

Virus tracking software 'draw lines' for hackers

Programs that monitor and record unusual phenomena on the Internet because security companies set up secrets are being discovered by hackers and take advantage of their attacks.



Programs that monitor and record unusual phenomena on the Internet because security companies set up secrets are being discovered by hackers and take advantage of their attacks.

Like surveillance cameras, programs called sensors are often hidden to avoid detection and response by hackers. Based on this program, Internet management centers can make announcements about changes in network activity, to assist analysts to track and find solutions.

However, in the "Combining Internet tracking software with reaction probe" at the Usenix Security Symposium on July 4 in the US, the University of Wisconsin research team recommended that Hackers can still locate sensors to perform nefarious behaviors without fear of being detected. John Bethencourt, one of the study's authors, said it was the announcements of network management centers that suggested the attacker wrote the algorithm to determine the program. All the hackers have to do is to populate the IP address with information packets and then check to see if this action appears in the notification. If not, "can safely conclude that the address is not under control," Bethencourt said.

After opening a fake attack on random IP addresses on the SANS network (USA), Bethencourt group did not need a week to discover and identify reconnaissance programs in this network and many other similar networks.

Some Japanese researchers also made similar conclusions in the "Internet Vulnerability Control Program" report. They claim to be able to create some reconnaissance software algorithms in a relatively short period of time.

"We believe that a new Internet threat has been discovered," the team said. "This is not a threat to the server system, but a higher level threat - the system is built to protect server security."

However, both groups affirmed that the level of danger would be eliminated if SANS and other management centers did not report details of the network activity diagram. Moreover, the expansion of IPv6, the new Internet generation, can also prevent attacks with longer IP addresses.

You finished reading the article "**Virus tracking software 'draw lines' for hackers**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.