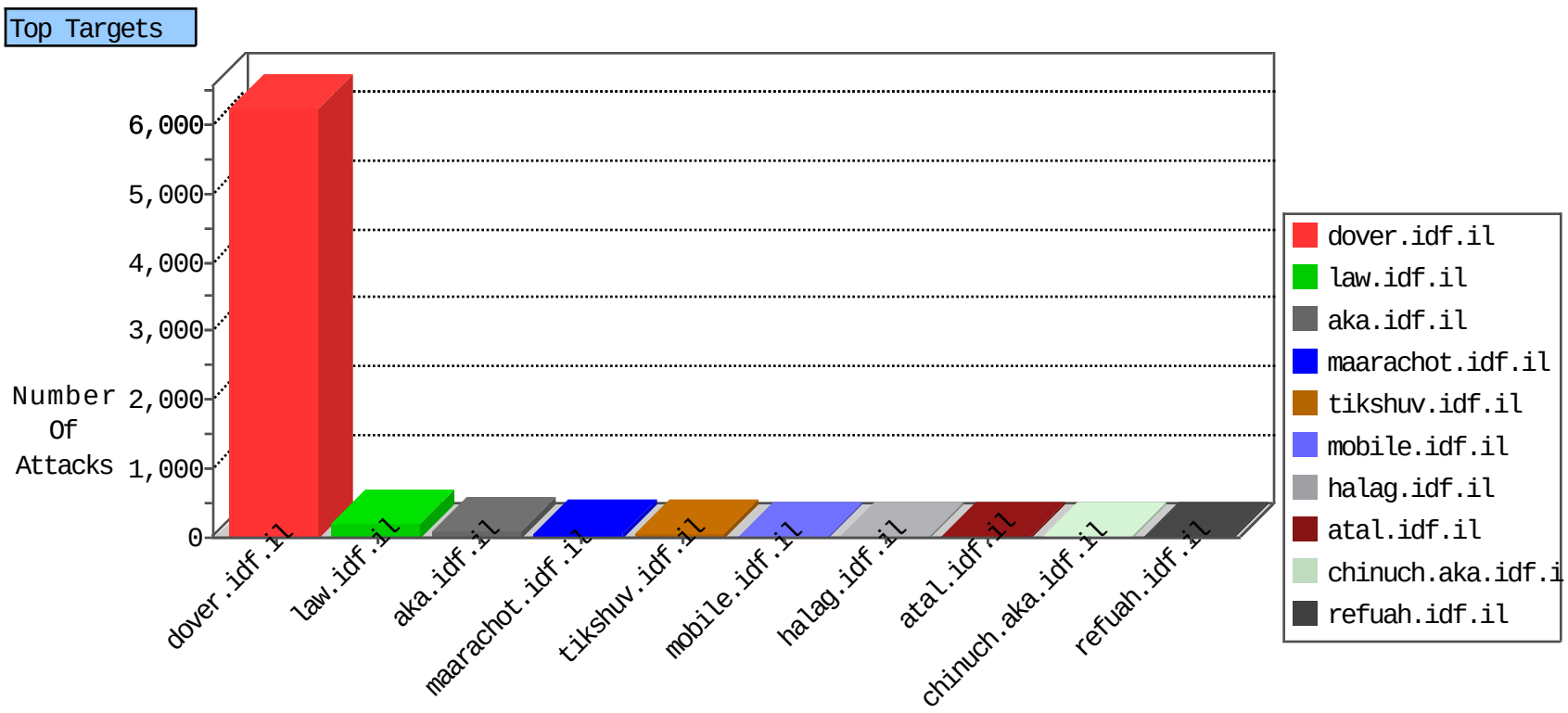
11-04-2015-03:04:00 to 11-04-2015-04:04:00

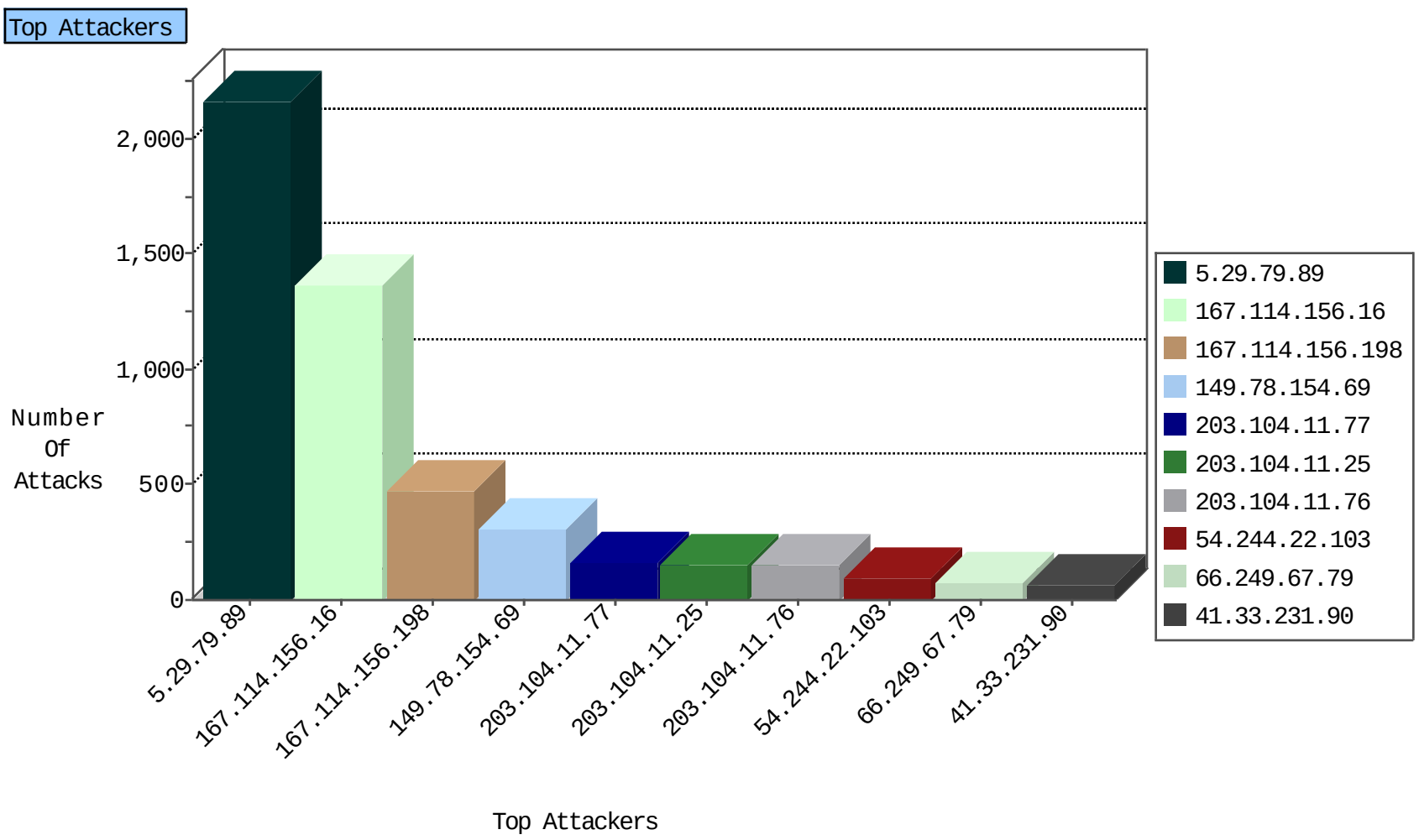
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-04-2015-03:04:00 to 11-04-2015-04:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3937
203.104.11.76	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3189
203.104.11.77	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2879
66.249.67.202	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2462
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2295
203.104.11.25	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2285
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1568
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1324
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	850
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	367
66.249.67.210	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	321
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	222
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	214
167.114.156.198	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	131
66.249.67.194	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	116
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	12
66.249.69.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
66.249.69.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
66.249.67.248	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	4
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
66.249.79.80	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2
70.133.149.130	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
157.55.39.32	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
108.59.253.71	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
193.242.218.6	Switzerland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
204.42.253.2	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

11-04-2015-03:04:00 to 11-04-2015-04:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.111.70	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
177.153.16.116	Brazil	147.237.77.170	maarachot.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

11-04-2015-03:04:00 to 11-04-2015-04:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.79.41	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
119.10.8.133	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
119.10.8.133	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.0.34	Sweden	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
68.65.121.91	147.237.77.227		e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.51	147.237.76.176	Germany	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
187.192.19.201	147.237.8.46	Mexico	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
119.10.8.133	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
119.10.8.133	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.0.19	Sweden	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
188.138.9.51	147.237.76.31	Germany	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

11-04-2015-03:04:00 to 11-04-2015-04:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.29.79.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2166
167.114.156.198	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	468
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	304
203.104.11.77	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	146
203.104.11.76	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	140
203.104.11.25	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	137
79.182.211.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
72.200.208.46	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
70.133.149.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
172.56.5.252	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
54.244.22.103	United States	147.237.0.34	tikshuv.idf.i	drop	First packet isn't SYN	drop	44
109.163.234.2	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
198.84.196.246	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
54.244.22.103	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	37
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.69.34	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
17.142.152.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
24.91.137.251	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
162.200.77.18	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
207.46.13.38	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
207.46.13.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.69.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
5.9.111.70	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
17.142.152.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
17.142.152.85	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
178.38.77.193	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
162.243.199.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
65.157.96.99	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
41.130.201.7	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
157.55.39.236	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
113.37.89.186	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
107.170.63.50	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.9.25.72	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.69.42	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12

11-04-2015-03:04:00 to 11-04-2015-04:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.50.74	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.181.50.74	Block	7
79.181.50.74	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	4
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	3
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf/console/search_resources.aspx	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
177.153.16.116	Brazil	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9182-he/refuah.aspx	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
167.114.156.198	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.74.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/109973.pdf	Block	1
66.249.67.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1399-he/atal.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1362-17477-he/kkkkkkk=6e8675d0kkkkkkk_6e8675d0	Block	1
74.82.47.3	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
46.19.86.95	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.74.106	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.74.106	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
184.105.247.196	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
176.31.191.26	France	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.74.108	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/112332.pdf	Block	1
66.249.67.209	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
192.228.148.212	Malaysia	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3350.jpg	Block	1
177.153.16.116	Brazil	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
82.118.237.101	Bulgaria	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1

11-04-2015-03:04:00 to 11-04-2015-04:04:00