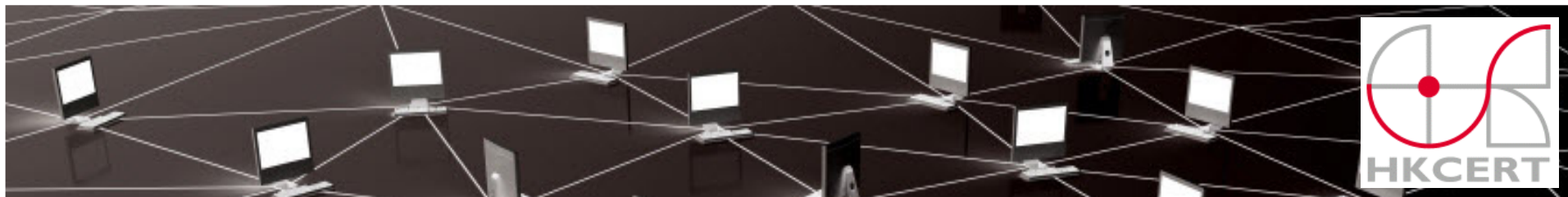


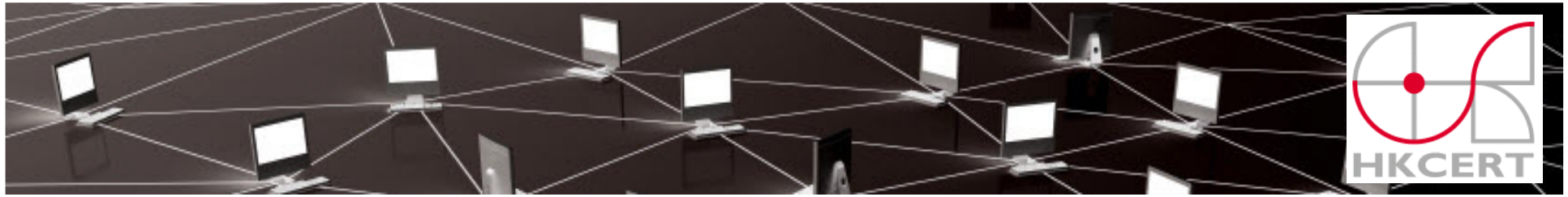
# Security Trend of New Computing Era

Presented by Roland Cheung  
HKCERT

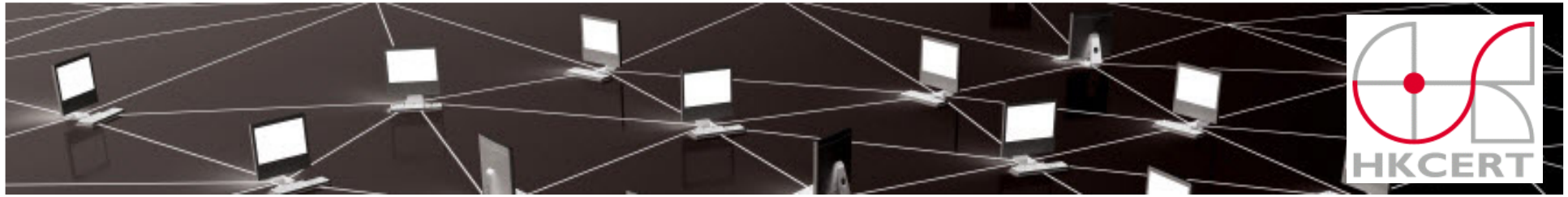


## Agenda

- Security Threat Overview
- Introduction of Botnet
- Impact of Botnet
- Fight Back Botnet
- Security Protection Scheme

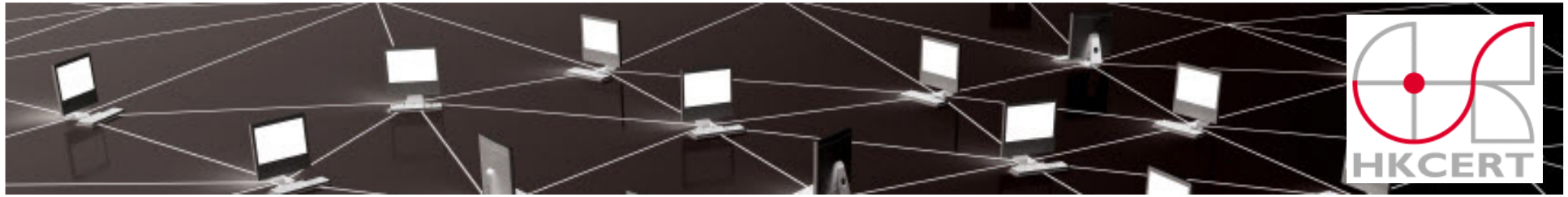


# Security Threat Overview



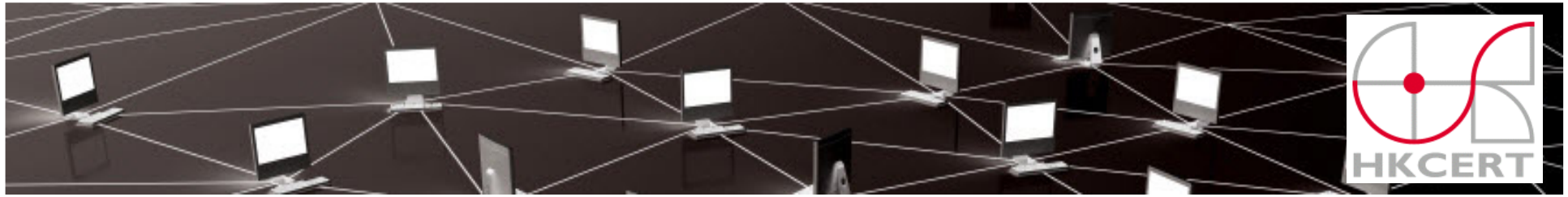
# Security Threat - Trend

- Cloud Computing
  - Data
- Social Network
  - Privacy
- Mobile Security
  - Apps



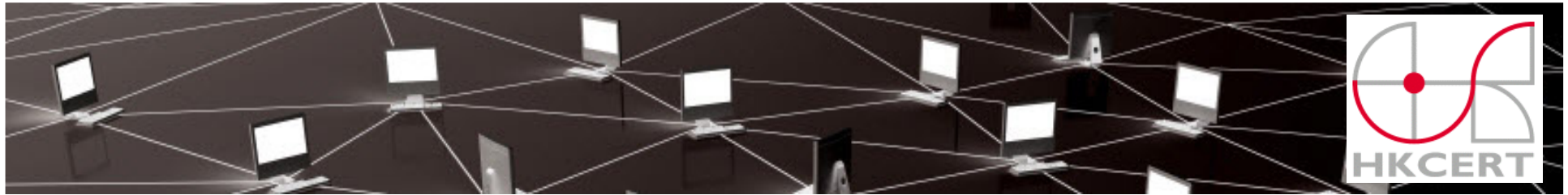
## Security Threat - Type

- Phishing/Defacement
- Malicious Code Injection / SQL Injection
- Distributed Denial of Service (DDoS)
- Malware
- **Botnet**
- etc...



# Security Threat - Impact

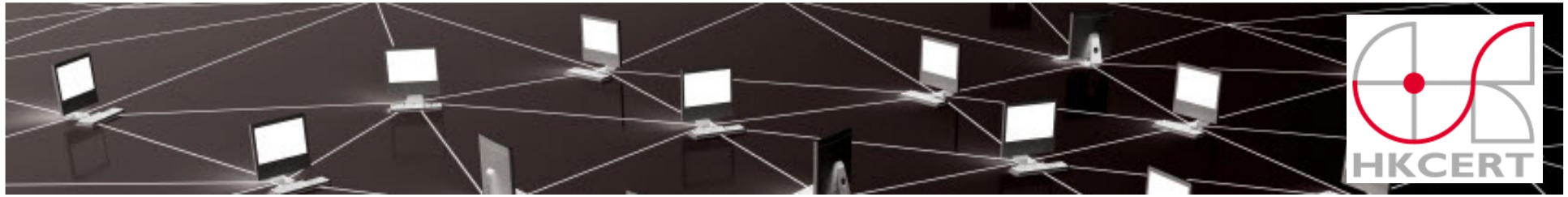
- Financial Loss
- Data Loss
- Identity Theft
- Service unavailability



# Security Threat -Underground Economy

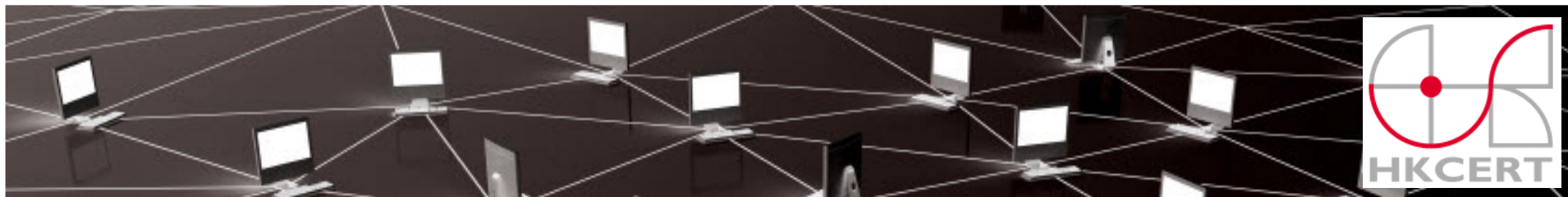
| Rank | Item              | Percentage | Range of Prices               |
|------|-------------------|------------|-------------------------------|
| 1    | Credit cards      | 28%        | \$1 - \$30                    |
| 2    | Bank accounts     | 24%        | \$10 - \$125                  |
| 3    | Email accounts    | 8%         | \$5 - \$12                    |
| 4    | Email addresses   | 5%         | \$5 - \$10 per MB             |
| 5    | Credit card dumps | 4%         | No specified prices           |
| 6    | R57 & C99 shells  | 3%         | \$2 - \$5                     |
| 7    | Full identity     | 3%         | \$3 - \$20                    |
| 8    | Mailers           | 3%         | \$1 - \$5                     |
| 9    | Attack toolkits   | 3%         | \$5 - \$20 or \$120 per month |
| 10   | Cash-out services | 2%         | \$200 - 100 or 50% - 70%      |

Fig 1 - Sales ranking on underground economy (Source from Symantec)



# Introduction of Botnet



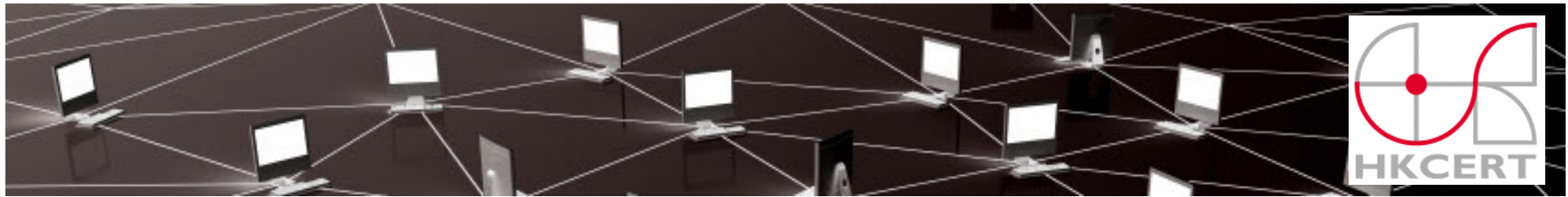


## What is Botnet?

- Botnet (aka Zombie Network, 殭屍網路)
- A collection of compromised computers (called bots, zombie) under a common command-and-control (called C&C) infrastructure.

<http://en.wikipedia.org/wiki/Botnet>





# Botnet Structure

- Bot Herder/Master
- Command and Control Servers (C&C, C2)
- Bots

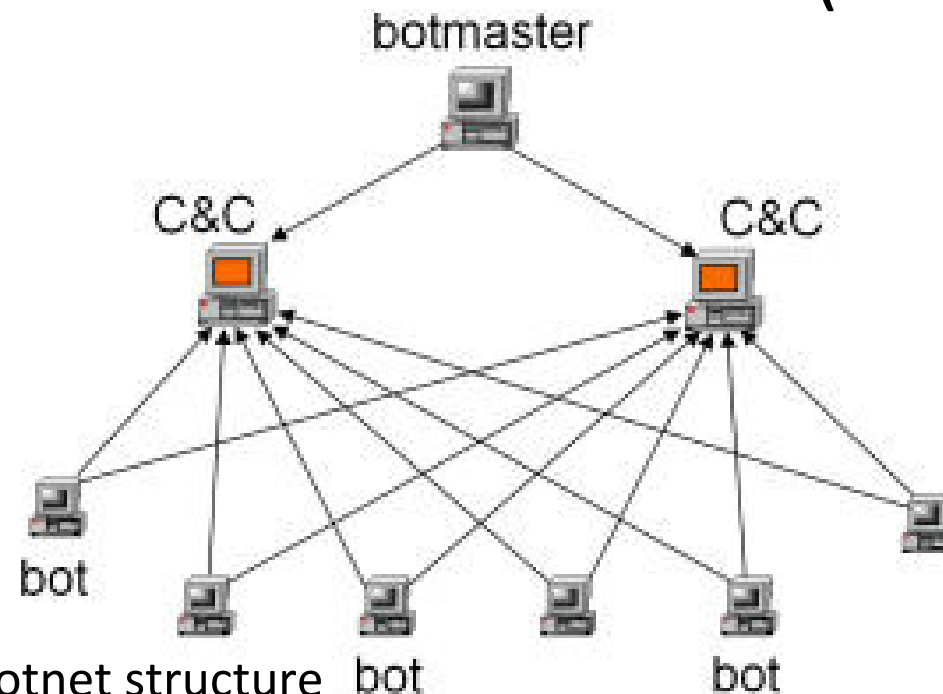
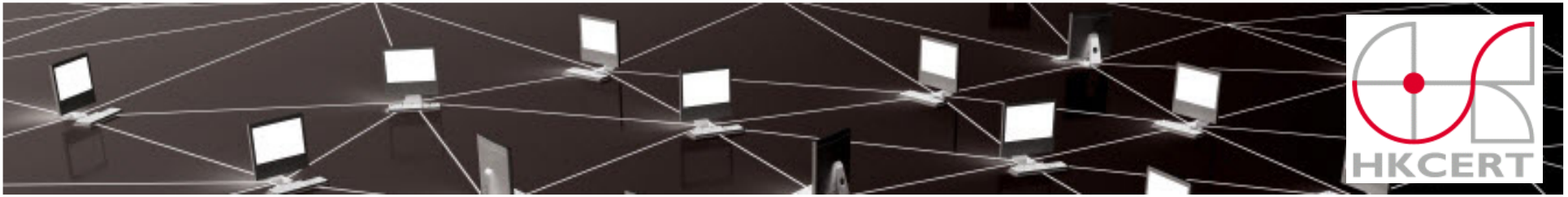


Fig 2 - Typical Botnet structure



## Spread Channel

- Website
- Email
- Instant Messenger (IM)
- P2P file sharing network
- Mobile device application



# Website

- Code Injection
  - Hidden iframe direct to the malicious website contains vulnerability exploit
  - 1H of 2010, over 2,500 Common Vulnerabilities and Exposures (CVE) recorded. Apple is top vendors of CVE, issued about 180.

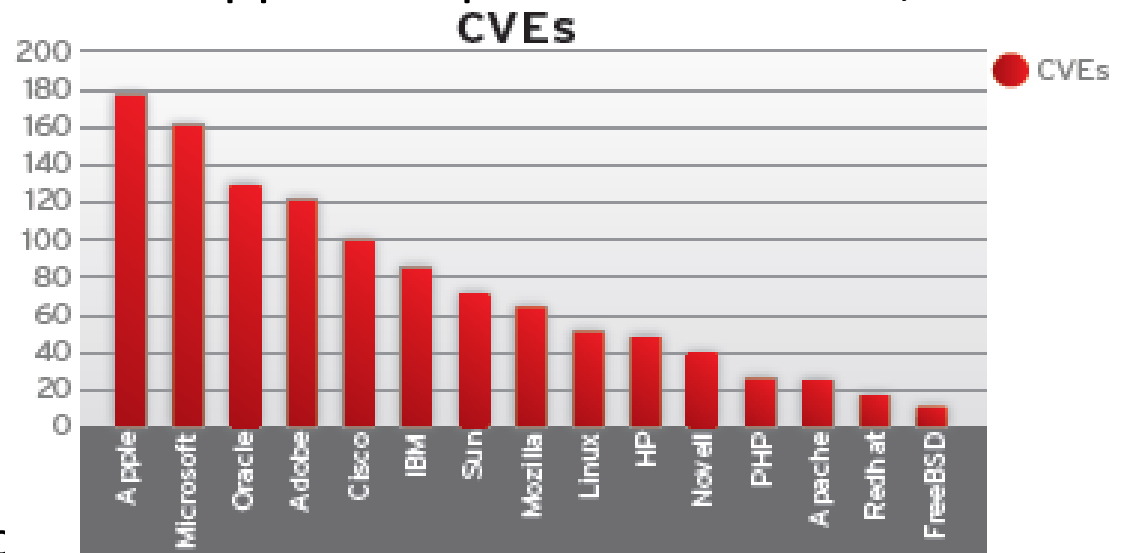
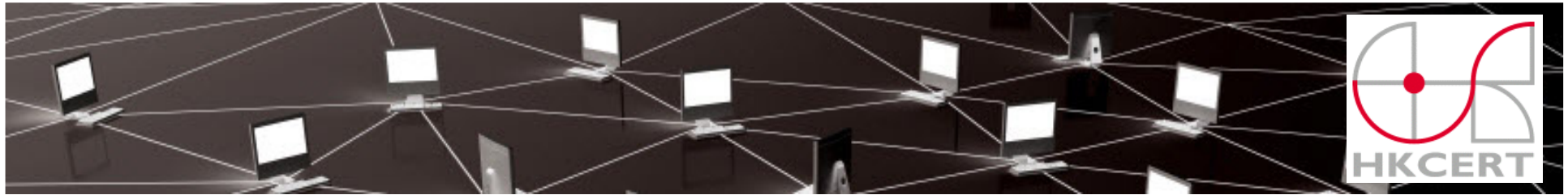


Fig 3 - Source from Trend Micro



# Website

- Malicious Multimedia Content
  - Exploit media player vulnerability
  - Malicious codec file installation

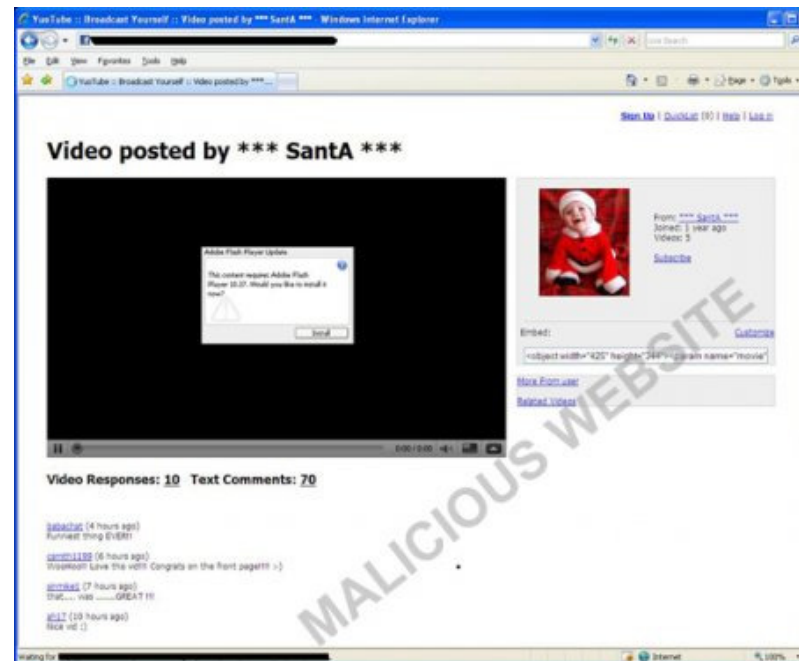
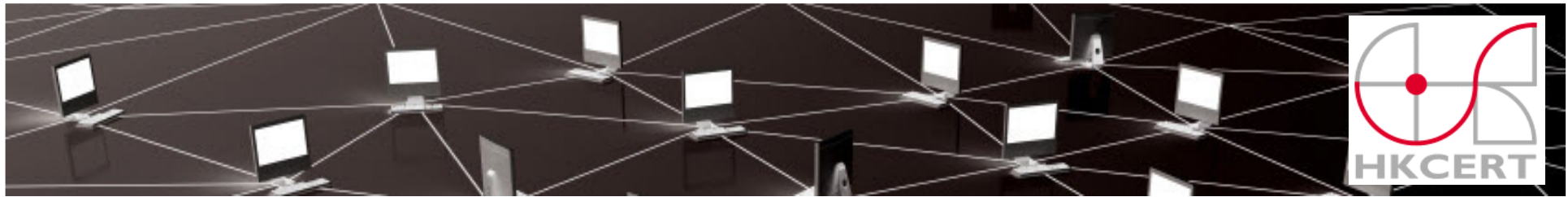


Fig 4 – Fake YouTube website delivers malware (Kooface)

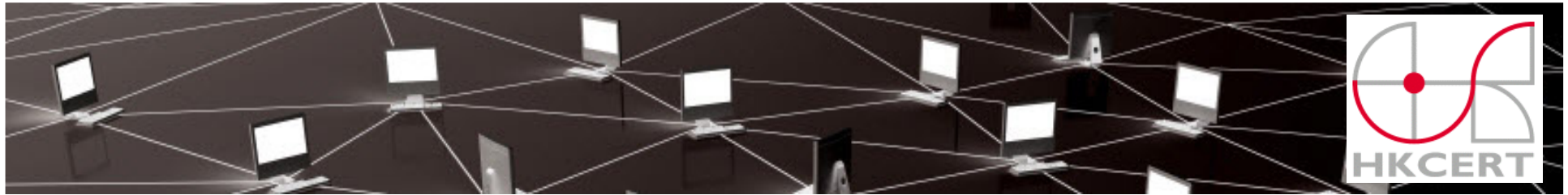


# Website

- Search Engine Optimization Poisoning (aka Black hat SEO)
  - Using unethical SEO techniques in order to obtain a higher search ranking to post malicious link on hot topic
  - Deliver Fake AV

The image illustrates a black hat SEO exploit. On the left, a Google search result for 'Prince William Engagement Ring' is shown, featuring a search bar and several search results. On the right, a Windows Security Alert window is displayed, indicating that a system scan has completed and 271 files have been scanned. The alert lists several detected trojans: Address.Trojan, zserv.Transponder.Tr, and Wstart.TrojanDownlo. A 'File Download - Security Warning' dialog box is also visible, asking if the user wants to run or save the file 'inst.exe'.

Fig 5 - Black hat SEO exploit Google search

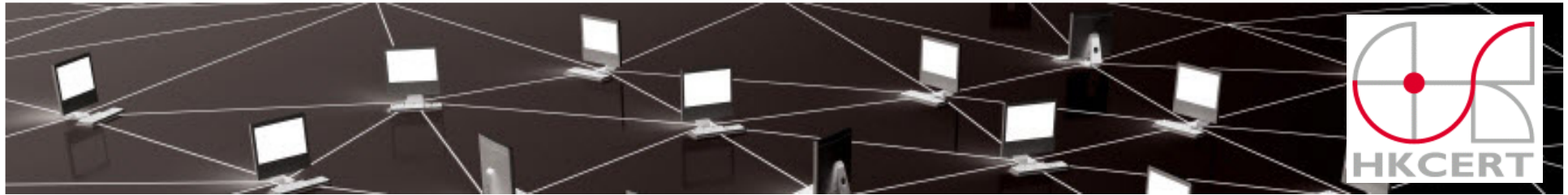


## Website

- Malvertising (malicious advertising)
  - Use of online advertising to spread malware



Fig 6 - In Apr 2010, malicious advertisement display fake security warnings

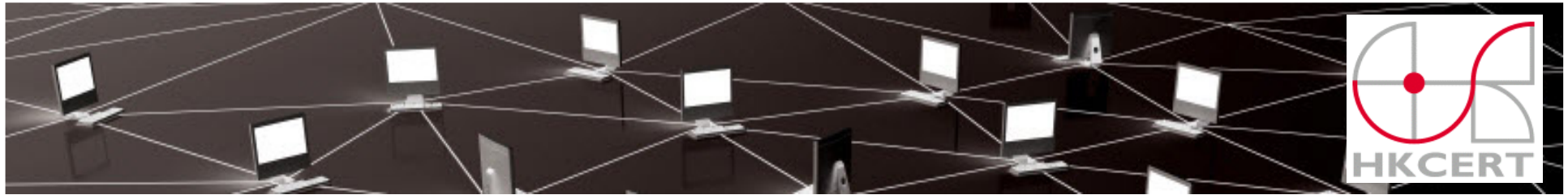


# Email

- Malicious attachment
  - Ms office document, .doc, .xls, .ppt
  - .pdf
  - .lnk
  - .swf
- Malicious link embedded

E.g. Pushdo, Waledac, Kooface

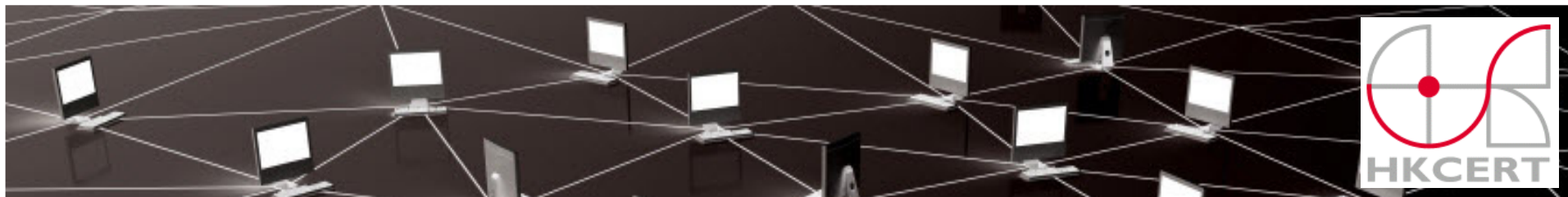




# Instant Messenger

- MSN, QQ
  - Embedding link
  - File transfer

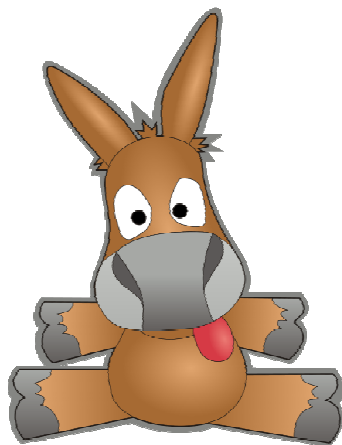
E.g. Mariposa



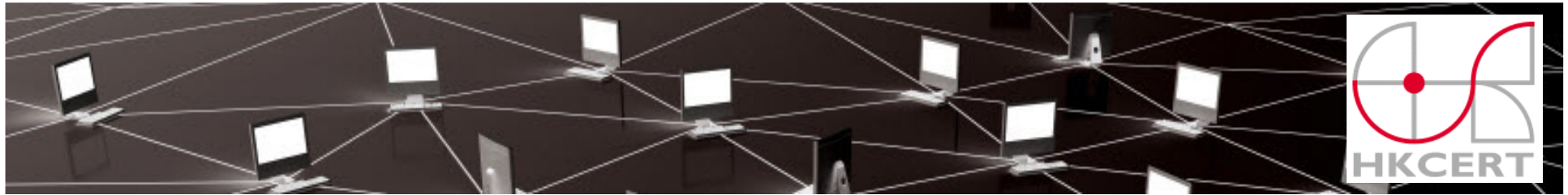
## P2P File sharing network

- BT, eMule, Foxy etc.

- 

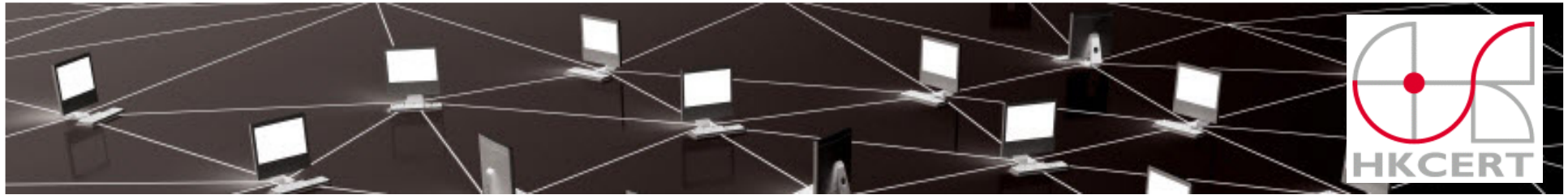


E.g. Storm, Waledac, Nugache

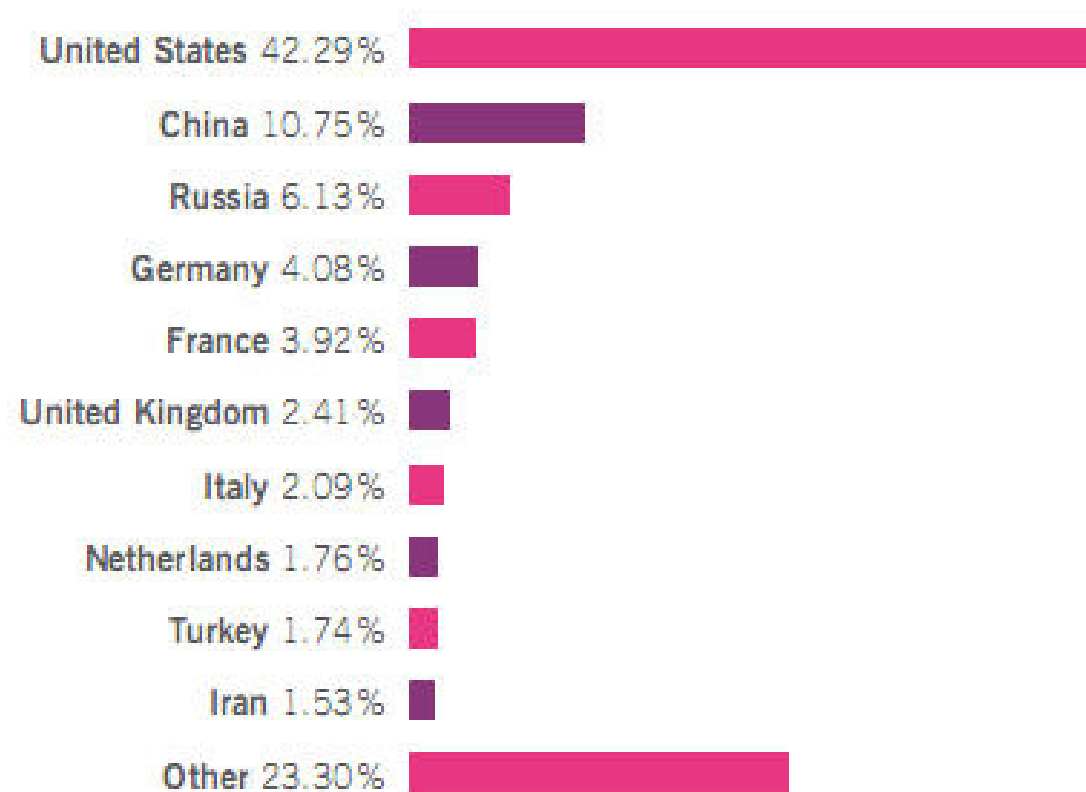


## Mobile Device Application

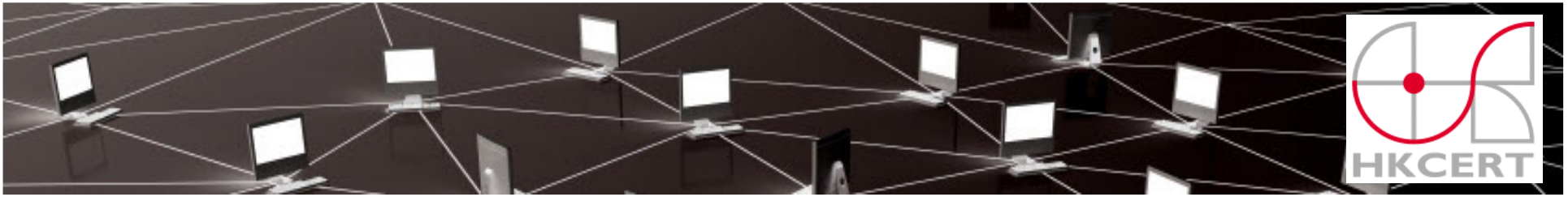
- Zeus ver 2.0, Man in the mobile (Mitmo)
- Reported in Sep 2010
- Installed in mobile devices like BlackBerry and Symbian mobile phones
- Sniff all the SMS messages that are being delivered.
- Steals both the online username and password



# Malware

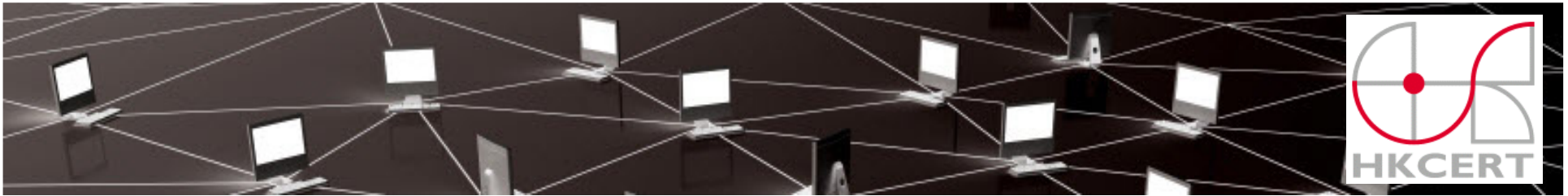


- Fig 7 - Top 10 malware hosting countries (Source from SOPHOS)



# Communication Channel

- IRC
- HTTP/HTTPS
- P2P
- Twitter



# Twitter

twitter Home Profile Find People Settings Help Sign out

**o\_o upd4t3**

Follow

**aHR0cDovL2JpdC5seS8xN2EzdFMg**  
about 2 hours ago from web

aHR0cDovL2JpdC5seS9MT2Z2STyBodHRwOi8vYml0Lmx5L0ltZ2  
about 2 hours ago from web

aHR0cDovL2JpdC5seS8xN2w0RmEgaHR0cDovL2JpdC5seS8xN  
about 4 hours ago from web

aHR0cDovL2JpdC5seS9wbVN1YyBodHRwOi8vYml0Lmx5LzE3b  
about 4 hours ago from web

Name upd4t3  
20 following 7 followers

Tweets 25

Favorites

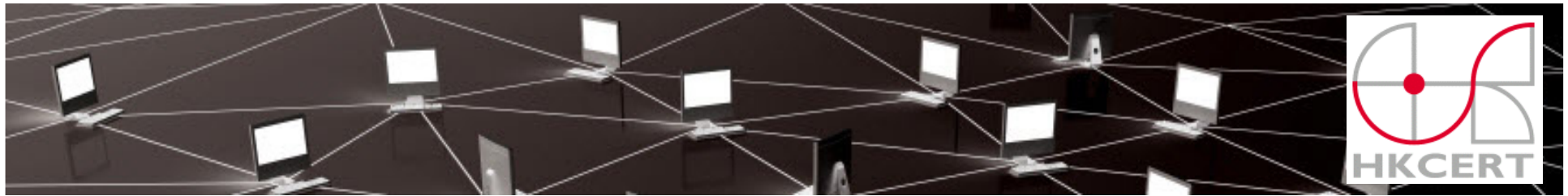
Actions  
block upd4t3

Following

RSS feed of upd4t3's tweets

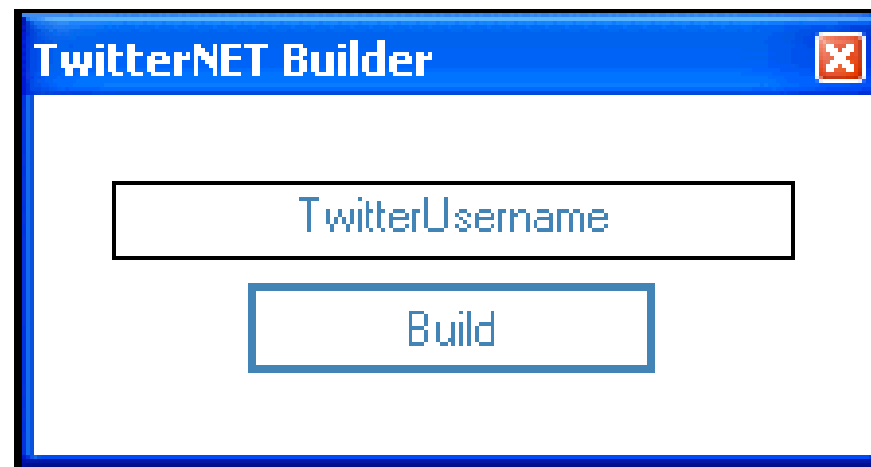
```
$ echo "aHR0cDovL2JpdC5seS9SN1NUViAgaHR0cDovL2JpdC5seS8yS29Ibw==" |  
openssl base64 -d  
hxxp://bit.ly/R6STV hxxp://bit.ly/2KoHo
```

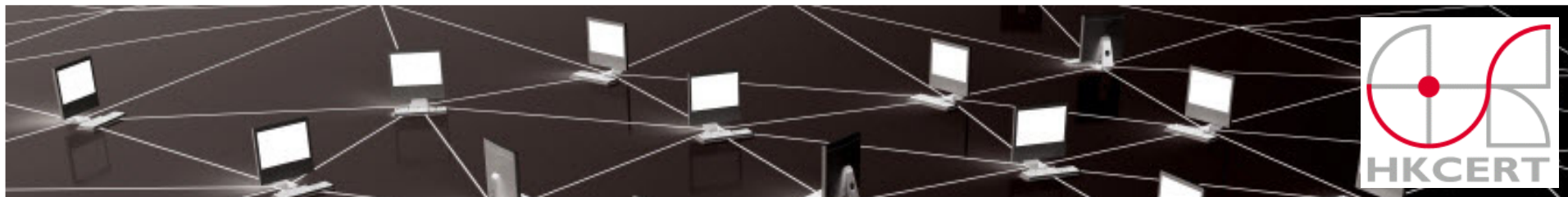
Fig 8 . Botnet use twitter to deliver the command (Source from Arbot Networks)



# Twitter

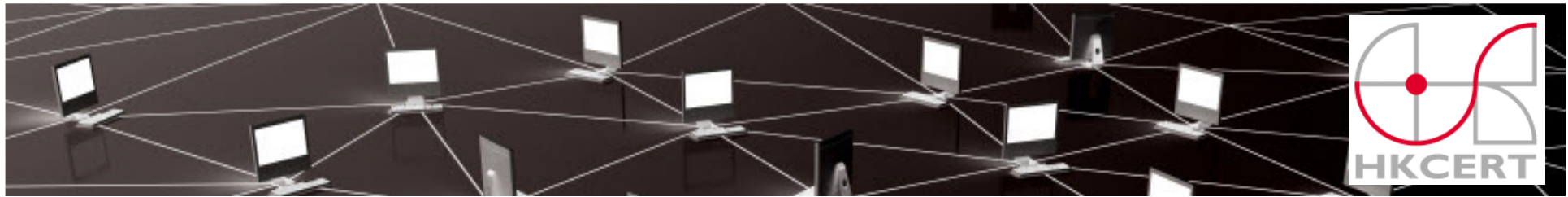
- TwitterNet Builder- A kit for building Twitter Botnet





# Impact of Botnet



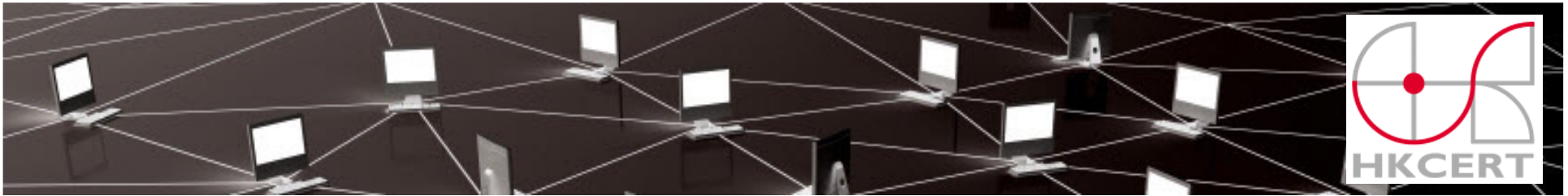


## Global botnet infection rate

| Country/Region   | 3Q09       | 4Q09       | 1Q10       | 2Q10       |
|------------------|------------|------------|------------|------------|
| Korea            | 6.3        | 6.1        | 17.4       | 14.6       |
| Spain            | 6.9        | 11.0       | 17.3       | 12.4       |
| Mexico           | 3.5        | 6.7        | 14.8       | 11.4       |
| <b>Worldwide</b> | <b>2.5</b> | <b>2.5</b> | <b>4.0</b> | <b>3.2</b> |
| China            | 1.4        | 1.0        | 1.3        | 1.0        |
| Hong Kong S.A.R. | 1.3        | 1.2        | 1.6        | 1.1        |

Fig 9 – Microsoft Security Intelligence Report Vol.9

- **88 locations around the world, no of computers cleaned for every 1,000 execution of MSRT.**



# Global botnet infection

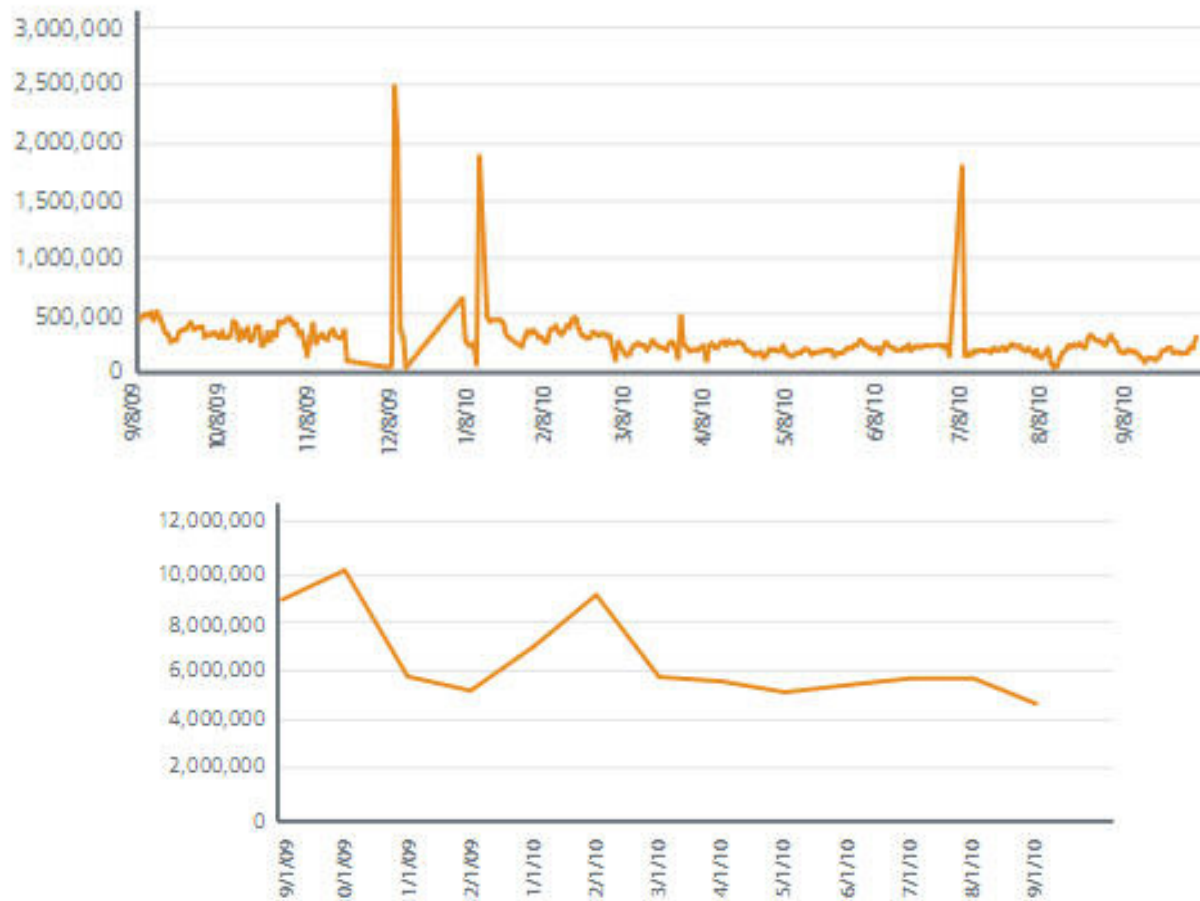
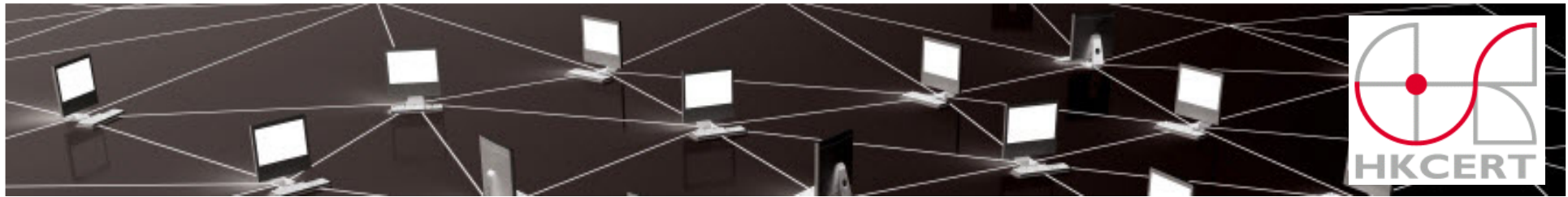


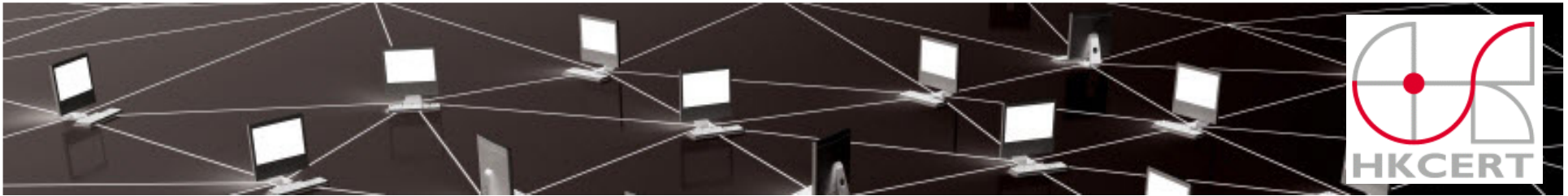
Fig 10 – Bot infection statistics (Source from McAfee)



# Active Botnet Families

|    | Family          | Primary Control Mechanism | Computers Cleaned (1Q10) | Computers Cleaned (2Q10) | Change   |
|----|-----------------|---------------------------|--------------------------|--------------------------|----------|
| 1  | Win32/Rimecud   | Other                     | 1,807,773                | 1,748,260                | -3.3% ▼  |
| 2  | Win32/Alureon   | HTTP                      | 1,463,885                | 1,035,079                | -29.3% ▼ |
| 3  | Win32/Hamweg    | IRC                       | 1,117,380                | 779,731                  | -30.2% ▼ |
| 4  | Win32/Pushbot   | IRC                       | 474,761                  | 589,248                  | 24.1% ▲  |
| 5  | Win32/IRCbot    | IRC                       | 597,654                  | 388,749                  | -35.0% ▼ |
| 6  | Win32/Koobface  | HTTP                      | 222,041                  | 383,633                  | 72.8% ▲  |
| 7  | Win32/FlyAgent  | HTTP                      | 221,613                  | 293,432                  | 32.4% ▲  |
| 8  | Win32/Virut     | IRC                       | 227,272                  | 284,519                  | 25.2% ▲  |
| 9  | Autolt/Renocide | IRC                       | 167,041                  | 178,816                  | 7.0% ▲   |
| 10 | Win32/Hupigon   | Other                     | 178,706                  | 177,280                  | -0.8% ▼  |

Fig 11 - Top 10 bot families detected (Source from Microsoft)



# Botnet Ecosystem

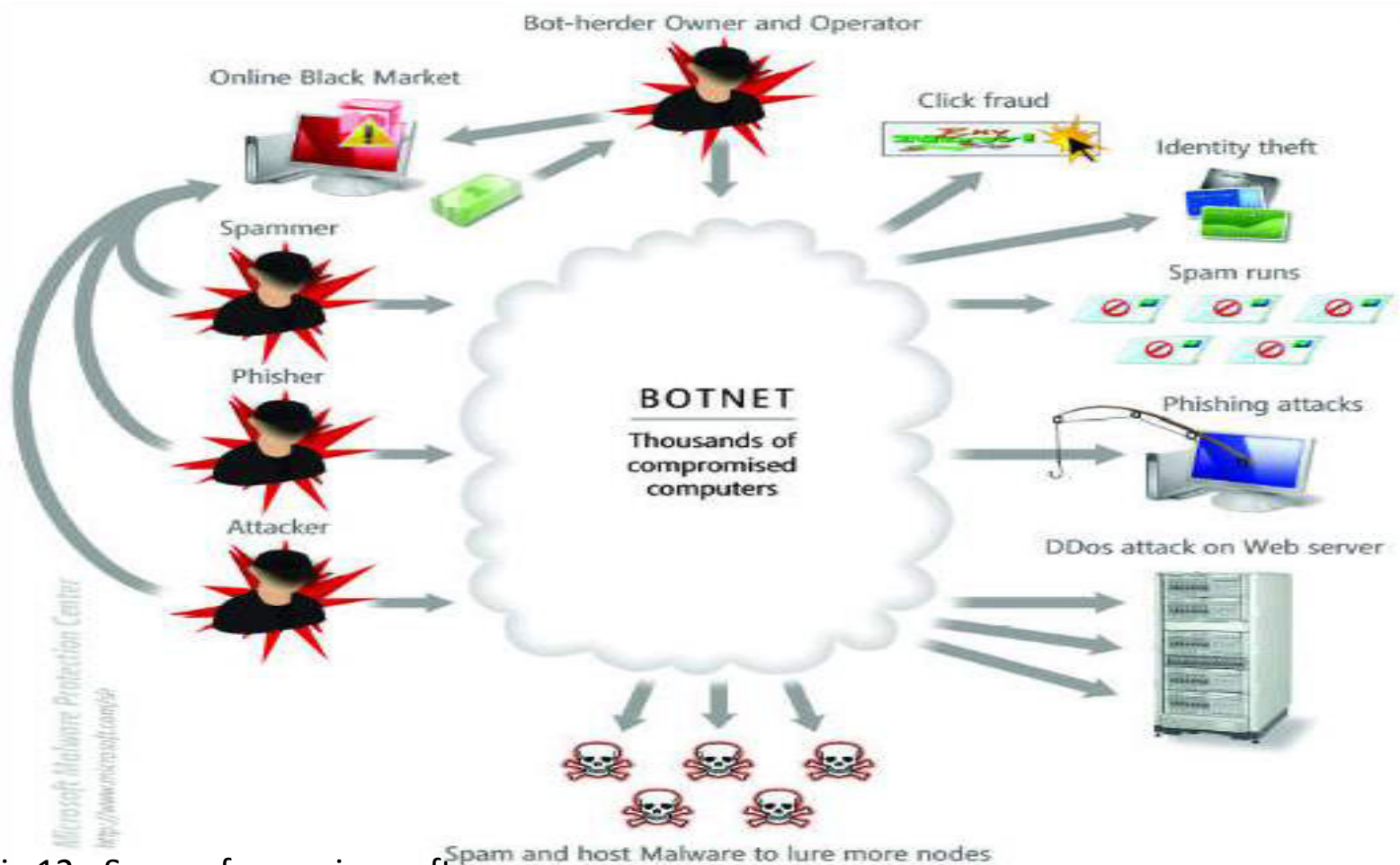
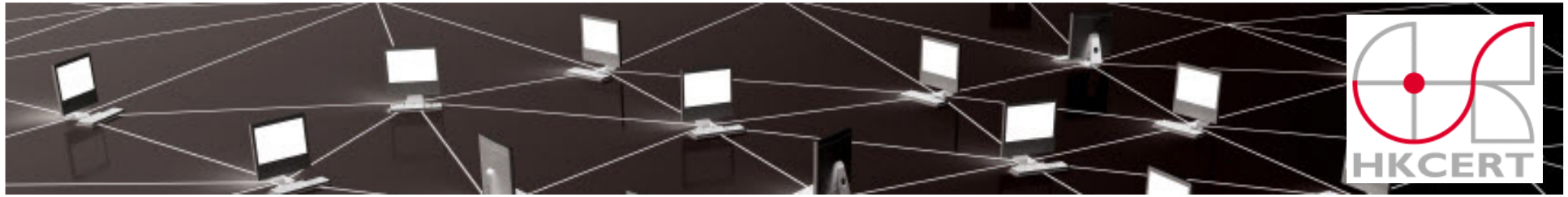
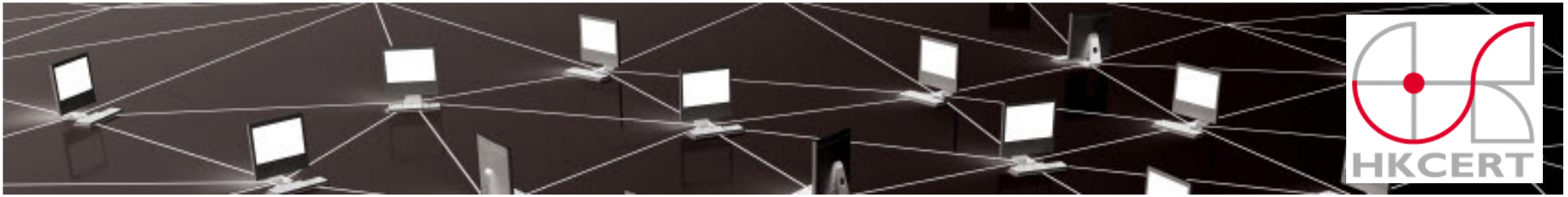


Fig 12 - Source from microsoft



# Fight Back Botnet



## Fight Back

Year 2010 is becoming a good year in shutting down big botnets.

- **Mariposa**
- **Waledac**
- **Bredolab**
- **Zeus**

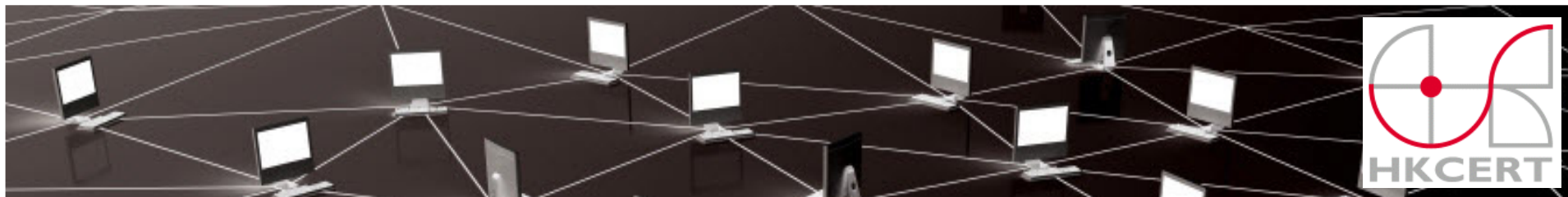




## Case Study - Mariposa

- Mariposa, (butterfly in Spanish)
- Discovered in December 2008
- 12.7 million bots in more than 190 countries (Top country – India, Top city - Seoul )
- Spread via IM, P2P file sharing, website exploit IE vulnerability





## Case Study - Mariposa

```
[22:33:01] EVENT: Timed-out .188.130:65400
[22:33:02] TALK 2: 88.253. 039: MSN link sent > @hotmail.com
[22:33:04] EVENT: Joined: 22.19:63464 L Vista SP1 GBR
[22:33:04] EVENT: Joined: 216.107:52290 W Vista SP2 USA
[22:33:06] EVENT: Joined: 49.134:62125 L WINXP SP2 DEU
[22:33:07] EVENT: Joined: 5.92:1073 L WINXP SP2 EGY
[22:33:10] EVENT: Joined: .37:63727 L Vista SP2 USA
[22:33:12] EVENT: Timed-out .140.35:2548
[22:33:13] EVENT: Quit: 20 24:20798
[22:33:14] EVENT: Joined: .124:20897 L WINXP SP3 SLU
[22:33:17] EVENT: Joined: 6.139:54794 L Vista SP2 ITA
[22:33:18] EVENT: Timed-out .88.241:53500
[22:33:18] EVENT: Timed-out 5.225.217:64727
[22:33:19] EVENT: Timed-out 08.203.197:3156
[22:33:20] EVENT: Joined: 200.1:1086 L WINXP SP2 BRA
[22:33:21] EVENT: Joined: 2.231:53576 W Vista SP0 AUT
[22:33:21] EVENT: Joined: 4.212:2920 W WINXP SP3 TUR
[22:33:22] EVENT: Joined: 92.120:4858 L WINXP SP2 RUS
[22:33:23] EVENT: Timed-out 6.26.113:53615
[22:33:25] EVENT: Timed-out 5.163.51:61309
[22:33:25] EVENT: Joined: .138:49884 L Vista SP0 GBR
[22:33:29] EVENT: Quit: 20 24:20897
[22:33:30] EVENT: Joined: .124:21012 L WINXP SP3 SLU
[22:33:32] EVENT: Timed-out 0.68.216:2185
[22:33:34] TALK 1: 89.143.: 901: MSN started, link: http://
.exe
```

Fig 13 – Mariposa C&C server

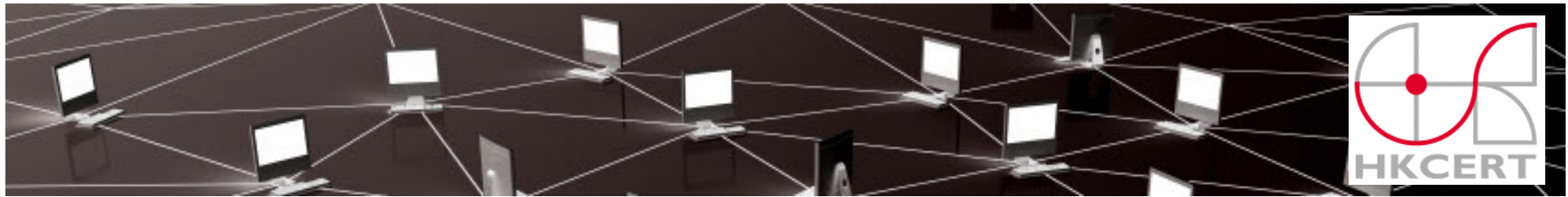
- More than 200 binaries
- Connect the C&C using anonymous VPN service





## Case Study - Mariposa

- Stole credit card, banking credentials, user identity (username, password)
- Belonging to more than 800,000 users.



## Case Study - Mariposa

- **Mariposa Working Group (MWG)** established in May 2009
- Members:

DefenceIntelligence.

**Directi**

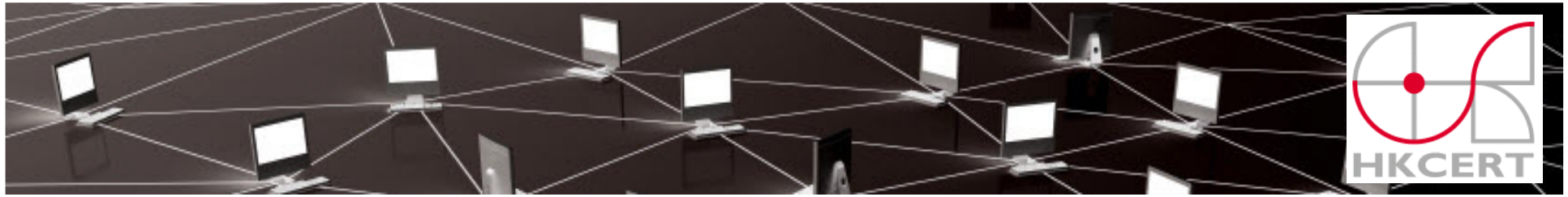


Georgia Institute  
of Technology



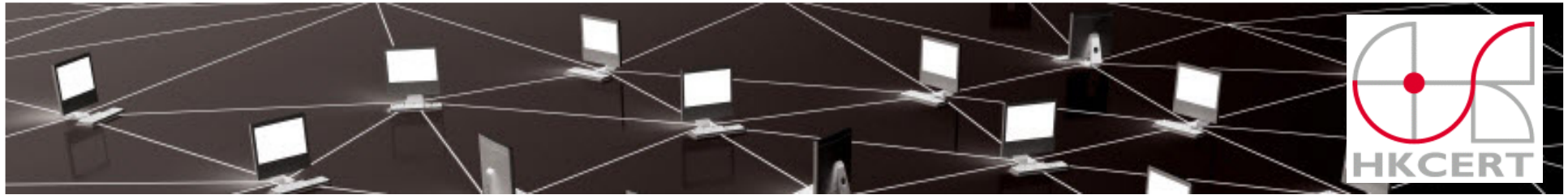
neustar

**PANDA**  
SECURITY



## Case Study - Mariposa

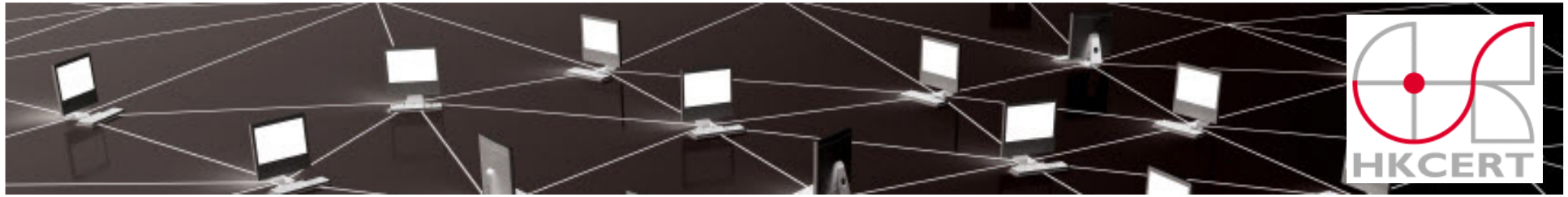
- In Dec 2009, MWG took control of the Mariposa Botnet
- In Feb 2010 arrested the leader (alias “**Netkairo**” ) by Spanish Civil Guard
- In Jul 2010, arrested the suspected creator (alias “**Iserdo**”)by Slovenian police



## Case Study - Mariposa

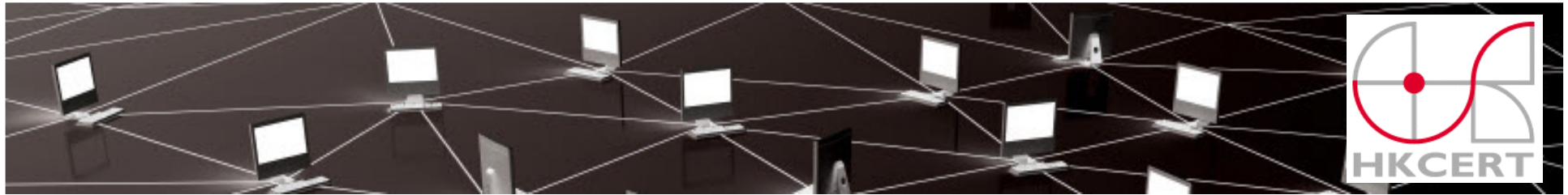
### Lesson Learned

- 97% bots use DNS to locate C&C, detect the bots by DNS activity
- Sinkhole the domain used by C&C server



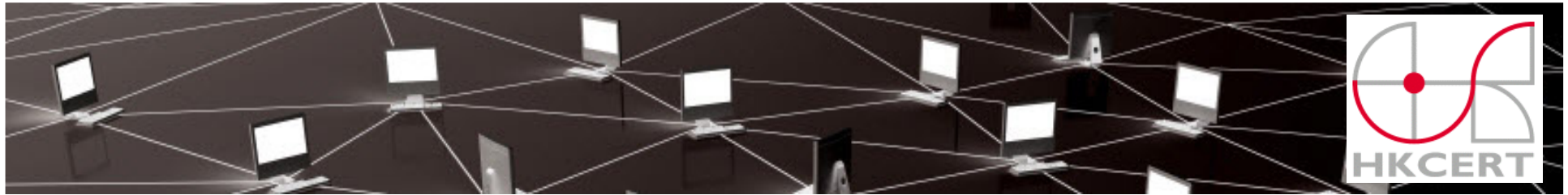
## Case Study - Waledac

- Waledac
- Discovered in Apr 2008
- Estimated 70,000 - 90,000 infected computers
- Spread via email
- 1.5 billion spam messages a day (about 1% of the total global spam volume)
- Connect the C&C using P2P network

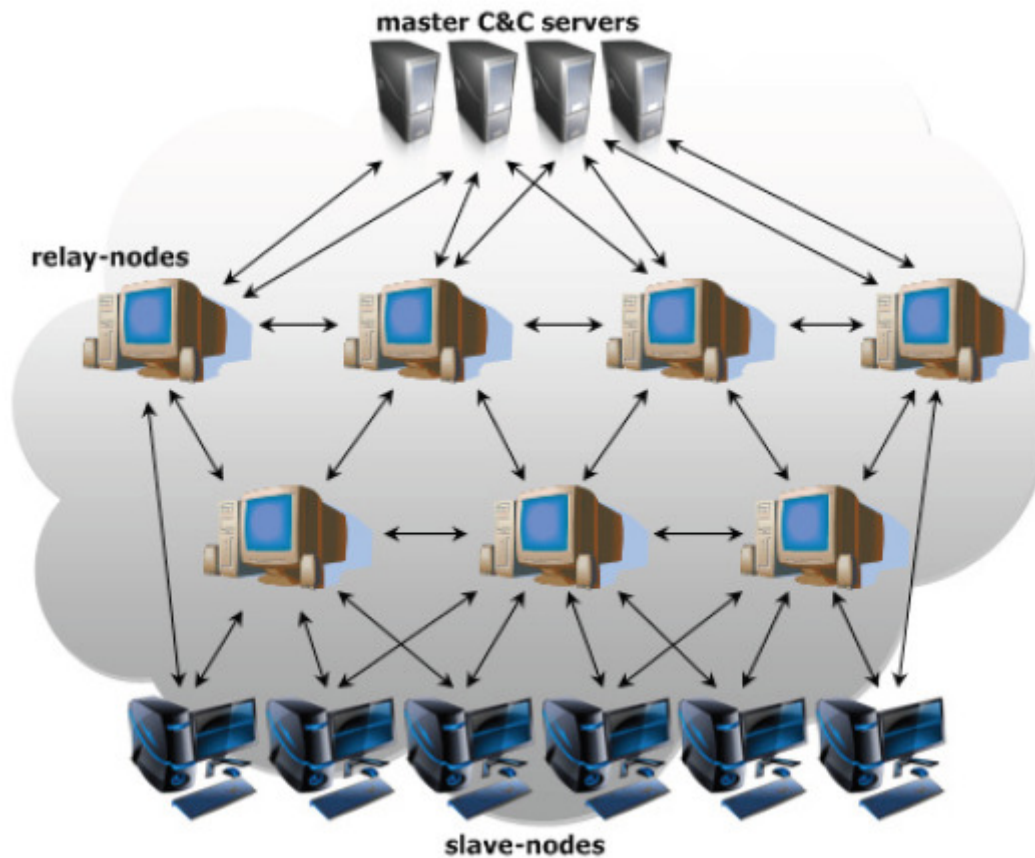


## Case Study – Waledac

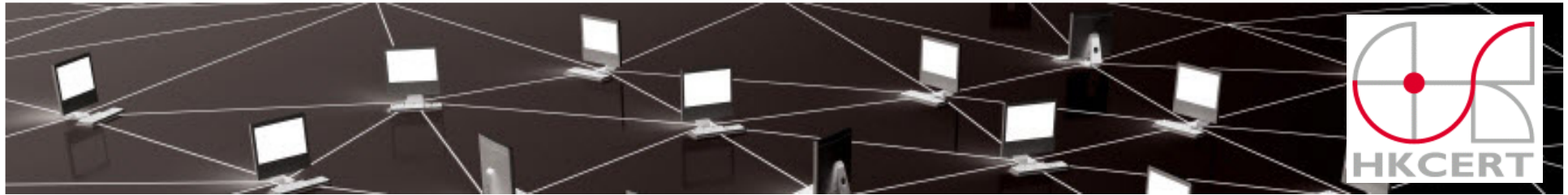
- Fraudulent greeting cards and breaking news events.
- Email contains a link point to a malicious websites
- Deliver exploit code when visited
  - Adobe reader, Flash, IE, MS Office components etc.



## Case Study - Waledac



- Fig 14 - Waledac P2P communication structure (Source from Symantec)



## Case Study - Waledac

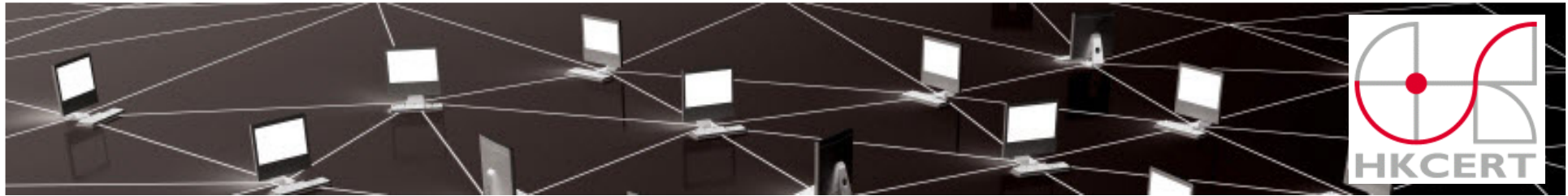
- “Operation b49” initiated by Microsoft’s Digital Crimes Unit

- Members:



- In Feb 2010, Cut off 273 “Harmful botnet domains used by Waledac





# Case Study - Waledac

- Waledac Tracker

<http://www.sudosecure.net/waledac/index.php>

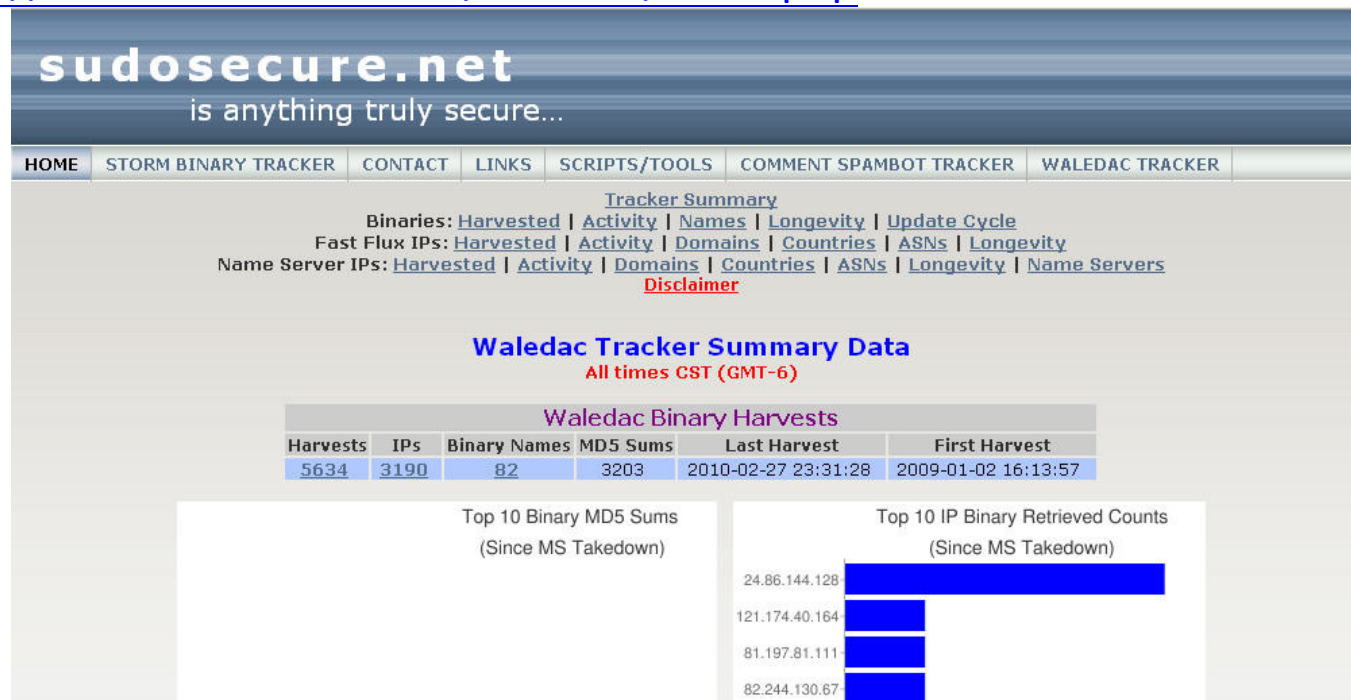
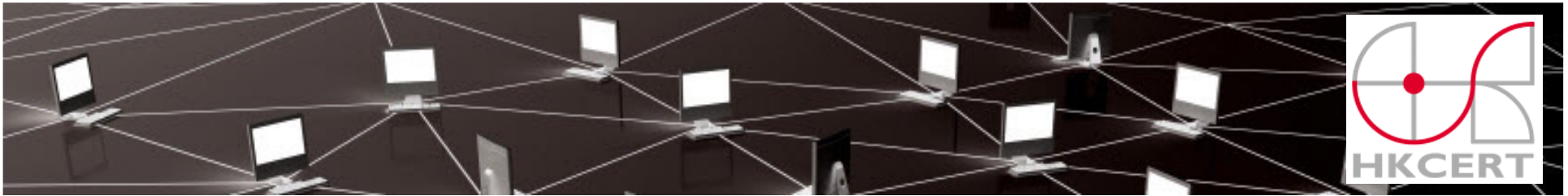


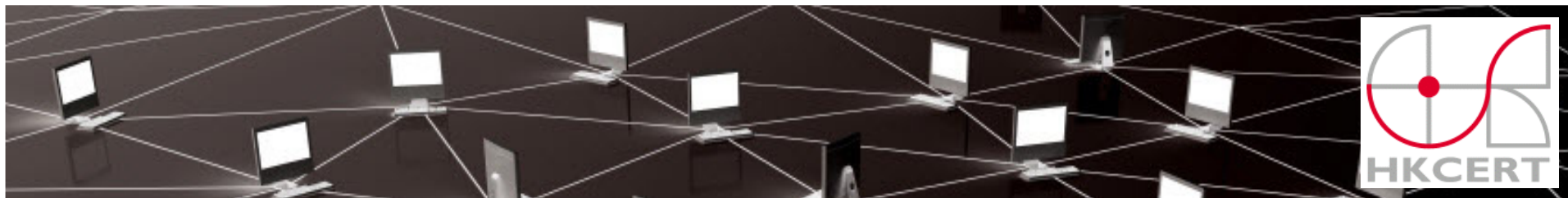
Fig 15 – Waledac Tracker (Source from sudosecure)



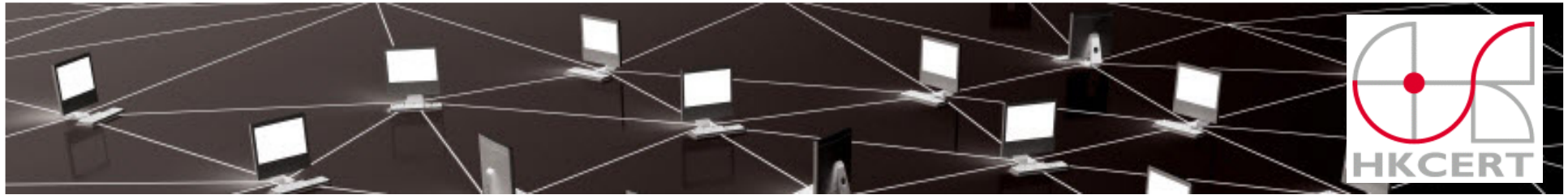
## Case Study - Waledac

### Lesson learned

- Solved legal issue
  - Microsoft Corporation v. John Does 1-27, et. al.  
<http://www.microsoft.com/presspass/events/rsa/docs/Complaint.pdf>

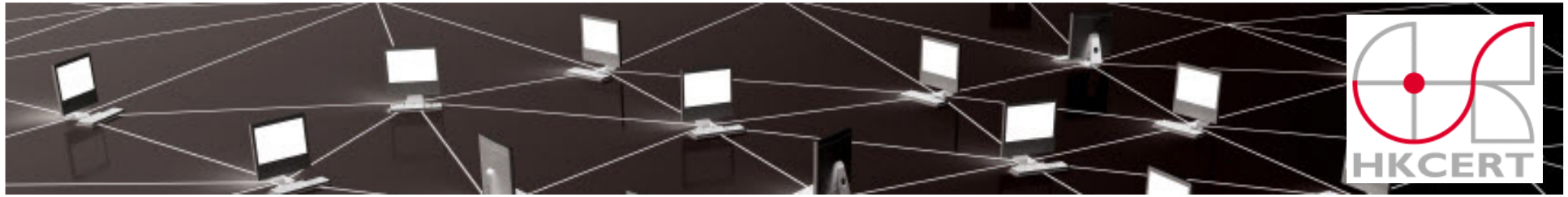


# Security Protection Scheme



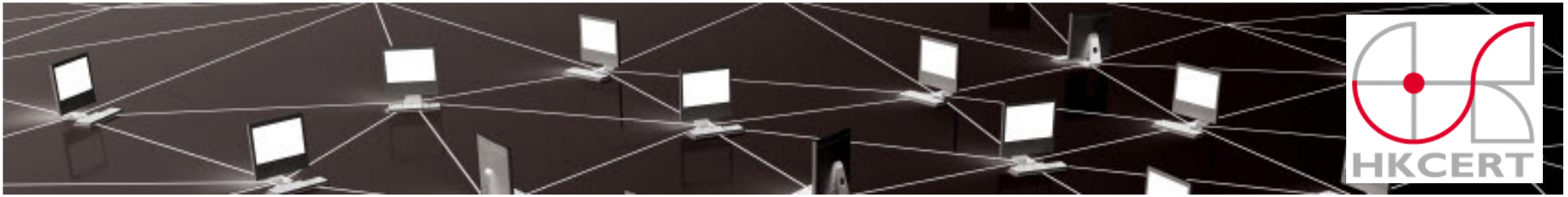
# Security Protection Scheme

- Anti-virus/Anti-malware
- Firewall
- Apply security patches
- Malicious Website detection
- File analysis



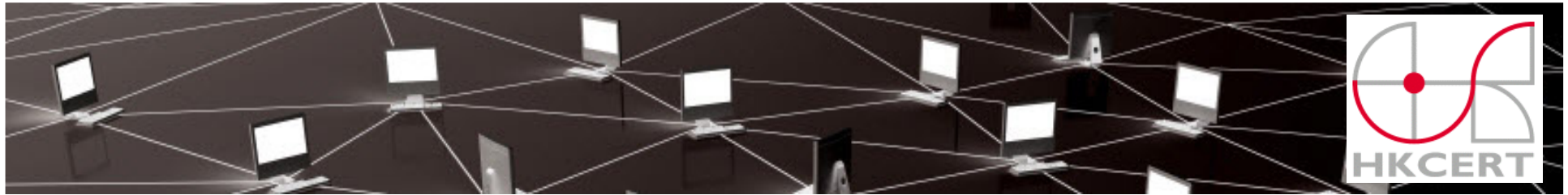
## Anti-virus/Anti-malware

- Deploy Cloud technology
- A unknown application is launched, ask the cloud network to look up this application
- Immediate protection against the latest threats



# Firewall

- In-bound and out-bound detection
- Open ports detection
- Unknown application warning
- System change warning
- Sandbox
- Logging



# Apply security patches

- Vendor's OS and application update checking features
- Secunia - Personal Software Inspector (PSI)

[http://secunia.com/vulnerability\\_scanning/personal/](http://secunia.com/vulnerability_scanning/personal/)

**Secunia PSI**  
**Personal Software Inspector (PSI) 2.0 BETA**  
Detects and installs missing security patches for your PC

**89%** Secunia System Score

**Patch Your PC**  
Dashboard  
Scan  
Results (17 missing)

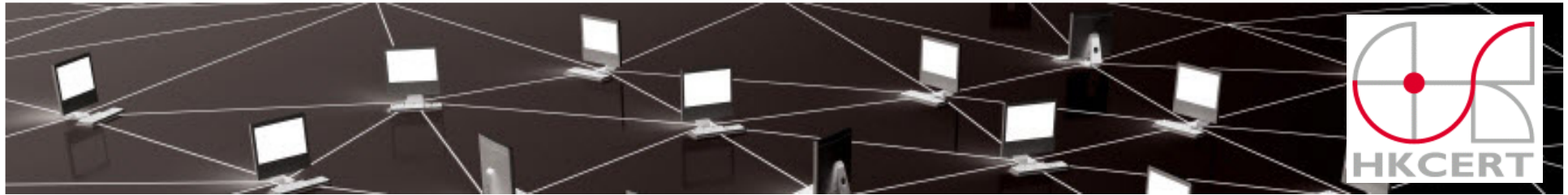
**Configuration**  
Settings  
Secunia Community Profile  
Integrate with Secunia CSI

**Learn More**  
Support / Forum  
Privacy Statement

**Scan Results**  
This view shows an aggregated list of programs detected on your PC with the latest Secunia PSI scan. Click any program for additional information and details.

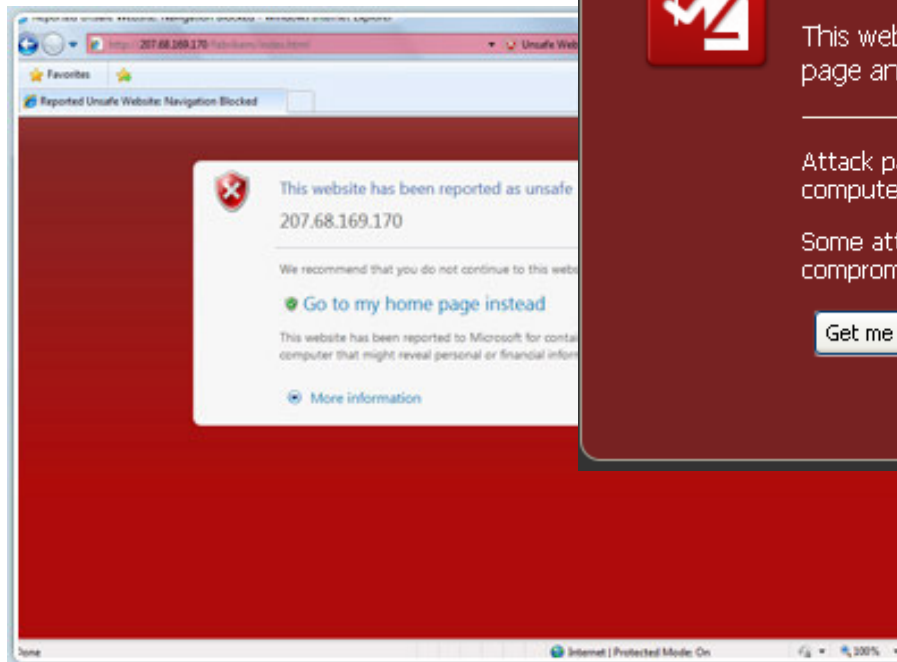
**Detected Programs**  
Limit Results To:  Insecure  End-of-Life  Patched  Auto-Updateable


| Program                                 | # | Program State | Threat Rating | Detected Version | Install Solution           |
|-----------------------------------------|---|---------------|---------------|------------------|----------------------------|
| Foxit Reader 3.x                        | 1 | End-of-Life   | ██████        | 3.3.1.518        | Waiting for update to c... |
| Microsoft Office PowerPoint Viewer 2003 | 1 | End-of-Life   | ██████        | 11.0.8164.0      | Install Solution           |
| Microsoft Silverlight 2.x               | 2 | End-of-Life   | ██████        | 2.0.40115.0      | Install Solution           |
| PC-Doctor for Windows 4.x               | 1 | End-of-Life   | -             | 4, 1, 0, 0       | -                          |
| PHP 5.1.x                               | 1 | End-of-Life   | ██████        | 5.1.6.6          | Install Solution           |
| Sun Java JRE 1.2.x                      | 1 | End-of-Life   | ██████        | 1.2.2.0          | Waiting for update to c... |
| TrueCrypt 6.x                           | 1 | End-of-Life   | -             | 6.3.1.0          | Install Solution           |



# Malicious Website detection

- IE 8, Firefox 3 built-in website detection features





### Reported Attack Page!

This web page at [http://207.68.169.170](#).net has been reported as an attack page and has been blocked based on your security preferences.

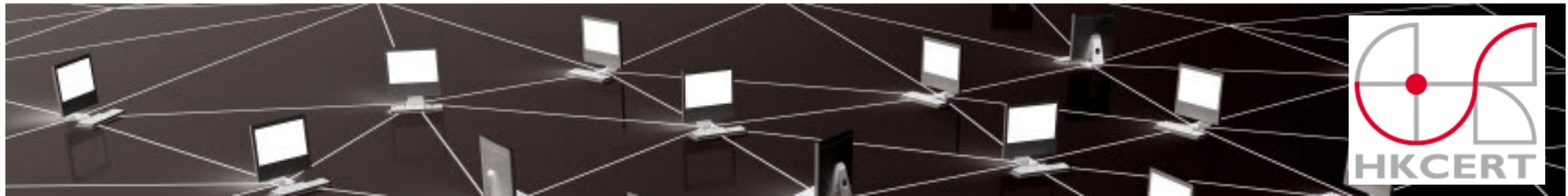
Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

[Get me out of here!](#)   [Why was this page blocked?](#)

[Ignore this warning](#)





# Malicious Website detection

- Google Safe Browsing

安全瀏覽  
ts12315.com的診斷頁面

建議提供者 Google

ts12315.com 目前的刊登狀態為何？  
網站已列為可疑網站，造訪此網站可能會損害您的電腦。  
過去 90 天以來，此網站的其中一部分已記錄 2

當 Google 造訪此網站時，會發生什麼事？  
過去 90 天來，我們在該網站上測試了 60 個網裝惡意軟體。Google 上一次造訪此網站的日期為 2010-10-10。  
Malicious software includes 73 trojan(s), 73 ex  
惡意軟體是由 7 網域 (包括 [9bic.net/](#), [teamsec](#)  
2 個網域 (包括 [xx7.in/](#), [1010gx.tk/](#)) 似乎是散佈  
This site was hosted on 2 network(s) including

ts12315.com 搜尋

約有 1,600 項結果 (需時 0.11 秒) 進階搜尋

ts12315.com WOT Safe Search [x]

门户- Powered by Discuz! ☆ 🔍 - [ 轉為繁體網頁 ]

這個網站可能會損害您的電腦。

我的中心 · 首頁Portal · 论坛BBS · 博客Space · 法律维权 · 人事投诉 · 医疗投诉 · 教育投诉 · 质量投诉 · 商业投诉 · 排行榜Ranklist · 今日 · 今日精彩推荐 ...

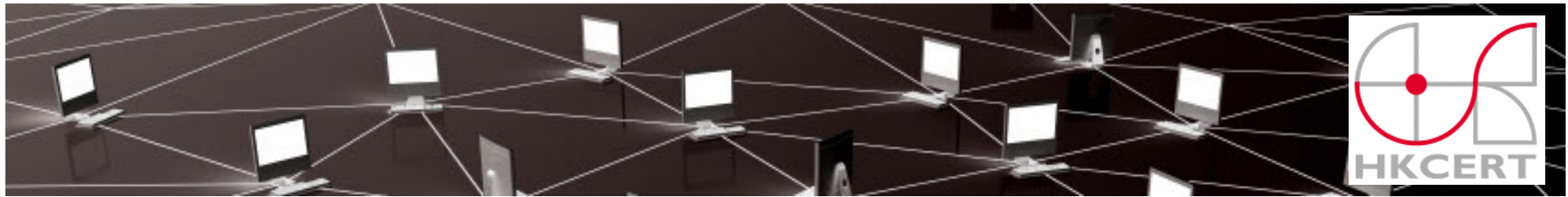
[www.ts12315.com/](#)

提示信息- 12315在线投诉网- Powered by Discuz! - Ts12315.com ☆ 🔍 - [ 轉為繁體網頁 ]

這個網站可能會損害您的電腦。

安全提示(未设置请忽略), 母亲的名字, 爷爷的名字, 父亲出生的城市, 你其中一位老师的名字, 你个人计算机的型号, 你最喜欢的餐馆名称, 驾驶执照最后四位数字. 我的中心 ...

[www.ts12315.com/portal.php?mod=list&catid=6](#)



# Malicious Website detection

- Wepawet

<http://www.mywot.com/en/download>

## Wepawet (alpha)

[Home](#) | [About](#) | [Sample Reports](#) | [Support](#) | [Tools](#) | [News](#)

WEPAWET is a service for detecting and analyzing web-based malware.

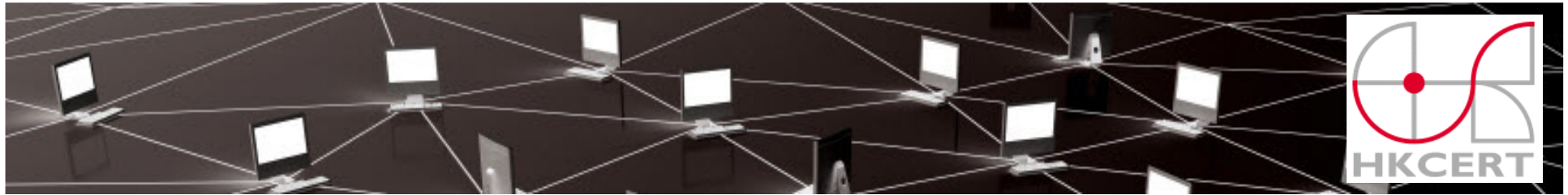
To use WEPAWET:

1. Upload a sample or specify a URL
2. Wait for the resource to be analyzed
3. Review the generated report

- MonkeyWrench

<http://monkeywrench.de/index.html>





# Malicious Website detection

- Blocklist

- Malware Domain Blocklist

**DNS-BH – Malware Domain Blocklist**

Malware Prevention through Domain Blocking (Black Hole DNS Sinkhole)

<http://www.malwaredomains.com/files/domains.txt>

- ZeuS Blocklist

<https://zeustracker.abuse.ch/blocklist.php>

abuse.ch ZeuS Tracker

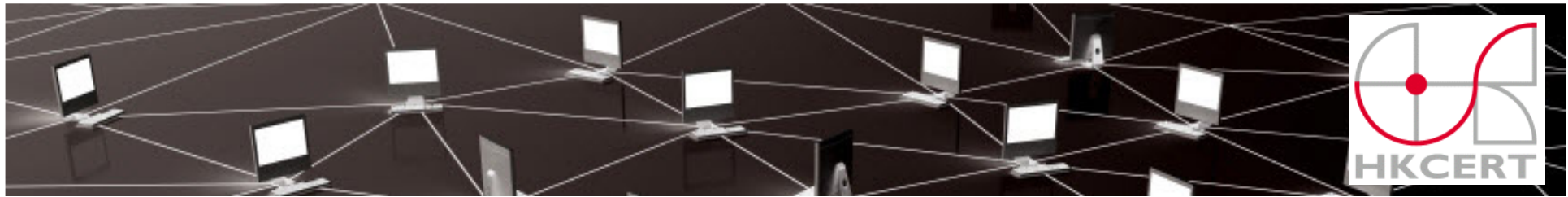
Home | FAQ | ZeuS Blocklist | ZeuS Tracker |

- SpyEye Blocklist

<https://spyeyetracker.abuse.ch/blocklist.php>

SET | SpyEye  
TRACKER

Home | News | FAQ | SpyEye Blocklist |



# File Analysis

- VirusTotal

<http://www.virustotal.com>



Virustotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: **40d09b7d94da70ede50866c55f48613c-2358.txt**  
 Submission date: **2009-08-09 09:02:30 (UTC)**  
 Current status: **finished**  
 Result: **19 /41 (46.3%)**

VT Community



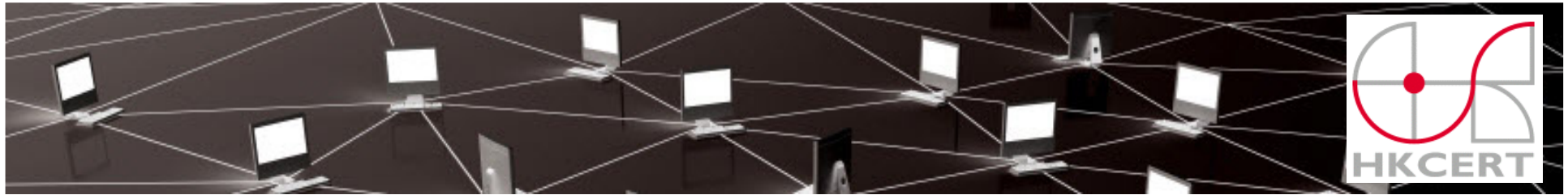
not reviewed  
Safety score: -

[Compact](#)

[Print results](#)

There is a [more up-to-date report](#) (30/41) for this file.


| Antivirus  | Version   | Last Update | Result                             |
|------------|-----------|-------------|------------------------------------|
| a-squared  | 4.5.0.24  | 2009.08.09  | Trojan-Downloader.Win32.Banload!IK |
| AhnLab-V3  | 5.0.0.2   | 2009.08.08  | -                                  |
| AntiVir    | 7.9.0.248 | 2009.08.07  | TR/Spy.77312.15                    |
| Antiy-AVL  | 2.0.3.7   | 2009.08.07  | -                                  |
| Authentium | 5.1.2.4   | 2009.08.09  | W32/Trojan-disguised-based!Maximus |



# File Analysis

- MalOffice

<http://mwanalysis.org/?site=7&page=submit>



CWSandbox
MalOffice
General

## Malware Analysis System

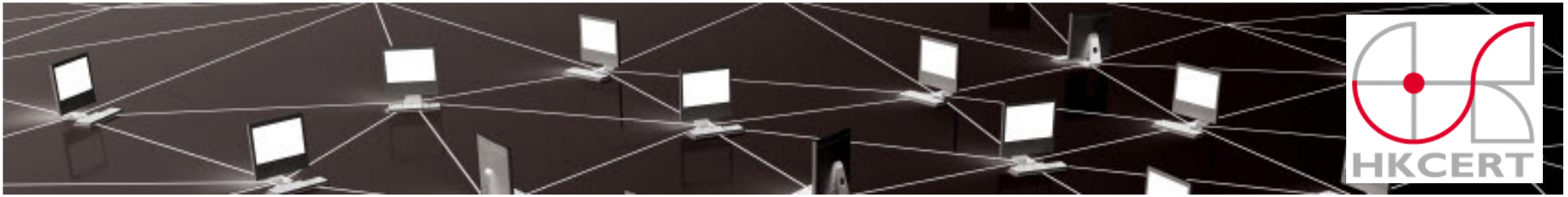
### MalOffice :: Document Details

Home
Submit Document

| General Information |                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------|
| Filename            | Security Trend of New Computing Era.doc                                                                     |
| Filesize            | 30208 byte                                                                                                  |
| MD5 hash            | 3ce5882e05a74adcc3a55632b28ec9e6                                                                            |
| SHA1 hash           | 4dd71916d0dbbcf86d321c255180e3e639a55484                                                                    |
| Document type       | Microsoft Word document                                                                                     |
| Added               | 23.11.2010 09:11:44                                                                                         |
| Total result        | <div style="width: 100%; height: 10px; background: linear-gradient(to right, green 20%, white 20%);"></div> |

| Embedded Objects |           |           |
|------------------|-----------|-----------|
| Comment          | SHA1 hash | MIME type |
|                  |           |           |

| Analyses of this document |                     |                 |          |
|---------------------------|---------------------|-----------------|----------|
| analyzer                  | date                | result          | findings |
| ClamAv & Avira AntiVir    | 23.11.2010 09:17:29 | not rated       |          |
| Office 2000 Professional  | 23.11.2010 09:17:05 | probably benign |          |



# Q & A

**Thank You**

**Emai: [hkcert@hkcert.org](mailto:hkcert@hkcert.org)**