EG-CERT ANNUAL REPORT

Activities and Incidents

This report summarizes the activities of EG-CERT Team during the year 2011. It also Summarizes the incidents that the team faced during this year

EG-Cert Team
1/29/2012

Annual summery of CERT activities

Conferences and Training

- Assembly course by dr. Samir
- Encase forensic I at RAYA
- CFCE Computer Forensic Certified Expert Certificate.
- IP Protocol (Riverbed, FireEye) event.
- Identity Management Event at ITIDA.

External Missions

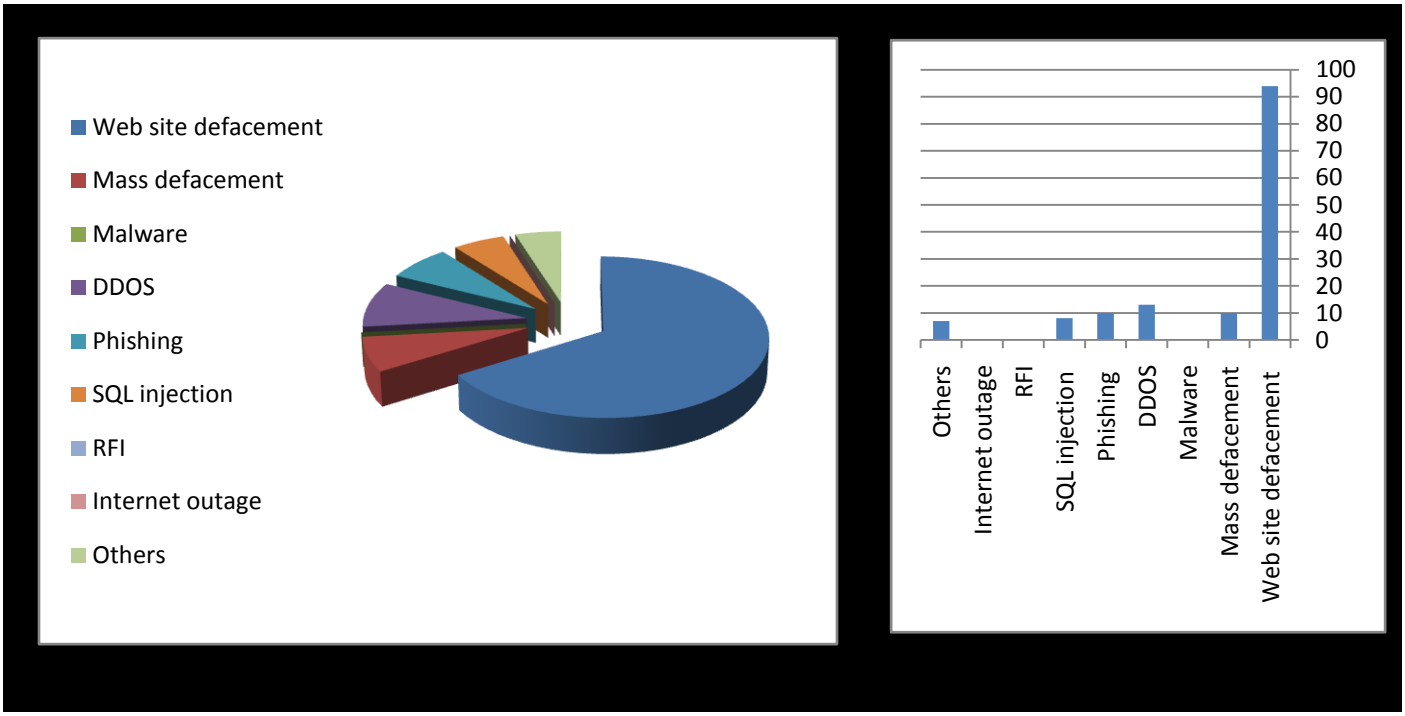
Internal Activities

- Link dsl connection
- TEdata's IP Addresses scanning
- Governmental sites assessment
- Reading and doing the practical parts in Reversing secrets of reverse engineering book.
- Reading and doing the practical parts in Malware analyst's cookbook book(8 chapters).
- Coding a script that do some analysis on the captured malwares from the honeynet project and send the generated report by email.
- Installing/Maintaining 2 HP Proliant Servers
- Building Honeynet project (nepenthes, dionaea, esxi, snort, snorby, pharm, bridge-tools, nfsen/nfdump, NFS storage, NTP Server)
- B4-B5 Leased line.
- LDN Link.
- Cymru Server Maintenance.
- Handling anonymous attack.
- CERT network topology.

- Malware Department Creation.
- Static and Dynamic analysis for malware samples (popshnoda - zeus - vanbot)

Annual summery of incidents

Incident Type	*No. of incidents*
Web site defacement (Accessing the server that hosts the site and changing its data)	94
Mass Defacement (Making defacement in a several sites which are hosted in the same server)	10
Phishing (Tricking user through tricky web pages and mails to steal their confidential date like credentials, credit card numbers…etc)	10
Malware (Downloading malware on victim machine while browsing an infected site)	0
DDOS (Stop the service or access to data and make computer resources unavailable)	13
RFI(Upload files to the victim in unauthorized way)	0
SQL Injection (Retrieving confidential data from database in unauthorized way)	8
Internet outage (Stopping Internet service due to accidents like cables cutting or server damage)	0
Others	7


Web site defacement
Mass defacement
Malware
DDOS
Phishing
SQL injection
RFI
Internet outage
Others
100
90
80
70
60
50
40
30
20
10
0
Others
Internet outage
RFI
SQL injection
Phishing
DDOS
Malware
Mass defacement
Web site defacement