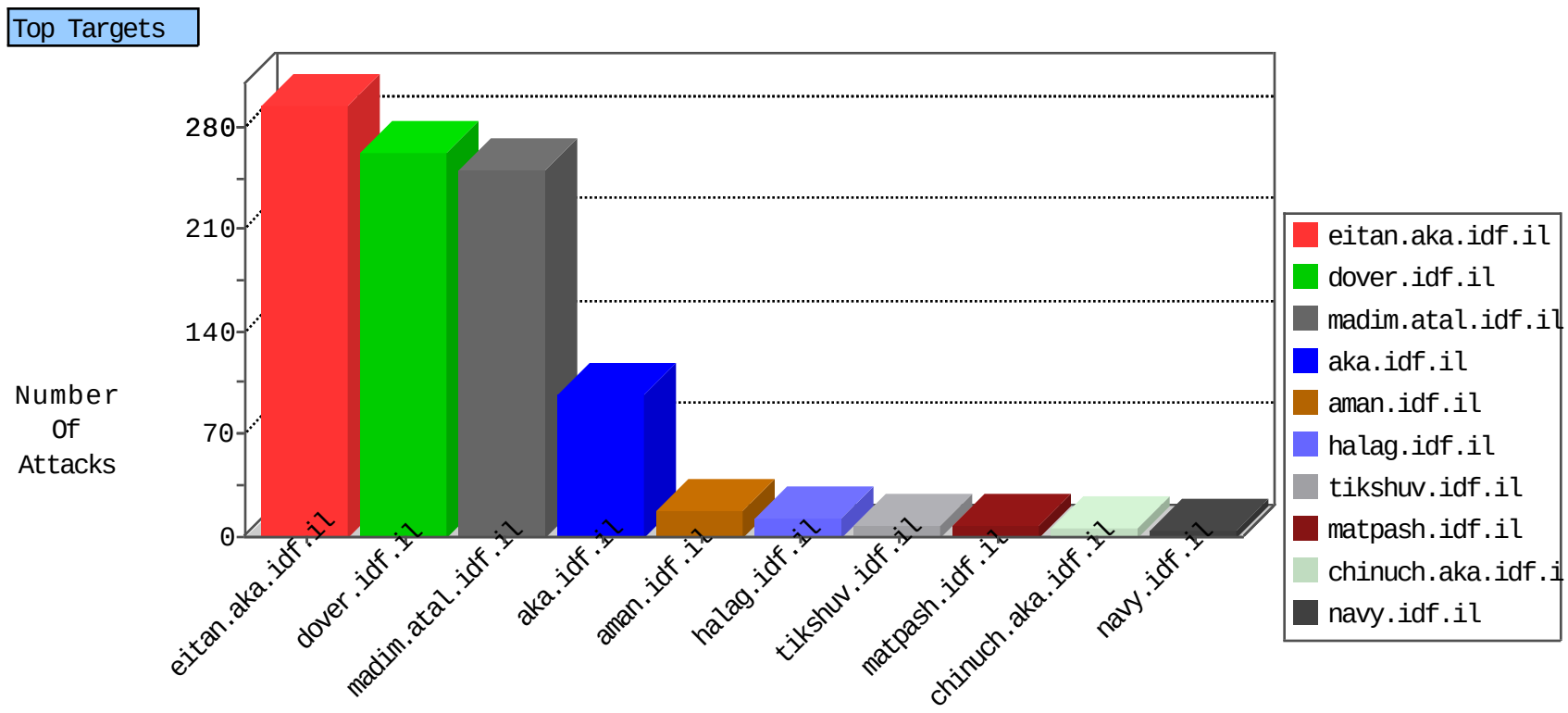
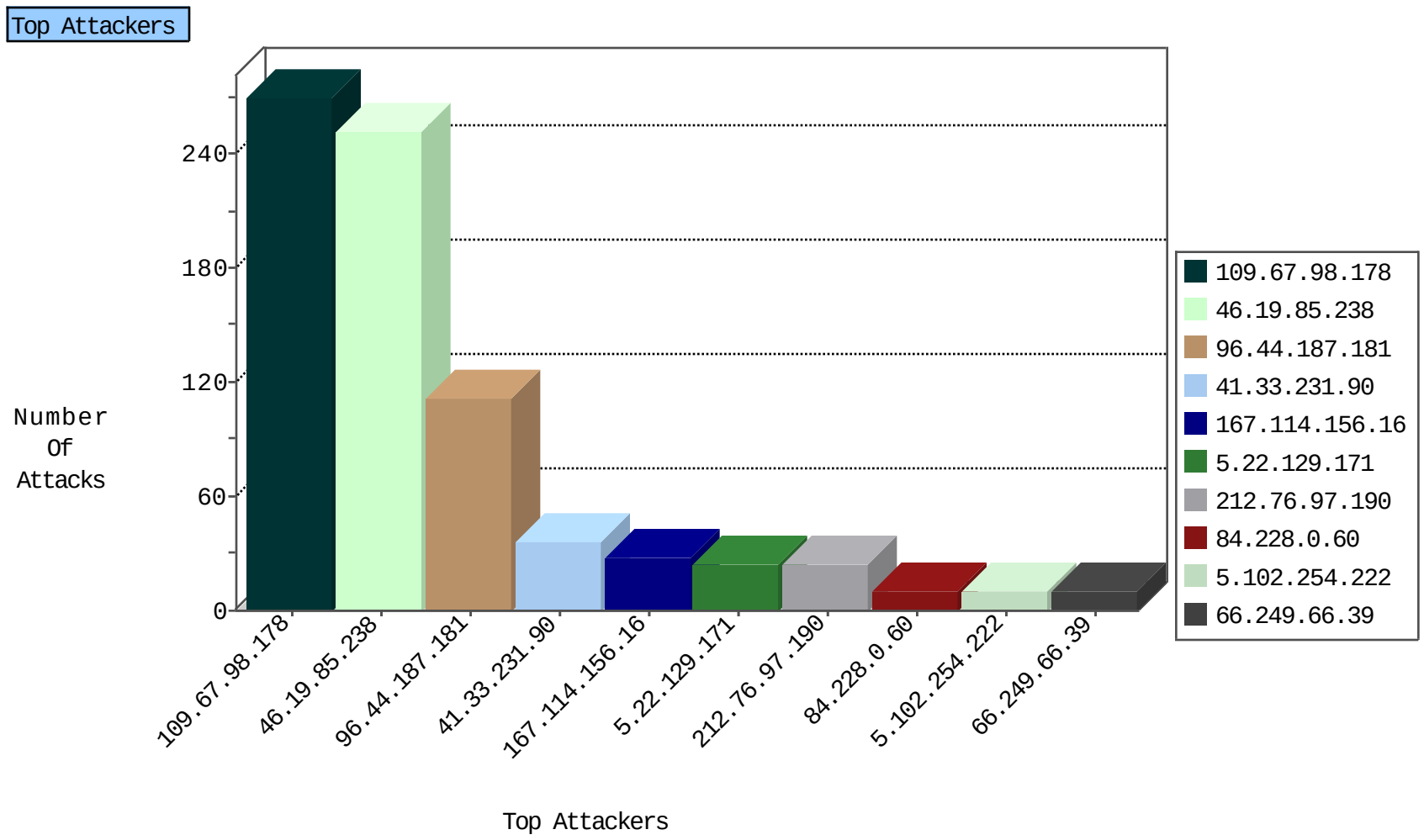
12-23-2015-01:07:01 to 12-23-2015-02:07:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-23-2015-01:07:01 to 12-23-2015-02:07:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	866
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
77.247.178.132	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

12-23-2015-01:07:01 to 12-23-2015-02:07:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
96.44.187.181	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
96.44.187.181	United States	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	12
41.234.207.238	Egypt	147.237.77.216	dover.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
96.44.187.181	United States	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

12-23-2015-01:07:01 to 12-23-2015-02:07:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
183.60.48.25	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.192.0.226	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
180.246.183.211	147.237.77.216	Indonesia	dover.idf.il	ET SCAN NMAP -sS window 3072	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

12-23-2015-01:07:01 to 12-23-2015-02:07:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.67.98.178	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	264
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
96.44.187.181	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	29
212.76.97.190	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
5.22.129.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
66.249.78.62	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.102.254.222	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.64.9.102	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
80.159.248.40	Germany	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
84.228.0.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.130.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
45.55.53.138		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
185.120.125.10		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
84.111.39.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
185.120.126.85		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
108.14.191.193	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
84.228.0.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
37.26.146.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.116.177.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
46.19.86.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
149.78.37.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.175.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
31.210.186.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.102.254.222	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
79.183.152.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
157.55.39.79	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	alert	2
79.176.7.194	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
212.179.90.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
66.249.66.45	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.250.111.90	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
79.176.136.252	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
46.19.85.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	alert	2
46.19.86.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.176.174.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
46.19.85.148	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.46.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.136	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
96.44.187.181	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
84.111.39.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.86	United States	147.237.0.35	akaws.idf.il	drop		drop	1
37.142.165.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
82.166.68.171	Israel	147.237.0.35	akaws.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
207.46.13.65	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

12-23-2015-01:07:01 to 12-23-2015-02:07:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.238	Block	117
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
96.44.187.181	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 96.44.187.181	Block	28
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.238	Block	24
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
157.55.39.79	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
45.55.53.138		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 45.55.53.138	Block	2
96.44.187.181	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
157.55.39.225	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
66.249.66.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
109.186.191.201	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
45.55.53.138		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
1.23.20.156	India	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
85.93.91.84	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
200.6.104.28	Chile	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
46.166.137.213	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.40	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
36.77.222.6	Indonesia	147.237.72.166	aka.idf.il	Unknown Parameter catId?' in www.aka.idf.il/brothers/skira/default.asp	None	1
78.47.17.5	Germany	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
220.181.132.216	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
157.55.39.225	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/shared/usercontrols/navmenu/undefined	Block	1
116.90.105.191	Pakistan	147.237.77.74	law.idf.il	PHP Attempt	Block	1
1.23.20.156	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
85.93.91.84	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
200.6.104.28	Chile	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.64.219	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
157.55.39.41	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
96.44.187.181	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fck/	Block	1
40.77.167.53	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
78.47.17.5	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
173.252.88.191	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
116.90.105.191	Pakistan	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
2.52.155.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.68.248.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
41.234.207.238	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/index.asp	Block	1
79.183.111.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.111.244.188		147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1759	Block	1
141.212.122.129	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /x	Block	1
2.54.56.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

12-23-2015-01:07:01 to 12-23-2015-02:07:01