Introduction

Qubee is operating a Wireless Broadband network with close to 80K subscribers nation-wide. It is a Wireless Broadband network using IEEE 802.16e WiMAX standard. With this large customer base, offering Wireless services with limited Radio Resources is challenging. One of the features provided by the WiMAX standard developers to save Radio Resources is IDLE Mode. A subscriber can go IDLE, i.e. a time when no internet activity is performed by end user. There are two major advantages associated with IDLE Time,

1) Power Amplifier of the subscriber terminal powers off which not only saves battery life of the terminal but also avoid excessive Uplink overshoots that can cause unnecessary Uplink transmission causing increased Interference Margin in the network due to Co-Channel re-use of frequency.

2) The other advantage of IDLE mode is saving per subscriber resources like dedicated traffic channel in Downlink and Uplink, when a subscriber is IDLE it can only listen to broadcast send by the Base Station and get active when traffic is destined towards or from it.

When we implemented IDLE mode in our network we found frequent switching between IDLE and ACTIVE modes by subscribers. During the troubleshooting process we applied live traces on random subscribers and test CPEs (Customer Premises Equipments) that were setup specifically; we found frequent communications of end subscriber with the Internet world. Upon deeper analysis we found automated communication of end subscriber stations with no intentional activity by the end customer system.

The automated communication that was observed throughout the network was Bots Activity. Bots or Internet Robots are automated software applications or scripts that run periodically from an end system. There are multiple purpose bots can perform like indexing on a search engine, fetching and analyzing files information from web servers. Bots may also be implemented where a response speed faster than that of humans is required (e.g., video gaming bots and auction-site robots) or less commonly in situations where the emulation of human activity is required.

With TCP/IP overlaid Wireless Communication Networks the communication between subscriber and end stations is limited like in GSM networks using GPRS/EDGE but in 4G networks like WiMAX the broadband channels are dedicated for IP packets and provide an open ground for such bots to perform activities with freedom. Add to that the end user Operating Systems that are vulnerable and facilitate such malicious bots activities.

Extracting the Data:

After completing the initial research we detected several suspected malicious and bots related domains residing in our network. Several different sources and techniques have been used to detect malicious activity in the network. Data fetched from DNS Logs, Blacklists, Malicious Domains and known DOS attacks on the network.

Following are the sources from domains were taken;

- Logs obtained from DNS.
- DNSTOP (a package used for view real time queries being served from name server).
- Authenticated Malware Database on the Internet.
- Known DOS attacks on Network.

Master list of malicious domains is available ISC website
https://isc.sans.edu/tools/suspicious_domains.html

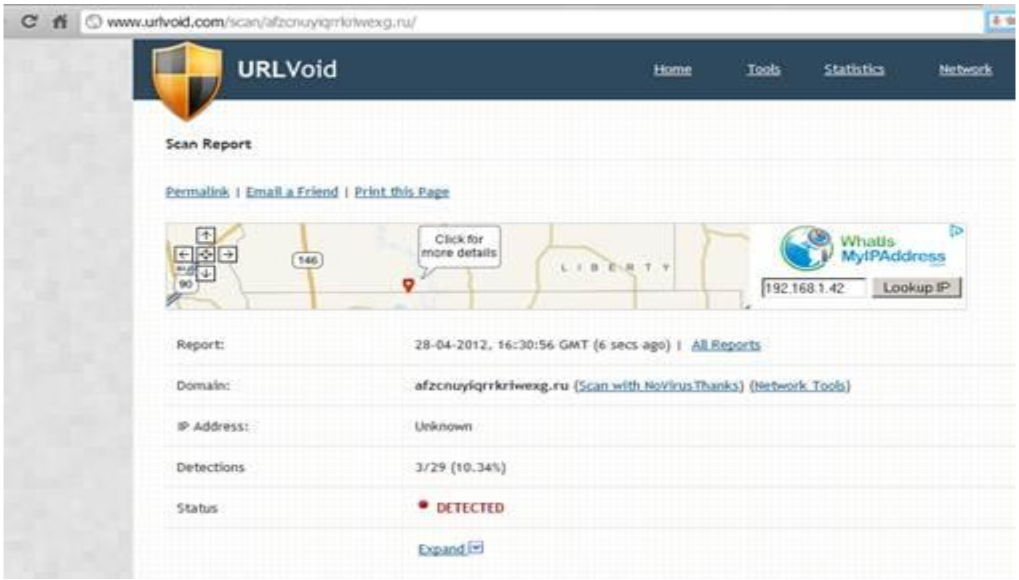
SAN project covers DB from

- www.abuse.ch
- www.malwaredomains.com
- www.threatexpert.com

From testing results of IDLE mode and traces of Mobile Subscriber Station, some domains gathered which were engaged in inviting DOS attack in the Network in the past.

Analyzing data:

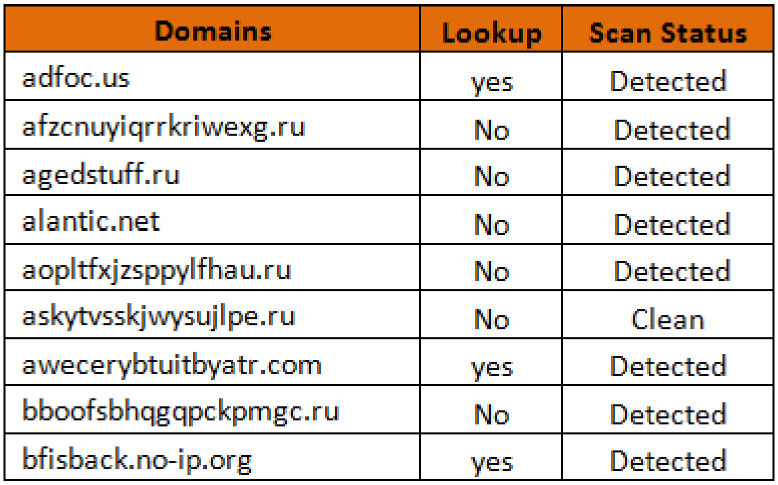
After collecting malicious domains, first we analyzed it with some web reputation engines



Scan Report

192.168.1.42

Report:	28-04-2012, 16:30:56 GMT (6 secs ago) | All Reports
Domain:	afzcnuyiqrrkriwexg.ru (Scan with NoVirusThanks) (Network Tools)
IP Address:	Unknown
Detections	3/29 (10.34%)
Status	● DETECTED
	Expand

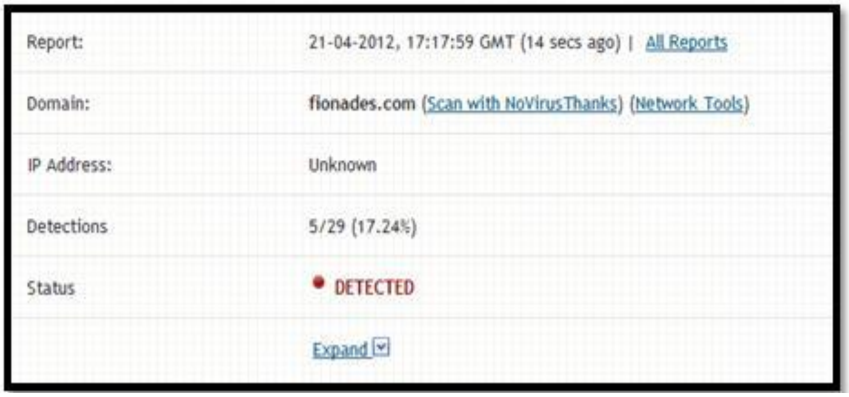


Domains	Lookup	Scan Status
adfoc.us	yes	Detected
afzcnuyiqrrkriwexg.ru	No	Detected
agedstuff.ru	No	Detected
alantic.net	No	Detected
aopltfxjzsppylfhau.ru	No	Detected
askytvsskjwysujlpe.ru	No	Clean
awecerybtuitbyatr.com	yes	Detected
bboofsbhqgqpckpmgc.ru	No	Detected
bfisback.no-ip.org	yes	Detected

Also compared extracted domains with master record of malicious domains (over 17,000 entries); to filter out the suspected domains, this was critical and necessary so as to avoid blocking of any legitimate domain.

For example, mentioned below is one of the cases;

fionades.com - malicious nature of this domain is also confirmed from multiple web reputation engines.

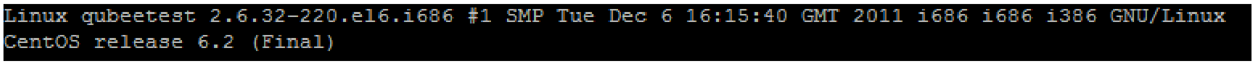


Report:	21-04-2012, 17:17:59 GMT (14 secs ago) | All Reports
Domain:	fionades.com (Scan with NoVirusThanks) (Network Tools)
IP Address:	Unknown
Detections	5/29 (17.24%)
Status	● DETECTED
	Expand

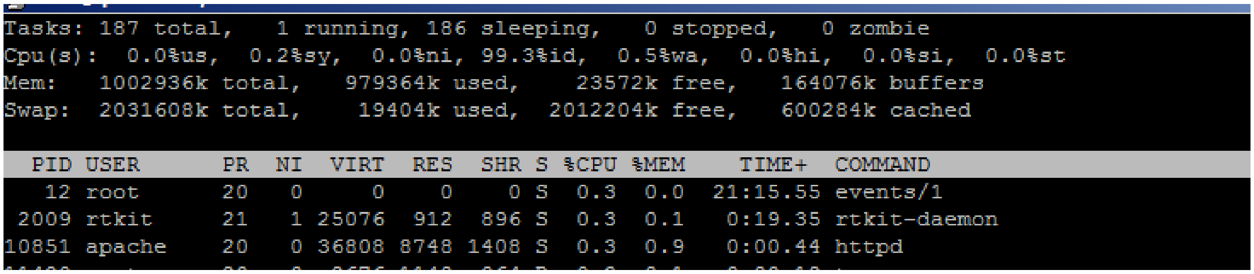
We redirected the malicious domains to a dedicated Server over which Web services were running by adding entries of malicious/suspected domains over DNS, due to Web services tracking and analyzing of data was possible.

Setting up redirection Server:

A dedicated server was setup for redirection purpose specifically;

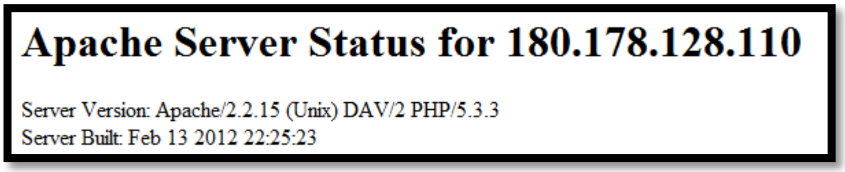


```
Linux qubeetest 2.6.32-220.el6.i686 #1 SMP Tue Dec 6 16:15:40 GMT 2011 i686 i686 i386 GNU/Linux
CentOS release 6.2 (Final)
```



```
Tasks: 187 total,   1 running, 186 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.2%sy,  0.0%ni, 99.3%id,  0.5%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   1002936k total,   979364k used,    23572k free,   164076k buffers
Swap:  2031608k total,    19404k used,  2012204k free,   600284k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
   12 root      20   0     0    0    0 S  0.3  0.0  21:15.55 events/1
 2009 rtkit     21   1 25076  912  896 S  0.3  0.1   0:19.35 rtkit-daemon
10851 apache    20   0 36808 8748 1408 S  0.3  0.9   0:00.44 httpd
```

Web services successfully setup;



Apache Server Status for 180.178.128.110

Server Version: Apache/2.2.15 (Unix) DAV/2 PHP/5.3.3
Server Built: Feb 13 2012 22:25:23

Addition in DNS

Entries added in named.conf file for every domain as,

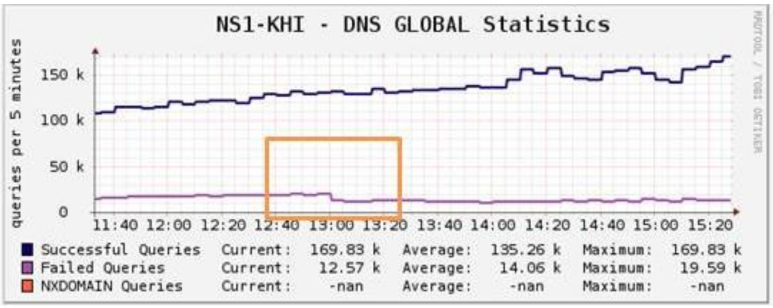
```
 zone "psplanet.com.au" in {

        type master;

        file"/var/named/bot/raptr.com.zone";

        };
```

Made a zone file for malicious domain, which could be used for all Malicious domains.

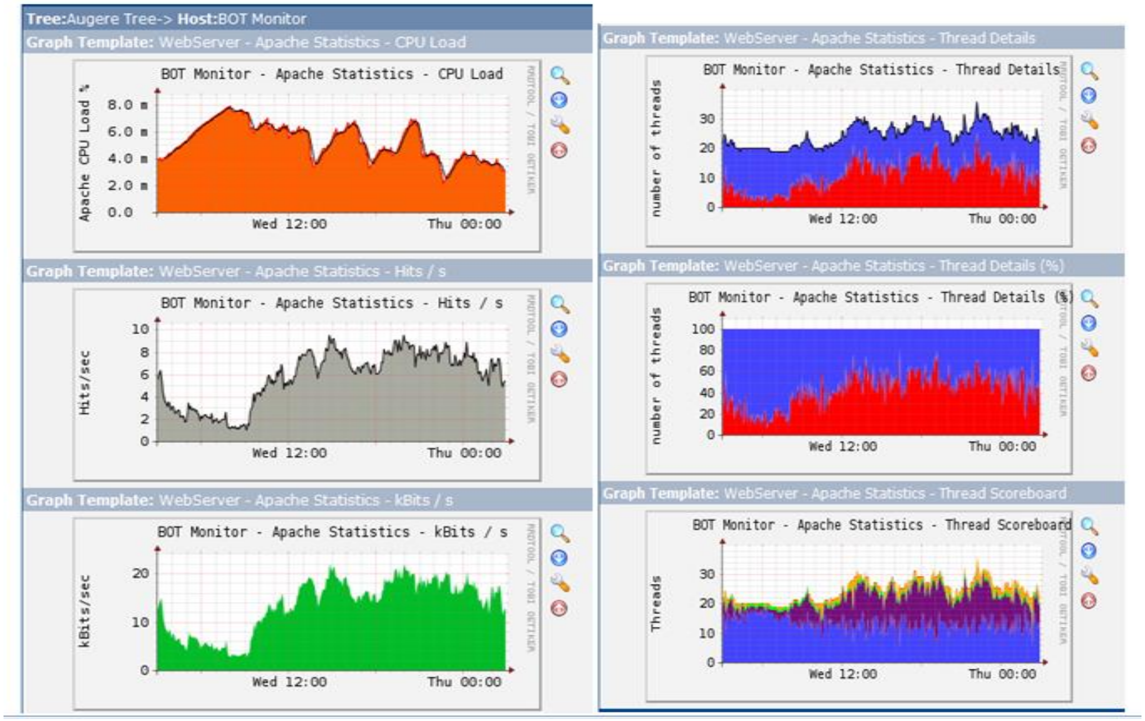
```
$ttl 38400

@ IN SOA ns1.qubee.com.pk. admin.qubee.com.pk. (

6;

10800;

3600;

604800;

38400;

);

@          IN        NS      any.countri1l.com.

@       IN       A       180.178.128.110

www     IN       A       180.178.128.110
```

Analyzing Phase:

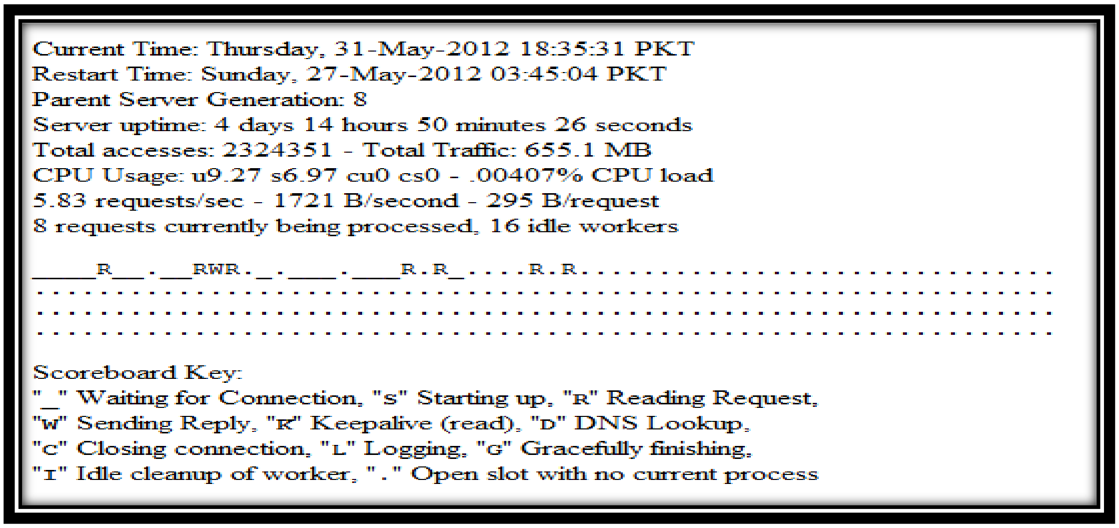
NS-lookup queries are pointing toward 180.178.128.110 that yields significant decrement in failed queries.



Plotted different types of graph for evaluating various performance counters.



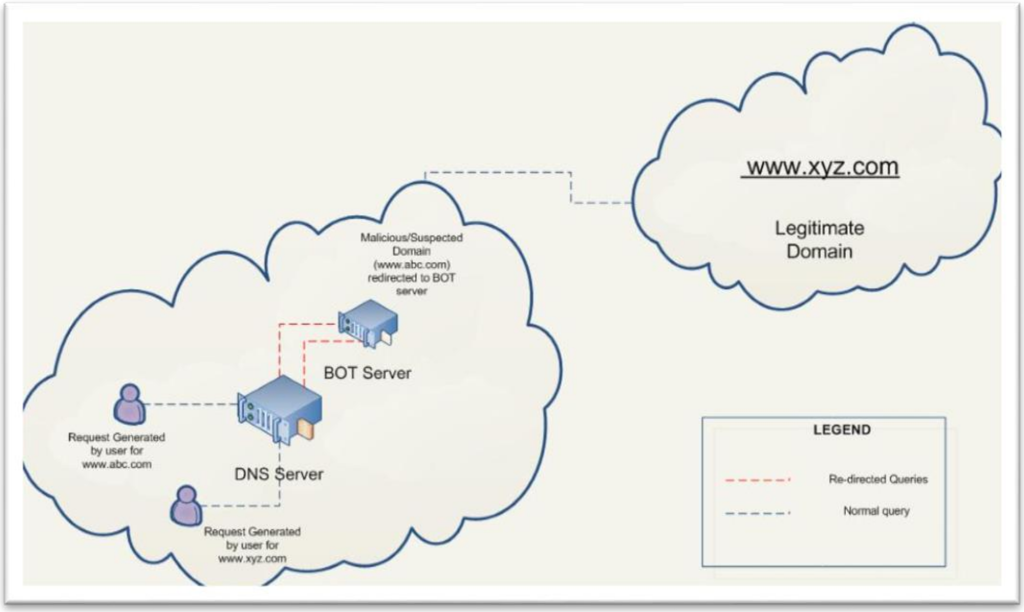
By web services visibility of access requests and data transmission made possible.



```
Current Time: Thursday, 31-May-2012 18:35:31 PKT
Restart Time: Sunday, 27-May-2012 03:45:04 PKT
Parent Server Generation: 8
Server uptime: 4 days 14 hours 50 minutes 26 seconds
Total accesses: 2324351 - Total Traffic: 655.1 MB
CPU Usage: u9.27 s6.97 cu0 cs0 - .00407% CPU load
5.83 requests/sec - 1721 B/second - 295 B/request
8 requests currently being processed, 16 idle workers

______R___.___RWR._.____.____R.R_....R.R.........................
.................................................................
.................................................................
.................................................................

Scoreboard Key:
"_" Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process
```

Working of BOT_Monitor:

All domains (malicious/suspected) loaded onto our DNS server. When a computer client requests a URL or file from one of these domains, it approaches DNS for name resolution; it will be redirected to BOT_Monitor.


www.xyz.com
Legitimate Domain
Malicious/Suspected Domain (www.abc.com) redirected to BOT server
BOT Server
Request Generated by user for www.abc.com
DNS Server
Request Generated by user for www.xyz.com
LEGEND
Re-directed Queries
Normal query

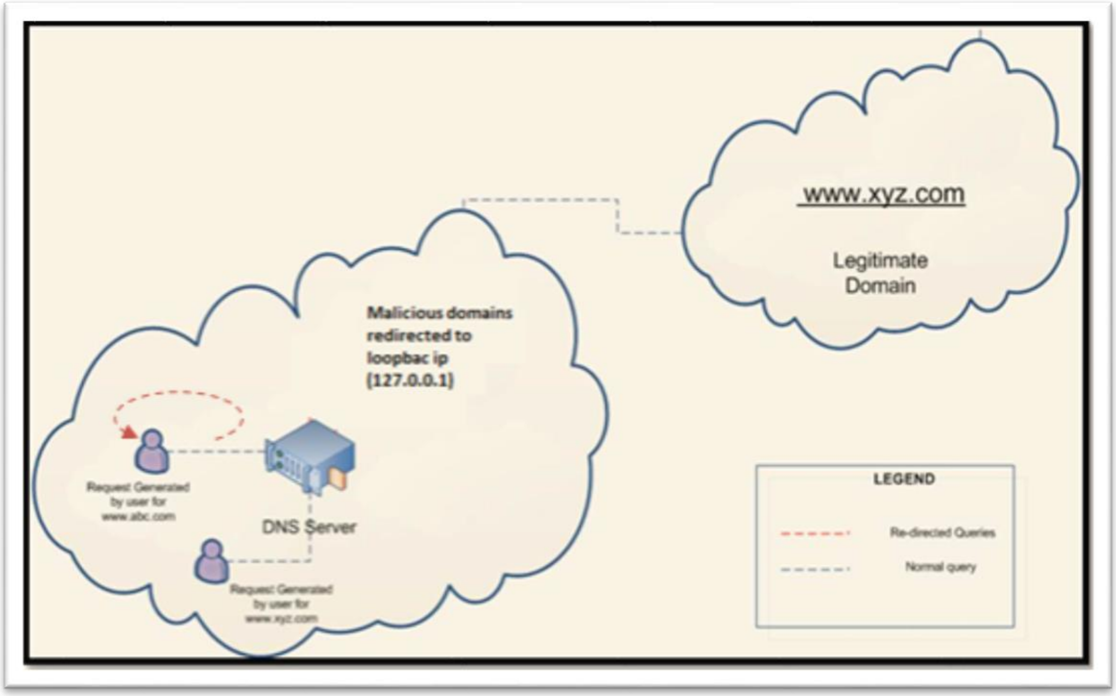
Project BOT – An Enhancement:

After analyzing data and gathered traces of queries; we tried to find some way to stop them. Because even when the queries are re-directed towards the webserver the precious Radio Resource of the network is still utilized which is the biggest hurdle in increased IDLE time of the network.

As a creative idea we decided to modify host entries of all such domains on our DNS with a Loopback IP Address (127.0.0.1). With the malicious domains queries resolving with local host address the traffic from end subscribers will be “Loop Holed” within the end user system. And it will not consume air resource of the Wireless system to reach either the Re-direction server or the intended Command and Control Center of Bots network.

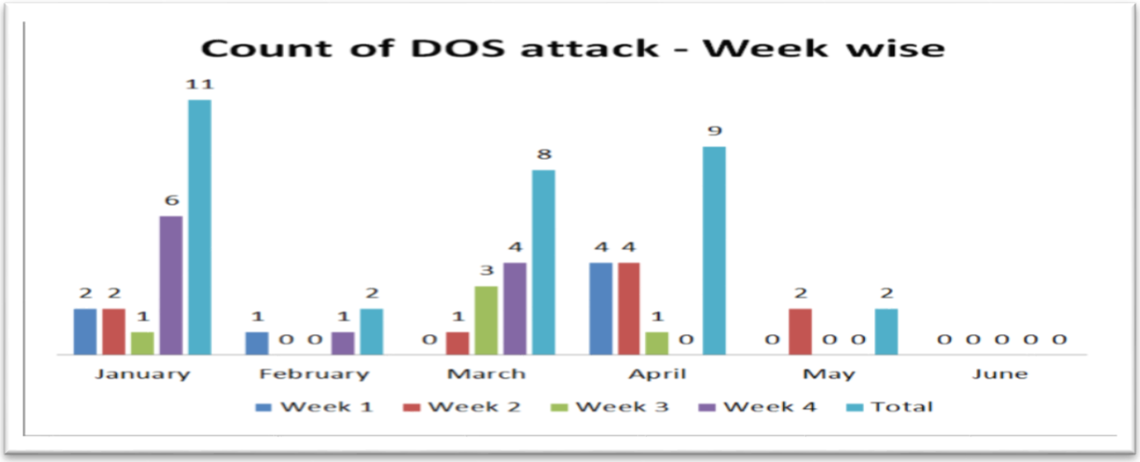
With this approach the intended benefits were:

- Saving additional unwanted bandwidth being used in redirection process.As an average traffic of 15kbps yields 162 MB of data transfer.
- For malicious domain queries will be first look at local cache then DNS cache; save from making querying repeatedly.
- Increase average IDLE time of the network, thus saving Radio Resources and improved Uplink Interference Margin, greater battery life of mobile subscribers.


www.xyz.com
Legitimate Domain
Malicious domains redirected to loopbac ip (127.0.0.1)
Request Generated by user for www.abc.com
DNS Server
Request Generated by user for www.xyz.com
LEGEND
Re-directed Queries
Normal query

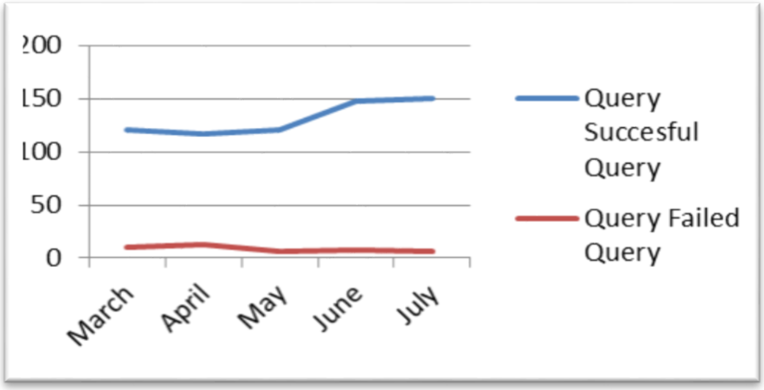
Results Achieved

- **DOS attack meditation.**
  Massive reduction of DOS/DDOS attacks over the networks



- **Saving unwanted uplink bandwidth.**
  Stopped communication of malicious domains with their Command & Control Centre

- **Reduction in Failed Queries in DNS**
  Due to sink-holing unwanted domains to loop-back, there is a significant reduction in failed query.



- **Quantity of SPAM decreased**
  Observed major decreased in SPAM email.

- **IDLE Time of the network increased**

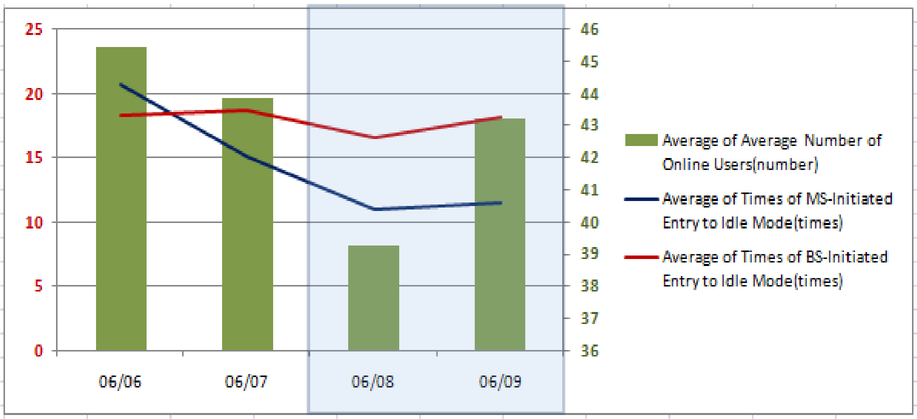


Figure Shows Both MS-Initiated and BS-Initiated IDLE Mode Requests decreased, this means the switching between IDLE and ACTIVE States decreased

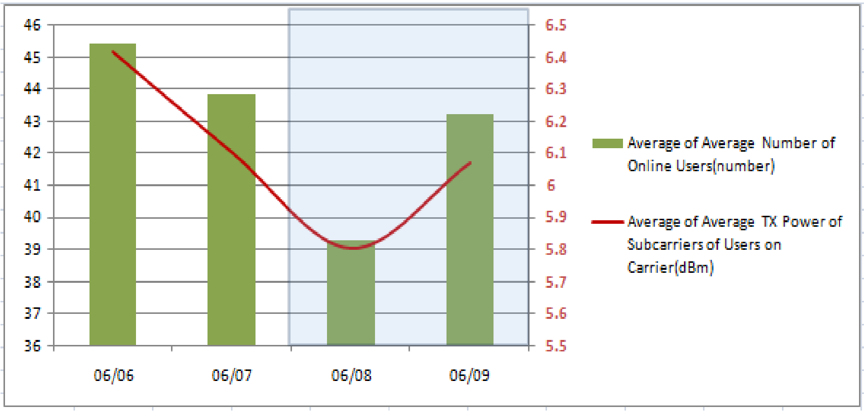


Figure Shows Uplink TX-Power of subscribers decreases, reflecting more IDLE time for users