Future viruses can overcome all sensors?

Researchers at the University of Wisconsin have come up with a study that suggests that some future viruses may be able to overcome the network security warnings SANS Internet Storm Center and Symantec have been proud of for a long time.

Researchers at the University of Wisconsin have come up with a study that suggests that some future viruses may be able to overcome the network security warnings SANS Internet Storm Center and Symantec have been proud of for a long time.

Computer science experts at the University of Wisconsin-Madison Usenix security conference say that future attackers will launch an extensive exploration attack on the Internet, after which they will use forms. Publicly popular data to detect virtual security sensors, and a special virus encoded as IP addresses can bypass network-based virus alerts to attack.Therefore, the long-standing 'aggressive' warning tools of SANS Internet Security Center and Symantec can become useless.

Three scientists Jason Franklin, John Bethencourt and Mary Vernon have launched a test strategy as follows: sending exploration packets to IP addresses on the Internet, then check the public announcements due to Survey networks offer activities to receive this data to identify probes, weaknesses, or missing of polling sets.

All activities of detecting these security sensors will be done by ghost computer networks.With a computer network of about 2000 computers, all network security sensors can be found in less than 3 days.With a computer network, about 200 broadband-connected computers will find sensors for about 5 days.

This is entirely possible with the evil hacker organizations, which are currently holding thousands of remote controlled computers by viruses, trojans or spyware that computer owners not knowing.

These researchers are currently focusing their research on SANS 'secure network because it considers that this network is one of the largest and most difficult to explore security networks.

Simulated exploration into the SANS network gives results that show that the sensors on this network can show up in less than a week, and if there are enough computers and enough bandwidth like ghost computer networks can be effective within less than 70 hours.Vernon commented: 'Obviously, they don't know that a secure network can be' drawn 'in such a fast time.Our 'network drawing' algorithm proved very effective. '

But even SANS and Symantec are not worried about this security report, which could make them 'unemployed' in the future.Johannes Ullrich, SANS Internet Storm Center's director of research, said: 'I hope that some people are trying to write a virus capable of eliminating all our security sensors. .But this also means that if you are equipped with security sensors on your network, the risk of attack will be very low. '

Alfred Huger, managing director of sensors, head of Symantec's security team admits: 'It is true that it may be possible, but the problem is who will do it?Even if they succeed and some modern virus can take advantage of this technology, it can still be detected and destroyed like other dangerous viruses. '

Both Ullrich and Huger have found that it is not easy to detect sensors and even take advantage of them for attacks because an attacker must list all sensors and all set of related IPs and also have to go through the separate firewall systems of each company, and many other complicated stages . but the chance of success has not been guaranteed.

Huger and Ullrich are still very confident when it is difficult to find viruses with intense attack like the Slammer or MSBlast children because of the current security technology. It was also quite effective, and virus makers had to calculate some effect before releasing a heavily invested virus.

HOANG KIM ANH (According to TechWeb News)