Innovate or lose in the fight against malware

The rate of malware infection in growing organizations suggests that anti-virus software has become obsolete, needs technological innovation and has different ways for this tough war.

The rate of malware infection in growing organizations suggests that anti-virus software has become obsolete, needs technological innovation and has different ways for this tough war.

In a report released just last week, security firm Check Point Software Technologies has been alerting an increase in malware and bot infections (illegal hackers to control the computer of the victim). remote kernel) in corporate and organizational networks.

Check Point's report is the result of recent network traffic analysis of thousands of organizations. The report pointed out that companies and organizations are currently having problems with malware and bots, and it's time they need to quickly have new methods to detect malware.

Results showed that up to 84% of organizations were infected with malware and about three-quarters of the surveyed organizations had at least one bot on their network.

Statistics such as infection rates will not say anything if only numbers. Because not all malware is the same, and some malware is more dangerous than others.

However, the concern in Check Point's Security Report, called '2014 Security Report', is about the trend. Data show that, in 2013, 58% of organizations with malware download staff every 2 hours or less, tripled in 2012 (only 14%).

The study also found that 73% organized 'bot' bots, compared with 63% a year earlier. In addition, 77% of bots have been active for more than 4 weeks.

These figures show that traditional signature-based security, such as anti-virus software, has been "dead," as stated by Brian Dye, Symantec's vice president of information security. interview with the Wall Street Journal last week.

'We no longer see viruses as a way to make money anymore,' Dye said.

That's a remarkable statement from a antivirus software company that has been around for over two decades.

Unfortunately, too many companies are still dependent on antivirus technology, leading to alarming figures led by research like Check Point. These businesses have to redirect the strategy to seek possible capabilities in hardware, software and network traffic that indicate an unusual sign of malware.

'Our recommendation is to spend more money on authentic identification, as opposed to relying on outdated findings and ineffective in recent years , ' said Tyler Shields, an analyst with the research firm. Save Forrester Research market.

More effective ways such as filtering in / out rights, such as monitoring and restricting reasonable flow of information transferred from one network to another.

It is also possible to use penetration detection systems and isolation technology to isolate potential malware.

Stricter policies such as restricting the download of files from unknown sites are also effective, said Kellman Meghu, Check Point's security manager. Using a strict policy that every executable file must be accepted in the long run will minimize malware infection.

'It seems like a burden, but it is nothing compared to having to clean up thousands of infected computers , ' Meghu said.

At the end of last year, when it was discovered that the Target retailer's payment system was compromised, technology alone was not enough to prevent record theft and credit card data from tens of millions of customers.

A network monitoring tool from supplier FireEye warned Target's network security personnel about malware on the network before the data was stolen. However, the warning was ignored, so the $ 1.6 million tool that Target invested did not work.

"Technology is for support, but you still need to be smart and conscious to capture what technology is trying to tell you , " said Chris Camejo, director of inspection services at NTT Com security company. Security Com, said.