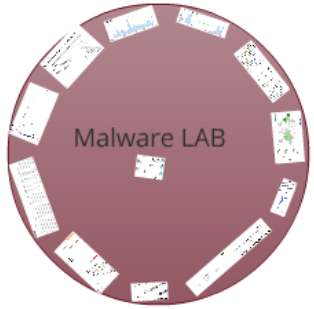
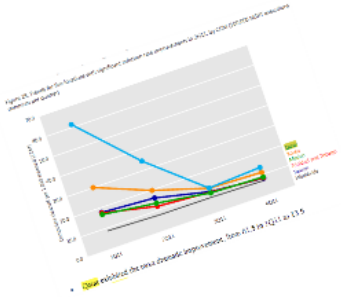
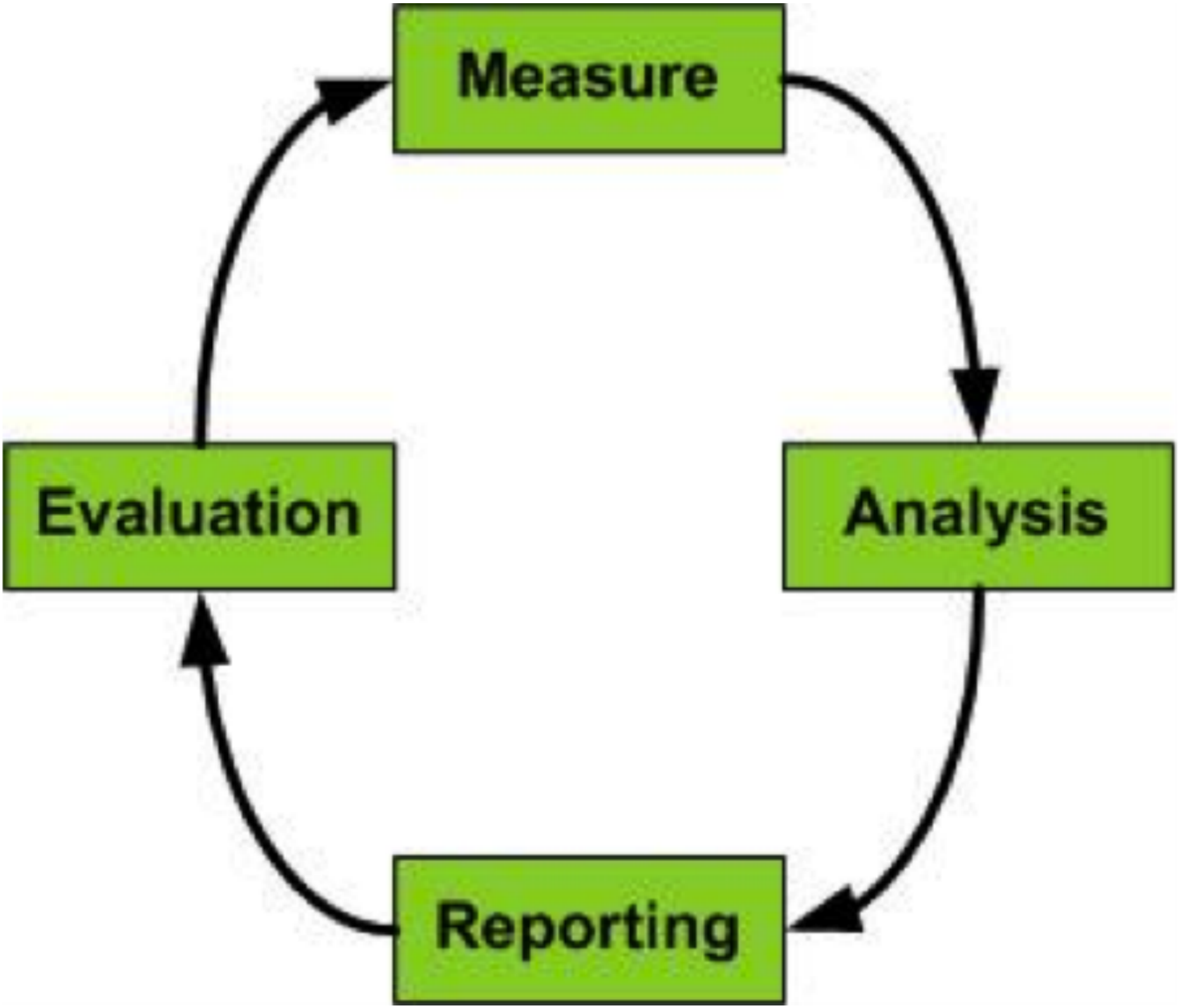

Q-CERT

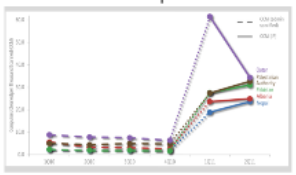

Malware LAB

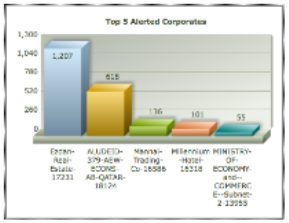


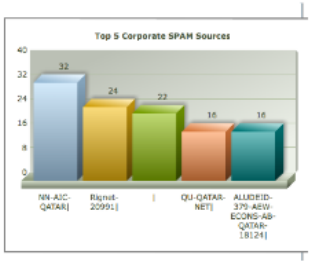

Q-CERT

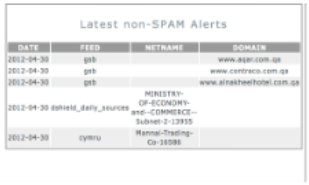

Measure
Analysis
Reporting
Evaluation

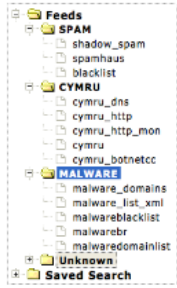
Microsoft Report 2011

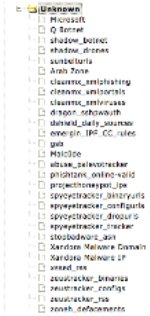




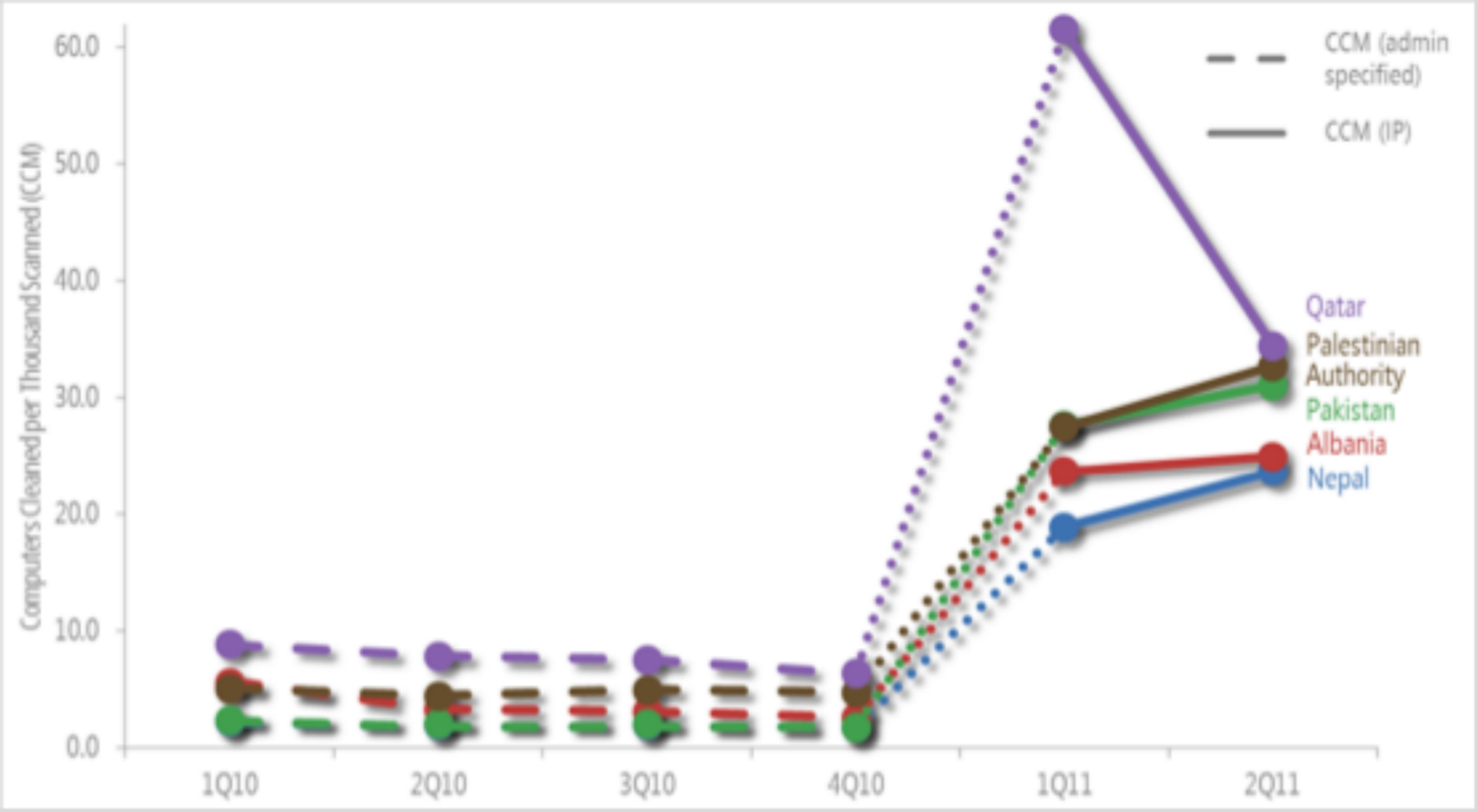


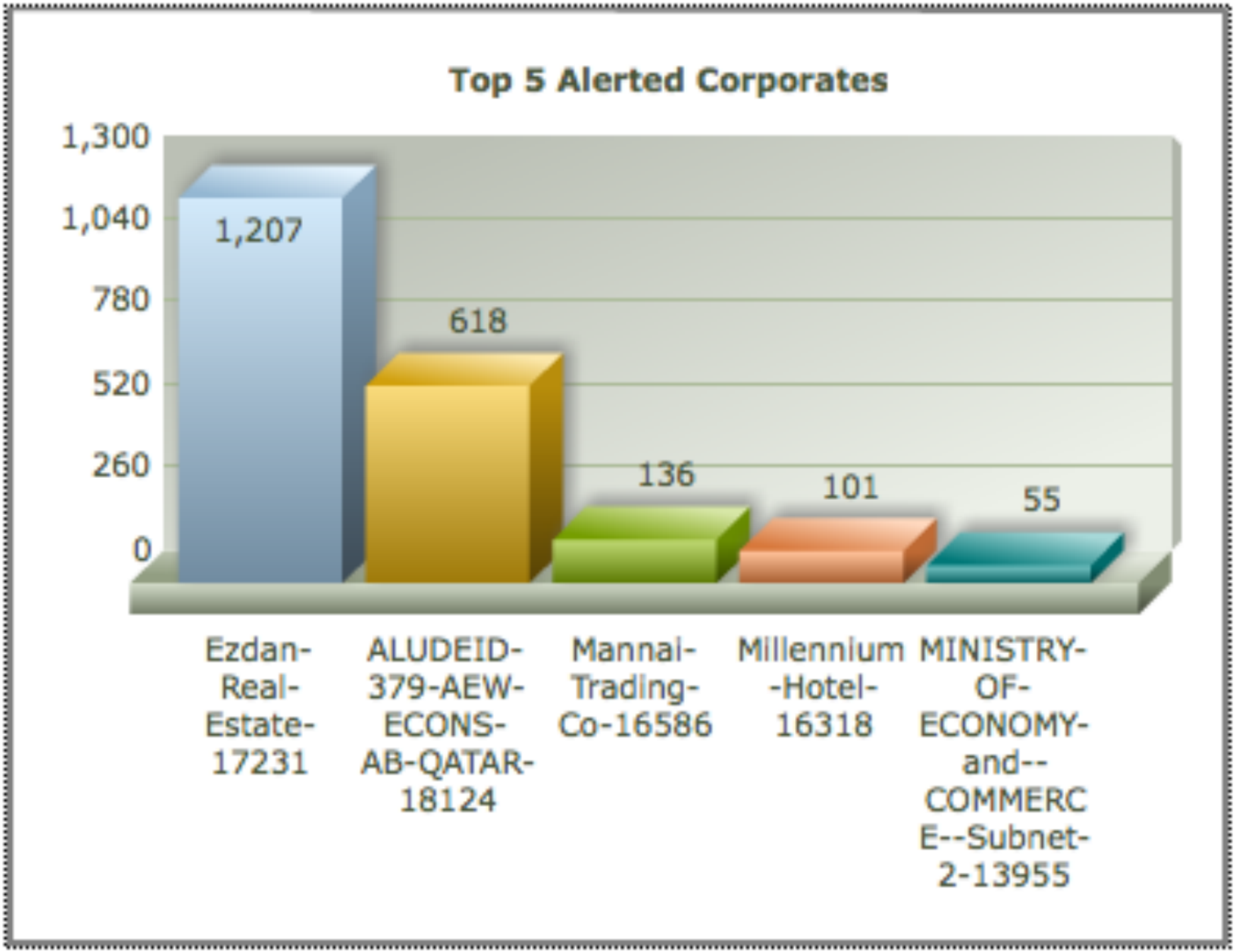


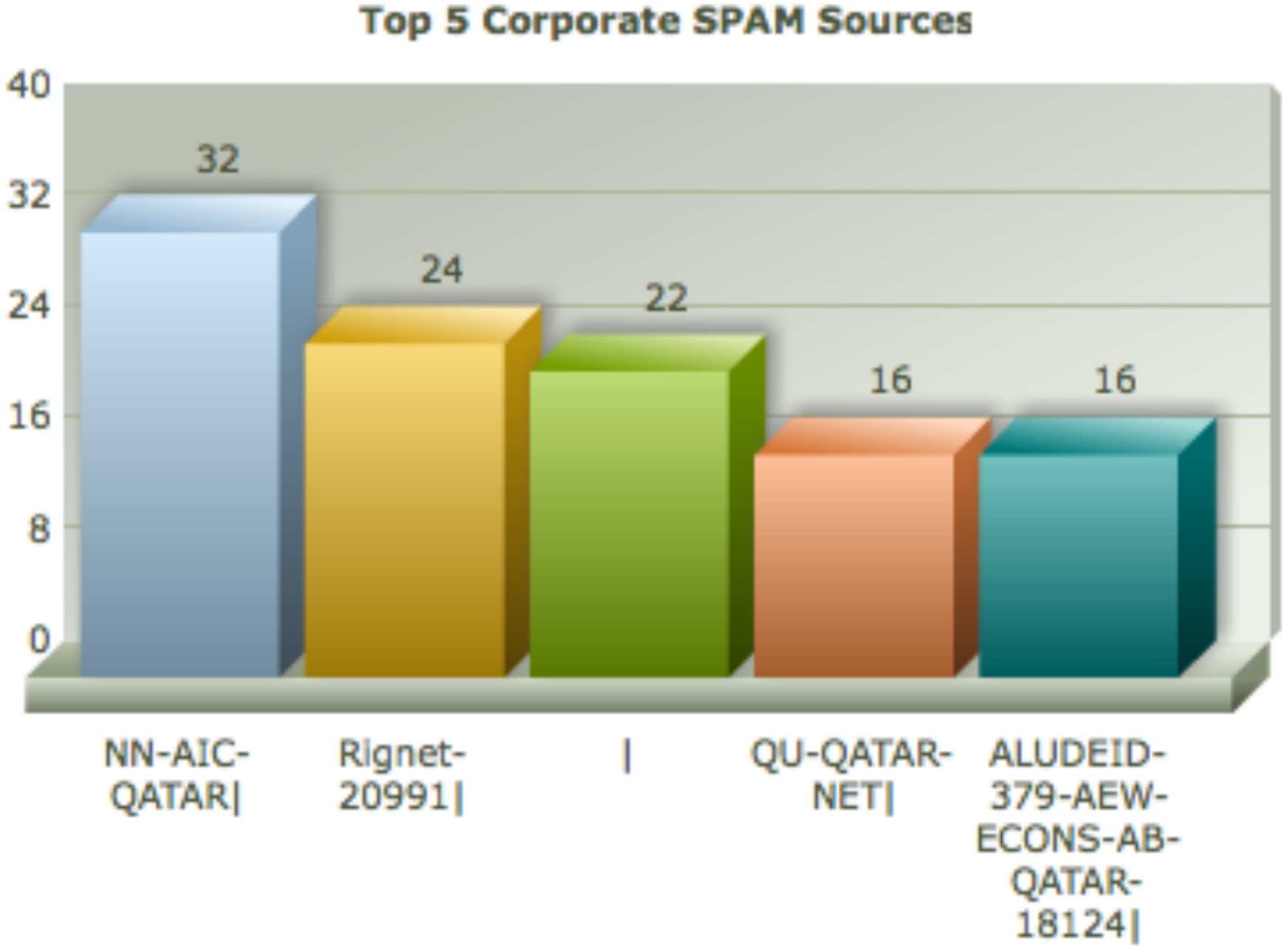




Microsoft Report 2011

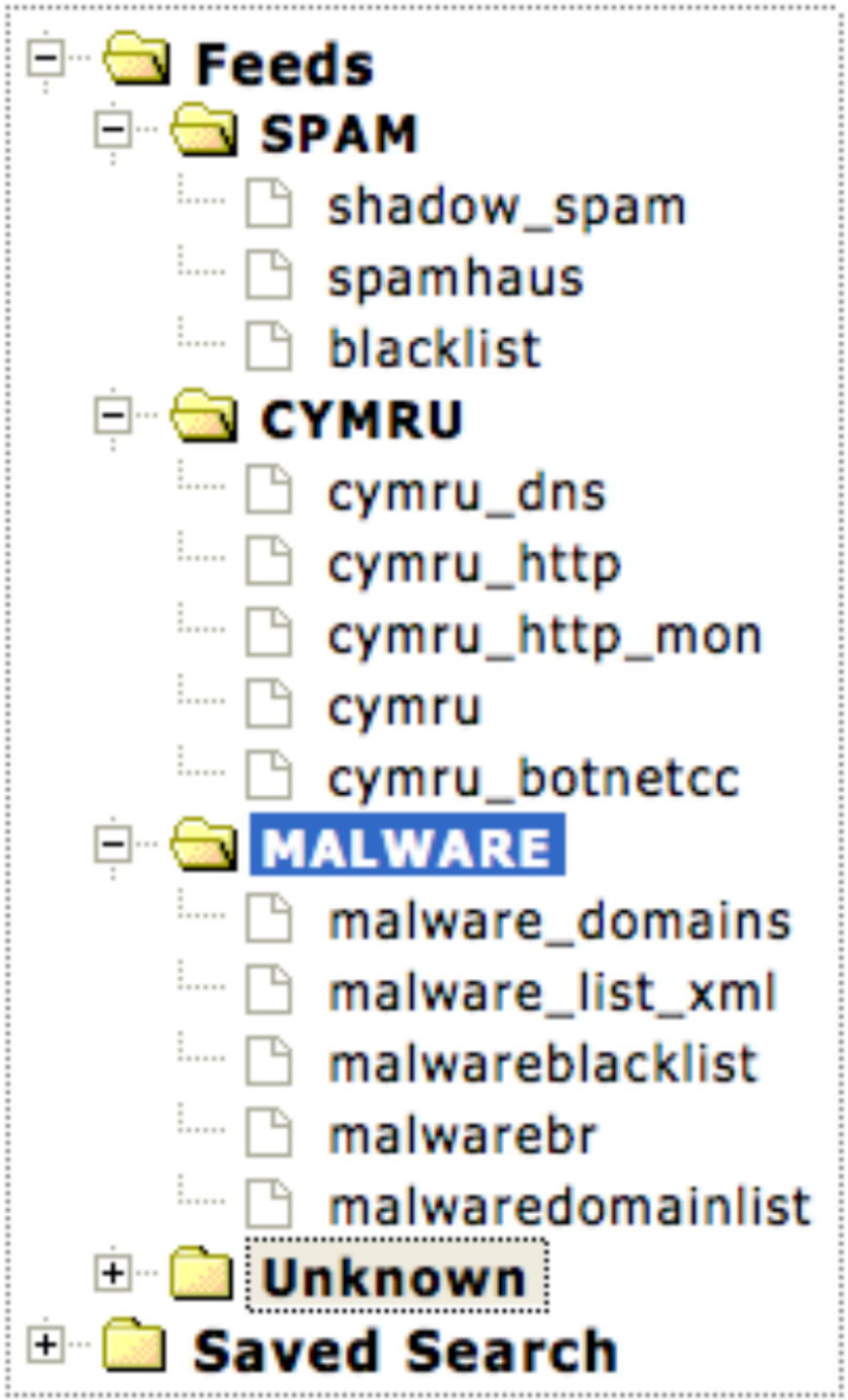


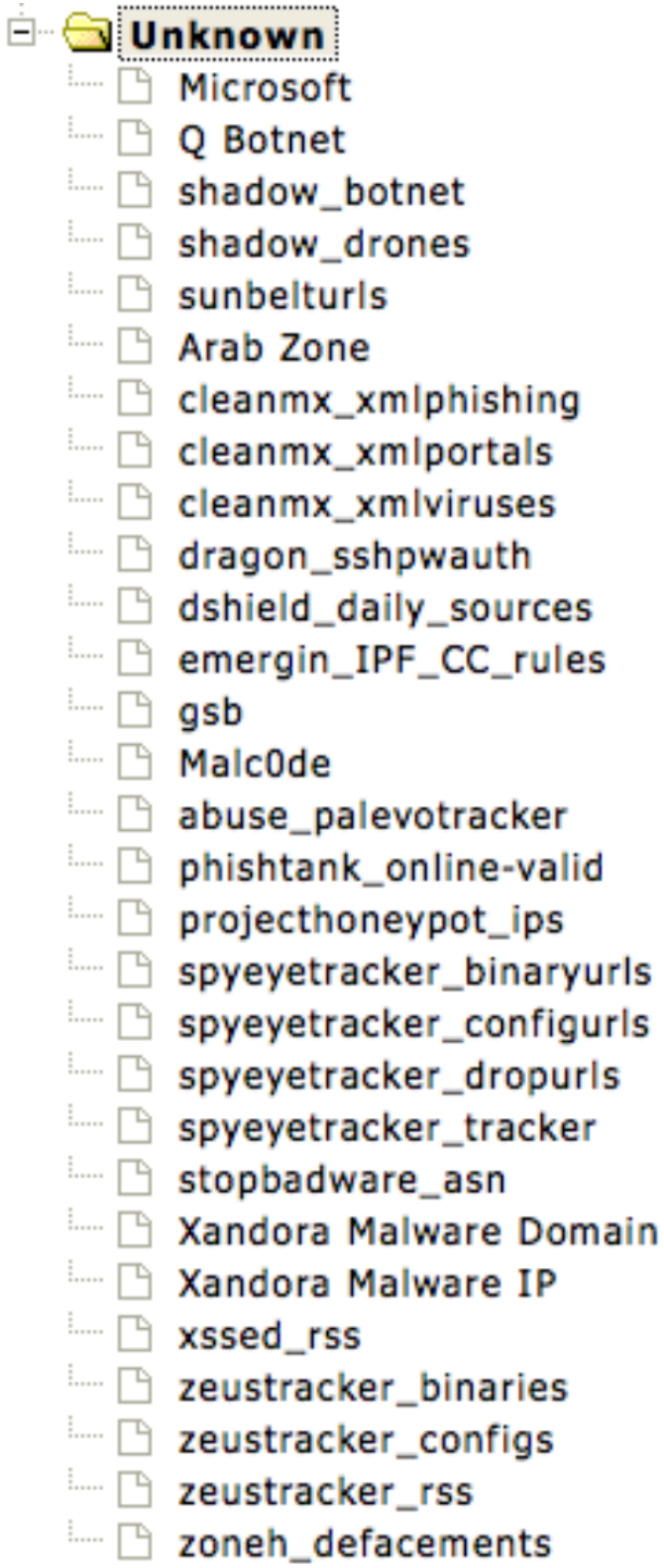

Top 5 Alerted Corporates
1,300
1,040
780
520
260
0
1,207
618
136
101
55
Ezdan-Real-Estate-17231
ALUDEID-379-AEW-ECONS-AB-QATAR-18124
Mannai-Trading-Co-16586
Millennium-Hotel-16318
MINISTRY-OF-ECONOMY-and--COMMERCE--Subnet-2-13955

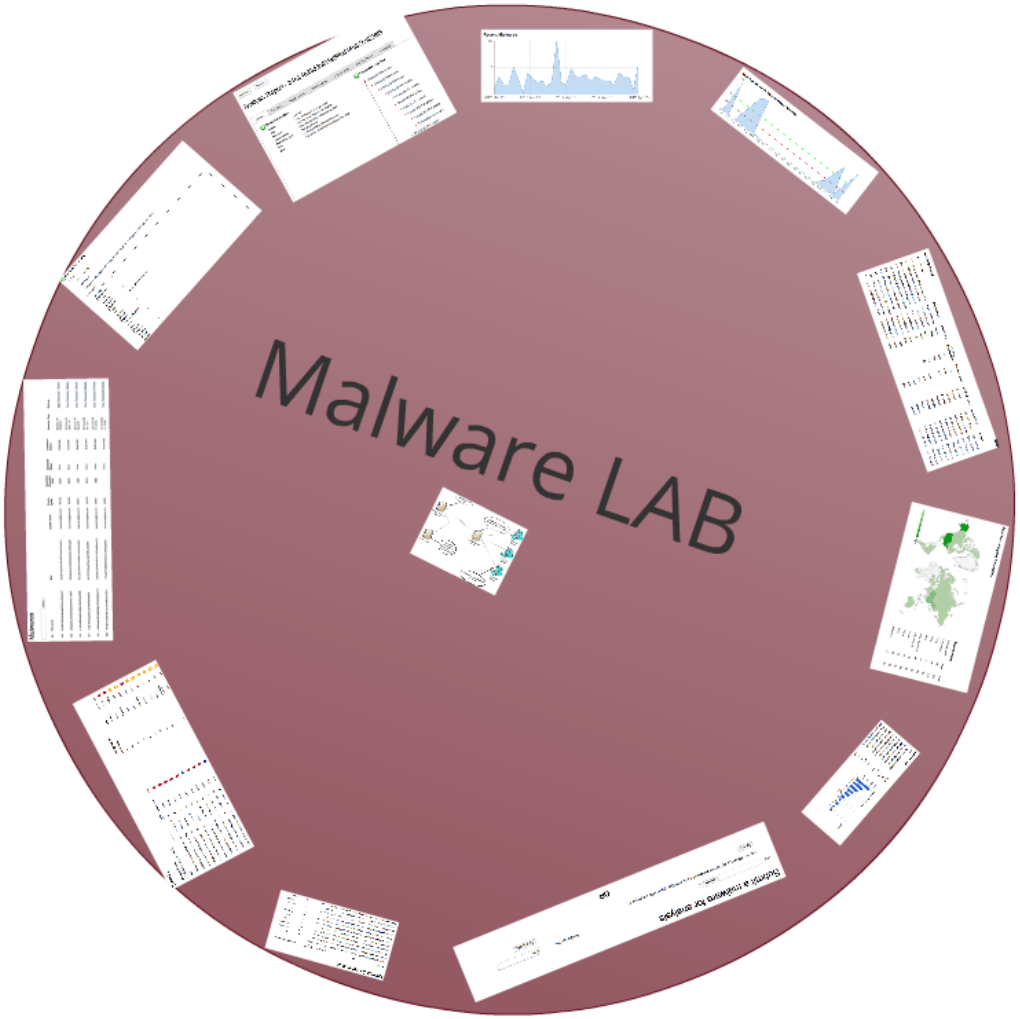

Top 5 Corporate SPAM Sources
40
32
24
16
8
0
32
24
22
16
16
NN-AIC-QATAR|
Rignet-20991|
|
QU-QATAR-NET|
ALUDEID-379-AEW-ECONS-AB-QATAR-18124|

Latest non-SPAM Alerts

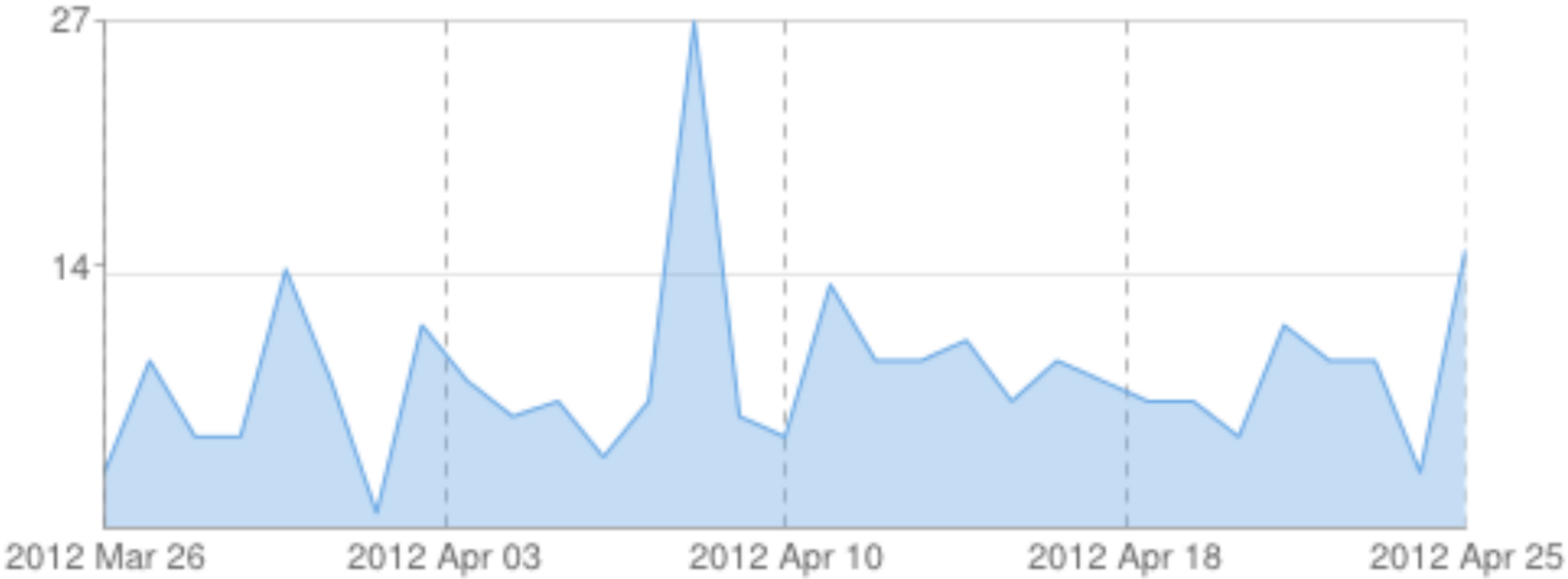
DATE	FEED	NETNAME	DOMAIN
2012-04-30	gsb		www.aqar.com.qa
2012-04-30	gsb		www.contraco.com.qa
2012-04-30	gsb		www.alnakheelhotel.com.qa
2012-04-30	dshield_daily_sources	MINISTRY-OF-ECONOMY-and--COMMERCE--Subnet-2-13955	
2012-04-30	cymru	Mannai-Trading-Co-16586	


Feeds
SPAM
shadow_spam
spamhaus
blacklist
CYMRU
cymru_dns
cymru_http
cymru_http_mon
cymru
cymru_botnetcc
MALWARE
malware_domains
malware_list_xml
malwareblacklist
malwarebr
malwaredomainlist
Unknown
Saved Search

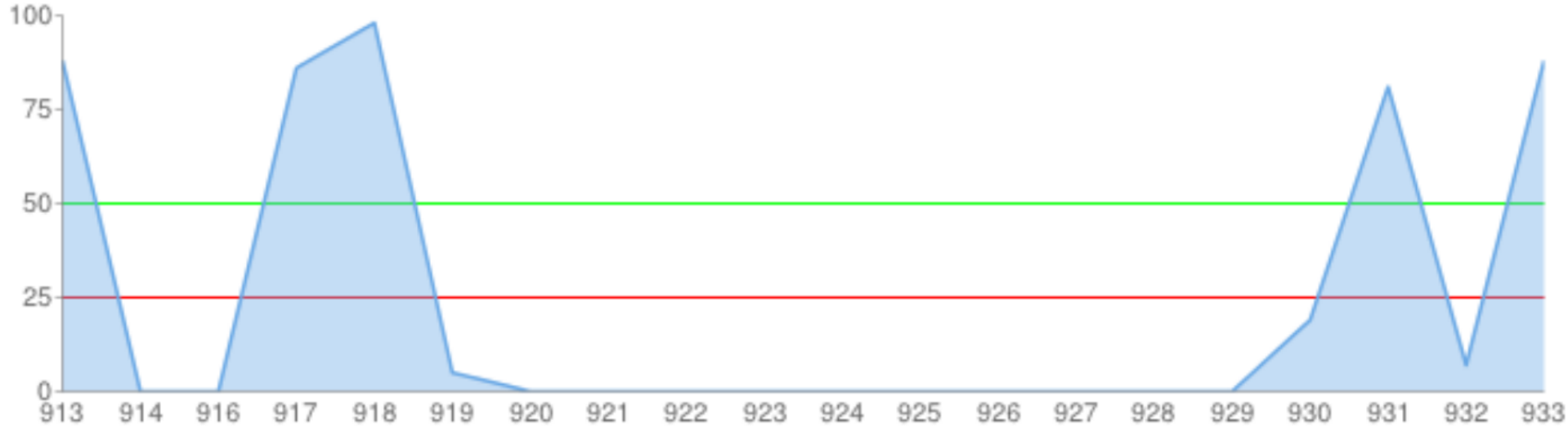

Unknown
Microsoft
Q Botnet
shadow_botnet
shadow_drones
sunbelturls
Arab Zone
cleanmx_xmlphishing
cleanmx_xmlportals
cleanmx_xmlviruses
dragon_sshpwauth
dshield_daily_sources
emergin_IPF_CC_rules
gsb
Malc0de
abuse_palevotracker
phishtank_online-valid
projecthoneypot_ips
spyeyetracker_binaryurls
spyeyetracker_configurls
spyeyetracker_dropurls
spyeyetracker_tracker
stopbadware_asn
Xandora Malware Domain
Xandora Malware IP
xssed_rss
zeustracker_binaries
zeustracker_configs
zeustracker_rss
zoneh_defacements


Malware LAB

Recent Malwares



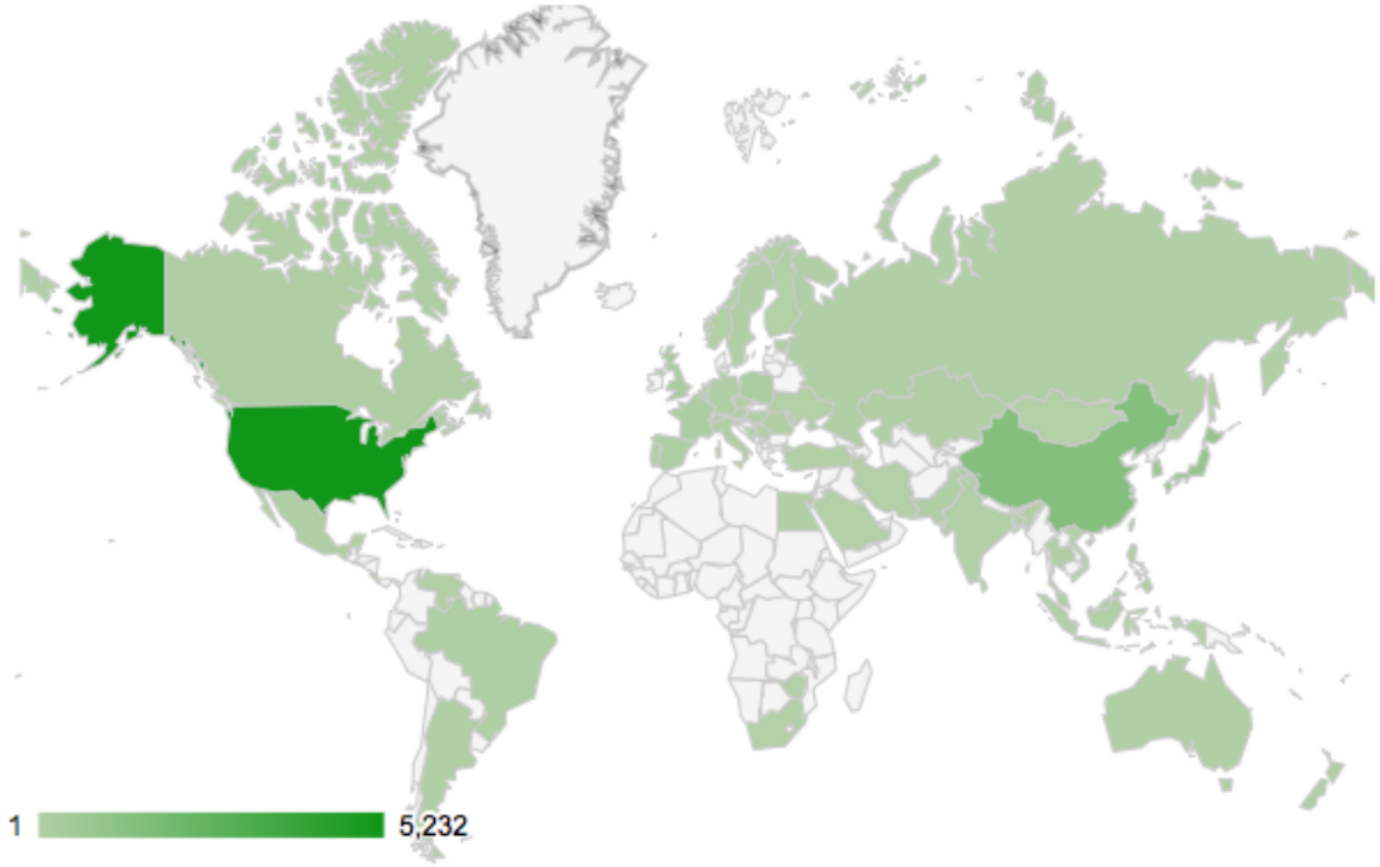
Virustotal (Recent 20 malwares through Dionaea)



Recent Malwares

ID	File name	Sender Email	Size(in bytes)	VirusTotal (Detection Rate)	Sandbox1 Status	Sandbox2 Status	Received Date	Analysis
934	320267a5832d36ed857fcc443fce467c	mounirme@me.com	167403	39/42	Done	Submitted	2012-04-25 16:48:45	View | Resubmit
933	d69a6b9cd4505b5fe8c663c4873da6f7	mounirme@me.com	165528	38/43	Done	Submitted	2012-04-25 15:41:19	View | Resubmit
932	b1e24e23d3ef21e6ffbd14b87ba238f5	mounirme@me.com	25600	3/42	Done	Submitted	2012-04-25 14:42:37	View | Resubmit
931	4530167b9aaf54aa3a045ffee5fef5f5	mounirme@me.com	154760	35/43	Done	Submitted	2012-04-25 14:15:11	View | Resubmit
930	92806ea03919e85b5e10f74b98decd15	mounirme@me.com	25600	8/42	Done	Submitted	2012-04-25 13:02:42	View | Resubmit
929	7f7a247c2f90d461dce4edd602a25fca	mounirme@me.com	63488	-	Done	Submitted	2012-04-25 01:32:48	View | Resubmit
928	63c1367aba427cbcac4bd1e7f427d7e2	mounirme@me.com	63488	-	Done	Submitted	2012-04-25 01:32:16	View | Resubmit
927	a9e46712b6ab9b68e4632ac7181d8ced	mounirme@me.com	63488	-	Done	Submitted	2012-04-25 01:28:38	View | Resubmit
926	4105c4f93a8ef9a43242dcac2c1ac48e	mounirme@me.com	63488	-	Done	Submitted	2012-04-25 01:27:48	View | Resubmit
925	0a7c42b386c995228c63feb7167affc4	mounirme@me.com	63488	-	Done	Submitted	2012-04-25 01:24:23	View | Resubmit

Geo Chart - Outgoing Connections

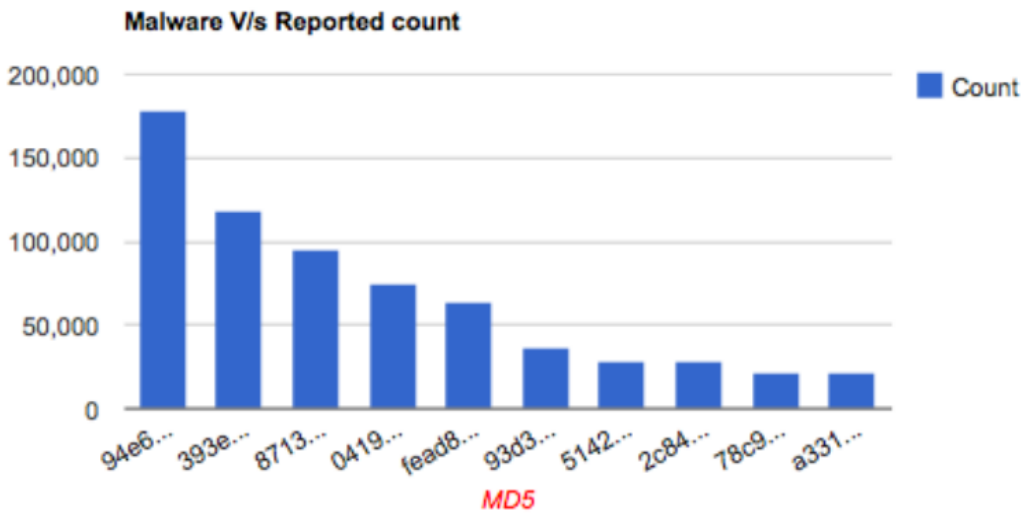


Top countries

Country name	Code	Count
United States	US	5232
China	CN	1518
Qatar	QA	983
Japan	JP	953
Korea, Republic of	KR	756
United Kingdom	GB	325
France	FR	234
Poland	PL	231
Spain	ES	198
Switzerland	CH	183

Malwares Count

MD5	Count
94e689d7d6bc7c769d09a59066727497	178903
393e2e61ff08a8f7439e3d2cfcb8056f	118773
87136c488903474630369e232704fa4d	95541
04199a5b981fd5a3d846d3f9d4c1d574	74677
fead84c5df2e585749a8da2ce583c926	63322
93d305c9094278e3e6da70e40b543c28	36722
5142a66aaeb9423066e8d53dc5f78294	29154
2c8442c4a9328a5cf26650fa6fe743ef	28902
78c9042bbcefd65beaa0d40386da9f89	22233
a331119fe6d70bcb1c423d28743a4d86	21295



Submit a malware for analysis

File [ ] Browse...

Are you uploading a zip file with password? If yes, then click here to enter the password.

Submit

OR

Suspicious URL [http://]

Submit URL

Malware Connections List

File name	Md5	Outgoing IP	Connection status	Country code	Country name
d69a6b9cd4505b5fe8c663c4873da6f7	d69a6b9cd4505b5fe8c663c4873da6f7	192.168.1.109	INVALID		
d69a6b9cd4505b5fe8c663c4873da6f7	d69a6b9cd4505b5fe8c663c4873da6f7	212.77.192.59	OK	QA	Qatar
d69a6b9cd4505b5fe8c663c4873da6f7	d69a6b9cd4505b5fe8c663c4873da6f7	207.150.212.134	OK	US	United States
d69a6b9cd4505b5fe8c663c4873da6f7	d69a6b9cd4505b5fe8c663c4873da6f7	91.198.22.70	OK	GB	United Kingdom
d69a6b9cd4505b5fe8c663c4873da6f7	d69a6b9cd4505b5fe8c663c4873da6f7	46.19.143.130	OK	CH	Switzerland
d69a6b9cd4505b5fe8c663c4873da6f7	d69a6b9cd4505b5fe8c663c4873da6f7	208.87.34.15	OK	BS	Bahamas
d69a6b9cd4505b5fe8c663c4873da6f7	d69a6b9cd4505b5fe8c663c4873da6f7	23.20.103.142	OK	US	United States
d69a6b9cd4505b5fe8c663c4873da6f7	d69a6b9cd4505b5fe8c663c4873da6f7	89.211.42.58	OK	QA	Qatar
d69a6b9cd4505b5fe8c663c4873da6f7	d69a6b9cd4505b5fe8c663c4873da6f7	143.215.143.11	OK	US	United States
d69a6b9cd4505b5fe8c663c4873da6f7	d69a6b9cd4505b5fe8c663c4873da6f7	143.215.130.33	OK	US	United States
d69a6b9cd4505b5fe8c663c4873da6f7	d69a6b9cd4505b5fe8c663c4873da6f7	221.8.69.25	OK	CN	China

Trends

Malware Trends

--- Select country ---- Export

Md5	Count	IP	Country code	Country name	Trend
94e689d7d6bc7c769d09a59066727497	641	114.173.244.196	JP	Japan	
93d305c9094278e3e6da70e40b543c28	286	118.9.91.60	JP	Japan	
4f48815b0b6bf1c51ee8e9082c763df7	2486	118.4.7.154	JP	Japan	
c3852074ee50da92c2857d24471747d9	3855	80.37.168.180	ES	Spain	
87136c488903474630369e232704fa4d	381	2.142.5.32	ES	Spain	
87136c488903474630369e232704fa4d	10	114.149.94.254	JP	Japan	
93d305c9094278e3e6da70e40b543c28	424	1.174.139.113	TW	Taiwan	
d2eabe15257a453416efa18992d1edbd	342	114.46.156.231	TW	Taiwan	
78c9042bbcefd65beaa0d40386da9f89	172	118.166.117.206	TW	Taiwan	
94e689d7d6bc7c769d09a59066727497	6	118.6.153.207	JP	Japan	

Country Trends

Country name	Code	Count	Trend
JP	Japan	674712	
TW	Taiwan	123525	
PH	Philippines	39445	
QA	Qatar	27742	
ES	Spain	20471	
US	United States	17332	
MA	Morocco	5927	
CN	China	2417	
CL	Chile	1474	
AE	United Arab Emirates	1366	
CA	Canada	1069	

Malwares

Search

No	File name	MD5	Sender Email	Size(in bytes)	VirusTotal (Detection Rate)	Sandbox1 Status	Sandbox2 Status	Received Date	Actions
934	320267a5832d36ed857fcc443fce467c	320267a5832d36ed857fcc443fce467c	mounirme@me.com	167403	39/42	Done	Submitted	2012-04-25 16:48:45	View | Resubmit | Delete
933	d69a6b9cd4505b5fe8c663c4873da6f7	d69a6b9cd4505b5fe8c663c4873da6f7	mounirme@me.com	165528	38/43	Done	Submitted	2012-04-25 15:41:19	View | Resubmit | Delete
932	b1e24e23d3ef21e6ffbd14b87ba238f5	b1e24e23d3ef21e6ffbd14b87ba238f5	mounirme@me.com	25600	3/42	Done	Submitted	2012-04-25 14:42:37	View | Resubmit | Delete
931	4530167b9aaf54aa3a045ffee5fef5f5	4530167b9aaf54aa3a045ffee5fef5f5	mounirme@me.com	154760	35/43	Done	Submitted	2012-04-25 14:15:11	View | Resubmit | Delete
930	92806ea03919e85b5e10f74b98decd15	92806ea03919e85b5e10f74b98decd15	mounirme@me.com	25600	8/42	Done	Submitted	2012-04-25 13:02:42	View | Resubmit | Delete
929	7f7a247c2f90d461dce4edd602a25fca	7f7a247c2f90d461dce4edd602a25fca	mounirme@me.com	63488	-	Done	Submitted	2012-04-25 01:32:48	View | Resubmit | Delete

VirusTotal Report (3/42)

- Date

  2012-04-25 09:57:25

- Permenant Link

  http://www.virustotal.com/file/c0fd60815419b23b83d2381a1af72adb44d76c6be1be4d6a6e96cc8c50b30d2c/analysis/

- Scan Details

NProtect	:
CAT-QuickHeal	:
McAfee	:
TheHacker	:
K7AntiVirus	:
VirusBuster	:
NOD32	: a variant of Win32/Injector.QNT
F-Prot	:
Symantec	:
Norman	:
ByteHero	:
TrendMicro-HouseCall	:
Avast	:
ESafe	:
ClamAV	:
Kaspersky	:
BitDefender	:
ViRobot	:
Emsisoft	:

Sandbox 1 | Sandbox 2

Analysis Report - b1e24e23d3ef21e6ffbd14b87ba238f5

Summary | File Activity | Registry Activity | Network Activity | Process Details | Virus Total Report | Downloads

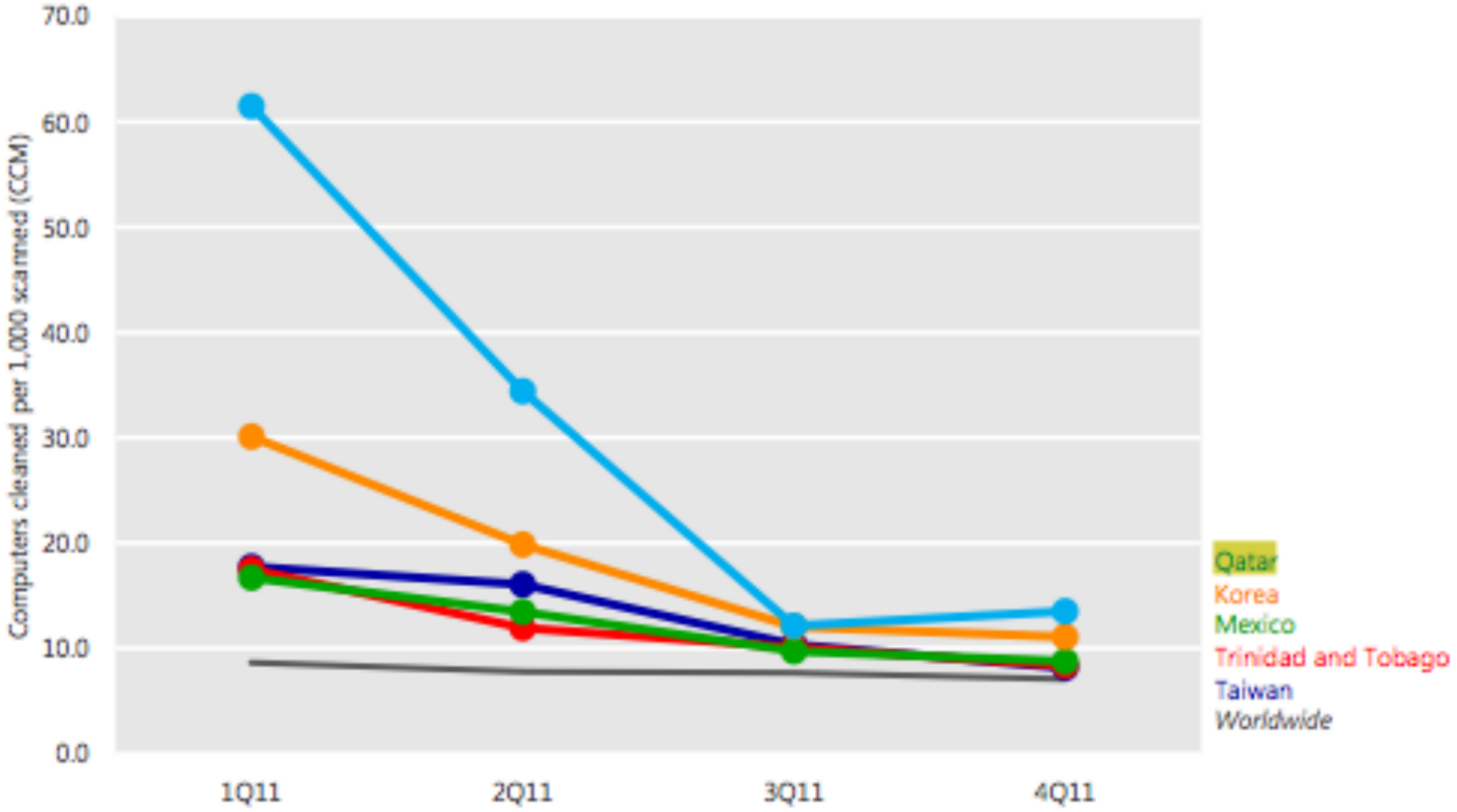
Basic Information

Version	: 3.4.147
Time	: Wed, 25 Apr 2012 11:45:08 +0000
Filename	: b1e24e23d3ef21e6ffbd14b87ba238f5
Commandline	: C:\b1e24e23d3ef21e6ffbd14b87ba238f5
Application_type	: Win32Application
Md5	: b1e24e23d3ef21e6ffbd14b87ba238f5
Sha1	: d06cc8096435d7df795f80de897abda535a31fe1

Processes Call Tree

- Process #1 (PID: 0x124)
  - Process #2 (PID: 0x1c8)
    - Process #3 (PID: 0xfac)
      - Process #4 (PID: 0x820)
        - Process #5 (PID: 0x398)
        - Process #6 (PID: 0x3cc)
        - Process #7 (PID: 0x3e4)
          - Process #60 (PID: 0x7b4)
            - Process #61 (PID: 0x308)
            - Process #62 (PID: 0x32c)
        - Process #8 (PID: 0x410)

Figure 28. Trends for five locations with significant infection rate improvements in 2H11, by CCM (100,000 MSRT executions minimum per quarter)



- Qatar exhibited the most dramatic improvement, from 61.5 in 1Q11 to 13.5