Abuse Management System (AMS)

Mon-Loi Perez

Associate Consultant

Singapore Network Information Centre Pte. Ltd. (SGNIC)

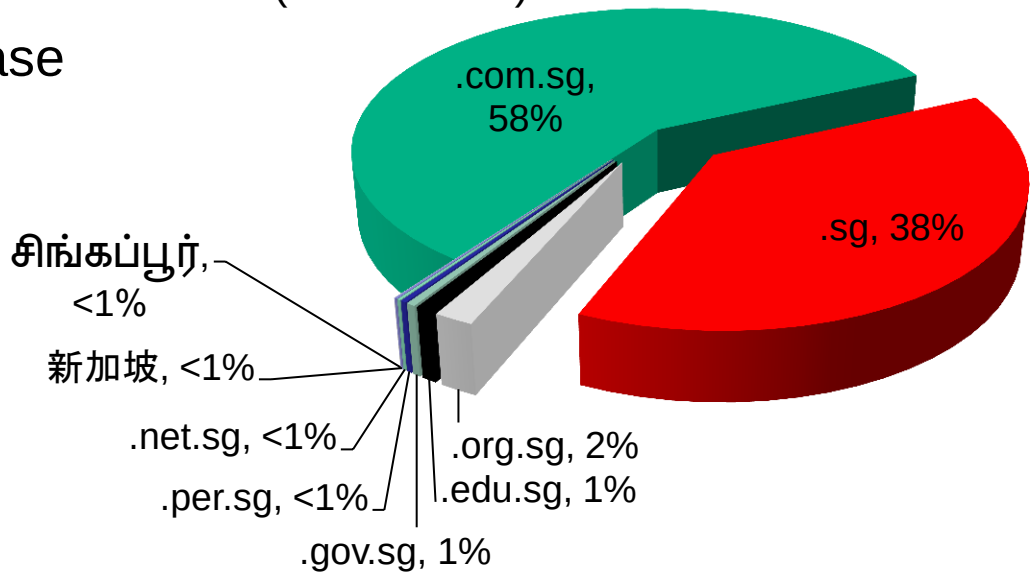
24 March 2014

Agenda

- About SGNIC
- Types of Abuse
- Measures (AMS)
- Statistics and Experiences (AMS)
- Conclusion

About Us

- SGNIC - National domain name (.sg) registry for Singapore
- Wholly-owned subsidiary of IDA Infocomm Development Authority of Singapore)
- Interact with external organizations (ICANN, IANA, APTLD, ccTLDs, APNIC, SingCert, APWG, etc)
- ~155,000 .SG domain names (in Dec 2013)
- ~7% annual increase

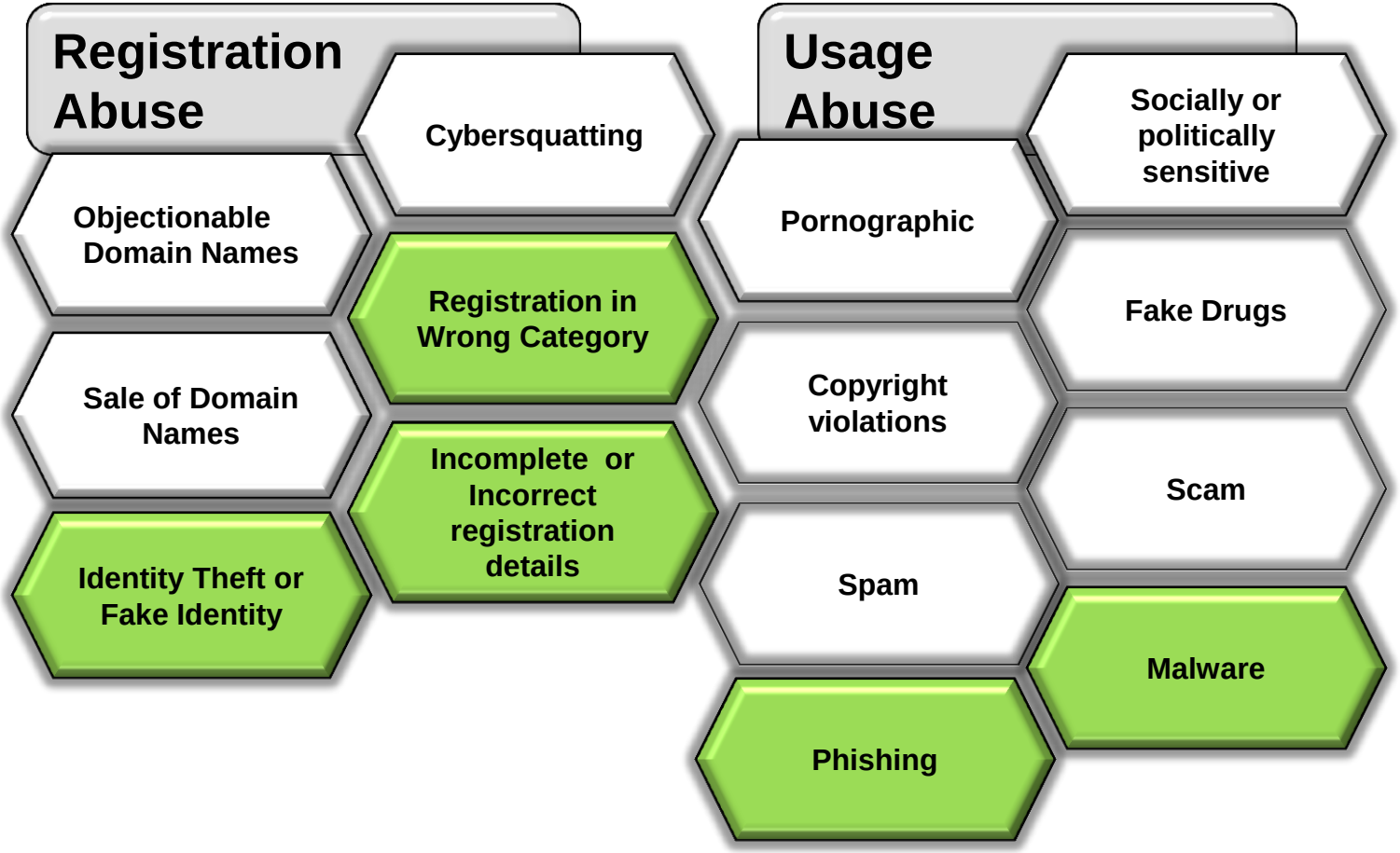


About Us

- 10 employees (3 technical)
- Shared Registry-Registrar System – SGR2R
  - Outsourced service
  - HA setup (x2 servers for critical applications, RAID 1, Redundant Power, Load Balancer, etc.)
  - Solaris and Linux Operating System
  - SPARC and Intel CPU
  - Java Web Application, Oracle Database
  - ~10 servers (will soon be virtualized to 3, 1 for DR)
- Monitoring Systems + NOC (SGR2R vendor and in-house)
  - Monitor uptime, performance and incident correlation.
- 4 secondary nameservers

Types of Abuse

- Abuses that SGNIC is concerned about
- In some areas we feel more effective measures can be done



Measure #1 - Detection and Tracking

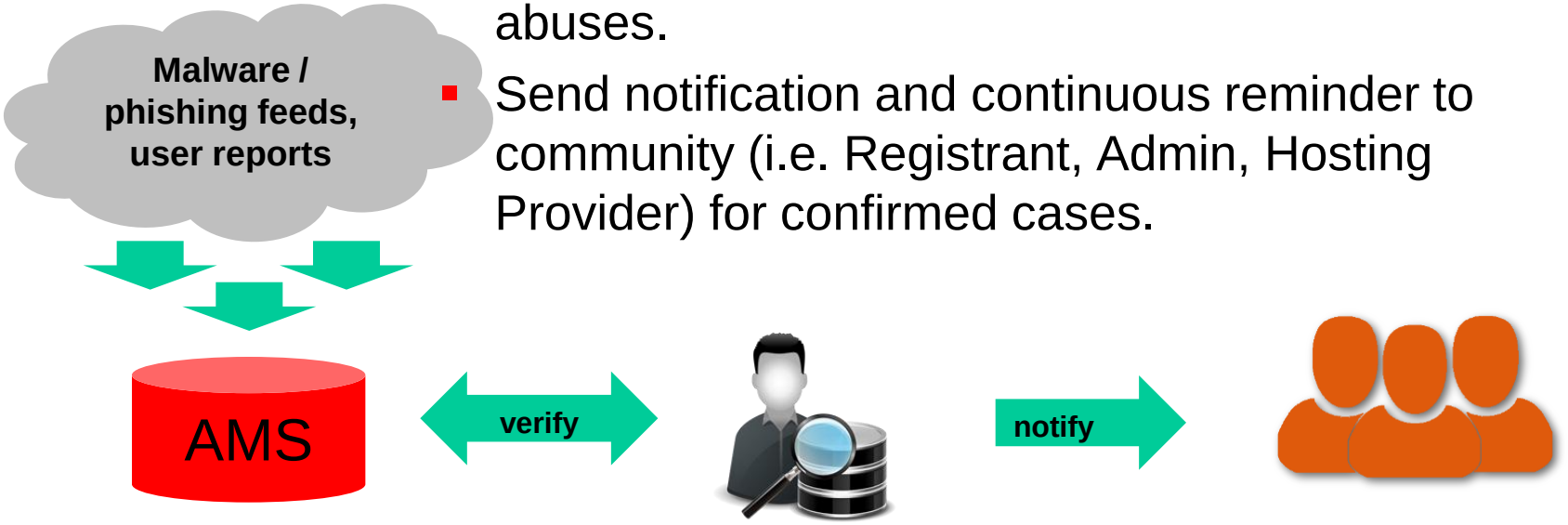
- Abuse Management System (AMS)
  - Software developed in-house
  - LAMP stack (Linux, Apache, MySQL, PHP)
  - Operational in 2011 (after 3-4 months of development)
  - Detects and tracks some domain name abuses (e.g. malware/phishing, incorrect/suspicious registration information, bulk registration, DNS wildcard usage)
  - Provides statistics for tracking and to better understand the nature of some abuses.

AMS
SG DOMAIN NAME
ABUSE MANAGEMENT SYSTEM

Detection and Tracking

AMS
SG DOMAIN NAME ABUSE MANAGEMENT SYSTEM

- Automated scanning of domain name against third party website scanner / reputation databases for malware distribution/phishing activities.
- Manual verification of flagged domains to confirm abuses.
- Send notification and continuous reminder to community (i.e. Registrant, Admin, Hosting Provider) for confirmed cases.



Detection and Tracking

AMS
SG DOMAIN NAME ABUSE MANAGEMENT SYSTEM

- AMS operations view
- Lists relevant information on suspicious domains

Domain name

Status

Application or System Used

Type of Attack

Third-party results

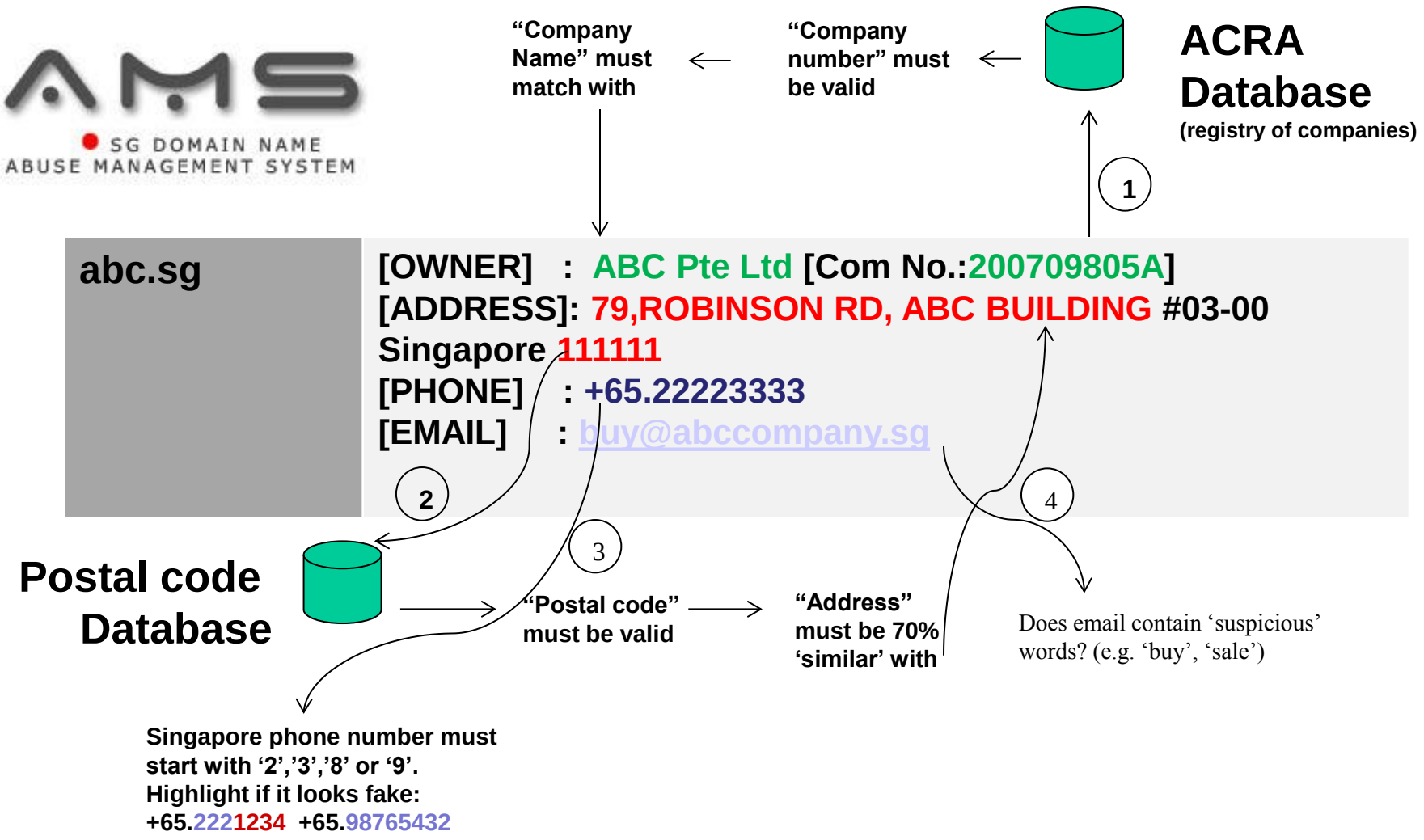
Domainname	Risk Level	Status*	Date Registered (Status)	Date Detected	Application/System Used at the time of the submission (by [redacted])	Type of Attack (by [redacted])	Schedule Tag	Next Scan	Third-party Results (Scanners) [redacted]	[redacted]	[redacted]	[redacted]
[redacted].sg WHOIS IP : [redacted].132	High (ABUSED)	MALWARE/PHISHING CHECKED - POSSIBLE ABUSE (OPEN)	29-Sep-2011 16:14:29 (A)	05-Feb-2014 19:24:08	Application : ... Running on: Microsoft-IIS/7.5 System info: eCommerce Server Powered by: ASP.NET	iFrame Injection Attack Details	H1 [REMOVE]	22-Feb-2014 (H1)	(19-Feb-2014 04:03:12) Scan	Not visited (19-Feb-2014 04:03:12) Scan	Malware found (20-Feb-2014 13:50:39) Scan	Clean (19-Feb-2014 01:45:30) Scan
[redacted].com.sg WHOIS IP : [redacted].130	High (ABUSED)	MALWARE/PHISHING CHECKED - POSSIBLE ABUSE (OPEN)	15-Jun-2010 15:29:03 (A)	09-Feb-2014 08:09:42	Application : ... Running on: Microsoft-IIS/6.0 Powered by: ASP.NET	Javascript Injection Attack Details	H1 [REMOVE]	22-Feb-2014 (H1)	(20-Feb-2014 03:55:21) Scan	Not visited (20-Feb-2014 03:55:21) Scan	Malware found (20-Feb-2014 13:04:43) Scan	Clean (20-Feb-2014 01:41:08) Scan
[redacted].sg WHOIS IP : [redacted]91	High (ABUSED)	MALWARE/PHISHING CHECKED - POSSIBLE ABUSE (OPEN)	16-Aug-2013 09:46:56 (A)	15-Jan-2014 18:33:47	Application : ... Running on: Apache	Others Attack Details	H1 [REMOVE]	22-Feb-2014 (H1)	(20-Feb-2014 04:12:44) Scan	Not visited (20-Feb-2014 04:12:44) Scan	Malware found (20-Feb-2014 14:03:49) Scan	Clean (20-Feb-2014 01:42:56) Scan
[redacted].com.sg WHOIS IP : [redacted].21	High (ABUSED)	MALWARE/PHISHING CHECKED - POSSIBLE ABUSE (OPEN)	05-Nov-2010 23:55:46 (A)	15-Jan-2014 21:43:32	Application : ... Running on: Apache Powered by: PleskLin	Javascript Injection Attack Details	H1 [REMOVE]	22-Feb-2014 (H1)	(20-Feb-2014 04:01:28) Scan	Not visited (20-Feb-2014 04:01:28) Scan	Malware found (20-Feb-2014 13:25:41) Scan	Clean (20-Feb-2014 01:41:35) Scan

Detection and Tracking

- Providing inaccurate registration information is often a precursor to domain abuse
- Provides early warning by checking the accuracy and completeness of new registrant information
  - E.g. Checks for address completeness based on postal code

AMS
SG DOMAIN NAME
ABUSE MANAGEMENT SYSTEM

Detection and Tracking



Detection and Tracking

AMS
SG DOMAIN NAME
ABUSE MANAGEMENT SYSTEM

- Checks suspicious registrations in bulk registrations (i.e. from same registrant, email, telephone number).
- e.g.
  - > 10 domains (all different registrant name) using same email in 1 day
  - > 50 domains (all different registrant name) using same email in 30 days

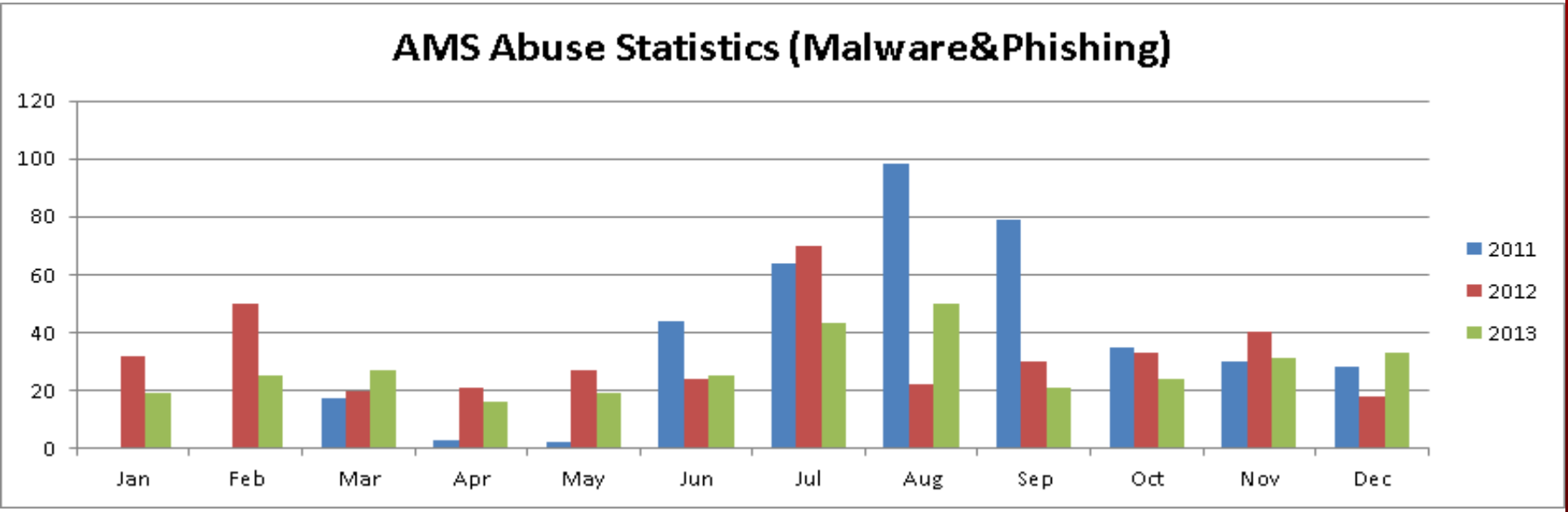
Example of cases detected:

Bulk Registration Tag	Description
BR4-1	66 registrations in 30 days using the email ben.xxx@hotmail.com.
BR4-2	54 registrations in 30 days using the phone no. +65.9872XXXX

Detection and Tracking

AMS
SG DOMAIN NAME ABUSE MANAGEMENT SYSTEM

- AMS continually monitors all domain names
  - All new names are scanned weekly for 3 months, then monthly scans
- Abuse statistics (in Jan 2014)
  - **~156,000** - Domain names scanned by AMS
  - **~30** – confirmed abuses per month

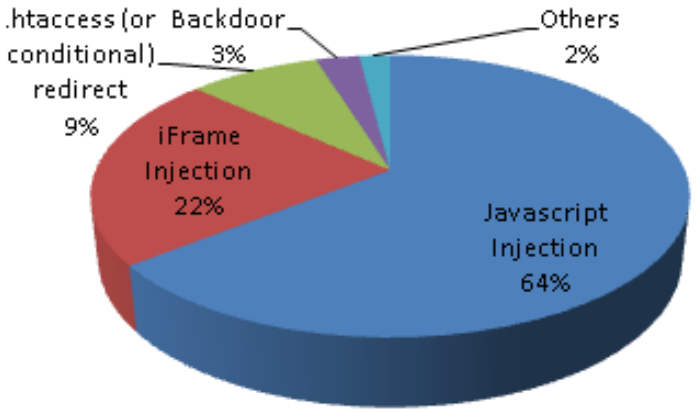


Detection and Tracking

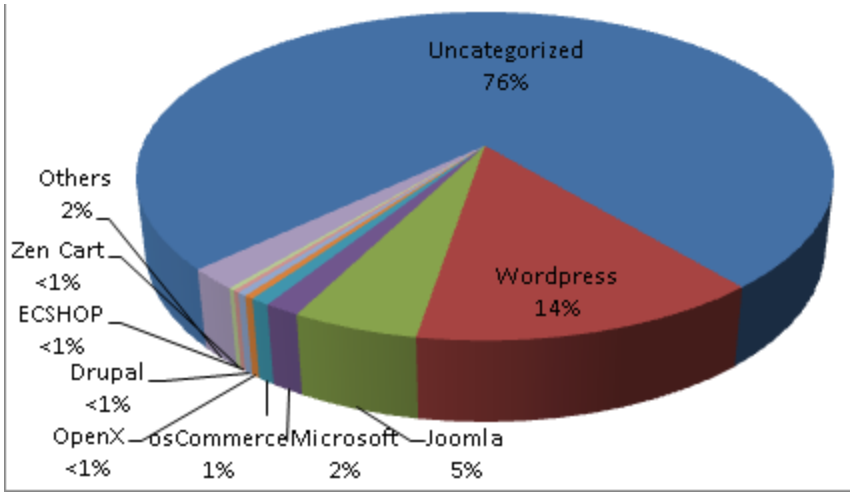
AMS
SG DOMAIN NAME ABUSE MANAGEMENT SYSTEM

- AMS gathers data over time
  - Attacks found on abused websites
  - Applications found on abused websites (usually plugins are insecure rather than the application)

Attacks found on abused websites



Applications found on abused websites



Measure #2 - Enforcement

- Actively enforce against all other types of abuses.
- For malware and phishing:
  - “Time is of the essence” hence its critical to send quick and timely advices to parties who may be involved (ISP, website hosting provider, registrant, admin and tech contact) for them to take action
  - Formalised collaboration with SingCERT who can provide expert opinion
  - For serious breaches: suspend or delete based on violations from registrant agreement

Success Stories

- In July 2012, a vulnerability in a popular web hosting panel was found.
  - Multiple .sg websites were affected
  - Contacted hosting provider to patch the vulnerability
  - Affected websites were cleaned
- Shorten the life of malicious domains on the internet
- ~80% resolution rate per month.

Challenges

- "Conditional redirects/.htaccess" malware
  - It only works based on certain conditions (i.e. Search engine based, IP-based, etc.)
  - Registrants and hosting providers are unaware of this hence they think it's a false detection.
- Some miscommunication…
  - SGNIC notified registrant and hosting provider
  - Hours after, hosting provider has acted but did not update SGNIC
  - Then registrant checks the issue and thinks its false-positive

Conclusion

- Be more proactive and informed, time is of the essence
  - More sources for more detection, work with local CERT for expert opinion, continuous reminders
- Registrant's domain name is critical to their business
  - Be mindful of your actions (e.g. domain suspension)
- Most registrants and hosting providers are keen to work with us
- Our efforts only help mitigate some abuses and may not solve the real issue which is to prevent abuse….
- But… at the end of the day, everyone seems to be happy with our efforts of taking harm away from the Internet

Any Questions?

Thank you!

Mon-Loi Perez