China 'using worms to steal trade secrets'

By *srlinuxx*
Created *25/07/2005 - 2:37am*
Submitted by srlinuxx on Monday 25th of July 2005 02:37:59 AM Filed under Security [1]

Cyberspace is becoming a new battleground for the US and China, amid growing concerns about Chinese industrial espionage through various types of computer worms, security professionals claim.

At least one trojan program used to steal files from infected computers has been traced to servers in China, providing further evidence that US companies may be targets, they say.

Security firms have long been concerned about various types of malicious software used to steal files or passwords. But some newer programs seem designed as a more sophisticated and targeted effort.

Joe Stewart, a researcher with the US security firm Lurhq, said that by reverse-engineering a recent PC worm known as Myfip, he found a clear connection to China.

"All the emails we've traced back with this particular attachment came from a single address in China," Stewart said, adding that it was "highly likely" that the program was used for espionage against US high-tech and manufacturing firms.

Stewart said the program appeared to have been originally developed as a way to steal student exam papers and then expanded so that it could now copy many types of documents, including computer-assisted drawings and Microsoft Word files.

Forbes magazine, which first reported the Chinese origin of Myfip, said the worm had been propagating by spam that activated the program when recipients clicked on attachments. Forbes said about a dozen versions of Myfip may have been in circulation and used to steal sensitive documents including mechanical designs and circuit board layouts.

Analysts point out that tracking attacks or malicious software can be tricky because the origins can be disguised.

But Marcus Sachs of SRI International, who also directs the industry-academic SANS internet Storm Centre that monitors cyberattacks, said the evidence against China is solid.

"I believe firmly that the Chinese are using tools like Myfip to conduct industrial espionage on the US and other industrial countries that have mature data networks," he said.

Sachs said the latest types of malicious software, or "malware," represent a new strategy by creators of the programs.

"Most of the credit card theft, money laundering and fraud is coming from Russia or former Soviet Union countries,"

Sachs said.

"The Chinese seem to be a bit more clever in covering their tracks and are more likely conducting covert raids for corporate secrets, rather than chasing money like their Russian organised crime counterparts."

But the techniques may not be limited to industrial espionage. Some analysts say similar malware may be targeting government agencies in a bid to steal other types of secrets.

The online newsletter SecurityFocus claims the wave of cyberattacks that hit Britain last month may have been part of an effort to obtain government documents from British and US agencies.

Britain's National Infrastructure Security Coordination Centre said last month that a series of trojan-laden email attacks were "targeting UK government and companies," in an apparent "covert gathering and transmitting of commercially or economically valuable information."

The June 16 warning did not specifically mention China but said most of the evidence pointed to computers in "the Far East."

AFP

Security
