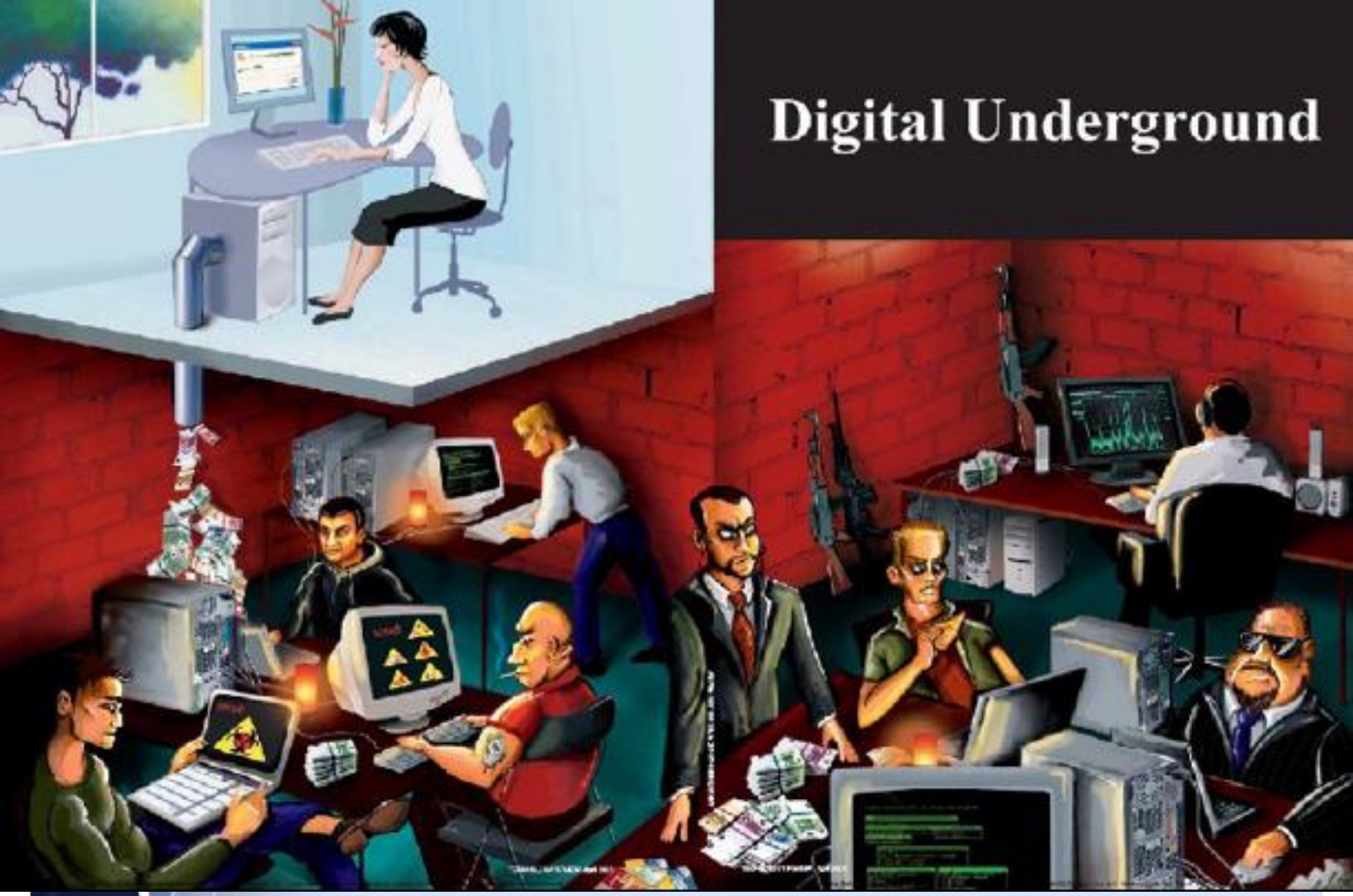
Technology Crime Trend – Where can we do to mitigate the threat?

Frank LAW
Chief Inspector
Technology Crime Division
Hong Kong Police

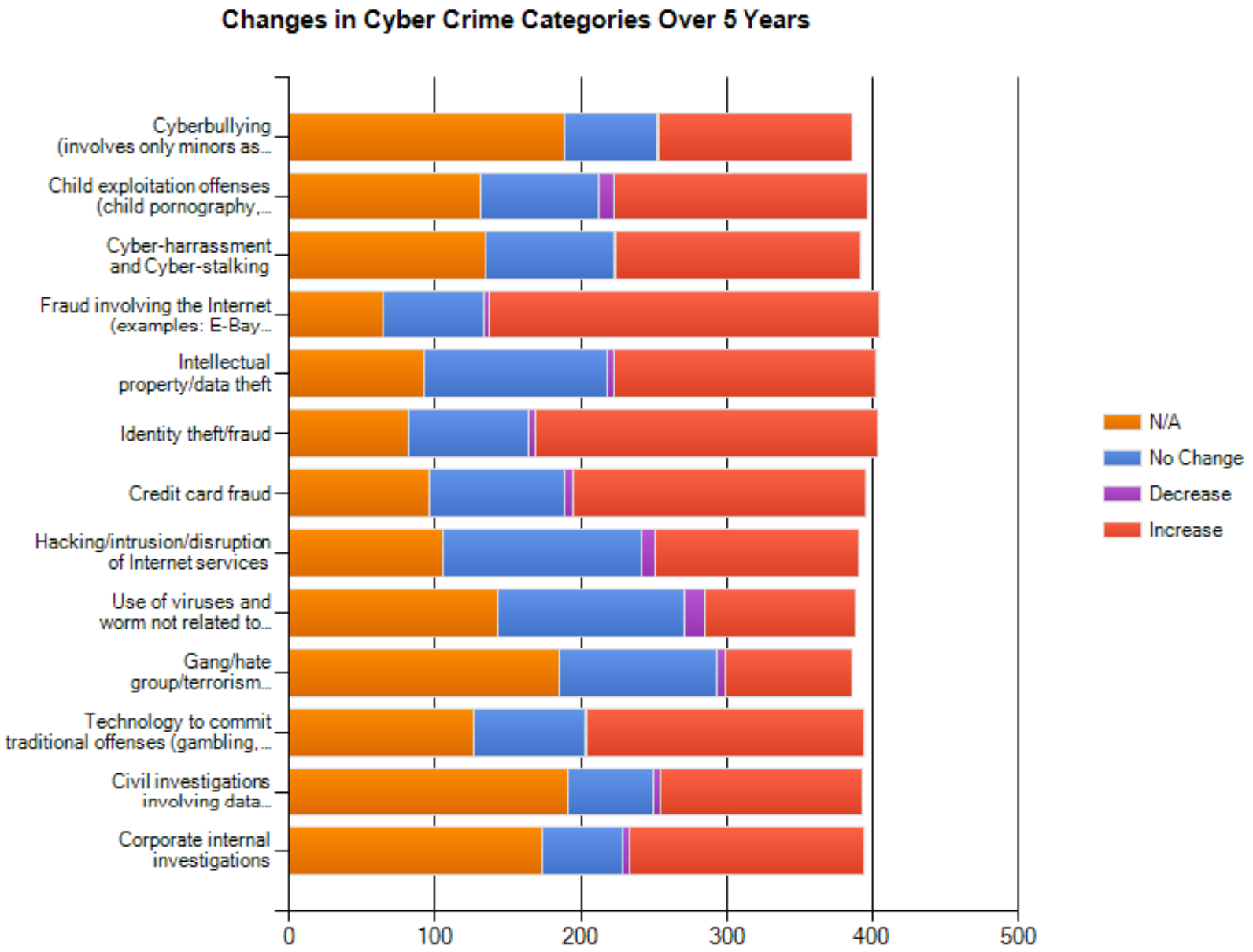


Source:
http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/trend_micro_2010_future_threat_report_final.pdf

Outline

- What is the current technology crime trend?
- Where are cyber criminals?
- Threat from BotNets
- How to tackle the problem?

HTCIA survey 2010



Wednesday, May 26, 2010

Cybercrime trend on the rise – Symantec

Symantec latest Internet Security Threat Report (volume XV) has revealed upward trends in cybercrime from Jan.1, 2009 to Dec. 31, 2009.

In a two very prominent cyber attacks - Conficker in the opening months of the year and Hydraq at the very end, the report otherwise known as the 'Corps' highlighted continued growth in both volume and sophistication of the attacks.

Regional Director, Africa at Symantec, Gordon Love said that attacks have evolved from simple scams to highly sophisticated espionage campaigns targeting some of the world's largest corporations and government entities.

"The scale of these attacks and the fact that they originate from across the world, make it a truly international problem requiring the cooperation of both the private sector and world governments," Love said.

The Director, also revealed that Nigeria ranked number 43 in Europe, Middle East and Africa (EMEA) and 70 in the world in 2009 for malicious activity.

"In comparison to the previous year, South Africa climbed seven places from 50 to 43 globally," he said.

In the EMEA region in 2009, 49 per cent of the volumes of top 50 potential infections were classified as worms; which shows an increase from 30 per cent in 2008.

"More specifically, Egypt was the top-ranked country for viruses while Saudi Arabia was the top-ranked country for worms," Love said.

Worms are malicious programs that replicate themselves from system to system without the use of a host file. This contrasts with viruses, which requires the spreading of an infected host file.

ITREALMS Online ... delivering news for ICT4D

Posted by ICTRealms at 8:49 PM

Labels: Cyber Security

Source: http://itrealms.blogspot.com/2010/05/cybercrime-trend-on-rise-symantec.html

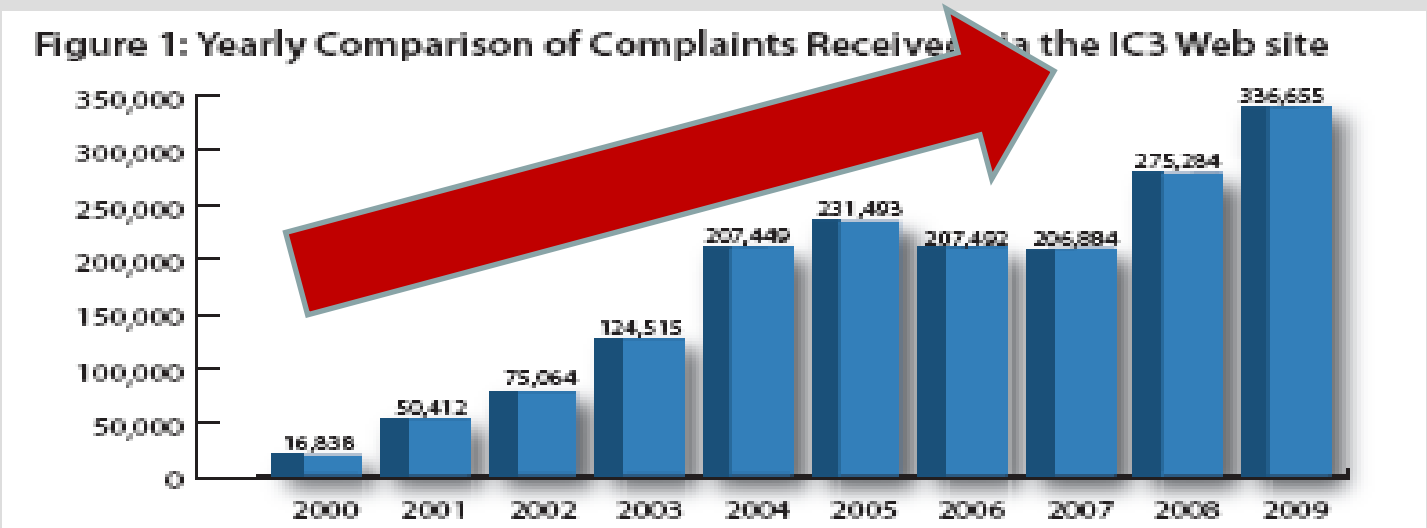
What are the targets?

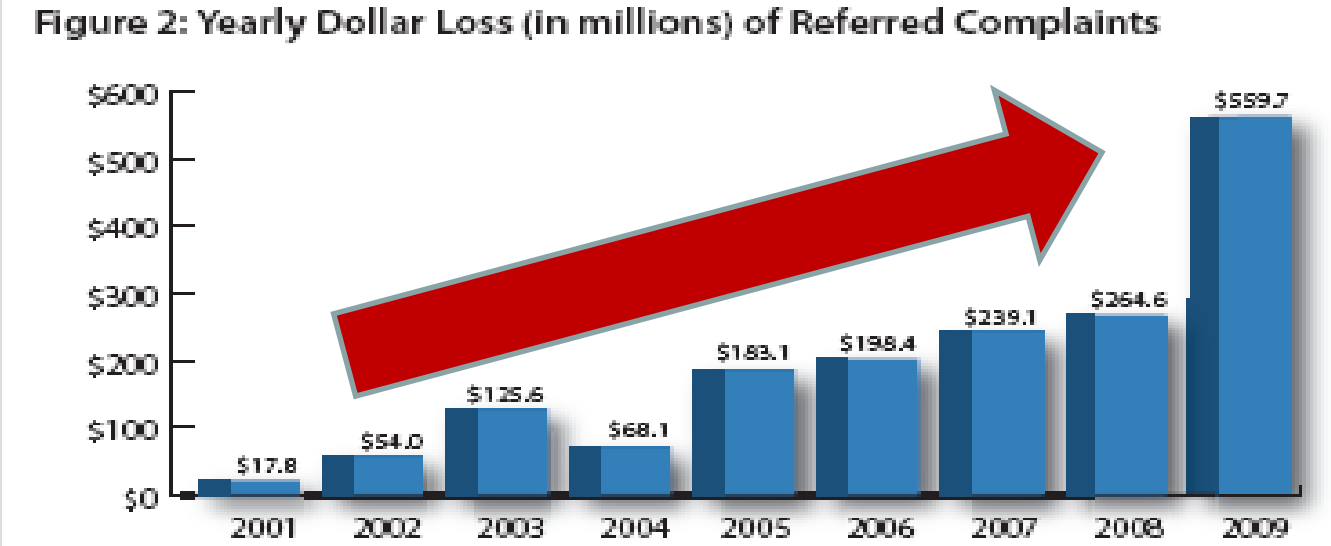
Overall Rank 2009	Overall Rank 2008	Item	Percentage 2009	Percentage 2008	Range of Prices
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

Table 21. Goods and services advertised for sale on underground economy servers

Source: Symantec

2009 Internet Crime Report from IC^3



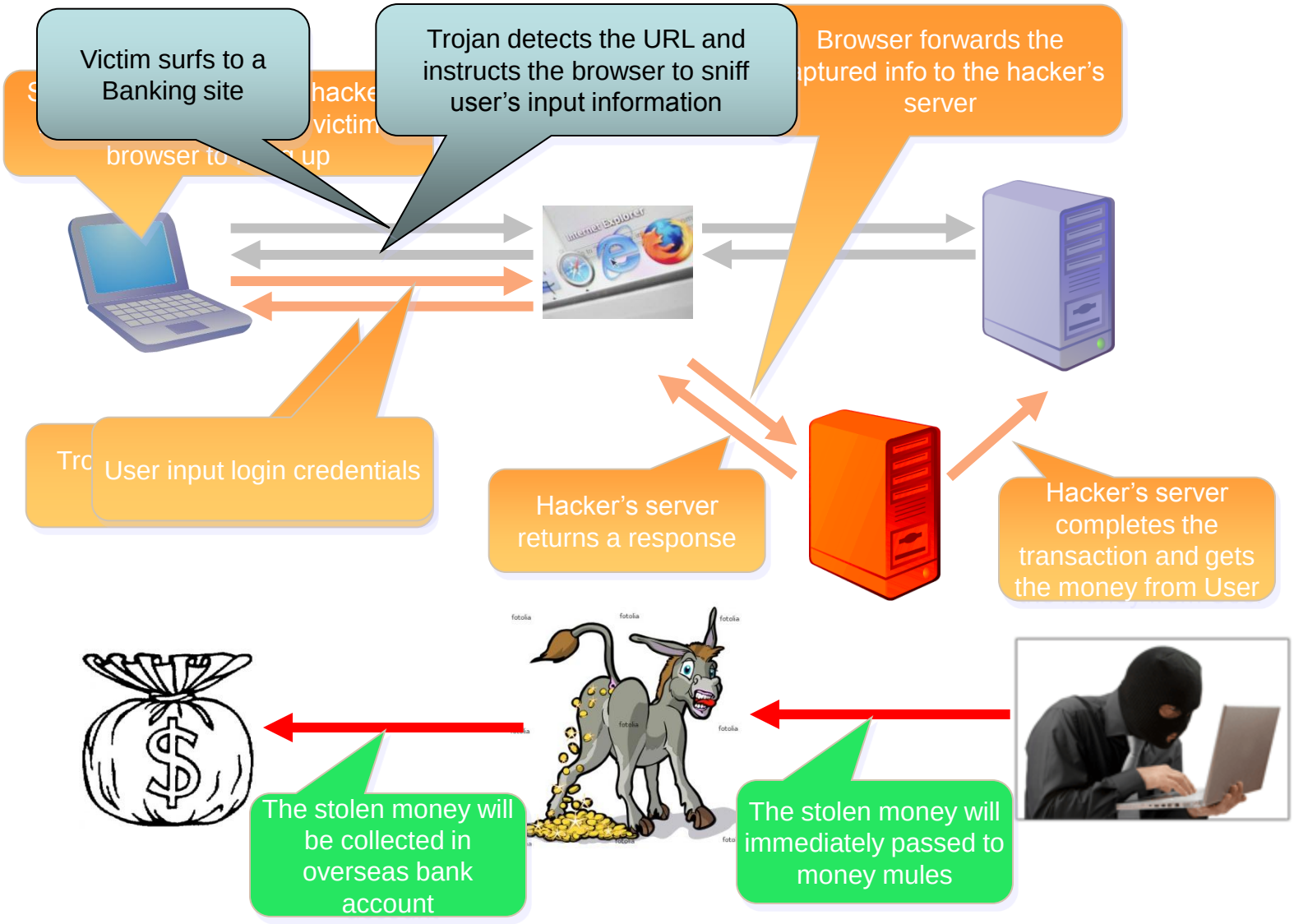


Source: http://www.ic3.gov/media/annualreports.aspx

Some observations from local and global trend

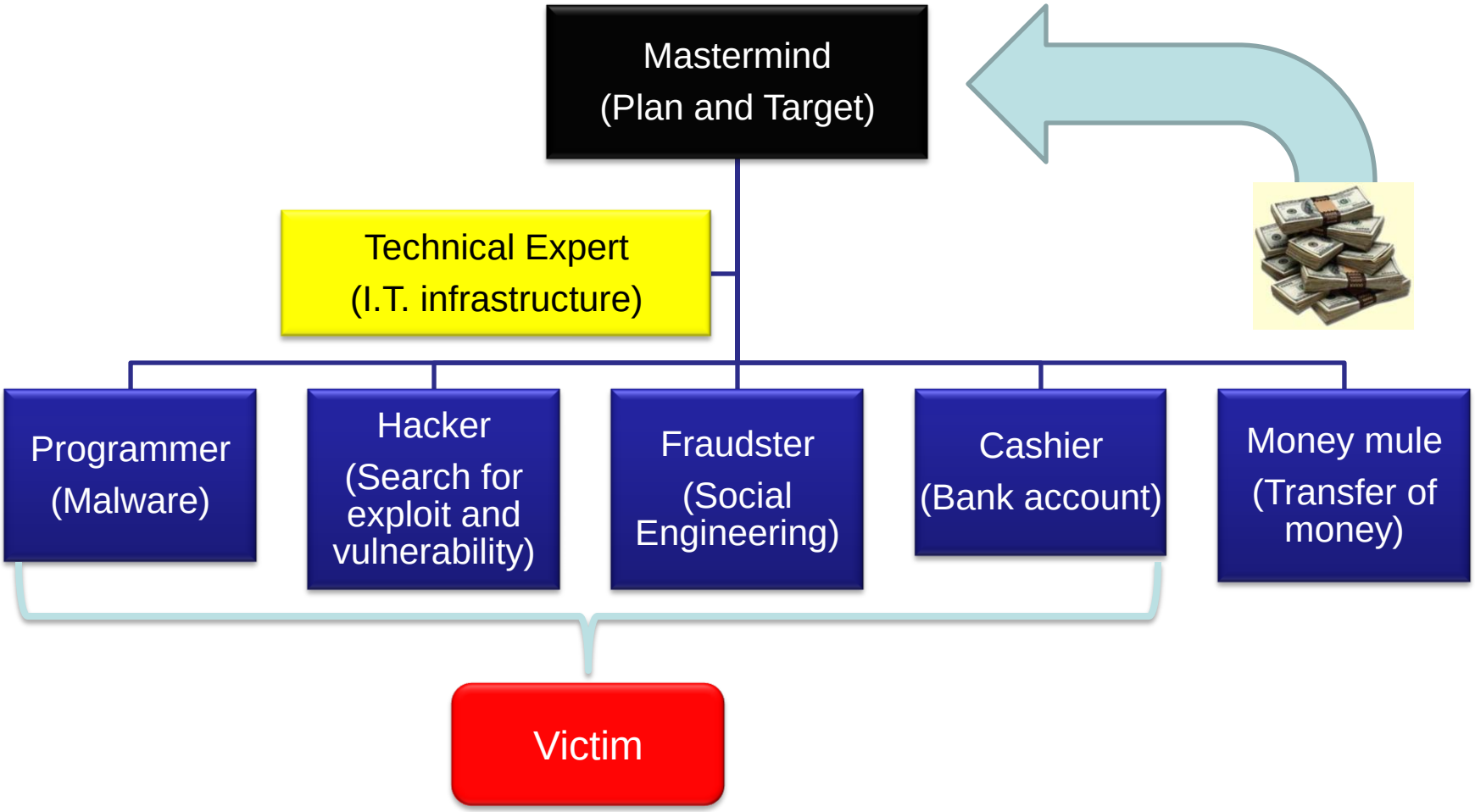
- The underground economy is largely unaware
- Small investment but reap huge profits
- Sophisticated scheme for monetizing stolen information
- More organized and often run like corporation!

Example of e-Banking Theft



How many criminal roles have been involved in the previous case?

Cyber criminal organization



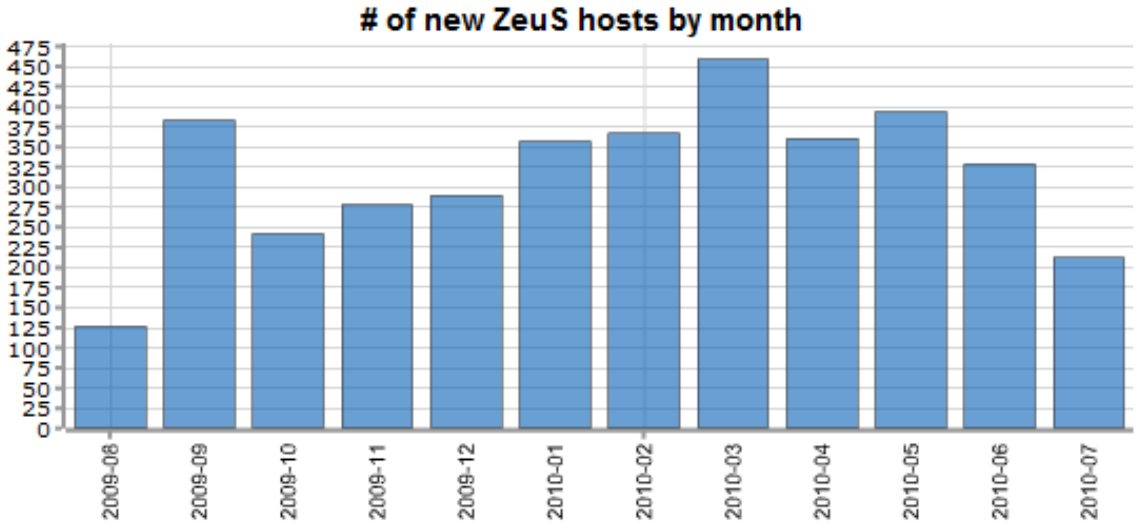
Characteristics of Cyber criminals

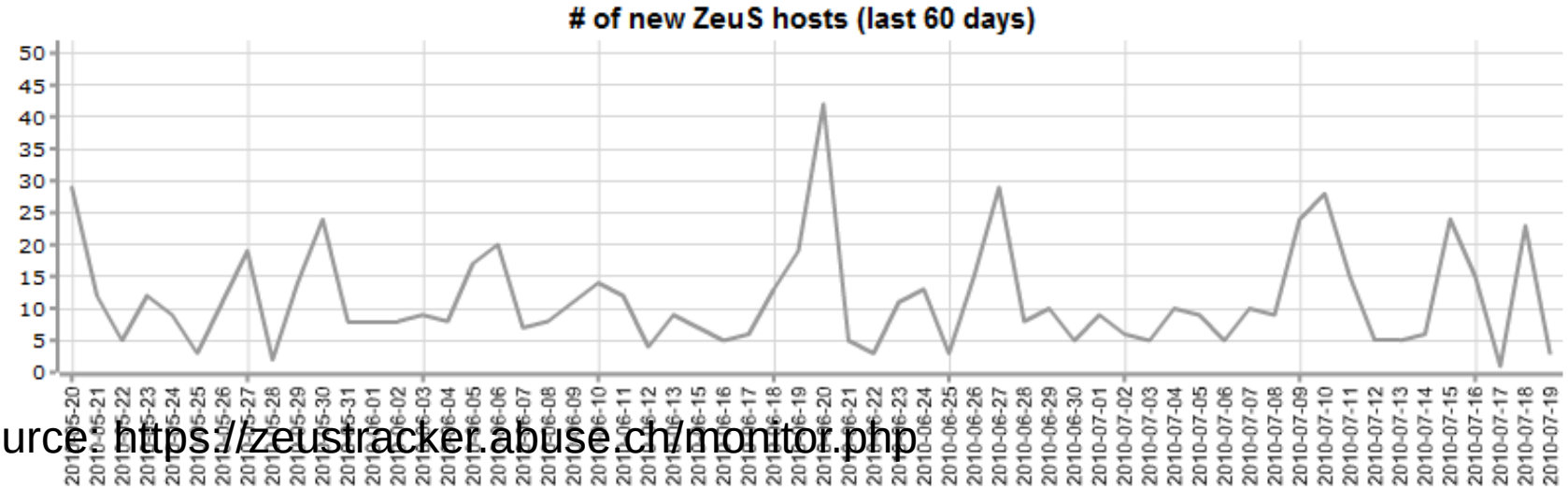
- Operate Worldwide
- Round the clock
- Swift response and planning
- Small investment
- Unknown to each others

Technologies that may assist Cyber criminals

- Encryption
- Fast-flux networks
- Bulletproof hosting
- Peer-to-peer network
- Robot Network (BotNet)

Information of ZeUS hosts





Source: https://zeustracker.abuse.ch/monitor.php

abuse.ch ZeuS Tracker

Home | FAQ | ZeuS Blocklist | ZeuS Tracker | Removals | ZTDNS *new!* | Statistic | RSS Feeds | Contact | Links

ZeuS Tracker :: Search results

You can search for Filenames, URLs or MD5 hashes.
Note: The page will display only the first twenty results.

search

Host result(s)

Host	A record	status	SBL	Level	dateadded (UTC)	AS number	last updated (UTC)
trastlifer.hk		offline	Not listed	4	2010-03-10	0	2010-03-26
narayanjik.hk		offline	Not listed	1	2010-03-14	0	2010-03-26
lopokerasandco.hk		offline	Not listed	1	2010-02-28	0	2010-03-26
pipiskin.hk		offline	Not listed	1	2010-02-28	0	2010-03-26

Config result(s)

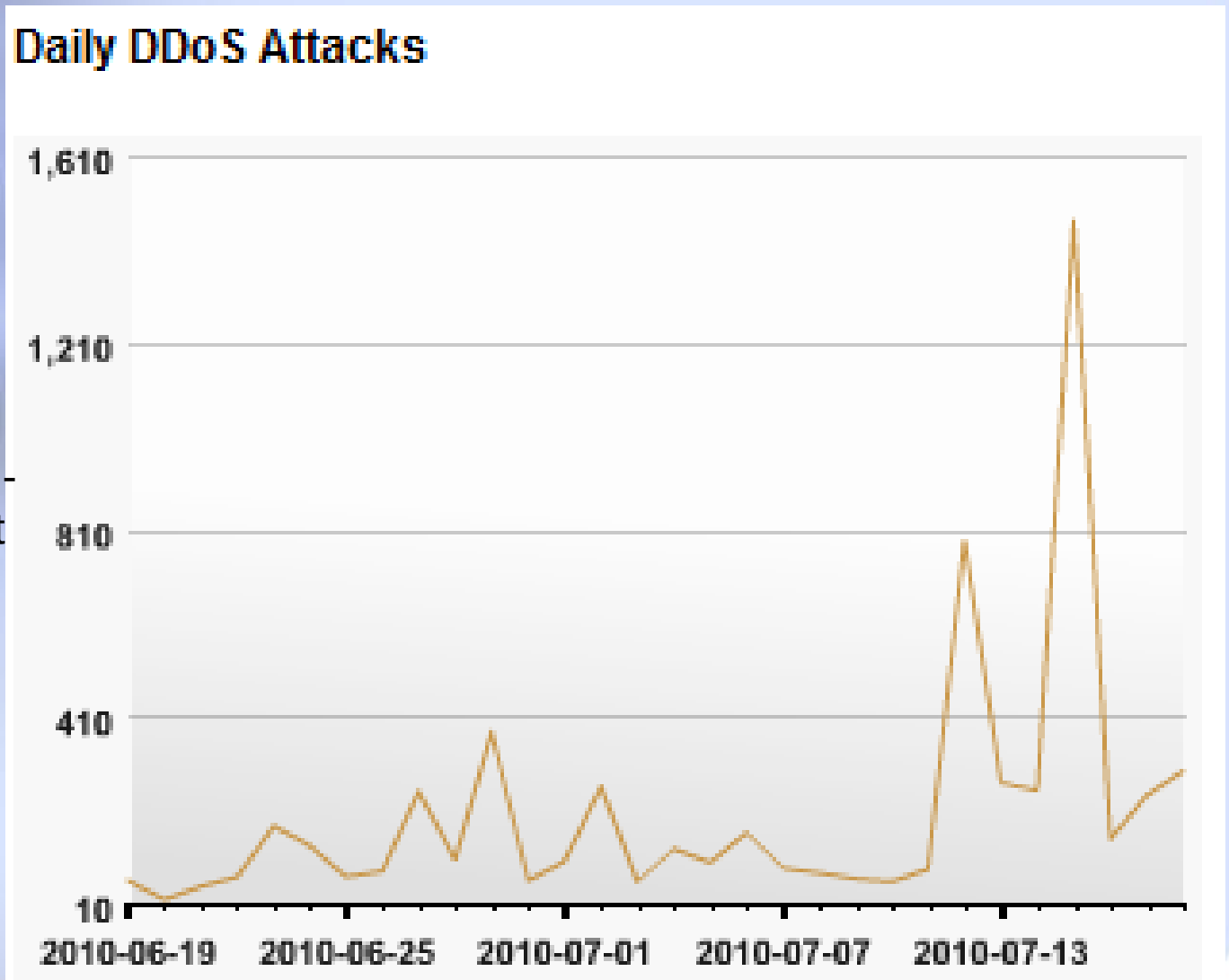
config URL	dateadded (UTC)	status	Filesize (in bytes)	MD5 hash	last updated (UTC)
narayanjik.hk/main/terms.doc	2010-03-14	offline	123'702	665c925e6c99c1db86ac154c6b982e5a	2010-03-16
lopokerasandco.hk/files/a.out	2010-02-28	offline	123'705	b47ab3a318ce8ab698e011d056fdbfaf	2010-03-18
lopokerasandco.hk/files/a2.out	2010-02-28	offline	123'705	b47ab3a318ce8ab698e011d056fdbfaf	2010-03-18
pipiskin.hk/ribbn.tar	2010-02-28	offline	35'140	390e834ebf3793520731f9d6eb51c7f7	2010-03-03
trastlifer.hk/ribbn.tar	2010-03-10	offline	11'299	aff90d73af69aa9939adf116402fd31e	2010-03-15

Binary result(s)

binary URL	dateadded (UTC)	status	Filesize (in bytes)	MD5 hash	AV detection	last updated (UTC)
narayanjik.hk/application/install.exe	2010-03-14	offline	95'744	68db38c23e6bba8b8e9d76086fa78c8e	no data	2010-03-16
lopokerasandco.hk/files/bot2.exe	2010-02-28	offline	119'296	7950103b3d98912dc32b6cd83ef979e7	24%	2010-03-03
lopokerasandco.hk/files/bot.exe	2010-02-28	offline	110'592	c49db769b790a899b3f593610e708ded	41%	2010-03-03
pipiskin.hk/java.exe	2010-02-28	offline	0		no data	2010-02-28
lopokerasandco.hk/files2/bot2.exe	2010-03-02	offline	119'296	7950103b3d98912dc32b6cd83ef979e7	24%	2010-03-18
trastlifer.hk/vmxts.exe	2010-03-10	offline	151'552	d70f3537dbda98be3a1e466b592ecdac	24%	2010-03-15

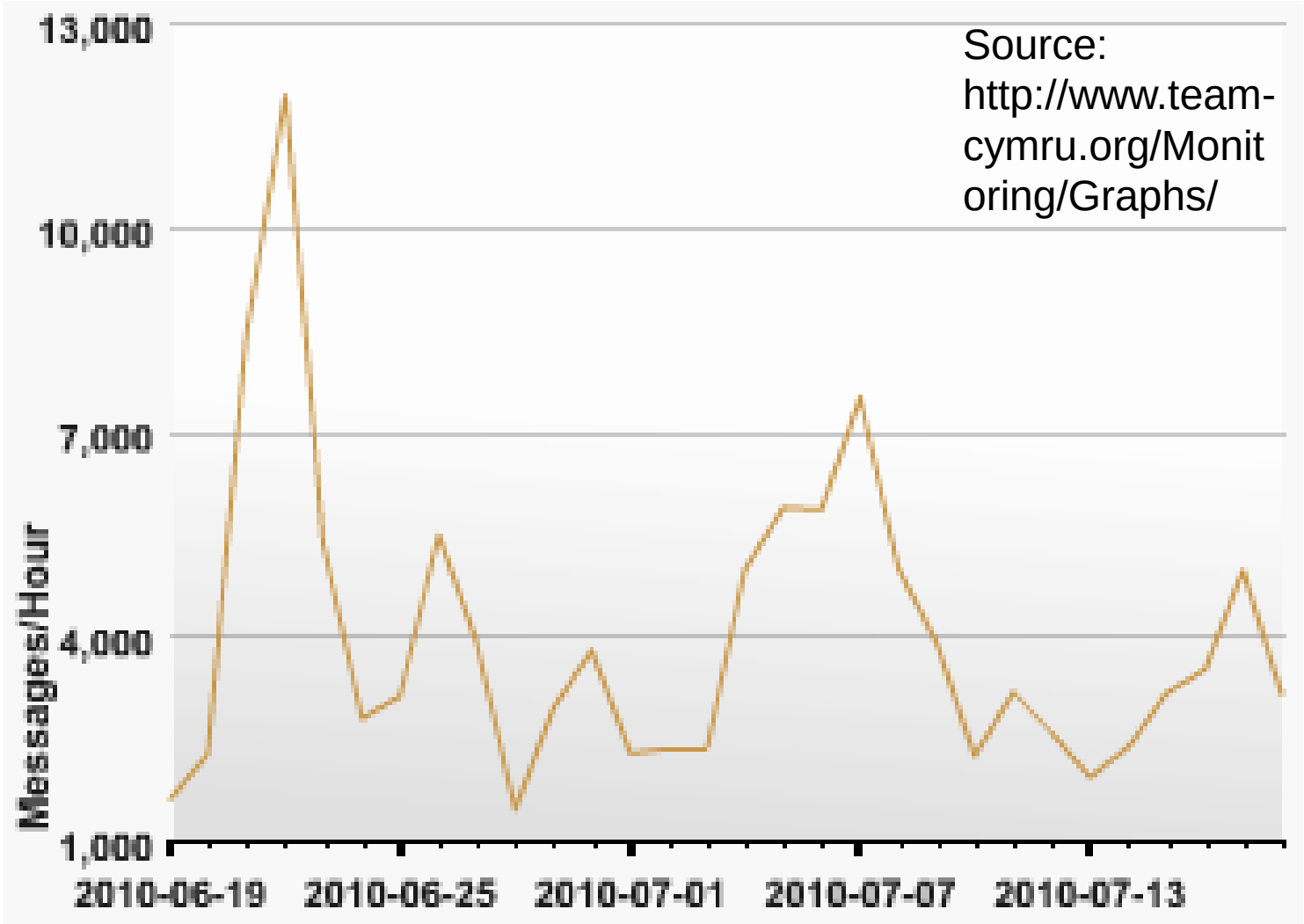
Source: https://zeustracker.abuse.ch/monitor.php

Daily DDoS Attacks



Source: http://www.team-cymru.org/Monitoring/Graphs/

Message send out from BotNets



Source: http://www.team-cymru.org/Monitoring/Graphs/

itnews
FOR AUSTRALIAN BUSINESS

Whirlpool suffers DDoS attack

Brett Winterford|Jun 29, 2010 9:40 AM

UPDATE: Blocked by upstream providers.

Broadband forum Whirlpool was brought down by a distributed denial of service attack this morning.

Update: Service restored at 10:30am. See below.

Update #2: **Site down again June 30th. See here for latest news.**

From 12:45am, Whirlpool host Bulletproof Networks noted irregular packet loss and investigated. The hosting company discovered a large number of HTTP requests from a number of source IP addresses, all targeting Whirlpool.

Bulletproof blocked the offending source IP addresses and asked its upstream providers to do the same, restoring the site at 1:45am.

The attack resumed five minutes later.

Again, Whirlpool was pulled offline whilst Bulletproof worked to block the attack. It was brought back online just before business hours, but was taken offline a third time as the attack resumed.

"The service provider owners of the offending IPs in Denmark and the US have been contacted to escalate blocking of their specific addresses at

Envision

Resolved Question Show me another »

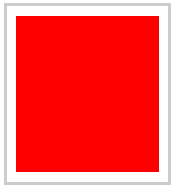
How do i stop a DDos Attack?

Ok so, People keep ddos attacking me. They do it about 4 times a day for 5 minutes at a time.

People say to reset or change my ip but it wont work because i have a static ip. Can some PLEASE FREAKING HELP ME... i feel like blowing up my comp

1 month ago

Report Abuse



G

TOP CONTRIBUTOR

Best Answer - Chosen by Voters

This may be some help.
http://www.linuxsecurity.com/content/vie...

1 month ago

Source:
http://answers.yahoo.com/question/index?qid=20100604214119AAiDdwP

100% 1 Vote

Report Abuse

How to mitigate the problem of DDoS attack?

- Understand normal traffic pattern
- Alerting system for DDoS specific event
- Filtering capability
- Trace-back mechanism
- Cooperation between various service providers
- Enforcement actions

How to mitigate the problem of DDoS attack?

- Proposed to establish a platform for sharing of information
- Effective points of contact for incident response
- Early warning mechanism to cyber attack

Question


Q & A