Barbara have broken into the nerve center of the Torpig botnet (also called Sinowal or Mebroot) to find a 10-day stash of 10,000 bank accounts and credit card numbers worth hundreds of thousands of dollars.

During the botnet hijack, the researchers exploited a weakness in the way the bots tried to locate their C&C servers and found an underground online crime operation collecting about 70GB of stolen data over just ten

days... more

Researchers hijack botnet, score 56,000 passwords in an hour

ars technica

May 4th, 2009

The Torpig botnet was hijacked by the good guys for ten days earlier this year before its controllers issued an update and took the botnet back. During that time, however, researchers were able to gain a glimpse into the kind of information the botnet gathers as well as the behavior of Internet users who are prone to malware infections.

Researchers at the University of California Santa Barbara have published a paper (PDF) detailing their findings after hijacking a botnet for ten days earlier this year. Among other things, the researchers were able to collect 70GB of data that the bots stole from users, including 56,000 passwords gathered within a single hour. The information not only gave them a look at the inner workings of the botnet, they also got to see how secure users *really* are when it comes to online activities. (Hint: they aren't.)... more

Related Links

UCSB Computer Security Group website

Torpig Botnet Hijacked and Dissected - Slashdot

Hijacked botnet exposes startling online habits

Researchers Take Over Dangerous Botnet