



Sunday Sport Hit man

Mateja Kezman's
Asian soccer adventure



Post Magazine

Reversal of fortune
Regina Ip's return to the
frontline of political life

Newsmaker

Trump card

Will the property mogul
really run in 2012?



Sunday Morning Post

A SOUTH CHINA MORNING POST PUBLICATION | VOLUME LXVII | NO. 98

April 10, 2011

see live updates at www.scmp.com

HK \$8.00

Local companies vulnerable to growing threat of attacks that paralyse online operations Cyber-extortionists target HK businesses

Nathan Griffiths

Online attacks aimed at crippling websites unless cash is paid are on the rise and authorities can do little to stop them, leaving businesses to fend for themselves.

Internet watchers say the attacks are becoming more complex, making the job of tracking down the culprits – who are usually based overseas – even more difficult.

One recent victim was the popular expat website GeoExpat.

Distributed denial-of-service

(DDoS) attacks work by flooding websites or servers with more data than they can handle.

They are launched from networks of infected computers – known as “botnets” – that can be sited and controlled from anywhere in the world.

When he saw the first e-mail on a Friday morning in January, titled “Partnership,” GeoExpat chief operating officer Shriram Chaubal ignored it, assuming it was a hoax.

The message was stark: “Hello. Your site will undergo DDos attack. Pay US\$300 for libertyreserve or

WesternUnion. You should contact us by e-mail for reception of the account for payment...”

It was dated from the night before and had Russian and Myanmar e-mail addresses as contact points.

The next evening Chaubal started receiving alerts warning him that his websites were not accessible. Then, just before 10pm, he received a second email upping the demand.

“Hello, your site has undergone Ddos to attack.” It demanded US\$350 to stop the attack.

As the operator of a popular

online forum and an online retail site, Chaubal could not afford to be offline for weeks at a time. More damaging was the possibility of losing clients and his online reputation.

S.C. Leung, a senior consultant at the Hong Kong Computer Emergency Response Team (HKCERT), a local chapter of computer security specialists focused on security awareness and co-ordination, said his organisation had received no more than a handful of reports on DDoS attacks such as those Chaubal experienced.

“That doesn’t mean there aren’t a lot of attacks. It’s just that such cases usually get reported to local internet service providers (ISPs) if they get reported at all,” he said.

Sean Lord, vice-president of sales at Nexusguard, a local anti-DDoS security firm, called DDoS extortion tactics “old-fashioned” when compared with more lucrative efforts by organised crime to harvest credit card and other banking information. He agreed DDoS attacks on local businesses were going unreported.

The only thing unique about

It doesn't mean there aren't a lot of attacks. ... just that cases usually get reported to local ISPs, if they get reported at all

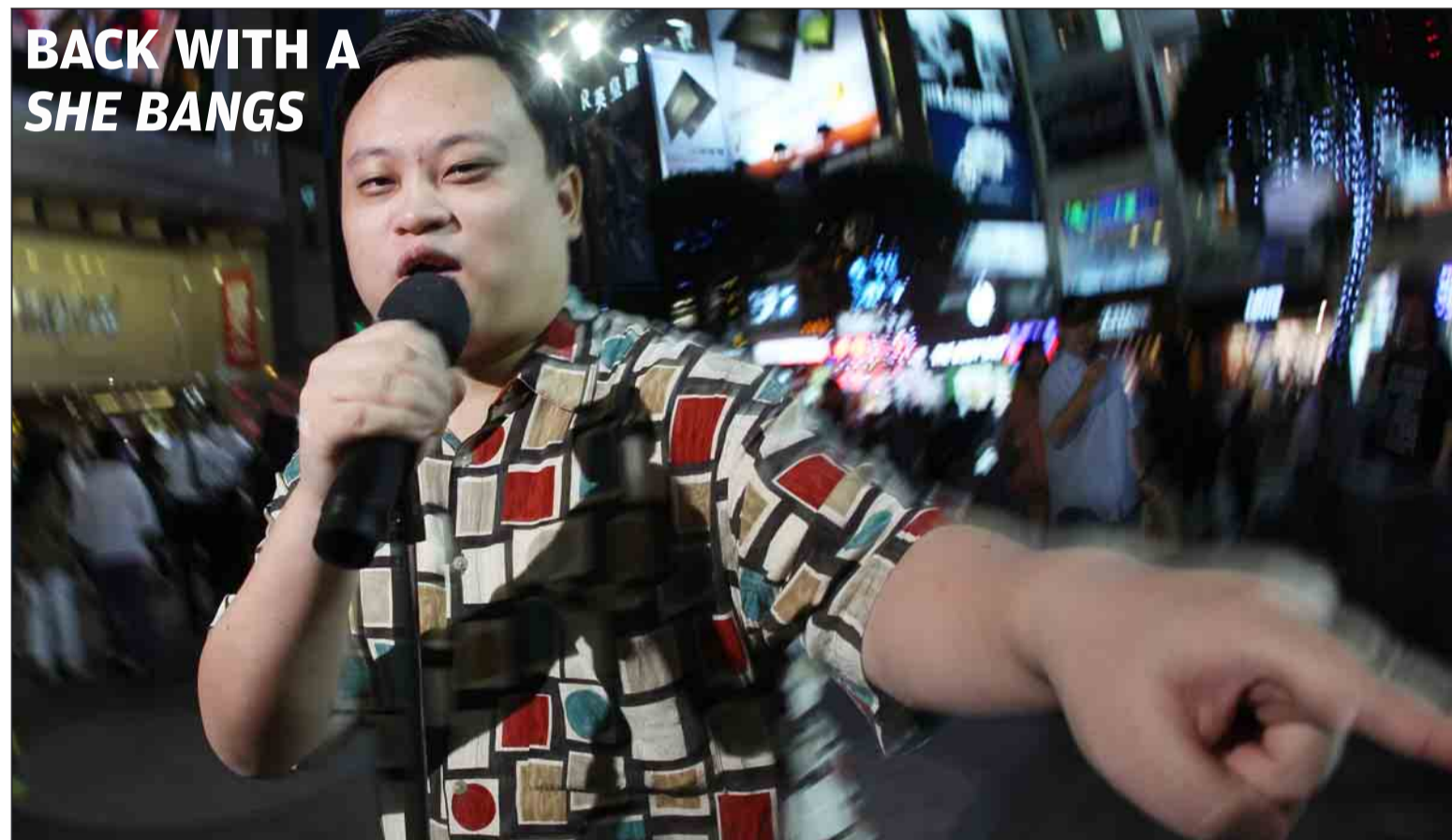
S.C. Leung, Hong Kong Computer Emergency Response Team

Chaubal's story was the fact that it made it to the press, he said.

Leung said HKCERT recommended any business experiencing attacks contact their ISP for help. He stressed that in cases such as Chaubal's, where extortion or other criminal activity was involved, the police should be contacted.

Chaubal, who contacted both HKCERT and his ISP when his sites came under attack, said neither were able to assist him. In an e-mail, HKCERT said they were unable to

CONTINUED ON PAGE 4



BACK WITH A SHE BANGS

Six years after he struck gold with an off-key performance of a Ricky Martin song on US television, William Hung last night played a three-song set for an upmarket crowd at Central's Dragon-i.

Full report
Page 5

Ai Weiwei under attack in propaganda offensive

Staff Reporter

Detained artist Ai Weiwei (艾未未) was accused of plagiarism in state media last night and described as a “third-grade” artist who only protested to seek media attention.

It was the first direct offensive against Ai in an article released by Xinhua, although *Global Times*, an English newspaper under *People's Daily*, ran two pieces against him last week, in a move widely seen as an attempt to build a legal case against the outspoken artist.

Ai has not been seen since last Sunday, when police stopped him from boarding a flight from Beijing to Hong Kong.

The Xinhua article referred to various accusations against Ai that had surfaced on the internet within hours of an investigation into his activities being announced. One said Ai stole an art professor's idea by using 1,001

ordinary Chinese as part of a “living exhibit” in a show in Germany in 2007.

Other online postings accused Ai of dodging income taxes and monopolising funds and resources in the art world, among other things.

“None of the claims, however, have been independently investigated,” Xinhua said.

It also quoted anonymous “participants in Chinese artistic circles” as

Ai's criticism of the government magnified due to his increasing exposure to the media

Part of the English-language Xinhua article attacking Ai Weiwei

“evaluating Ai's achievements as third rate” and describing him as an “amateur artist”.

And it quoted people who challenged Ai's sincerity in his protests, saying he only took part as an onlooker and put others in danger.

“Ai's criticism of the government became increasingly open and magnified in the past two years due to his increasing exposure to the media,” the Xinhua piece said.

It did not mention the start of Ai's activism – when he began an independent count of the death toll of the Sichuan (四川) earthquake in 2008.

The article, which was only released in English, did not give details of the possible charges resulting from the police investigation.

On Wednesday the agency said Ai was being investigated for economic crimes, but it gave no details.

Reports of actor's death greatly multiplied

Amy Nip

As runs of misfortune go, it really is hard to beat. While veteran TVB actor Law Lok-lam is very much in the land of the living, he now holds what could be a television record for dying. Soap opera fans saw him die five times, as five different characters in five shows, in a 24-hour period last week.

Such was the level of superstition at such a feat, production crews sought blessings from the gods before shooting the episodes and Law, 63, was given lai see packets.

“When I get a job, I don't care if my character in the drama will die. If he is supposed to die, he should go on and

die,” the actor said in a video uploaded by TVB to YouTube amid heated discussion on the internet.

Law's roles were diverse and all had tragic endings. Two were bloody in martial arts drama *Grace Under Fire*, Law's character, Mok Ping, died in a fierce fight. In *Fate to Fate*, he vomited blood before dying. In *Relic of an Emissary*, he played the first Ming dynasty emperor, Zhu Yuanzhang, who died after an illness.

In retro thriller *Police Station No 7* and comedy *Virtues of Harmony*, he played the partner of actress Nancy Sit Ka-yin. Law didn't die on screen but his death was discussed. “I've been in this business for years. I've

tried lying in a coffin, even with a lid on. It doesn't bother me,” Law said.

Actors whose characters die get a red packet as a sign of good fortune: “We get red packets, but not much. There is a dollar or fifty cents in it,”



One of Law's five screen deaths

Law said. Although the father of three is not superstitious, numerous posts about his “death” on the internet saddened his daughter.

“Why would dying in a drama matter? It's not for real. So my daughter, you shouldn't be unhappy. The most important thing is I've done my job well,” Law said.

Internet surfers wrote in forums that “TVB is cruel to make Law die five times”. Others talked about how the broadcaster was so short of actors it needed Law in every drama.

A TVB spokesman responded that the free-to-air broadcaster had a lot of actors: “It was purely a coincidence that Law died five times,” he said.

Inside News

Hong Kong

Memories of post-war HK

When Jim Stoner first saw Hong Kong it was ravaged. The second world war had just ended when the 19-year-old arrived on the Empress of Australia troopship, and what he saw stayed with him for life. **Full report Page 5**



National

Beijing cancels university debate

Organisers of an inter-university debating event on the 1911 revolution are told to call it off, a day before it was to open. Writer Wen Yunchao says the timing, participants and topics probably hit a raw nerve with Beijing. “University students were going to debate topics related to democracy and revolution,” he says. **Full report Page 6**

The Review

The write stuff

There may be problems with censorship, but everyone agrees Chinese literature is flourishing, helped by the rise of a generation of writers who are challenging readers' expectations. Meet five of the best. **Review Pages 2-3**

Contact us

News Hotline
2565 2252
Classified Ads
2565 8822
Subscriptions & Deliveries
2680 8822



Inside

NEWS SECTION
Weather 2
Hong Kong 2-5
National 6
International 7-10
Agenda 11
Leaders & Letters 12
Your Money 13-16

THE REVIEW
Main feature 2-3
Sight & Sound 4-9
Arts 10-12
Books 13-17
The Planner 18
Film 19
Cinemas 20

SUNDAY SPORT
Soccer, Cricket 1
Motor Racing, Baseball 2
Golf 3
Racing 4-6
Results 5
Insight 7
Extra Time 8

Free views

Get a free trial of SCMP online. Registration is simple. Log on to www.scmp.com



CORUM
LA CHAUX-DE-FONDS - SUISSE

ADMIRAL'S CUP LEGEND

Watch with small seconds, 18K red gold case water-resistant to 50 meters. CORUM automatic movement.

www.corum.ch

Corum Hong Kong Boutique: Century Square, I-13 D'Aguijar Street, Central, Hong Kong. Tel: 2151 0918



PRINT

CLOSE

Cyber-extortionists target HK businesses

Local companies vulnerable to growing threat of attacks that paralyse online operations

Nathan Griffiths
Updated on *Apr 10, 2011*

Online attacks aimed at crippling websites unless cash is paid are on the rise and authorities can do little to stop them, leaving businesses to fend for themselves.

Internet watchers say the attacks are becoming more complex, making the job of tracking down the culprits - who are usually based overseas - even more difficult.

One recent victim was the popular expat website GeoExpat.

Distributed denial-of-service (DDoS) attacks work by flooding websites or servers with more data than they can handle.

They are launched from networks of infected computers - known as "botnets" - that can be sited and controlled from anywhere in the world.

When he saw the first e-mail on a Friday morning in January, titled "Partnership," GeoExpat chief operating officer Shriram Chaubal ignored it, assuming it was a hoax.

The message was stark: "Hello. Your site will undergo DDos attack. Pay US\$300 for libertyreserve or WesternUnion. You should contact us by e-mail for reception of the account for payment ..."

It was dated from the night before and had Russian and Myanmar e-mail addresses as contact points.

The next evening Chaubal started receiving alerts warning him that his websites were not accessible. Then, just before 10pm, he received a second email upping the demand.

"Hello, your site has undergone Ddos to attack." It demanded US\$350 to stop the attack.

As the operator of a popular online forum and an online retail site, Chaubal could not afford to be offline for weeks at a time. More damaging was the possibility of losing clients and his online reputation.

S.C. Leung, a senior consultant at the Hong Kong Computer Emergency Response Team (HKCERT), a local chapter of computer security specialists focused on security awareness and co-ordination, said his organisation had received no more than a handful of reports on DDoS attacks such as those Chaubal experienced.

"That doesn't mean there aren't a lot of attacks. It's just that such cases usually get reported to local internet service providers [ISPs] if they get reported at all," he said.

Sean Lord, vice-president of sales at Nexusguard, a local anti-DDoS security firm, called DDoS extortion tactics "old-fashioned" when compared with more lucrative efforts by organised crime to harvest credit card and other banking information. He agreed DDoS attacks on local businesses were going unreported.

The only thing unique about Chaubal's story was the fact that it made it to the press, he said.

Leung said HKCERT recommended any business experiencing attacks contact their ISP for help. He stressed that in cases such as Chaubal's, where extortion or other criminal activity was involved, the police should be contacted.

Chaubal, who contacted both HKCERT and his ISP when his sites came under attack, said neither were able to assist him. In an e-mail, HKCERT said they were unable to take action because the event might have included "criminal activity".

They advised that he speak to police, who sent officers to collect log files from his servers. Chaubal has yet to hear back from the police.

An officer investigating the case told Chaubal that he had never seen such a large attack. At one point the traffic hitting Chaubal's sites reached nearly 600Mbps - over 70 times the level of traffic the sites normally receive, completely shutting them down.

The company hired to protect his sites said the attack on his servers included roughly 50,000 computers scattered across the globe, including 500 computers from within Hong Kong itself. They called the attack "one of the toughest" and said it was "incredibly difficult ... to block".

In an attempt to keep up with the rapid developments in online crime, HKCERT organises a number of local and regional drills involving the police and ISPs.

Lord said the focus on ISP and infrastructure level protection was critical because by the time an attack was at the front door of a website, it was already too late. Although ISPs had traditionally relied on relatively simple techniques in responding to DDoS attacks, they were increasingly aware of the need for more proactive defences.

Greg Burns, vice-president of marketing at Prolexic, a company that specialises in DDoS protection, said: "All of our stats show increases, year after year, in both the number ... and complexity of attacks. In the foreseeable future we're going to see an increase in the use of DDoS."

The increase in denial-of-service attacks comes just after one of the oldest, largest and most technically sophisticated computer networks producing spam e-mails was "taken down" by Microsoft in co-operation with industry and academic experts. The Rustock botnet was responsible for between 20 per cent and 30 per cent of all e-mail spam traffic in Hong Kong in the first three months of the year.