

Responding to Security Incident: MyCERT approach and case study

FIRST TC 2012 @ KYOTO
13-15 November 2012

By: Megat Muazzam Abdul Mutalib
Manager Emergency Response (Cyber999),
MyCERT



Agenda

- About MyCERT
- Trends + Statistic
- Case Study
- Success and Challenges



MyCERT

- Established in 1997
- Roles:
 - Incident Handling & Response
 - Technical Co-ordination
 - Alert and Advisories
 - National Cyber Security Exercises
- Works closely with various partners, locally and Internationally
- Constituents: ALL Internet users in Malaysia



MyCERT (2)

- 2 Core Groups
 - Cyber999 / Incident Response
 - Malware Research Centre
- Strengths
 - 20 Personnel
 - > 10 until 2007
 - Supported by other departments and initiatives at CyberSecurity Malaysia

 Cyber999

 CyberSecurity Malaysia
malware
research centre



MyCERT (3)

- No 'Enforcement Power'
 - Based on trust
 - Provide technical expertise for assisting victims of cyber security incidents
- Collaboration
 - Vast network of contacts via other security teams, vendors and law enforcement agencies



Cyber999 Statistical Reports

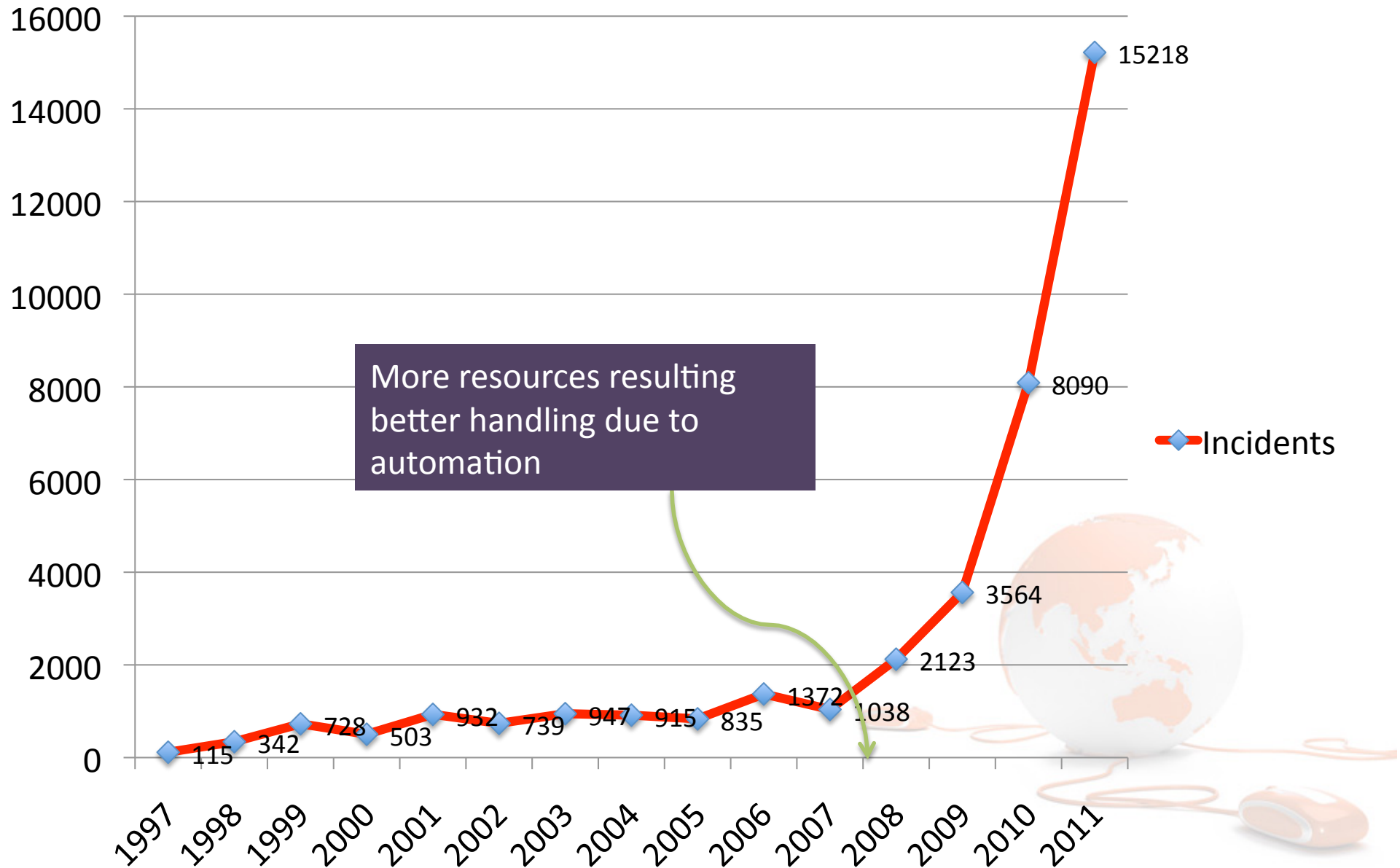


Overview of Stats

- Growth of Incidents reflect ‘changing’ times and more reliance of the Internet
 - i.e. rise of harassment and scam due to prevalence of social networking
 - Ability for the team handle more incidents increased after 2007 due to more resources
- National CERT fills in the gap in dealing with emerging threats – i.e. malware, phishing, targeted attack, cyber harassment and more
- Incident data created awareness, generate interests and pushed forward other initiatives
 - CNII Protection, Cyber Crisis Management, Training and Awareness



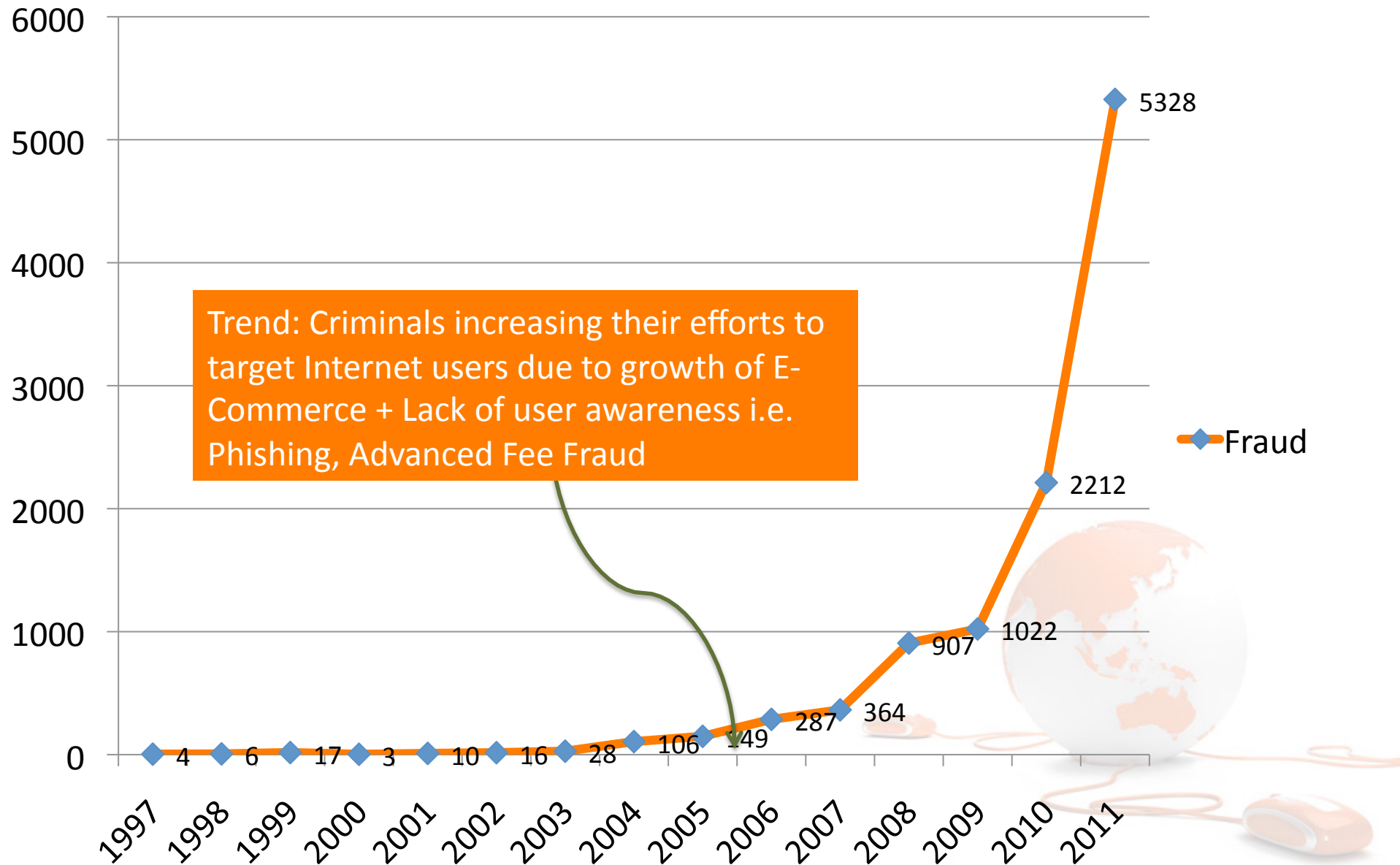
Incidents Handled 1997 – 2011



More resources resulting better handling due to automation

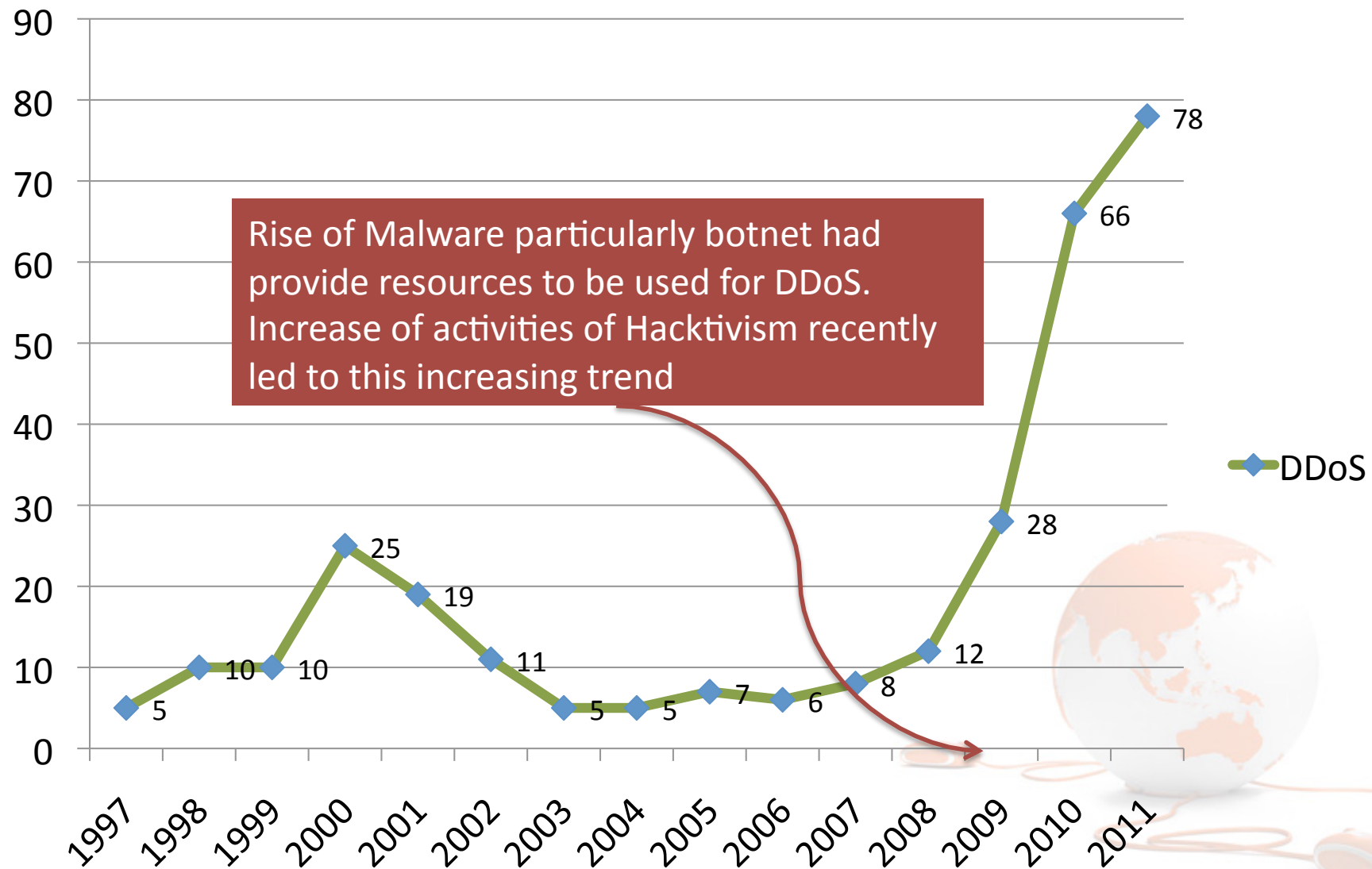
Source: www.mycert.org.my

Fraud Incidents 1997 – 2011

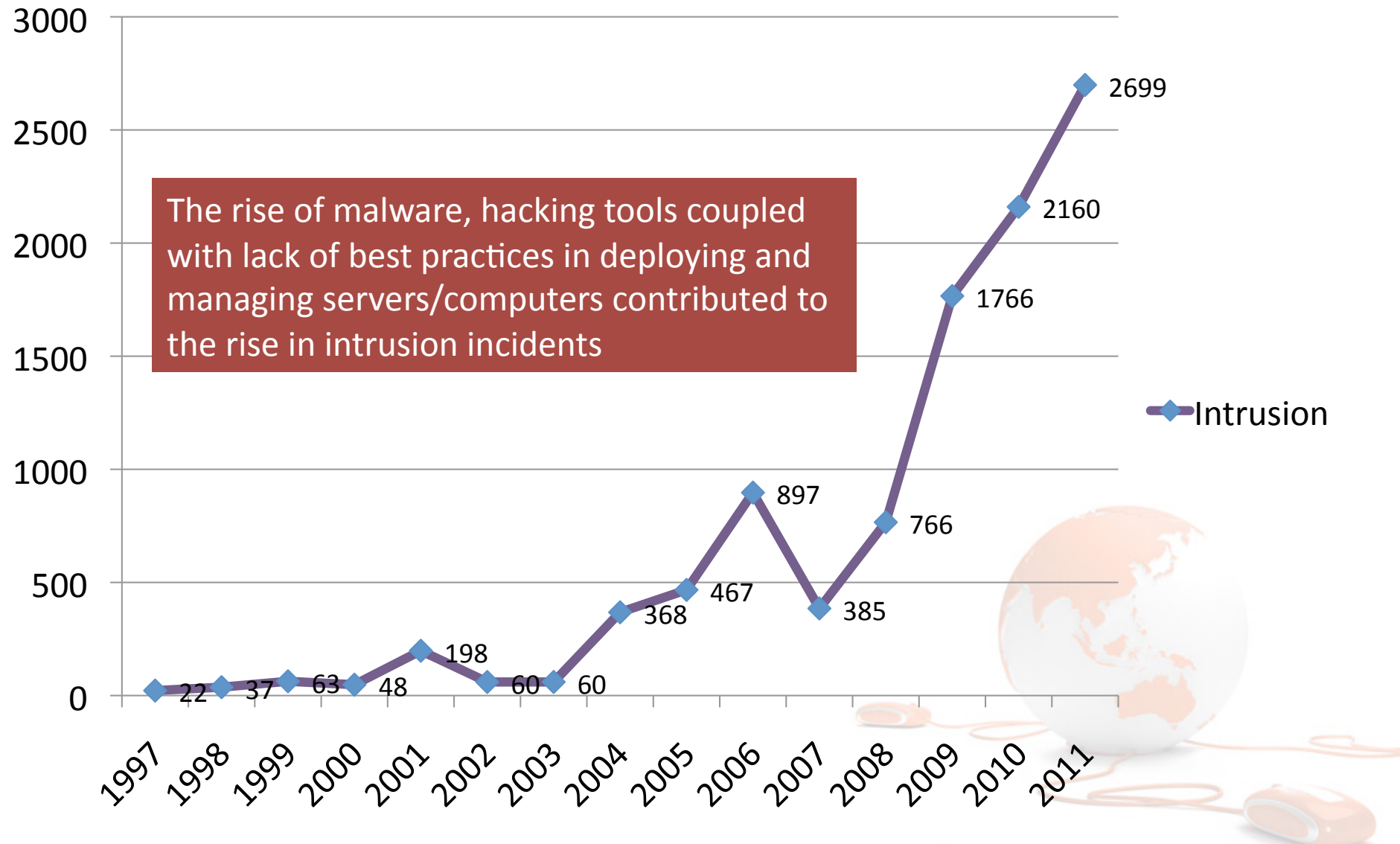


Source: www.mycert.org.my

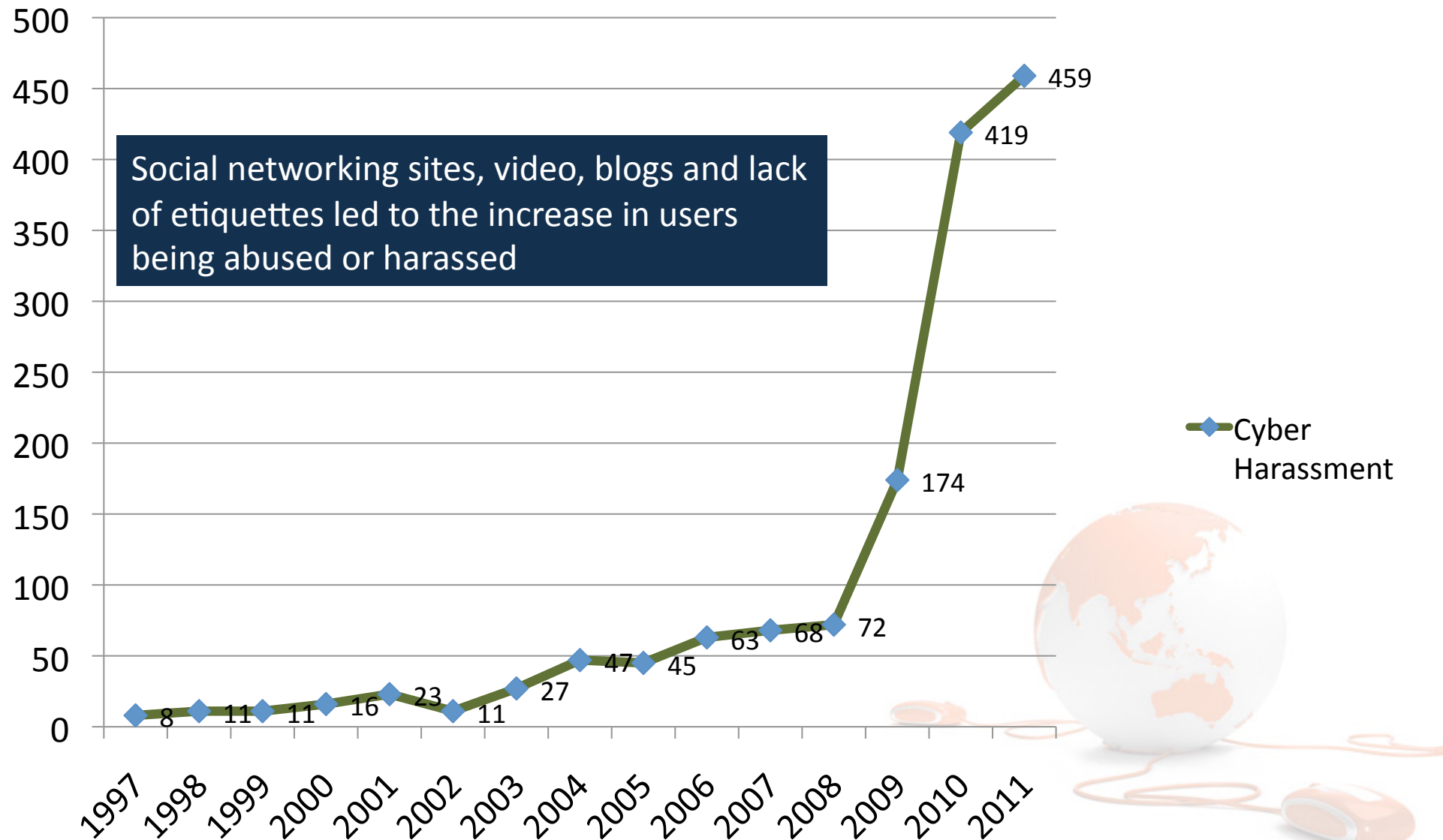
DDoS Incidents 1997 - 2011



Intrusion Incidents 1997 - 2011

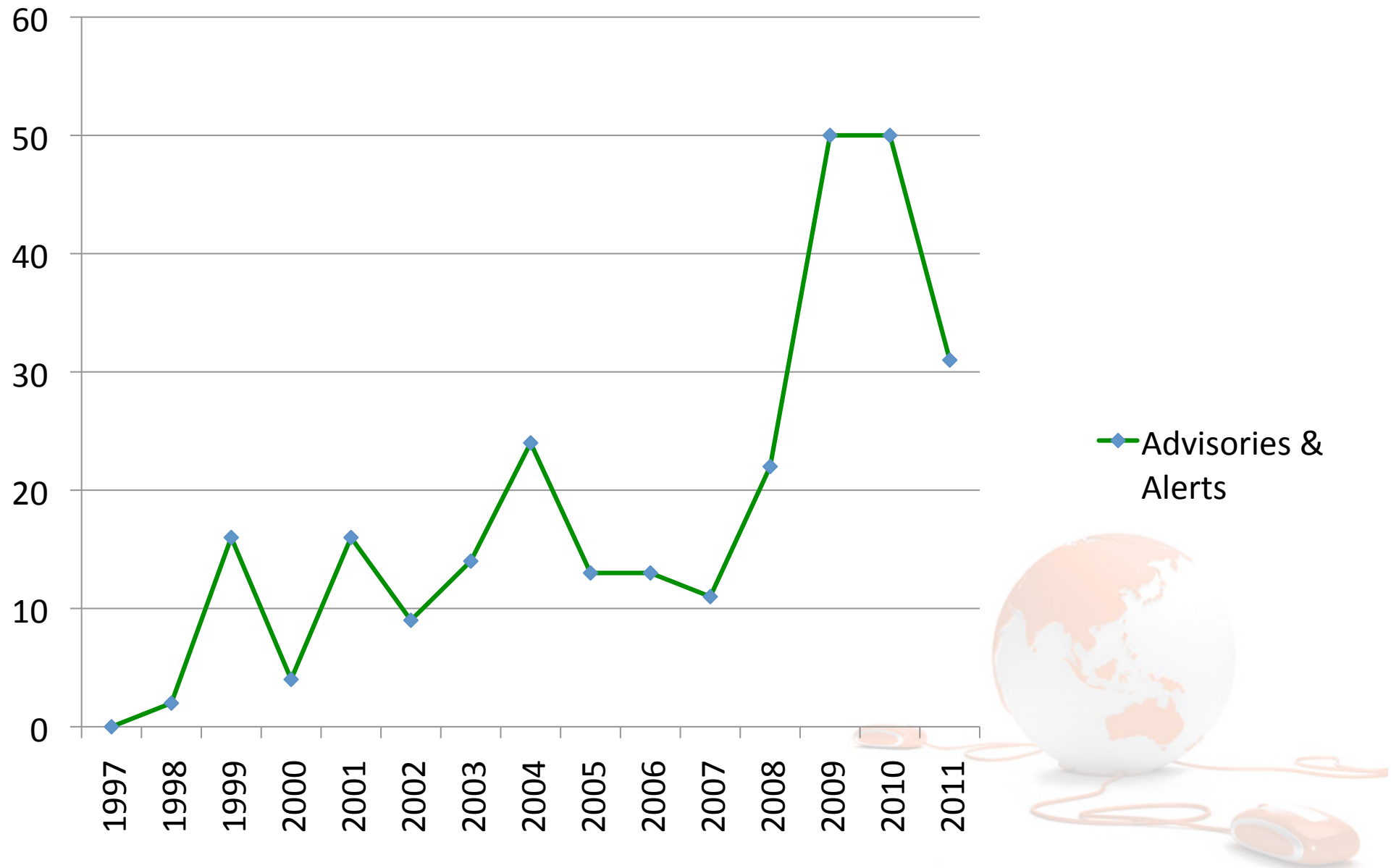


Cyber Harassment Incidents 1997 - 2011

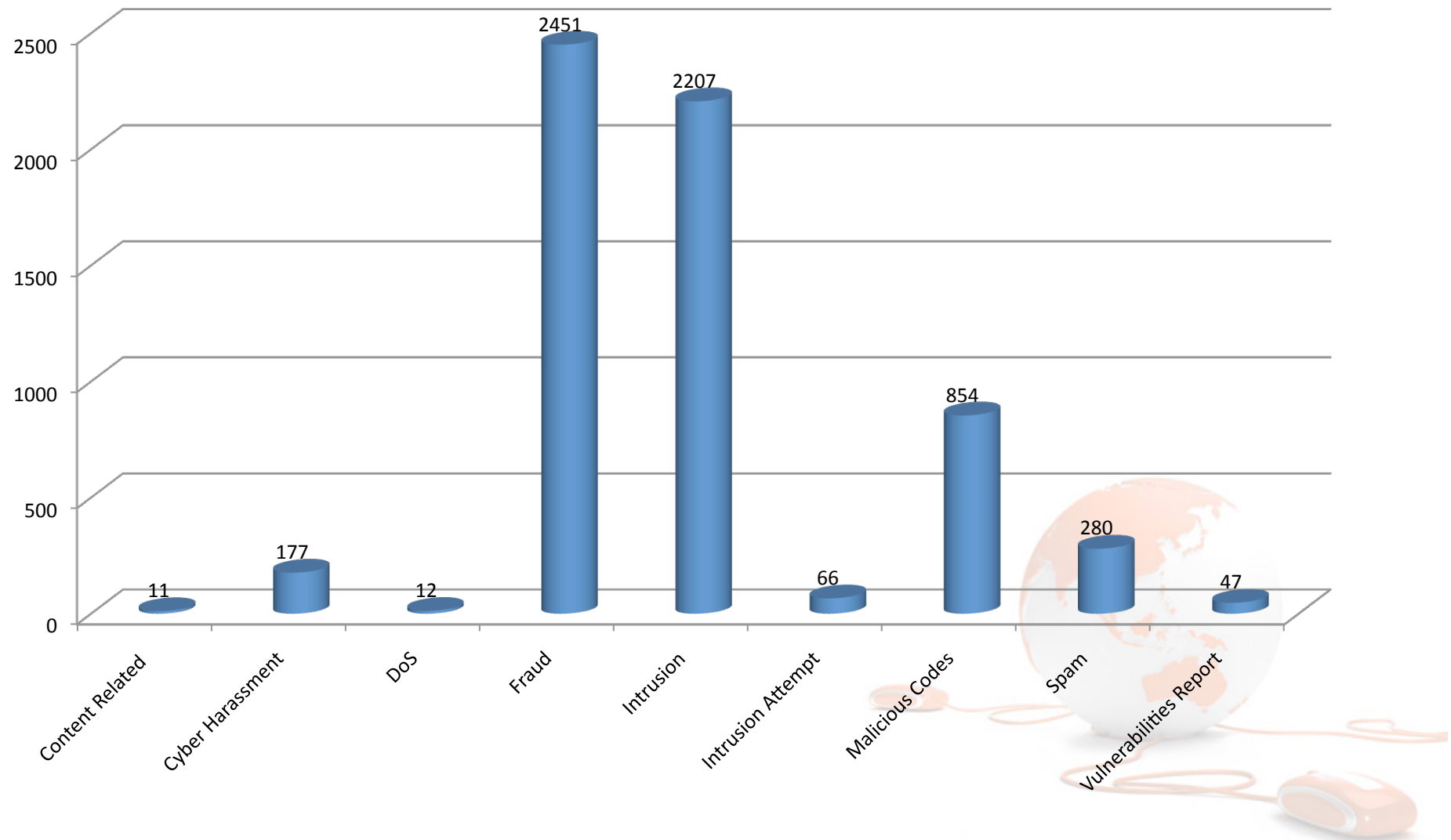


Source: www.mycert.org.my

Advisories & Alerts Published 1997 - 2011



Statistic by Incident (1st Half 2012)



Case Study



Case Study : Job Scam

- The Setup
 - Poses as a recruitment agency
 - Email sent to potential victim that really looking for job
 - Impersonate local MNC – usually in oil and gas industry
 - Victim most of it is not local

- What actual happen
 - Email sent usually spoof
 - Entice victim by giving job description / salary / attractive perk
 - Eventually a charge is required as a processing fee for Employment Registration Certificate / Visa / Registration Card

- The Risk
 - Money lost
 - Still end up without a job



From: petronas476@xyz.com

Subject: JOB OPPORTUNITIES@ PETRONAS OIL COMPANY MALAYSIA

Date: Wed, 22 Dec 2010 18:23:33 +0000

Dear Employee,

We have confirmed your CV/Resume, in the below mail you will find the current positions where expatriates are needed in our Company..

All the positions include these below benefits:

1. Five Bedroom Flat Duplex
2. Free Medical & Travel Insurance
3. 10 Days Leave / break/ Vacation after every 90 working days
4. Flight Fares (Air Tickets)
5. Free Toyota Camry 2007 Model.

- A. Current CV/Resume
- B. One Reference Letter.
- C. Passport Copy.

The Documents should be provide to us through scan e-mail attachment For fast processing, because all the positions need expatriates" who Can be able to start up employment on January/March 2011, and all the Arrangement need to be made as fast as possible.



Case Study : Job Scam (Sample)



We refer to your earlier forwarded application for job engagement with relations to **SAPURACREST PETROLEUM BERHAD (MALAYSIA)**

On the above subject matter **SAPURACREST PETROLEUM BERHAD (MALAYSIA)** hereby congratulates you on your successful emergence based on detailed by our career department.

Further details are as follows: **JOB REFERENCE NUMBER:**
SCP/01310/KLM

EMPLOYMENT AGREEMENT

We refer to your earlier forwarded application for job engagement with relations to **SAPURACREST PETROLEUM BERHAD (MALAYSIA)**

On the above subject matter **SAPURACREST PETROLEUM BERHAD (MALAYSIA)** hereby congratulates you on your successful emergence based on detailed by our career department.

Further details are as follows: **JOB REFERENCE NUMBER:**
SCP/01310/KLM

APPOINTMENT LETTER 11#03#20

NAJIM KAMAR DAHAM

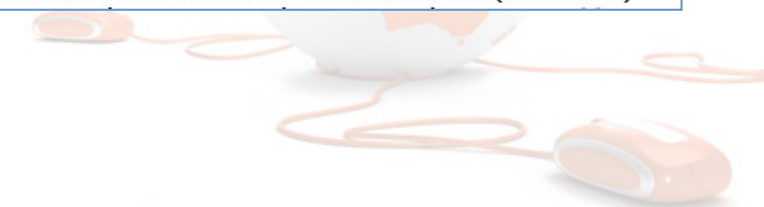
consideration in this contract, the **PETRONAS** employs the he following terms.

EMPLOYMENT: Subject to the provisions for termination set his agreement begins on **11th March 2011**, unless sooner

: SENIOR DESIGN ENGINEER

s duties may be reasonably modified at the **PETRONAS** n time to time.

SUME WORK DATE: 26th April 2011
NTRACT DURATION: Two (2) Years
B LOCATION: PETROLIAM NASIONAL BERHAD (PETRONAS)



Case Study : Fraud Purchase

- The Setup
 - Send in your money and get nothing
- What actual happen
 - Never get the product promised
 - Promises don't match the product
 - Product description may be vague, incomplete or completely fake
- The Risk
 - Get ripped off
 - Losing time and money



Case Study : Nigerian Scam

- The Setup

- Receive an email written in screaming capital letter or very lengthy

Example - "DEAR SIR/MADAM: I REPRESENT THE RECENTLY DEPOSED MINISTER OF AGRICULTURE FOR NODAMBIZIA, WHO HAS EMBEZZLED 30 MILLION DOLLARS FROM HIS STARVING COUNTRYMEN AND NOW NEEDS TO GET IT OUT OF THE COUNTRY..."

- Scammers are seeking an accomplice to transfer funds and you will get the cut – 10%
- But before transfer can be finalized you must pay for unnecessary advance fees

- What actual happen

- There is no minister and no money
- Except the money victim have put in advance

- The Risk

- Serious financial loss or worse
- Losing time and could probably threaten



Case Study : Fraud Site + Lottery/Sweepstake Scams

- The Setup
 - Selling product or services to potential victim
 - Company not legally registered
 - Perpetrated via mail which contain colorful brochure or scratch card
- What actual happen
 - One of the card always a winning card
 - To claim price always asked to provide payment for various fees via wire transfer
- The Risk
 - Serious financial loss
 - Losing time



Pro-Link International Express Courier

BRINGING YOU THE WHOLE PACKAGE

Instant Tracking

Search

- Home
- About Us
- Sustainability
- Careers
- Shipment Tracking
- Contact Us



Pace

BRINGING YOU URGENT COURIER SERVICES



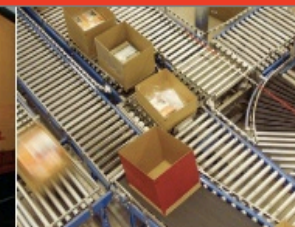
CourierPost

BRINGING YOU NEW ZEALAND'S MOST EXTENSIVE DELIVERY NETWORK



Roadstar

BRINGING YOU PALLETISED TRANSPORT SOLUTIONS



Contract Logistics

BRINGING YOU MANAGED WAREHOUSING AND DISTRIBUTION



TAKING CARE

[More Info](#)

Variable Fuel Rate
March 2010 2.70%

[More Info](#)

Welcome to Pro-Link

As UK & New Zealand's leading express courier, logistics and distribution company, Direct Post brings you The Whole Package.

Combining the capabilities of Pace, Courier Post, Roadstar and Contract Logistics, with the transport strength of New Zealand Post, our Whole Package brings you speed, reach and control within a customized solution for your business.

Direct Post is the partner of choice for a number of UK companies including ACP Media, Postie Plus, Ezibuy and OfficeMax. We proudly support worthwhile causes such as the Starship Foundation and KidsCan Charitable Trust as a way to support the New Zealand communities we operate in everyday.



What We Are Seeing



The Source of ~~all~~ A Lot of Evil

- Information Loss
- Financial Loss
- Badness
 - Denial of Service Attacks
- Your PC might be hosting malware or serving malware



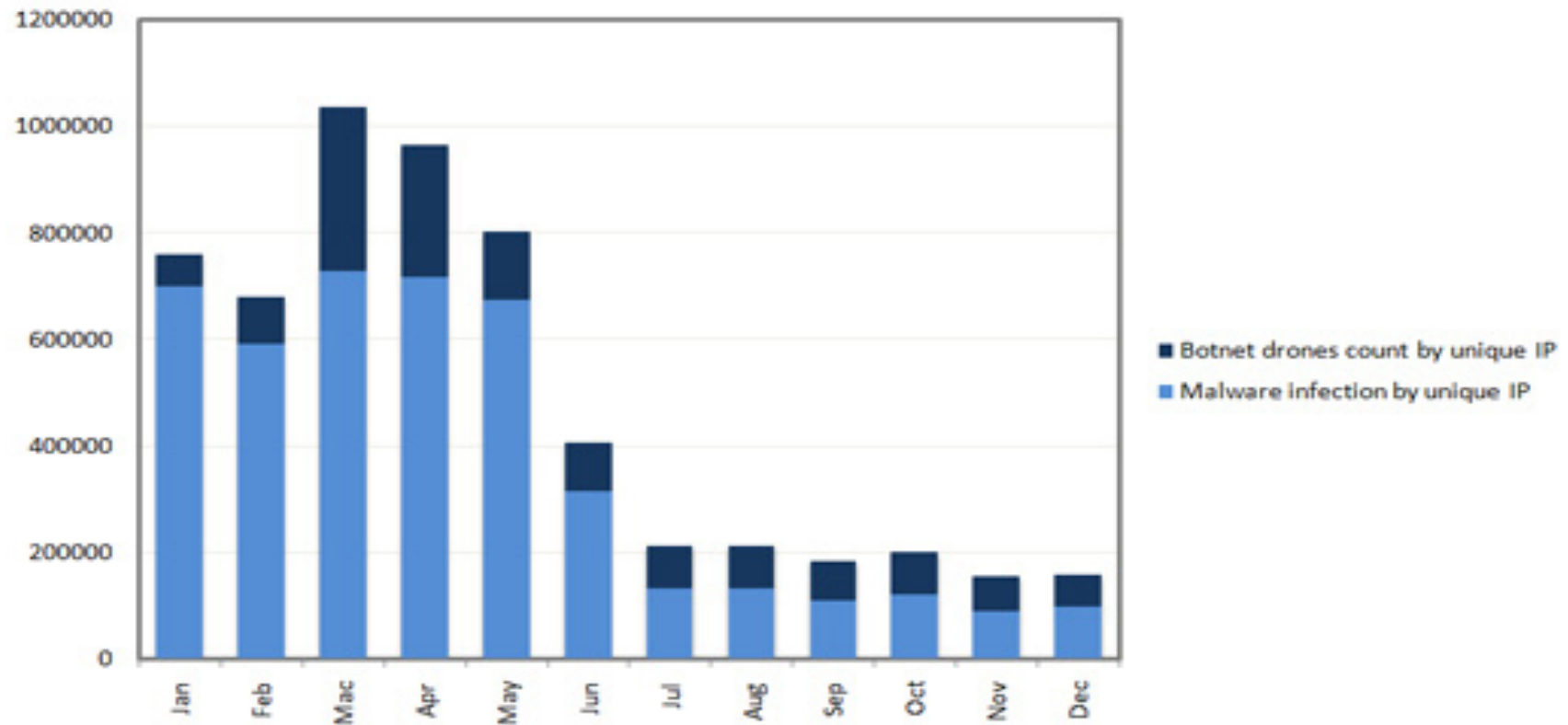
Malware Research Centre

- Malware Response since 1997
 - Infected Machines feeds
 - Command and Control take downs / Monitoring
 - Removing evilness* from servers/sites
 - Tracking and Analysis
 - Advisory and Alerts
 - “I think I got something in My PC” requests
 - Malware samples & Feed Exchange



Malware Incident 2011

Malaysia Botnet Drones and Malware Infection 2011



Malware Research Centre (MRC)

Projects/Activities



Innovative Tools Produced

<p>Malware Sandbox</p>	<p>AntiPhishing Plugin</p>	<p>Malicious PHP Analyzer</p>	<p>PHP WebApp IPS</p>
<p>PDF Analyzer</p>	<p>AntiPhishing Portal</p>	<p>.My Malware Project</p>	<p>DNS Watch – Site detection</p>

(FREE) Tools from the Lab



DontPhishMe!



DNSWatch



PKaji

More at http://www.mycert.org.my/en/resources/security_tools/main/main/detail/768/index.html

Dontphishme: Plugin for Firefox and Chrome

Mozilla Add-On: <https://addons.mozilla.org/en-us/firefox/addon/dontphishme/>

Chrome Add-On:

<https://chrome.google.com/webstore/detail/ekhmajimailppllbglbkopdjfenocpln>

Currently support local Financial Instituion / Bank at Malaysia

ADD-ONS

ADD-ons for Firefox > Extensions > DontPhishMe

DontPhishMe 1.5.2
by MyCERT

DontPhishMe is an Anti-Phishing addon for Mozilla Firefox which utilizes the pattern matching techniques to provide the Malaysian Internet user with information and notification to protect them against online banking phishing website.

[Continue to Download →](#)

Updated	April 29, 2011
Website	http://www.mycert.org.my
Works with	Firefox 2.0a1 - 4.2a1pre
Rating	★★★★★ 3 reviews
Downloads	5,079

[Add to collection](#)
[Share this Add-on](#)

ADD-ONS

EXTENSIONS | PERSONAS | THEMES | COLLECTIONS | MORE...

search for add-ons

Welcome to Firefox Add-ons. Choose from thousands of extra features and styles to make Firefox your own.

» Extensions » DontPhishMe

DontPhishMe 1.6.0
by Adnan Mohd Shukor

★★★★★
3 user reviews
953 users

DontPhishMe is an Anti-Phishing addon for Mozilla Firefox which utilizes the pattern matching techniques to provide the Malaysian Internet user with information and notification to protect them against online banking phishing website.

[Continue to Download →](#)

[Add to collection](#)
[Share this Add-on](#)

[About this Add-on](#)
[Add-on home page](#)



Why Are You Here

APWG Committed to wiping out internet scams and fraud
www.antiphishing.org

Carnegie Mellon
CyLab
Supporting Trust Decisions Project
cups.cs.cmu.edu/trust



WARNING!

The web page you tried to visit might have been trying to steal your personal information. That page was removed after being identified as a "phishing" web page. A phishing web page tricks people out of bank account information, passwords and other confidential information.

How You Were Tricked

This email is from my bank. It asks me to update my information. I better click on the link and update it.

STOP!
Don't fall for

How to Help Protect Yourself

- 1 Don't trust links in an email.
DANGER! <http://www.amazon.com/update>
- 2 Never give out personal information upon email request.
DANGER! Name:
- 5 Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.

Credit Card Statement
For Customer Service

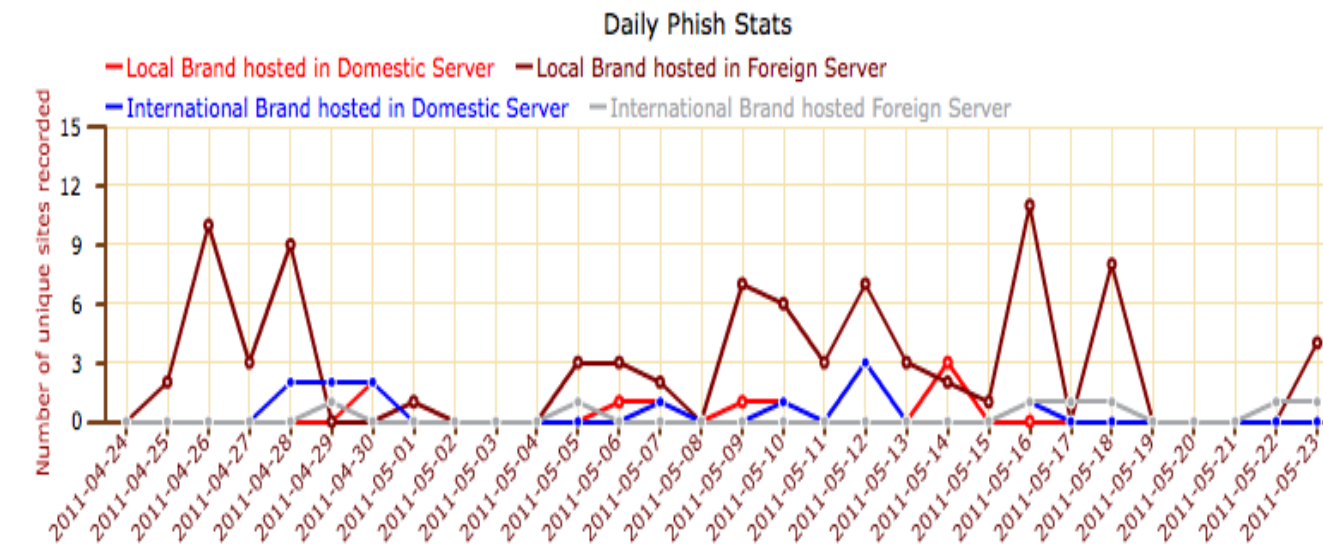


Submit to us the suspicious links and let us verify

REPORT HERE

Received a phishing email? Send it to us by forwarding the email that contains the URL. Our incident response team will help in verifying the submitted URLs and taking necessary actions.

MyCERT collects and handles URLs related to phishing. In the table below, you can find the latest URLs used in phishing scams.



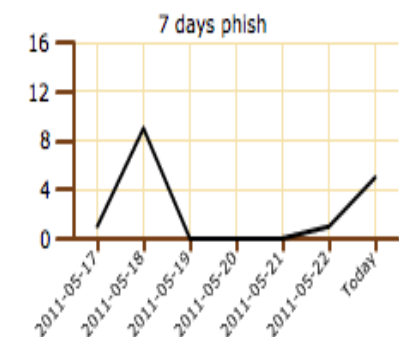
*Please contact us to get more details on the phishing URL

What is Antiphishing.my?

Antiphishing.my is a portal that provides information related to phishing sites targeting Internet users in Malaysia. We hope that this work will help to make the Internet a safer place for everyone.

[Better viewing with firefox, chrome or safari](#)

Quick Stats



Upcoming Events

counter ecrime operations summit

DNSWatch (Service)

- Released in August 2011 as a service
- Started initially as a different project (DNSMon) as a result of monitoring conficker infected clients querying known_malicious_dns
- What do we do with a list of known 'bad' URLs?
 - From honeypots and other public/non-public sources
- We offer a DNS Service, when users visit a potentially malicious site that has been blacklisted, redirect to a landing page
 - This will alert and hopefully get user curious enough to fix the problem




DNSwatch (alpha version)

http://landingpage.mycert.org.my/?url=[REDACTED]9.com

Apple Yahoo! Google Maps YouTube Wikipedia

Oops.. you are redirected to DNSwatch landing page



The page that you are trying to access is known to be hosting malware




You are trying to access a [REDACTED]9.com which is associated with known malicious domain. For more information please contact us

WARNING: visiting this site may harm your computer

[go back](#)

False positive? Report to [honeyne\[at\]cybersecurity.my](mailto:honeyne[at]cybersecurity.my)

DNSwatch (alpha version)
Brought to you by



DNSChanger Malware Cleanup

- What is DNSChanger
 - malware that infect computers with the purpose of diverting traffic to potentially illegal and malicious websites. The malware modifies the infected computer's DNS server setting replacing it with DNS server belonging to the attackers.
- MyCERT Advisory
 - <http://www.mycert.org.my/en/services/advisories/mycert/2012/main/detail/855/index.html>



DNSChanger Malware Cleanup

- Detection (<http://dnschanger.detect.my>)
- Removal Step available at MyCERT website
http://www.mycert.org.my/en/resources/security_tools/main/main/detail/854/index.html

The screenshot shows the DNSChanger detection page. At the top, there is a navigation bar with links for Home, Removal, About, and Contact. Below the navigation bar are logos for CyberSecurity MALAYSIA, MyCERT (Malaysia Computer Emergency Response Team), and DCWG. The main content area features a 'Welcome' message stating that the user is at the DNSChanger detection page operated by MyCERT, with a 'Learn more »' button. A large green box contains the heading 'DNSChanger Check-Up' and a message: 'Congratulations! Your system appears to be looking up IP address correctly. If you are infected by DNS Changer, you would have seen a red background.' Below this, there is a section titled 'What is DNSChanger?' which explains that DNSChanger is malicious software that changes DNS settings to divert traffic to illegal sites. It also mentions that in November 2011, the FBI closed down a ring of cyber-criminals responsible for the worldwide spread of DNSChanger, affecting an estimated four million users. To avoid internet service loss, the FBI worked with the Internet Systems Consortium (ISC) to set up a temporary DNS solution.

DNSChanger Malware Cleaning

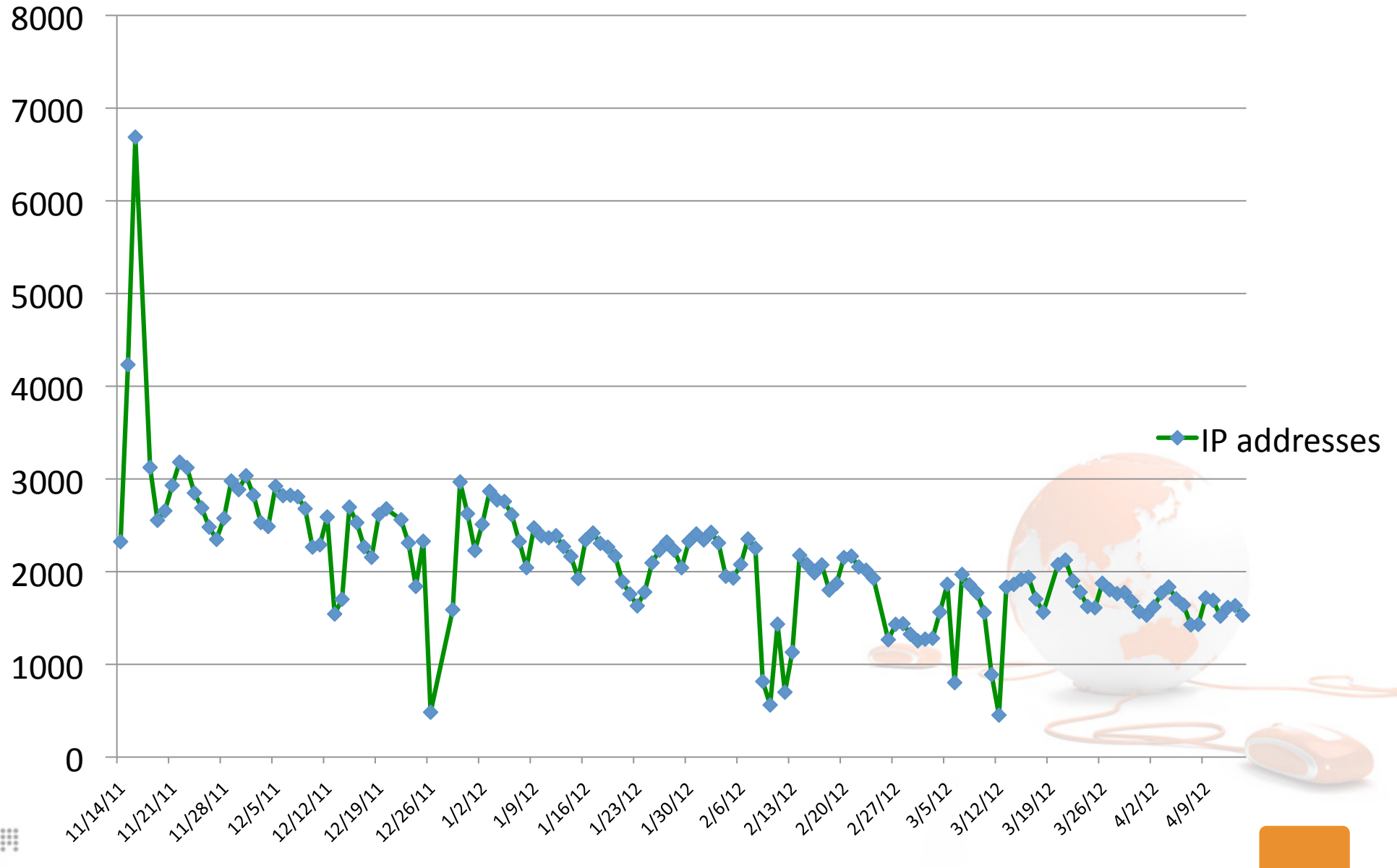
The image is a collage of four main components related to DNSChanger malware cleaning:

- Top Left:** A browser window titled "DNSChanger Landing Page" showing a "Welcome" message and navigation links like "Home" and "Removal".
- Top Center:** A browser window displaying a "MyCERT Alert - DNSChanger Malware" advisory. The alert title is "MA-308.042012 : MyCERT Alert - DNSChanger Malware". It includes an introduction and instructions for users.
- Bottom Left:** A green banner titled "DNSChanger Check-Up" with a shield icon containing a checkmark. The text reads: "Congratulations! Your system appears to be looking good. If you are infected by DNS Changer, you would have seen this message." Below it, a section titled "What is DNSChanger?" explains that it is malicious software that changes DNS settings.
- Bottom Right:** A "Change DNS" dialog box titled "DNSChanger Removal v0.1.23". It contains the message: "Your DNS configuration has been modified by the DNSChanger malware. Please reset your DNS with one of the following options:" followed by radio button options: DHCP, Enter DNS server IP address manually (Ask your IT administrator), Google DNS, and MyCERT's DNSWatch. A note at the bottom says: "Note: Please email cyber999@cybersecurity.my if you need assistance." and a "Change" button is at the bottom right.

Figure 3. Option for user to change their DNS setting



DNS Changer: IP Addresses Count – Based on Reports from Shadow Server Foundation



Awareness

- CyberSAFE Project
 - Cyber Security Awareness for Everyone
 - <http://www.cybersafe.my>
- Addresses amongst other things, Phishing and ID Theft issues
- Engagement with Media and Public to promote the message
- Production of educational materials (feel free to re-use)



Publish Advisory / Alert / News

- Came out with advisory

“MA-228.042010:MyCERT Advisory - Phishing Attempts Targeting Public Bank Malaysia Users”

<http://www.mycert.org.my/en/services/advisories/mycert/2010/main/detail/749/index.html>

“MA-276.042011:MyCERT Alert – Job Scam On the Net”

<http://www.mycert.org.my/en/services/advisories/mycert/2011/main/detail/815/index.html>

- Publish newspaper article

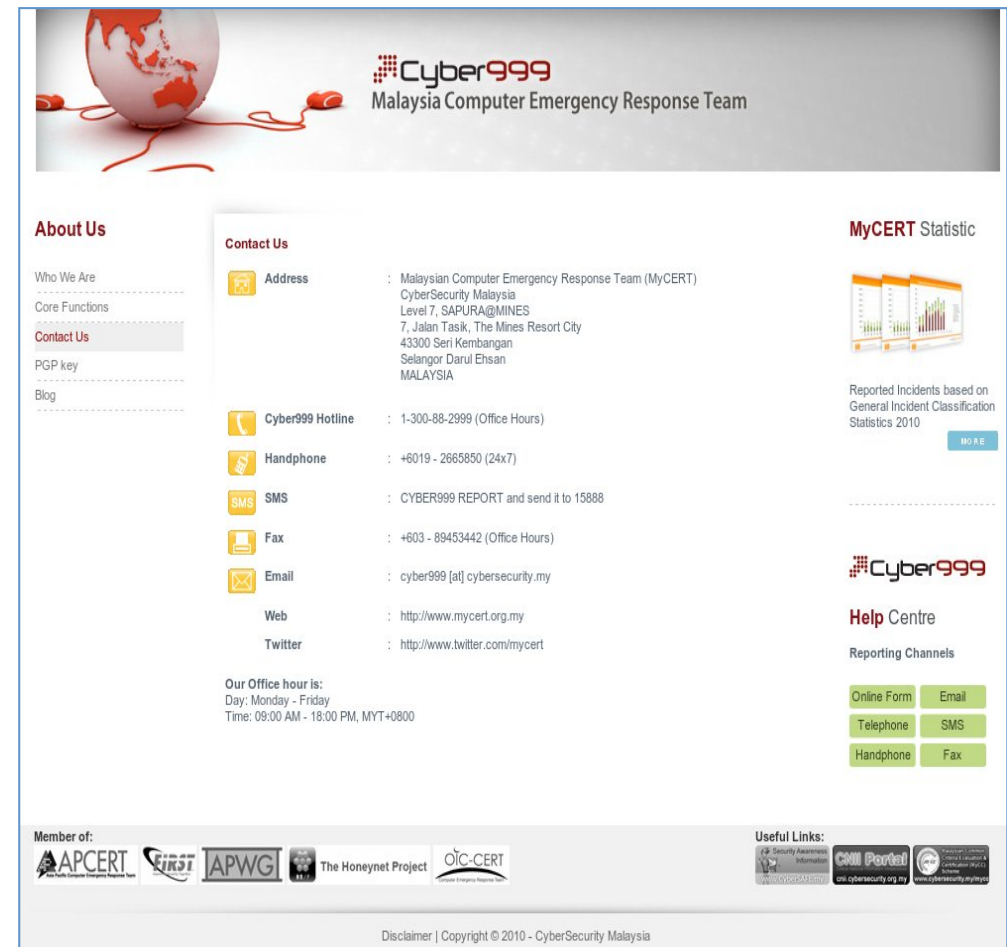
“Steer clear of phishing sites”

<http://thestar.com.my/news/story.asp?file=/2010/4/21/focus/6095783&sec=focus>



Mode of Incident Reporting

- Email
 - cyber999@cybersecurity.my
- Phone/Hotline
 - +603 8992 6969
 - 1 300 88 2999
- Fax
 - +603 8945 3442
- SMS
 - 1 5888 “Cyber999 Report”
- Mobile (24x7)
 - +6019 266 5850
- Online – <http://www.mycert.org.my>
- Walk In - Office Hours: MYT 0830 – 1730



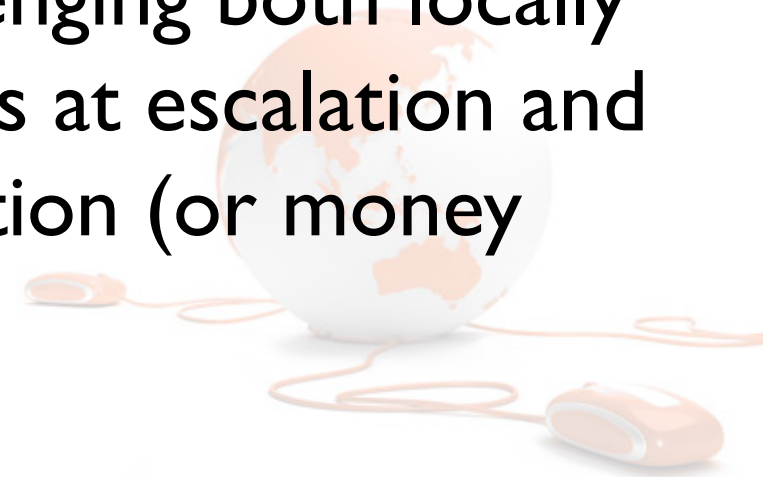
The screenshot shows the website for Cyber999 Malaysia Computer Emergency Response Team. The header features a globe icon and the text "Cyber999 Malaysia Computer Emergency Response Team". The main content area is divided into several sections:

- About Us:** Includes links for "Who We Are", "Core Functions", "Contact Us", "PGP key", and "Blog".
- Contact Us:** A central section listing various contact methods:
 - Address:** Malaysian Computer Emergency Response Team (MyCERT), CyberSecurity Malaysia, Level 7, SAPURA@MINES, 7, Jalan Taski, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, MALAYSIA.
 - Cyber999 Hotline:** 1-300-88-2999 (Office Hours)
 - Handphone:** +6019 - 2665850 (24x7)
 - SMS:** CYBER999 REPORT and send it to 15888
 - Fax:** +603 - 89453442 (Office Hours)
 - Email:** cyber999 [at] cybersecurity.my
 - Web:** <http://www.mycert.org.my>
 - Twitter:** <http://www.twitter.com/mycert>
- MyCERT Statistic:** A section with a bar chart and the text "Reported Incidents based on General Incident Classification Statistics 2010".
- Help Centre:** A section titled "Reporting Channels" with buttons for "Online Form", "Email", "Telephone", "SMS", "Handphone", and "Fax".

At the bottom, there is a "Member of:" section with logos for APCERT, FIRSI, APWGW, The Honeynet Project, and OIC-CERT. A "Useful Links:" section includes "Security Awareness Information", "CNN Portal", and "CyberSecurity Malaysia". A footer contains the text "Disclaimer | Copyright © 2010 - CyberSecurity Malaysia".

Success and Challenges (I)

- A “I-Stop-Centre” work to a certain extent. Incidents experienced by Public and Private Organizations and Individuals provided the bigger picture for the stakeholders
- Cost savings is there but no hard data
- End-to-end resolution is challenging both locally and internationally. Often stops at escalation and does not translate to prosecution (or money returned in the case of Fraud)



Success and Challenges (2)

- Being able to focus allow expertise to be developed. The CERT were able to release tools and services to deal with problem of the day
 - i.e. DontPhishMe!, PDF Analyzer, LebahnetMini (Honeypot)
- Lessons learned can be translated into awareness materials. But how do we measure the state of awareness? Number of incidents keep to continue
 - See www.cybersafe.my



Conclusion

- Security incidents happen!
- Managing security incidents is critical both at the enterprise, country and global level
- Having a dedicated team to handle incidents will ensure that potential damaged is contained and lessons can applied for improvements to steer other initiatives



Thank you

Corporate Office

CyberSecurity Malaysia,
Level 8, Block A,
Mines Waterfront Business Park,
No 3 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan, Malaysia.

T : +603 8946 0999
F : +603 8946 0888
H : +61 300 88 2999

www.cybersecurity.my
info@cybersecurity.my



www.facebook.com/CyberSecurityMalaysia



twitter.com/cybersecuritymy



www.youtube.com/cybersecuritymy



Best Brand
Internet Security
2008 & 2009



CERTIFIED TO ISO/IEC 27001:2005
CERT. NO. : AS4026



MS ISO/IEC 17025
TESTING
SAMM NO. 458
MYRIF LABORATORY

