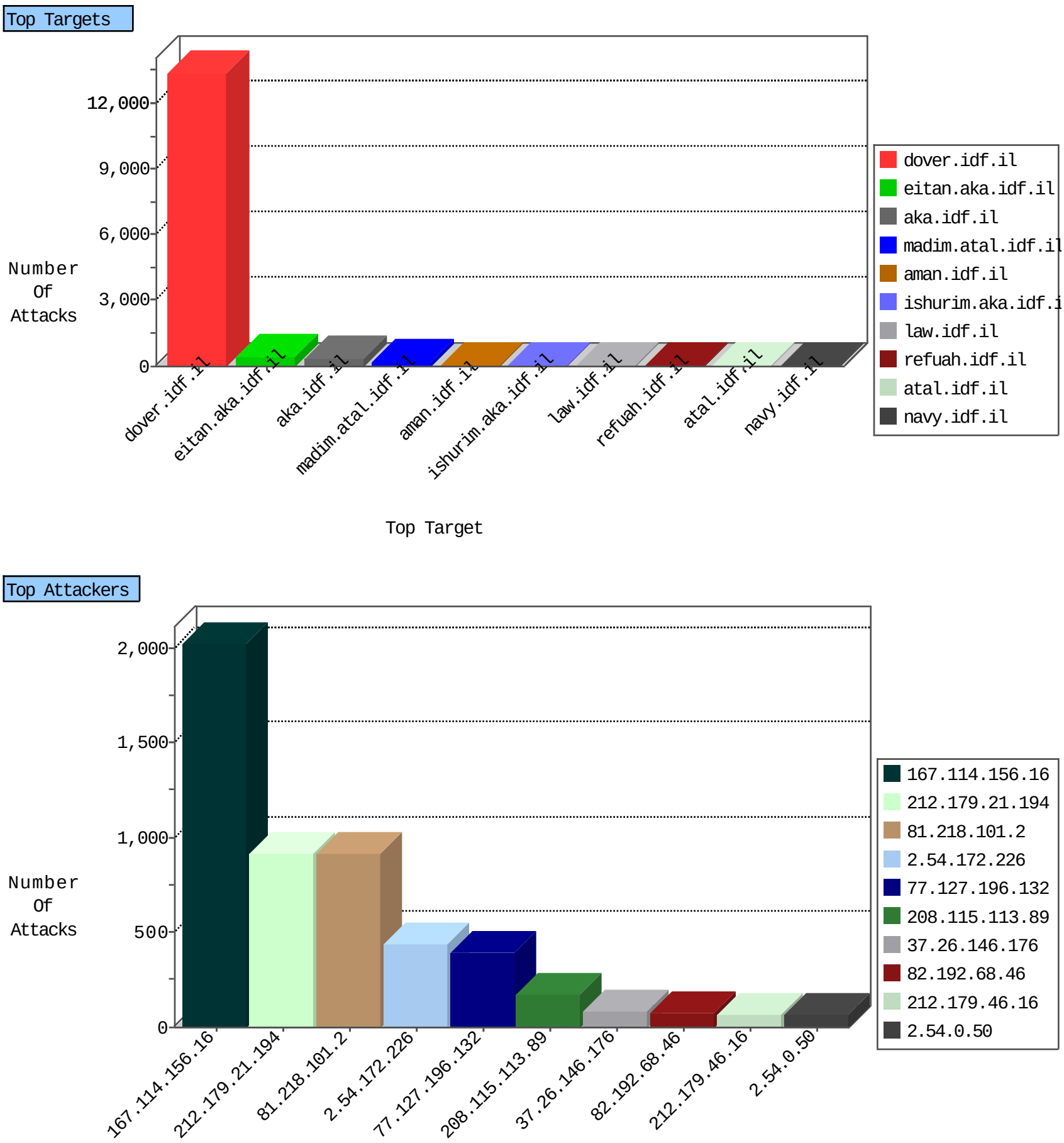
11-08-2015-09:04:08 to 11-08-2015-10:04:08

IDF Under Attack
Daily Report



11-08-2015-09:04:08 to 11-08-2015-10:04:08

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	3008
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	519
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	219
149.78.235.51	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	38
80.246.139.85	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
46.117.128.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
95.86.68.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
37.142.68.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
46.19.85.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
213.8.73.4	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
62.219.115.209	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
5.22.129.190	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
109.67.29.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
80.246.139.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
5.22.129.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
37.26.148.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
2.52.19.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.52.23.96	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.1.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.120.136.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.172.180	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
213.151.52.216	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.26.148.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.140.188	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.21.69	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.150.214.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.135.90	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
64.19.78.243	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.143.120.151	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
46.19.86.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
93.173.2.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
95.86.125.165	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
60.234.87.105	New Zealand	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.179.28.80	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
192.114.23.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
185.32.179.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
149.78.50.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
87.68.78.110	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.140.188	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.54.132.32	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
185.32.179.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.26.148.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.172.180	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
5.28.171.150	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
84.228.199.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2

11-08-2015-09:04:08 to 11-08-2015-10:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.169.231	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
46.118.118.215	Ukraine	147.237.77.74	law.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
82.166.197.93	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-08-2015-09:04:08 to 11-08-2015-10:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.67.224	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
217.194.196.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.95.100.192	147.237.0.33	Russian Federation	idf.il	ET SCAN NMAP -sS window 1024	1
66.249.73.228	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1
46.19.85.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.10.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.160.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.160.196	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1

11-08-2015-09:04:08 to 11-08-2015-10:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.101.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	915
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	865
2.54.172.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	417
77.127.196.132	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	369
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	170
37.26.146.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
212.179.46.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
2.54.0.50	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
46.19.85.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
197.156.122.192	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
2.54.140.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
65.49.68.186	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
66.249.65.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
65.49.68.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
79.182.142.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
192.114.23.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
194.90.25.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
46.19.86.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
37.26.148.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
209.48.43.22	United States	147.237.77.216	dover.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	37
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
192.114.23.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
212.143.3.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
31.168.13.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.65.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
77.127.23.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
84.95.255.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
199.203.215.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
149.78.235.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
46.19.85.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
5.22.129.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.93.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
5.28.181.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
2.52.136.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
2.52.23.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.26.146.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24

11-08-2015-09:04:08 to 11-08-2015-10:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.132.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
80.246.136.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
77.127.196.132	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
2.54.20.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
176.13.20.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
176.13.4.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
77.127.244.51	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.127.244.51	Block	7
46.19.85.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
79.183.140.172	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	4
2.54.153.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.146.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
87.69.173.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.115.252.2	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
95.86.125.165	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1620.jpg	Block	2
46.19.86.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/catalog.asp	Block	1
87.68.56.139	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
46.19.85.193	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
77.127.244.51	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
212.179.132.202	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteyerua/	Block	1
109.65.34.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
46.19.86.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.147.224	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
2.54.17.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$comboQuestion in www.aka.idf.il/main/giyus/faq.aspx	None	1
216.218.206.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
176.51.4.193	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.law.idf.il/327-en/patzar.aspx	Block	1
79.181.223.86	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
31.13.100.119	Ireland	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/6/69056.pd	Block	1
212.199.57.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.67.90	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
109.67.64.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
46.118.118.215	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
37.26.147.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.79.31	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
216.218.206.68	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan.	Block	1
176.106.227.35	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
89.139.33.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.253	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
79.182.155.108	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
37.26.146.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.199.57.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.118.118.215	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
157.55.39.1	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/imagevideogallerylobby/imagevideogallerylobby.aspx	Block	1

11-08-2015-09:04:08 to 11-08-2015-10:04:08