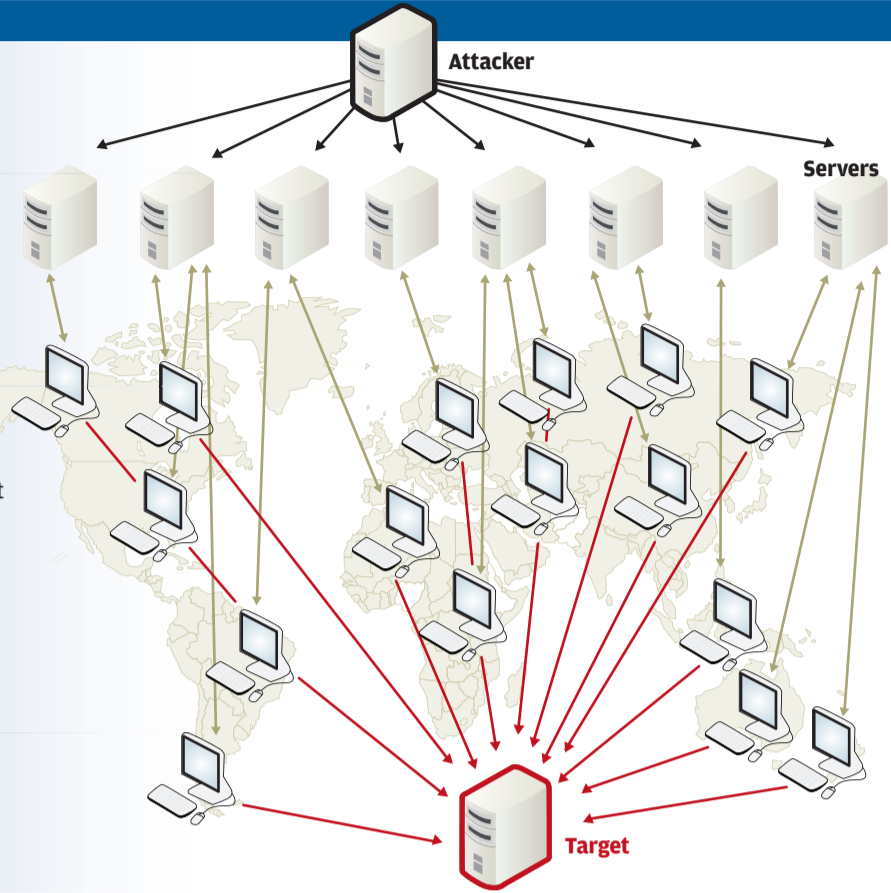


Experts warn of rising numbers of distributed denial-of-service attacks on business sites

# Hong Kong a sitting duck for online crime

## Creating chaos

1. **Attacker** sends out commands to servers
2. **Servers** push out commands to infected computers, known as "botnets", telling them to flood target with requests
3. **Infected computers** receive commands and begin to make repeated requests from the target computer
4. **Target** is overloaded with requests and can no longer be reached from the internet



SMP GRAPHIC

## Nathan Griffiths

Hong Kong's reputation as a finance and e-commerce hub and its proximity to the mainland make the city an attractive target for online crime, say security firms who specialise in preventing such crimes.

Greg Burns, vice-president of marketing at Prolexic, one of the earliest companies in the world to deal in distributed denial-of-service (DDoS) protection, said online attacks were increasingly moving into the mainstream and targeting businesses such as financial institutions and e-commerce sites, where DDoS attacks were usually part of a larger effort to collect sensitive banking and credit card information.

The attacks work by flooding websites or servers with more data than they can handle, leaving them unable to respond to legitimate requests.

The attacks are launched from networks of infected computers - known as "botnets" - that can be situated and controlled from anywhere around the globe.

According to a report recently released by Prolexic, the company saw DDoS attacks on e-commerce sites rise 200 per cent last year.

Despite this rise, DDoS attacks on local businesses were going largely unreported, said Sean Lord, vice-president of sales at Nexusguard, a local anti-DDoS security firm.

In a global survey of information technology professionals released in February, 60 per cent of respondents admitted they did not refer DDoS attacks to the authorities.

The report, conducted by Arbor Networks, a leading network security and research firm, cited a lack of faith in the ability of law enforcement to successfully prosecute online crime as one of the main reasons for not reporting attacks. As one survey respondent noted: "In the end, [police investigations] go nowhere."

Hong Kong already suffered from higher-than-average levels of online crime, said Lord and according to police figures, those numbers have been rising rapidly.

There were 1,643 online crimes reported last year, a record number and a 600 per cent rise from reports in

2001, the year the police force's Technology Crimes Division (TCD) was established.

Cases involving unauthorised access to computers, which includes attempts to hack into or hijack computers, have risen 632 per cent since 2008, the last year police were able to provide a detailed breakdown of technology crime statistics.

In an effort to combat the rapidly growing threat of online crime, the division hired 26 additional officers in 2009-2010 and stepped up training. Plans are also under way to upgrade the TCD's computer forensics laboratory.

Police refused to provide the number of arrests made for online crime in Hong Kong.

## Seventy per cent of infected computers, or botnets, identified by Prolexic were on the mainland

Prolexic's annual Distributed Denial-of-Service Attack Report

Worldwide, there has only been a handful of successful prosecutions against DDoS and other botnet operators. Successful prosecution is extremely rare for both legal and technological reasons.

The international and anonymous nature of DDoS attacks meant the people controlling them were often "three or four layers removed from the actual attack", Burns said.

The attackers were typically located in another country, well outside the jurisdiction of local authorities and were often operating at the request of another party.

"The technology generally doesn't point to who is actually behind the attack," he said.

This has led, rightly or not, to a poor view of law enforcers' abilities to handle the crime.

Only 14 per cent of respondents from the Arbor Networks survey reported having confidence in the ability of law enforcement to investi-

gate and prosecute DDoS-related crimes. Burns said his company worked with local authorities on an educational level, but would only share "attack-specific information" at the request of their customers.

Prolexic's annual DDoS Attack Report, published early this year, said the number of attacks per client was "consistently higher" in Asia than other regions.

It noted that 70 per cent of infected computers identified by Prolexic were located on the mainland.

Team Cymru, a non-profit internet security research firm, reported roughly 2,700 websites running as botnet controlled servers on the mainland at any given time last year, making the mainland home to the largest concentration of botnets in Asia and one of the largest in the world.

Lord said that the high rate of pirated software in use on the mainland was probably an important factor in the number of infected computers.

Earlier this year, Microsoft chief Steve Ballmer reported his company estimated that 90 per cent of the Microsoft operating systems running on the mainland were pirated copies.

Out-of-date security updates made these systems easy targets for criminals looking to gain access to computers, Lord said.

A police spokesman said police maintained an effective liaison with the mainland and overseas law enforcement agencies, but was unable to provide information on the number or types of requests made to them; claiming that police did not maintain any statistics on cases referred to outside agencies.

Proximity to sprawling networks of infected computers is not Hong Kong's only concern. Many of the city's infrastructure-level network connections are relatively low bandwidth, making them easy to flood with DDoS traffic, according to both Lord and Burns.

These limitations meant anti-DDoS efforts in Hong Kong needed an especially "advanced strategy and platform to be effective", said Burns. "There's no easy fix to DDoS. It's like a war game."

## Net casino operators target competitors

While distributed denial-of-service attacks have begun targeting traditional businesses like finance and e-commerce sites, most attacks in Asia still focus on the largely illegal world of online gambling.

According to Sean Lord, vice-president of sales at Nexusguard, a "significant percentage" of the attacks in Asia that his company deals with are online casino operators targeting their competitors. Online casinos make attractive targets since revenue depends on millions of transactions taking place every hour - often under time-sensitive conditions.

A gambling site knocked offline for even a short period stands to lose millions in revenue. Competing sites benefit from the flood of customers looking to place bets.

Using DDoS attacks to take out competitors is hardly a new tactic in the online gambling world.

Before 2006, most DDoS attacks around the world targeted online casinos and their related payment processing sites, said Greg Burns, vice-president of marketing at DDoS mitigation specialist Prolexic.

The cost of being offline and a desire to keep under the radar of the authorities meant that operators often accepted DDoS as a cost of doing business.

While an exact correlation between online gambling and DDoS is not easy to prove, there certainly appears to be a connection.

Over the course of seven months in 2009, mainland authorities closed more than 100 illegal gambling sites and arrested dozens of groups - including several connected to organised crime - that ran servers hosting the sites and related online payment processing services.

According to Lord, this led to a dramatic drop in the number of DDoS attacks across Asia. After the crackdown, DDoS attacks in the region returned to regular levels.

Nathan Griffiths

## Cyber extortionists target businesses

CONTINUED FROM PAGE 1

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.

## Old cameras capture a new generation of photographers

### Lana Lam

A plastic toy camera that used to be made in Hong Kong in the 1960s has been reborn by an Austrian company as a trendy must-have for local teens thanks to a resurgence in film photography.

Vienna-based Lomography sells a range of analogue cameras that are known for their lo-fi characteristics which give photos a dreamy quality, vibrant colours or heavy shadowing around the edges of a picture.

One is the Diana F+ which used to be made in Hong Kong but is now produced on the mainland.

"It was a kid's camera, that's why it was all plastic," said Justin Tsui, marketing manager for Lomography Asia. She said their cameras have gained a cult following in the past few years as some photographers reject the digital era and return to film.

The number of Lomographers - the name given to photographers who use the range of cameras - has increased significantly in the past 12 months, Tsui said. "It's growing really fast. There are at least 80,000 people in the Lomography community in Hong Kong. But a year ago, it was half that number," she said.

"Even the kids, around 12 to 15, they also play with our cameras. It's affordable compared to the digital camera. You could say it's a very niche market, but in the last couple of years a lot of young people started to fall in love with our cameras."

A large-scale exhibition of Lomography photos opens in Times Square tomorrow. It will include a photo wall dedicated to Hong Kong images and 4-metre high replicas of the cameras.

"A lot of people get the wrong impression about Lomography because

With digital cameras, you take one shot several times but you may miss chances for other images

Onyee Lok, a freelance designer and Lomography camera enthusiast

they think nobody uses analogue cameras or film any more," Tsui said.

"But the truth is, a lot of people - especially the very young people born after the '90s - they know all about digital cameras, however, they have absolutely no idea what an analogue camera is so they try it."

"So it's kind of a trigger. In fact, there's quite a lot of new customers who are curious about this product."

"Sometimes we get older people - especially when we take out the Lubitel twin lens camera. People around 60 years old say, 'Oh, I used to have one', and they come into our shop to ask about our cameras."

Another signature camera is the Spinner 360, which has a cord that you pull to take a 360-degree photo. Prices range from HK\$200 to HK\$5,000.

Onyee Lok is an avid fan of Lomography cameras. She stumbled across the range three years ago and has been shooting with the models ever since.

"It is now part of my life because I use Lomography cameras to capture moments in my life," the freelance designer said.

"This is the way that I can create and express my thoughts through photography."

"With digital cameras, you take one shot several times but then you may miss chances for other images. I can concentrate on enjoying my life instead of pressing the shutter all the time."

Lok has more than 10 Lomography cameras and one of her favourites is the all-plastic Diana F+ model.

"The photos are quite dreamy and there's strong vignetting. I find the Diana has many surprises - and it's great fun."



Lomography Asia marketing manager Justin Tsui with giant camera replicas at the brand's exhibition held in Times Square. Photo: Sam Tsang

## Stella heads home after brain surgery

### Lana Lam

Stella Sipma, a two-year-old Clearwater Bay girl who has a rare genetic disease, is set to fly back to Hong Kong tomorrow after a series of complex brain operations in New York.

Meanwhile, the Stella Standing Tall fund-raising campaign has raised more than HK\$1 million to help the family pay medical bills estimated to be US\$300,000.

Stella's mum, Alison, said her daughter, who has tuberous sclerosis

which causes seizures and tumours, was recovering slowly.

"Although there have been some complications, Stella's neurosurgeon and neurologist believe these are to be expected after such complex brain surgery," she said.

"Overall, I think her body and brain just need time to heal and adjust. Her cuts are healing well and she is already much more alert and energetic. She can climb into her stroller by herself now, something she could not do before her surgery."

She thanked the local community for their tireless efforts in raising so much money.

"We have so many people to thank for helping us through this time and for helping to ease our financial burden," she said.

Stella's father, Marcel, said the family was desperate to come home: "We've been away for one month now."

"Our other daughter, Sophie, misses school and we miss our home and friends."



PRINT

CLOSE

## Hong Kong a sitting duck for online crime

**Experts warn of rising numbers of distributed denial-of-service attacks on business sites**

Nathan Griffiths  
Updated on *Apr 10, 2011*

Hong Kong's reputation as a finance and e-commerce hub and its proximity to the mainland make the city an attractive target for online crime, say security firms who specialise in preventing such crimes.

Greg Burns, vice-president of marketing at Prolexic, one of the earliest companies in the world to deal in distributed denial-of-service (DDoS) protection, said online attacks were increasingly moving into the mainstream and targeting businesses such as financial institutions and e-commerce sites, where DDoS attacks were usually part of a larger effort to collect sensitive banking and credit card information.

The attacks work by flooding websites or servers with more data than they can handle, leaving them unable to respond to legitimate requests.

The attacks are launched from networks of infected computers - known as "botnets" - that can be situated and controlled from anywhere around the globe.

According to a report recently released by Prolexic, the company saw DDoS attacks on e-commerce sites rise 200 per cent last year.

Despite this rise, DDoS attacks on local businesses were going largely unreported, said Sean Lord, vice-president of sales at Nexusguard, a local anti-DDoS security firm.

In a global survey of information technology professionals released in February, 60 per cent of respondents admitted they did not refer DDoS attacks to the authorities.

The report, conducted by Arbor Networks, a leading network security and research firm, cited a lack of faith in the ability of law enforcement to

successfully prosecute online crime as one of the main reasons for not reporting attacks. As one survey respondent noted: "In the end, [police investigations] go nowhere."

Hong Kong already suffered from higher-than-average levels of online crime, said Lord and according to police figures, those numbers have been rising rapidly.

There were 1,643 online crimes reported last year, a record number and a 600 per cent rise from reports in 2001, the year the police force's Technology Crimes Division (TCD) was established.

Cases involving unauthorised access to computers, which includes attempts to hack into or hijack computers, have risen 632 per cent since 2008, the last year police were able to provide a detailed breakdown of technology crime statistics.

In an effort to combat the rapidly growing threat of online crime, the division hired 26 additional officers in 2009-2010 and stepped up training. Plans are also under way to upgrade the TCD's computer forensics laboratory.

Police refused to provide the number of arrests made for online crime in Hong Kong.

Worldwide, there has only been a handful of successful prosecutions against DDoS and other botnet operators. Successful prosecution is extremely rare for both legal and technological reasons.

The international and anonymous nature of DDoS attacks meant the people controlling them were often "three or four layers removed from the actual attack", Burns said.

The attackers were typically located in another country, well outside the jurisdiction of local authorities and were often operating at the request of another party.

"The technology generally doesn't point to who is actually behind the attack," he said.

This has led, rightly or not, to a poor view of law enforcers' abilities to handle the crime.

Only 14 per cent of respondents from the Arbor Networks survey reported having confidence in the ability of law enforcement to investigate and prosecute DDoS-related crimes. Burns said his company worked with local authorities on an educational level, but would only share "attack-specific information" at the request of their customers.

Prolexic's annual DDoS Attack Report, published early this year, said the number of attacks per client was "consistently higher" in Asia than other regions.

It noted that 70 per cent of infected computers identified by Prolexic were located on the mainland.

Team Cymru, a non-profit internet security research firm, reported roughly 2,700 websites running as botnet control servers on the mainland at any given time last year, making the mainland home to the largest concentration of botnets in Asia and one of the largest in the world.

Lord said that the high rate of pirated software in use on the mainland was probably an important factor in the number of infected computers.

Earlier this year, Microsoft chief Steve Ballmer reported his company estimated that 90 per cent of the Microsoft operating systems running on the mainland were pirated copies.

Out-of-date security updates made these systems easy targets for criminals looking to gain access to computers, Lord said.

A police spokesman said police maintained an effective liaison with the mainland and overseas law enforcement agencies, but was unable to provide information on the number or types of requests made to them; claiming that police did not maintain any statistics on cases referred to outside agencies.

Proximity to sprawling networks of infected computers is not Hong Kong's only concern. Many of the city's infrastructure-level network connections are relatively low bandwidth, making them easy to flood with DDoS traffic, according to both Lord and Burns.

These limitations meant anti-DDoS efforts in Hong Kong needed an especially "advanced strategy and platform to be effective", said Burns. "There's no easy fix to DDoS. It's like a war game."