FINANCIAL TIMES

February 10, 2015 6:53 pm

Chinese hackers attack blue-chip groups via Forbes website

Sam Jones in London and Hannah Kuchler in San Francisco Author alerts

Chinese hackers hijacked the Forbes website and used it to target thousands of computers linked to blue-chip companies, including US defence contractors and banks, in one of the most brazen cyber espionage campaigns apparently launched by Beijing-linked groups so far.

During a four-day period from November 28 to December 1 last year, any visitor to the Forbes website would have been infected by the Chinese attack, according to the cyber security company iSIGHT Partners, which detected the intrusion on some of its clients' networks, among them a top-tier US arms manufacturer. It blamed a Chinese hacking group known as Codoso.

A spokesperson for Forbes said the vulnerability had now been closed.

The company launched an investigation immediately after discovering files on its system had been tampered with and had subsequently found there was "no indication of additional or ongoing compromise", they added

Visitors to Forbes during the period it was compromised who have not subsequently cleaned or scanned their systems are still likely to be infected, however, and might be being spied on by the Chinese group.

The attack is the latest evidence of a cyber espionage war against western businesses from groups within China that has expanded dramatically in recent months and left many governments struggling to stem the threat.

Chinese authorities have consistently denied they sponsor such attacks, but western security agencies insist Beijing is involved.

As well as online espionage attempts from state-backed groups, security officials are also having to grapple with a deluge of blunter, damaging attacks that have grown in scale against the backdrop of an increase in geopolitical tensions in the past 12 months.

Earlier on Tuesday, hackers sympathetic to the Islamic State of Iraq and the Levant, the brutal jihadi insurgency also known as Isis that has taken over much of eastern Syria and western Iraq, took over Newsweek's twitter account, broadcasting threats to the family of US President Barack Obama.

iSIGHT said the hackers used two so-called "zero day" exploits — previously unknown loopholes in widely used software — to crack security systems such as firewalls and antivirus software and indiscriminately infect readers of the business news site.

"It's one of the most brazen [attacks] we have seen in terms of what it targeted," said Patrick McBride, vice-president at iSIGHT. "It's probably one of the most popular websites we have ever seen leveraged for an attack like this. Using [Forbes] gave them a tremendous amount of options after they had got their initial foothold [in visitors' systems]."

Visitors to Forbes who worked for defence companies and banks were those who were subsequently targeted most, Mr McBride said.

"An attacker would choose to use a major publisher because it is a legitimate website that earns the trust of users who visit on a regular basis with confidence," said Oren Falkowitz, a former NSA employee who runs Area 1 Security, another cyber security firm. "What they want is a platform with a large audience so they can get the users that they want in that pool and then be very discriminating about who they want to go to the next stage with."

In depth
Cyber warfare

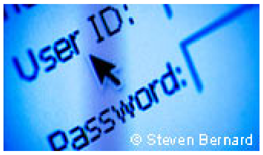
The attack was launched through Forbes' "thought for the day" pop-up screen that welcomes visitors to the site and is run using Adobe software.

Codoso, the Chinese hacking group, was able to exploit the pop-up because of a loophole they had discovered in Adobe's software. A second loophole then enabled them to bypass security on Microsoft operating systems that would ordinarily have blocked the attack.

iSIGHT said they were confident the attack was state-backed. Codoso is one of the more prominent and well-resourced hacking groups in China and has been followed by western security analysts and cyber security agencies for years. In 2010 the group performed a similar attack on the Nobel Prize website after the honour was awarded to a leading Chinese dissident Liu Xiaobo.

Software exploits identical to those used to target Forbes have also been used to infiltrate websites associated with the Hong Kong protests and the restive Uighur minority population in western China in recent weeks, iSIGHT said.

Adobe found and closed the loophole on December 9. Microsoft released a patch to fix the loophole in its software on Tuesday.



As online threats race up national security agendas and governments look at ways of protecting their national infrastructures a cyber arms race is causing concern to the developed world

Further reading

After using a vulnerability in a website — often called a watering hole because it lures the victims — cyber criminals will select which companies that visit the site they want to target and use other vulnerabilities to access their networks, said Chris Eng, vice-president of research at cyber security company Veracode.

"Once they have control, they will target certain people, see who they are connected to, what information is on their system, what might they siphon off as interesting data," he said. The Chinese have long been interested in hacking to steal intellectual property from western companies and defence contractors, and banks have often been prime targets, he said.

RELATED TOPICS United States of America, China, China - Politics & Policy, Cyber Security, China Society

Printed from: http://www.ft.com/cms/s/0/d61b711c-b148-11e4-831b-00144feab7de.html