

Security and Fraud Prevention

Asia Pacific TLD Association

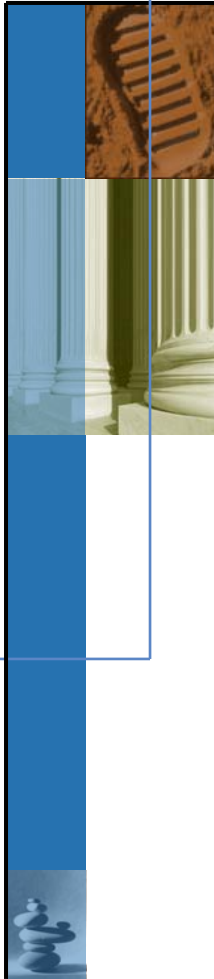
HOSTS: .HK Internet Registration Corporation Ltd

VENUE: Regus, Wanchai, Hong Kong.

18th February 2011.



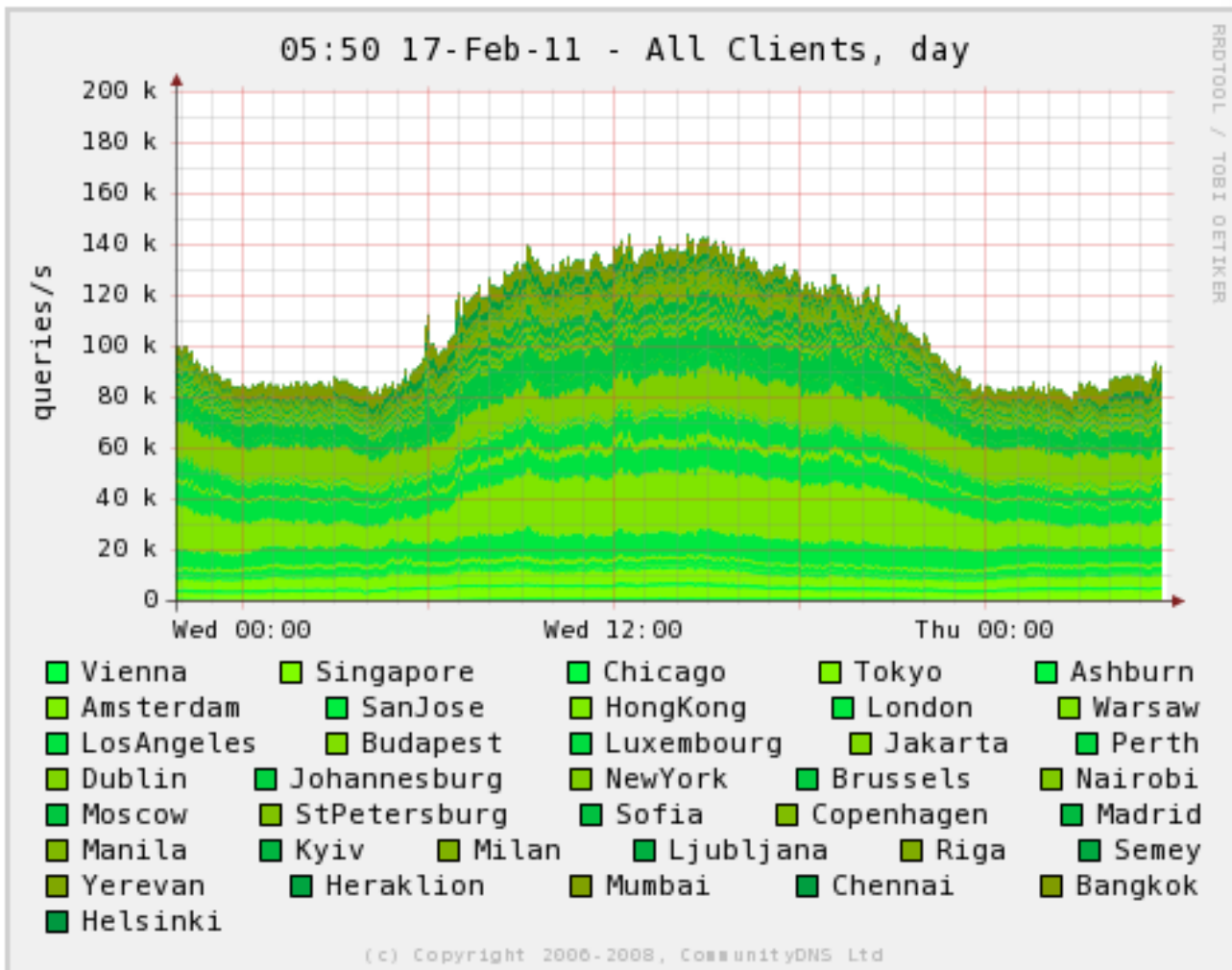
Paul M Kane
Director,
www.CDNS.net



Only “Good” guys should use the Internet

- **Cyber-espionage**
 - > Ability to “see” what and who is contacting a competitor
 - > Read communications to and from organisations / individuals to save “development costs”
- **Cyber-extortion**
 - > Denial of Service – growing fast; large corporations are “paying” to be left alone ☹
 - > Reputation damage – use Social networks and “hacker” services to bring name into disrepute.
 - > Collecting remote PC/Router devices to frustrate user experience

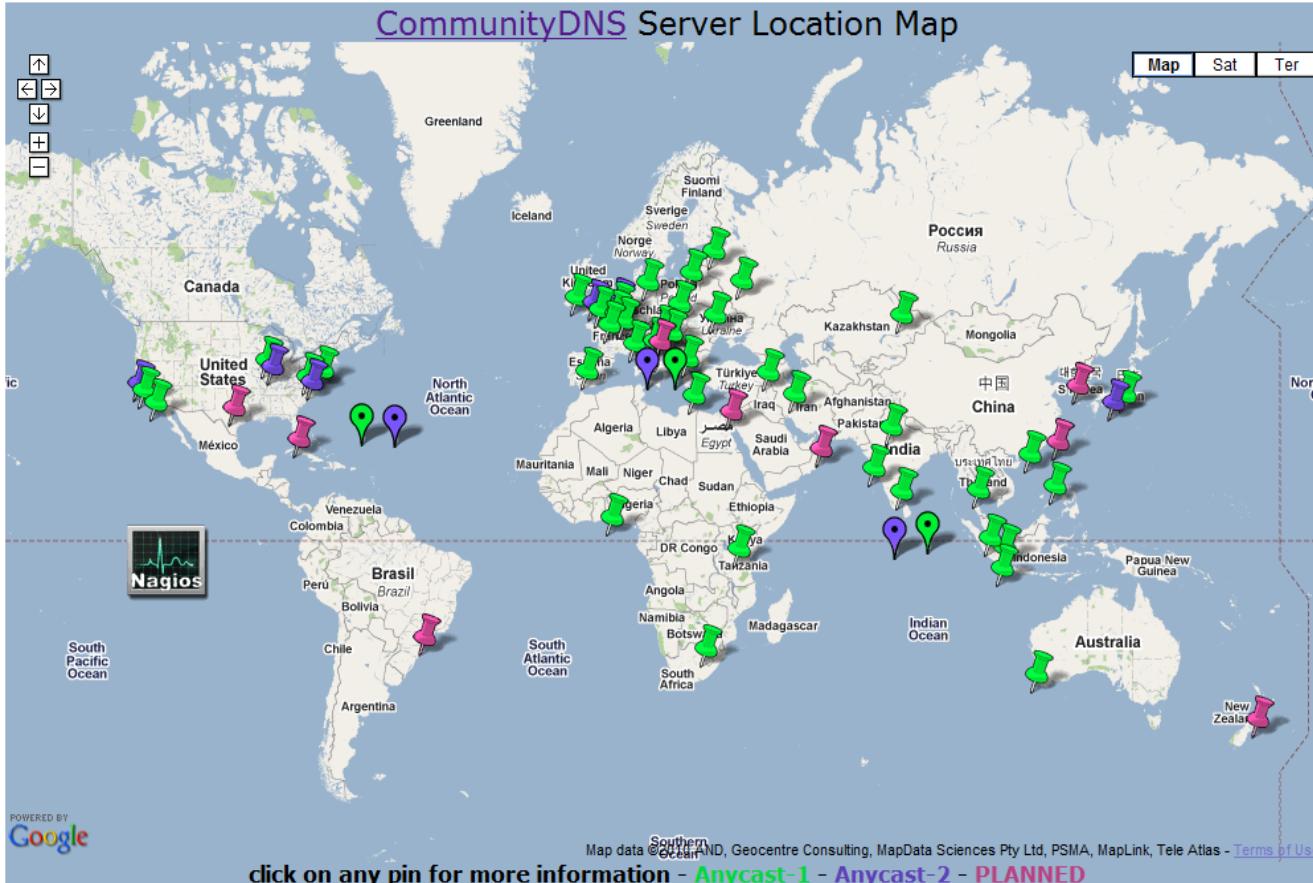
Real Time Data – 17th Feb 2011



- 141,858,904 names on the platform
- 73% of global Internet
- 409,998 updates on 16th Feb 2011
- 5 Anycast Clouds
- Capacity is 855 billion per second!
- 41 global locations and growing

CDNS - Server Locations – more welcome

CommunityDNS Server Location Map



We are happy to host your TLD in these locations – frequently FREE

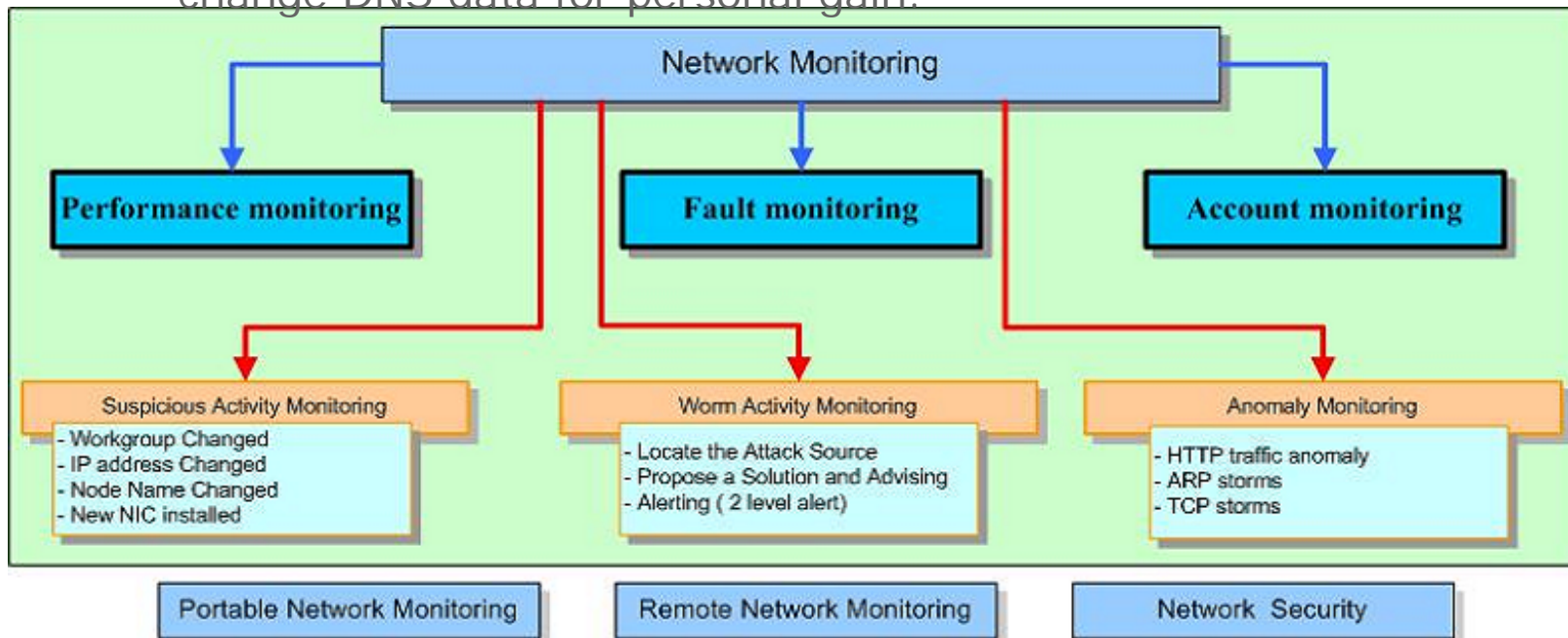
By working together we make the Internet more robust

Host a cDNS server in YOUR country - FREE

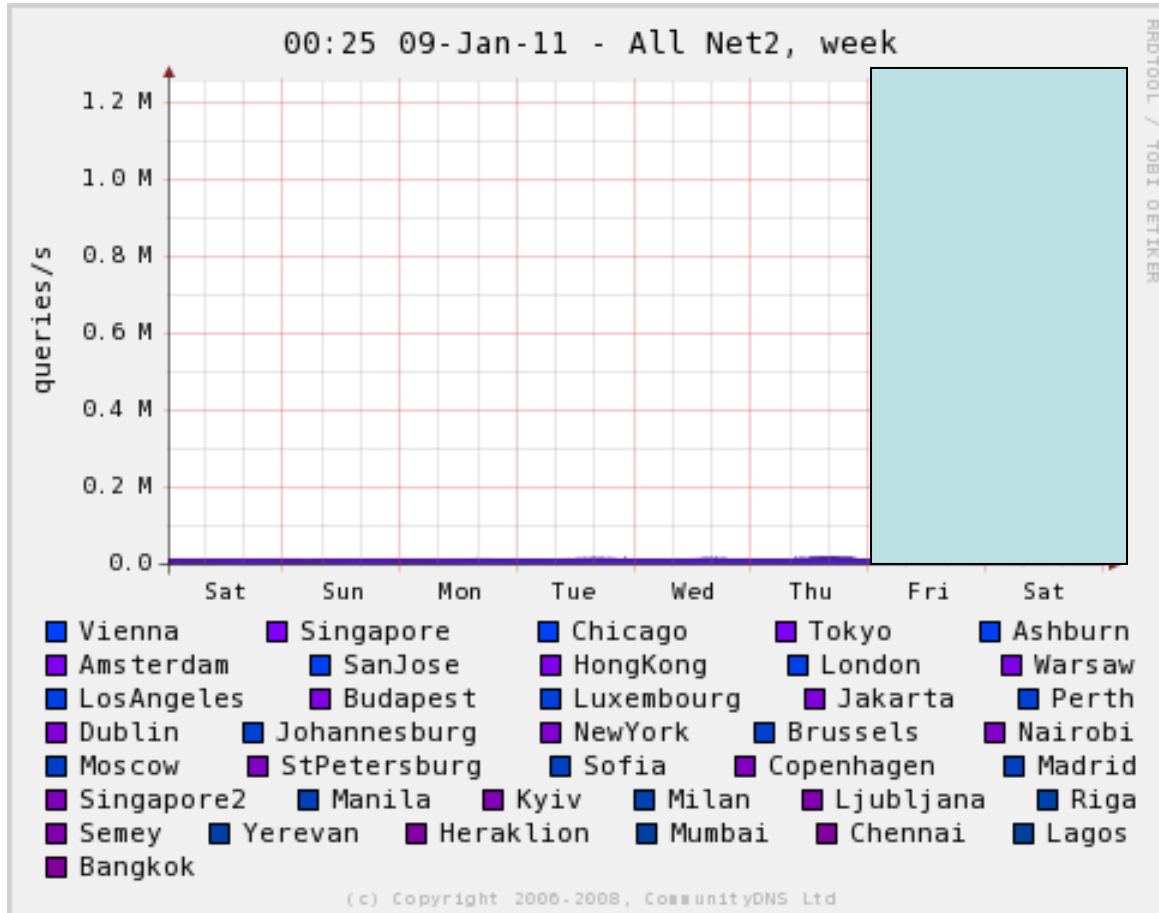
Robust service requires a reliable network monitoring

- Moving from DNS Resolution to Internet Security

- > Managing Anycast cloud represents approximately 30% of the job and is technically relatively easy.
- > 70% is network monitoring, looking for “bad” guys who seek to change DNS data for personal gain.

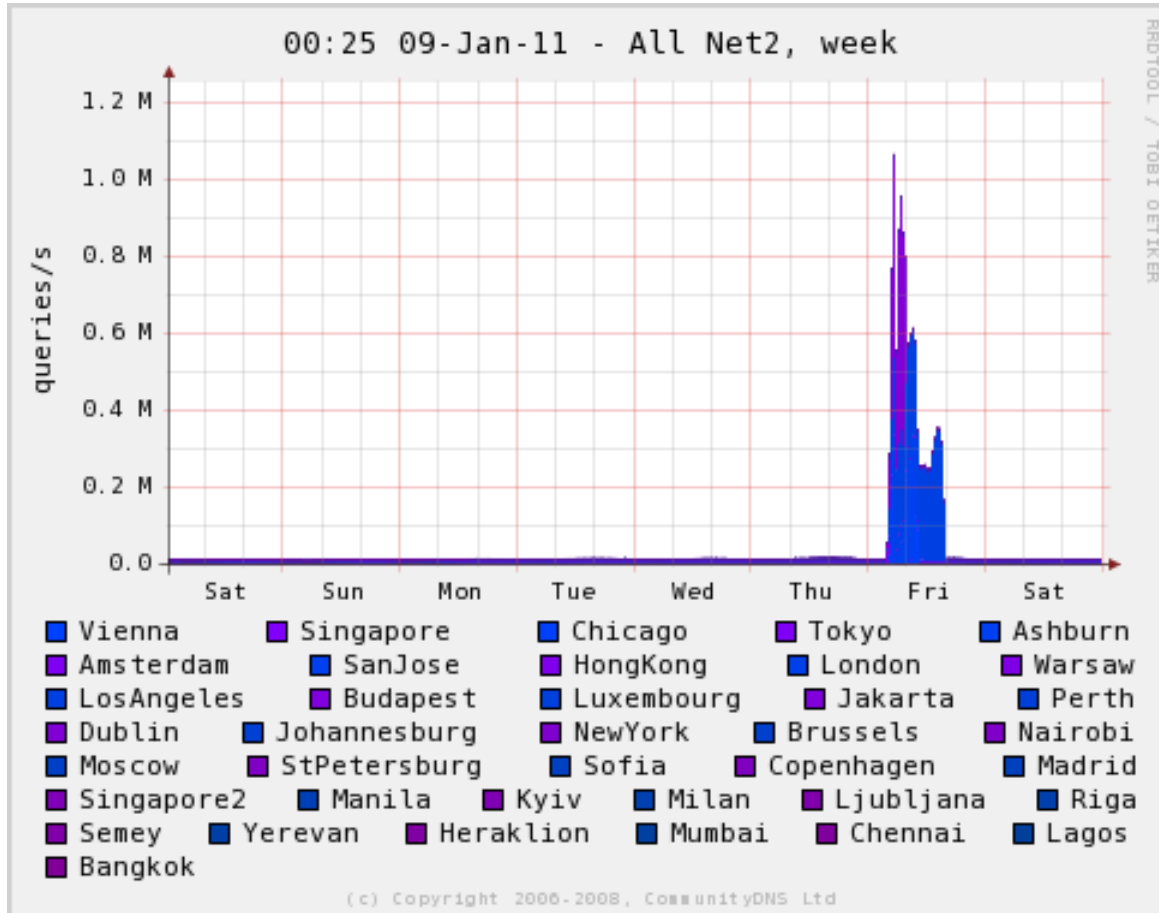


Bad guys at work!



Normal Activity
on Net 2 is
approx 12,000 to
15,000 queries
per second

Bad guys at work!



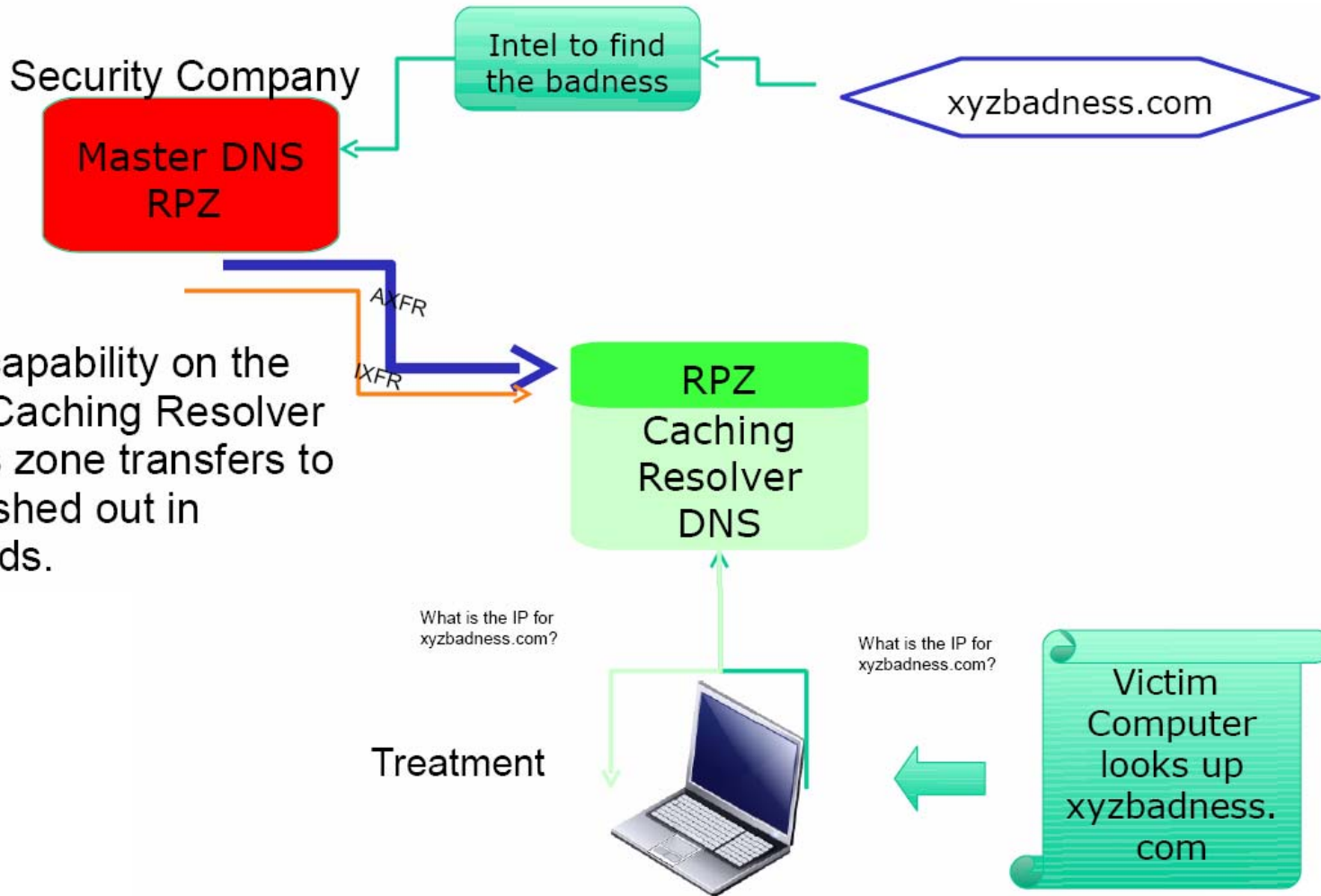
Normal Activity on Net 2 is approx 12,000 to 15,000 queries per second

8th Jan (0318) peaked at 1.6 million DNS queries per second focused on 1 TLD

Advantages – DNS White Lists (Theory).

- Turns a recursive DNS server into a powerful security tool!
- Block or redirect malicious drop sites
 - > Known Malware and Phishing sites can be blocked!
- Block ability for bots to find the Command & Control
 - > Bad guys no longer use the DNS to control their Botnets – just IP!
 - > Walled garden treatment for infected clients
- IP Reputation Addresses can be included
 - > Both “bad” IPv4 and IPv6 addresses can be included in the “block” list.

Integrating White List DNS Service.



RPZ capability on the DNS Caching Resolver allows zone transfers to be pushed out in seconds.

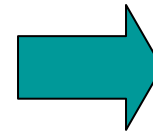
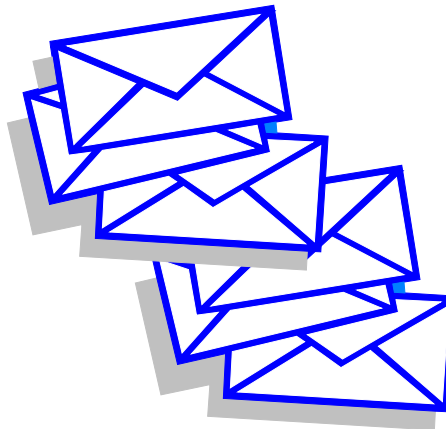
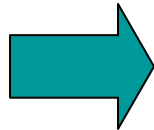
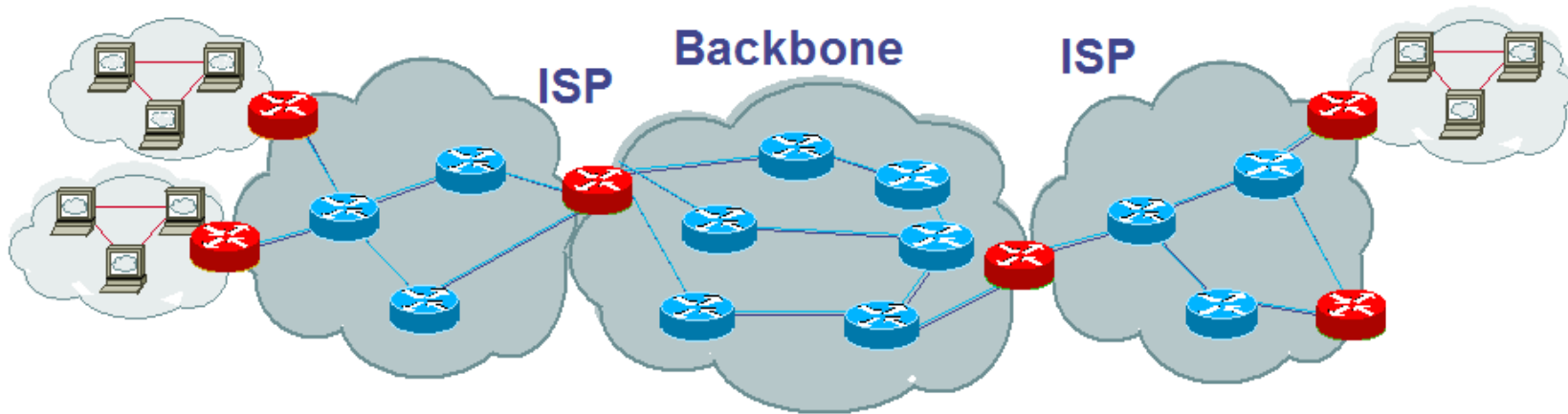
What is the IP for xyzbadness.com?

Treatment

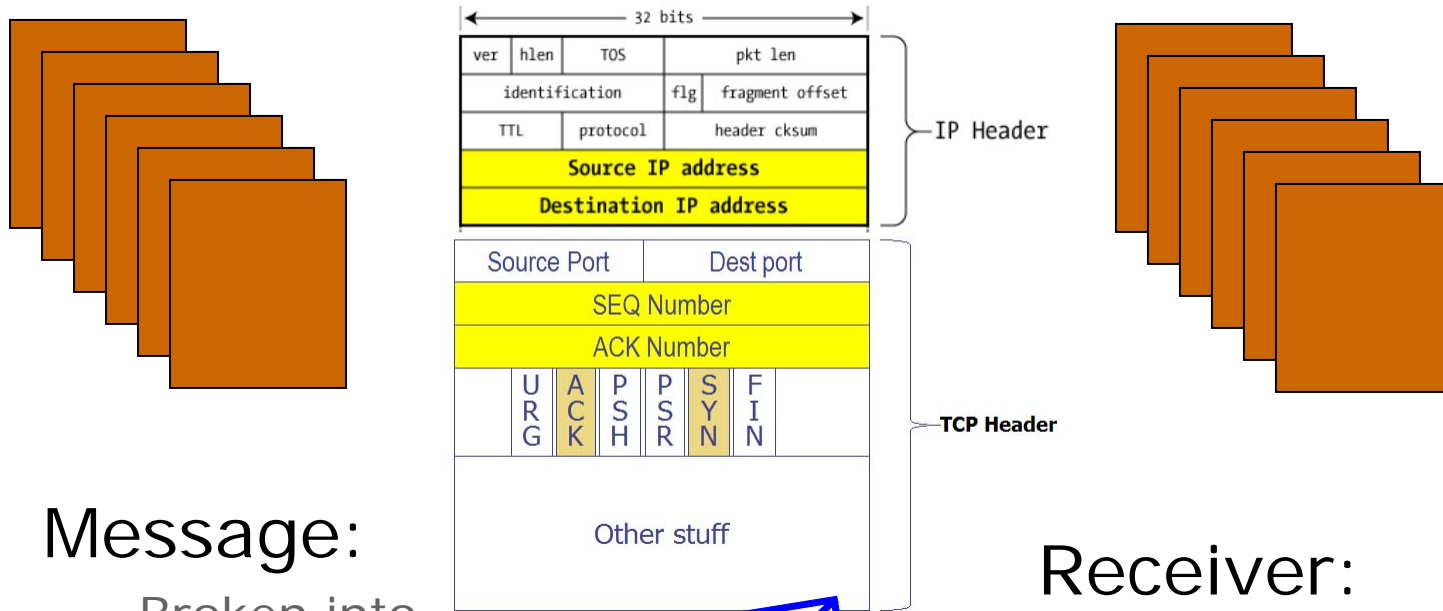
What is the IP for xyzbadness.com?

Victim Computer looks up xyzbadness.com

You've got mail!

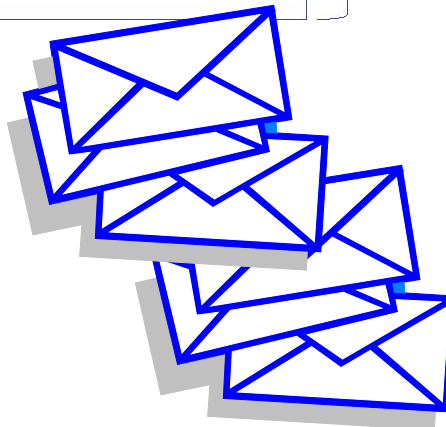
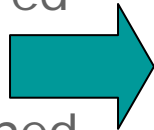


How mail system works....



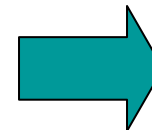
Message:

Broken into
Packets,
Numbered
and
dispatched



Receiver:

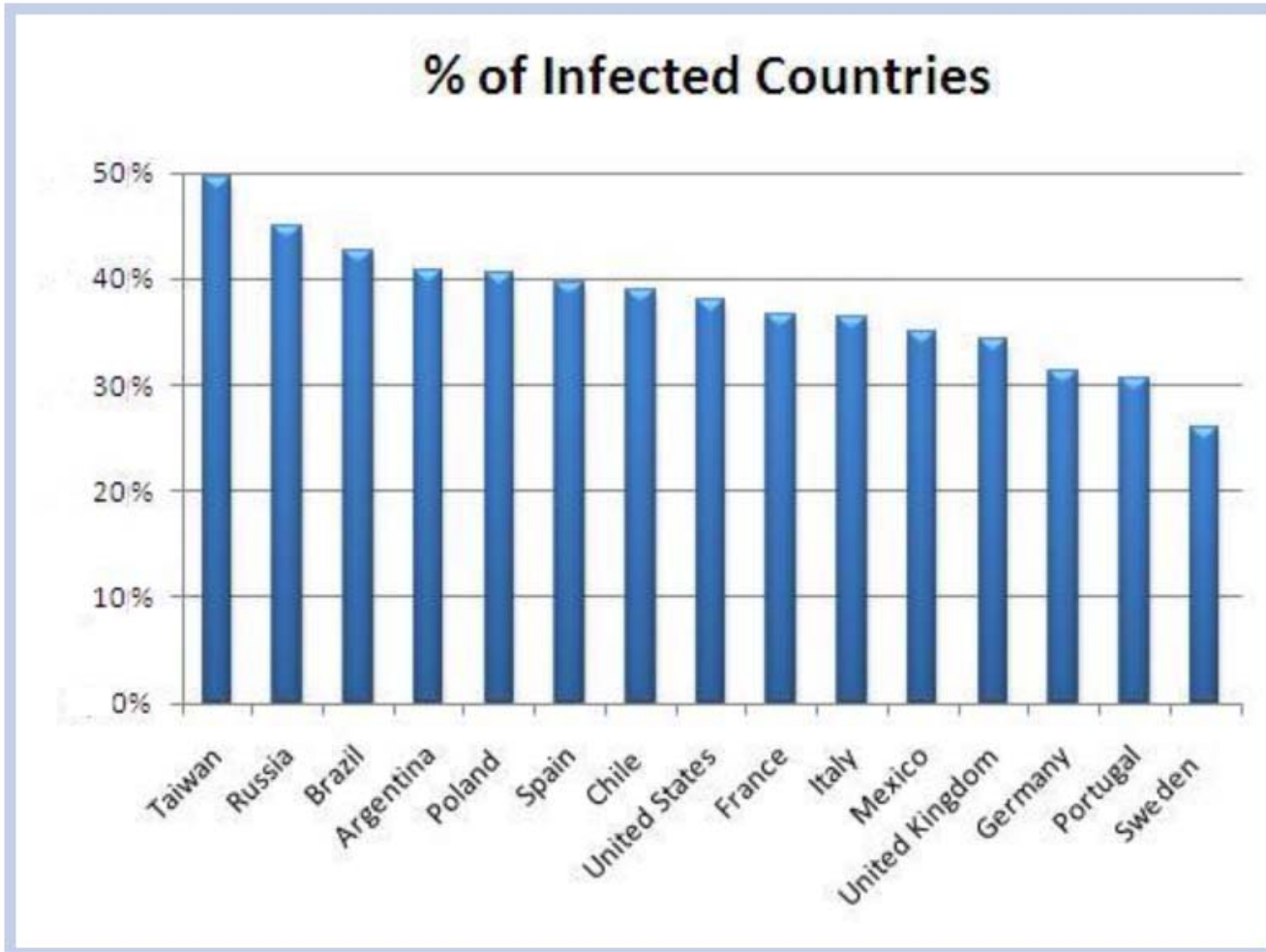
Acknowledge
receipt, lost
packets are
resent,
Reassembled
in order



Disadvantages – White Lists (Practice).

- Bad guys spoof IP addresses of legitimate organisations:
 - > A cheap yet very effective way of having IP addresses included on automated “black” lists.
 - > Removal policy from “black” lists takes days and that is considered fast
- ISP / DNS Resolver operator hands control to third party:
 - > Customer Support staff will receive irate calls from customers yet little ability to edit the Reputation Zone file data
 - > Liability for inappropriate “good” content or “legitimate” bad content being blocked – hit both ways.
- Poor DNS service Users migrate:
 - > Change ISPs
 - > Use external providers like 8.8.8.8
 - > DNSSEC – “Secure” Industry sectors loath to deploy as preventing customer’s access to services is not attractive.

Compromised Routers or PCs by Country



Home DSL Router vulnerability test results

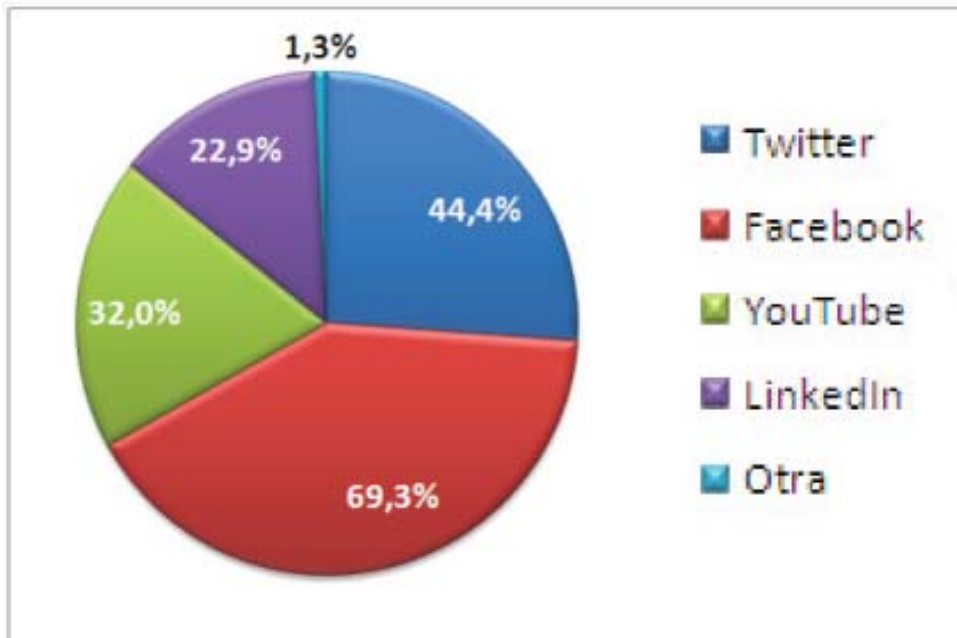
Routers Tested : Sheet1

Vendor	Model	H/W Version	F/W Version	Successful
ActionTec	MI424-WR	Rev. C	4.0.16.1.56.0.10.11.	YES
ActionTec	MI424-WR	Rev. D	4.0.16.1.56.0.10.11.	YES
ActionTec	GT704-WG	N/A	3.20.3.3.5.0.9.2.9	YES
ActionTec	GT701-WG	E	3.60.2.0.6.3	YES
Asus	WL-520gU	N/A	N/A	YES
Belkin	F5D7230-4	2000	4.05.03	YES
Belkin	F5D7230-4	6000	N/A	NO
Belkin	F5D7234-4	N/A	5.00.12	NO
Belkin	F5D8233-4v3	3000	3.01.10	NO
Belkin	F5D6231-4	1	2.00.002	NO
D-Link	DI-524	C1	3.23	NO
D-Link	DI-624	N/A	2.50DDM	NO
D-Link	DIR-628	A2	1.22NA	NO
D-Link	DIR-320	A1	1	NO
D-Link	DIR-655	A1	1.30EA	NO
DD-WRT	N/A	N/A	v24	YES
Dell	TrueMobile 2300	N/A	5.1.1.6	YES
Linksys	BEFW11S4	1	1.37.2	YES
Linksys	BEFSR41	4.3	2.00.02	YES
Linksys	WRT54G3G-ST	N/A	N/A	YES
Linksys	WRT54G2	N/A	N/A	NO
Linksys	WRT160N	1.1	1.02.2	YES
Linksys	WRT54G	3	3.03.9	YES
Linksys	WRT54G	5	1.00.4	NO
Linksys	WRT54GL	N/A	N/A	YES
Netgear	WGR614	9	N/A	NO
Netgear	WNR834B	2	2.1.13_2.1.13NA	NO
OpenWRT	N/A	N/A	Kamikaze r16206	YES
PFSense	N/A	N/A	1.2.3-RC3	YES
Thomson	ST585	6sl	6.2.2.29.2	YES

- It works!! - leave it alone
 - > Majority of home users buy their router and do not install security patches.
 - > UK – 19m DSL Routers, 35% compromised, average upstream say 0.5Mbps = DDoS of 3.3Tbps or 3325Gbps

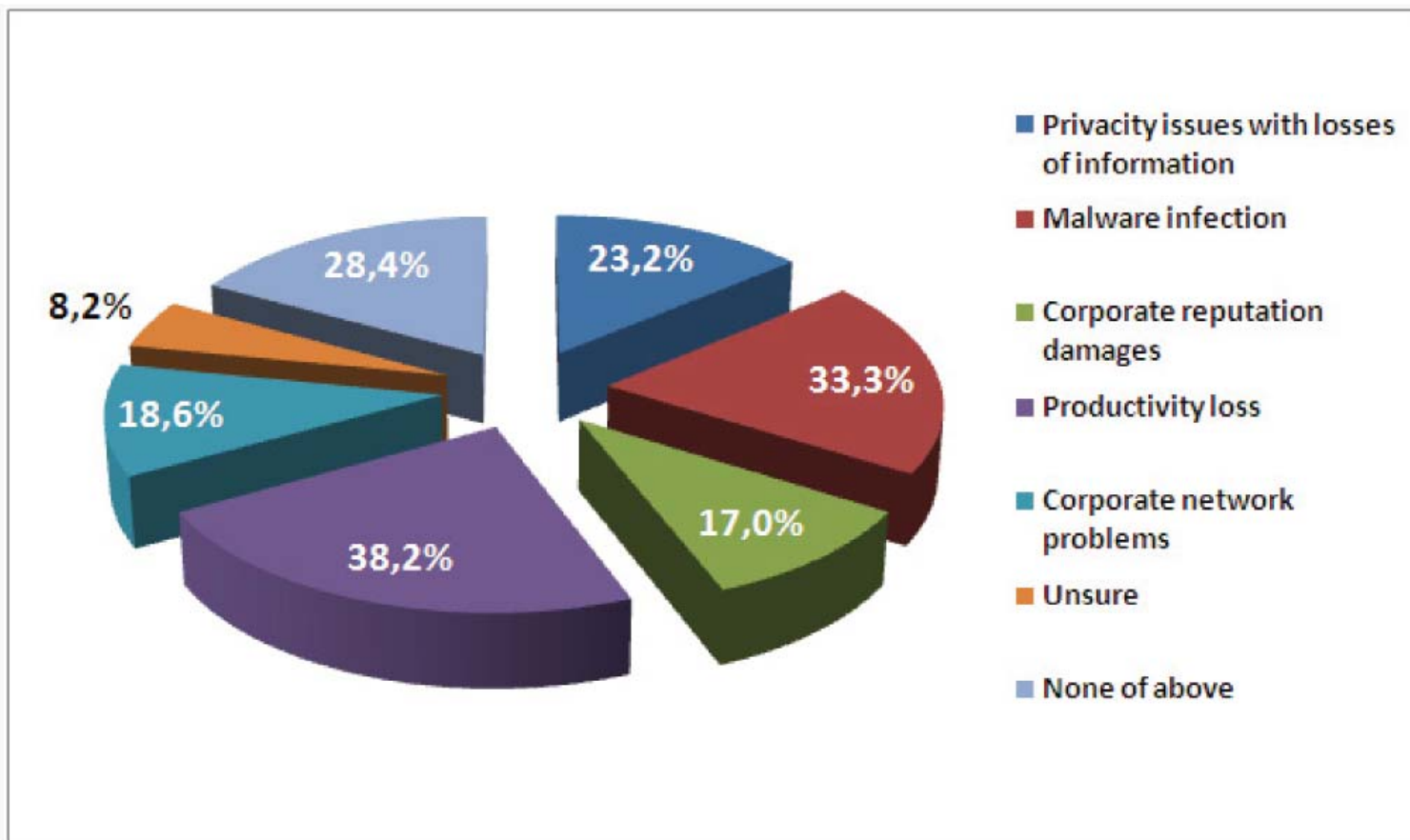
Work - Bad guys "fish, where fish are!"

- In US – 77% of employees use social media during worktime.
- 33% of companies have been infected by malware through social media channel

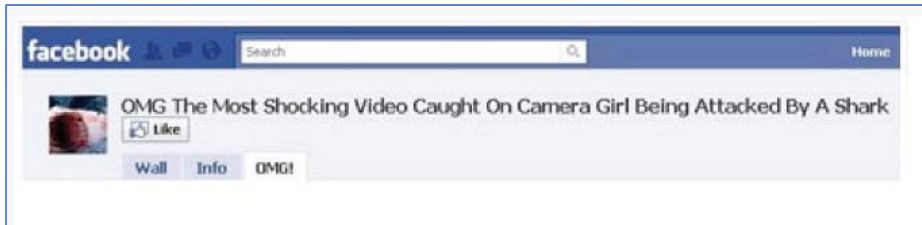


- > 57% of companies have Policies regulating use
- > 81% have staff dedicated to monitoring and implementing Policies
- > 62% do not allow these sites to be accessed
- > Android smart phone are the new target

Why do they do it - Reason for cyber-crime



How the "bad guys" corrupt systems



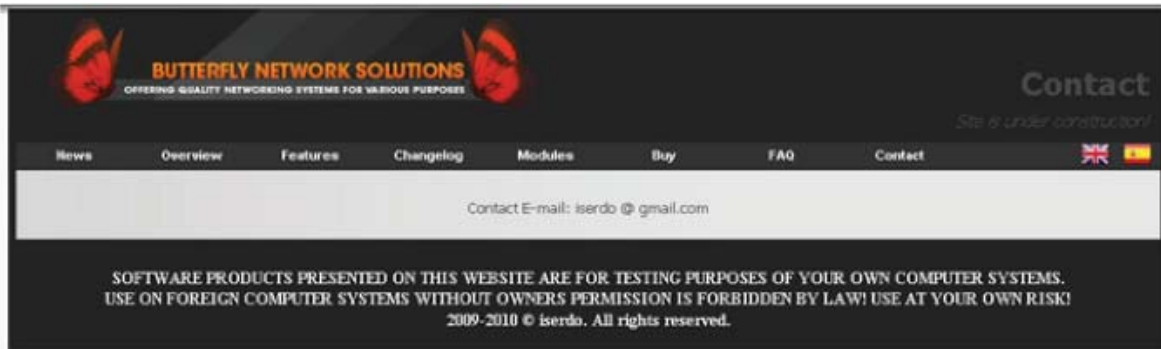
VIDEO
click here to start



Game Apps



Botnets as a Service.



BUTTERFLY NETWORK SOLUTIONS
OFFERING QUALITY NETWORKING SYSTEMS FOR VARIOUS PURPOSES

Contact
Site is under construction!

News Overview Features Changelog Modules Buy FAQ Contact

Contact E-mail: iserdo@gmail.com

SOFTWARE PRODUCTS PRESENTED ON THIS WEBSITE ARE FOR TESTING PURPOSES OF YOUR OWN COMPUTER SYSTEMS.
USE ON FOREIGN COMPUTER SYSTEMS WITHOUT OWNERS PERMISSION IS FORBIDDEN BY LAW! USE AT YOUR OWN RISK!
2009-2010 © iserdo. All rights reserved.

News Overview Features Changelog Modules Buy FAQ Contact

ButterFly Flooder Overview

ButterFly Flooder (BFF) is an advanced command&control system for remote PCs that allows you to fully stress performance and stability of network applications. Besides flooding capabilities it also provides extended commanding options that no other solutions have. The third big feature is modular design, allowing you to pick&load modules on your own. All this built on top of newest Butterfly protocol gives you the best experience and reliability ever!

Purposes of this software are following:

- Flooding your network applications to test performance and stability
- Using as downloader (due to support of downloading files via own protocol; no need to use third party web or ftp servers)
- Using as stable client on your remote PCs for later use
- Using as spreader in your own environment
- Grabbing data sent by browsers with POST method
- Redirecting browsers target websites
- Visiting websites with or without browsers
- Displaying ads (pop-ups) on remotely controlled computers
- Stuffing your own cookies into browsers of remotely controlled computers
- Using clients as proxy servers for personal usage or professional reselling

ButterFly Flooder software system contains:

- Server application (for Windows and Linux based operating systems)
- Master Client application (for Windows)
- Client Builder application (for Windows)
- Reverse Socks Receiver application (for Windows)
- Reverse Socks Server application (for Windows and Linux)
- Manual on how-to-install and how-to-use
- Extra scripts and examples
- Lifetime support and free updates

How much to know your competitors next move?

- **BASIC: 350 EUR**
(BFF core with modules: External Downloader, USB Spreader, MSN Spreader)
- **PREMIUM: 400 EUR**
(BFF core with modules: External Downloader, Basic Flooder, Slowloris Flooder)
- **BUSINESS: 450 EUR**
(BFF core with modules: External Downloader, Visit, Cookie Stuffer, Adware Simple)
- **STANDARD: 600 EUR**
(BFF core with modules: External Downloader, USB Spreader, MSN Spreader, Basic Flooder, Visit, Reverse Socks Simple)
- **SELECTED: 600 EUR**
(BFF core with modules: External Downloader, USB Spreader, MSN Spreader, Basic Flooder, Slowloris Flooder)
- **PROFESSIONAL: 900 EUR**
(BFF core with modules: External Downloader, Visit, Reverse Socks Grabber, Cookie Stuffer, Adware Simple)
- **ULTIMATE: 1100 EUR**
(BFF core with modules: External Downloader, Basic Flooder, Slowloris Flooder, Visit, Reverse Socks Simple, Connect Hook, Post Data Grabber)
- **CUSTOM: price depends on chosen modules**
(BFF core with modules you can choose!)

Prices of modules*

- Basic Flooder: 100 EUR
- Slowloris Flooder: 200 EUR
- USB Spreader: 100 EUR
- MSN Spreader: 100 EUR
- Visit: 100 EUR
- Reverse Socks Simple: 100 EUR
- Post Data Grabber: 200 EUR
- Connect Hook: 200 EUR
- Adware Simple: 100 EUR
- Cookie Stuffer: 200 EUR

* Modules can be purchased seperatedly later at any time. There are no rebuilds needed. Using newly purchased module is very simple (Plug&Play mechanism).

Licenses*

- 3 months: 150 EUR
- 6 months: 250 EUR
- 12 months: 400 EUR

Resilient Internet – Think Contingency!

- Internet is VERY Resilient – BUT
Progress means things are changing.....
 - > To keep ahead of the bad-guys, needs careful monitoring
 - > Encourage staff to regularly scan systems for inconsistencies
 - > Periodically check for inconsistencies such as the way staff terminals use the Internet.
 - > Smart Phones are now the target, so they need scanning where users interact with social media sites and may download viruses.

Security and Fraud Prevention



Paul.Kane@CDNS.net

Thank you