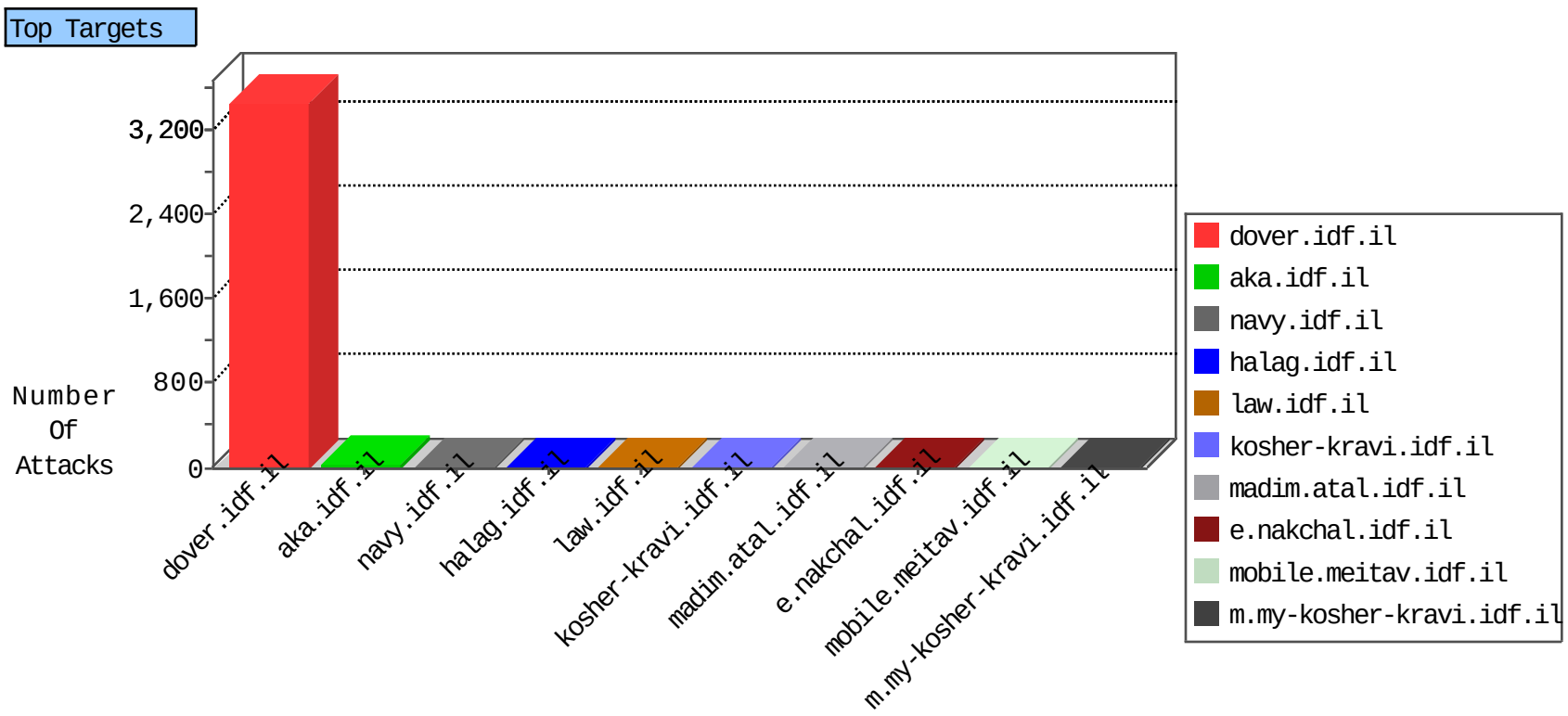
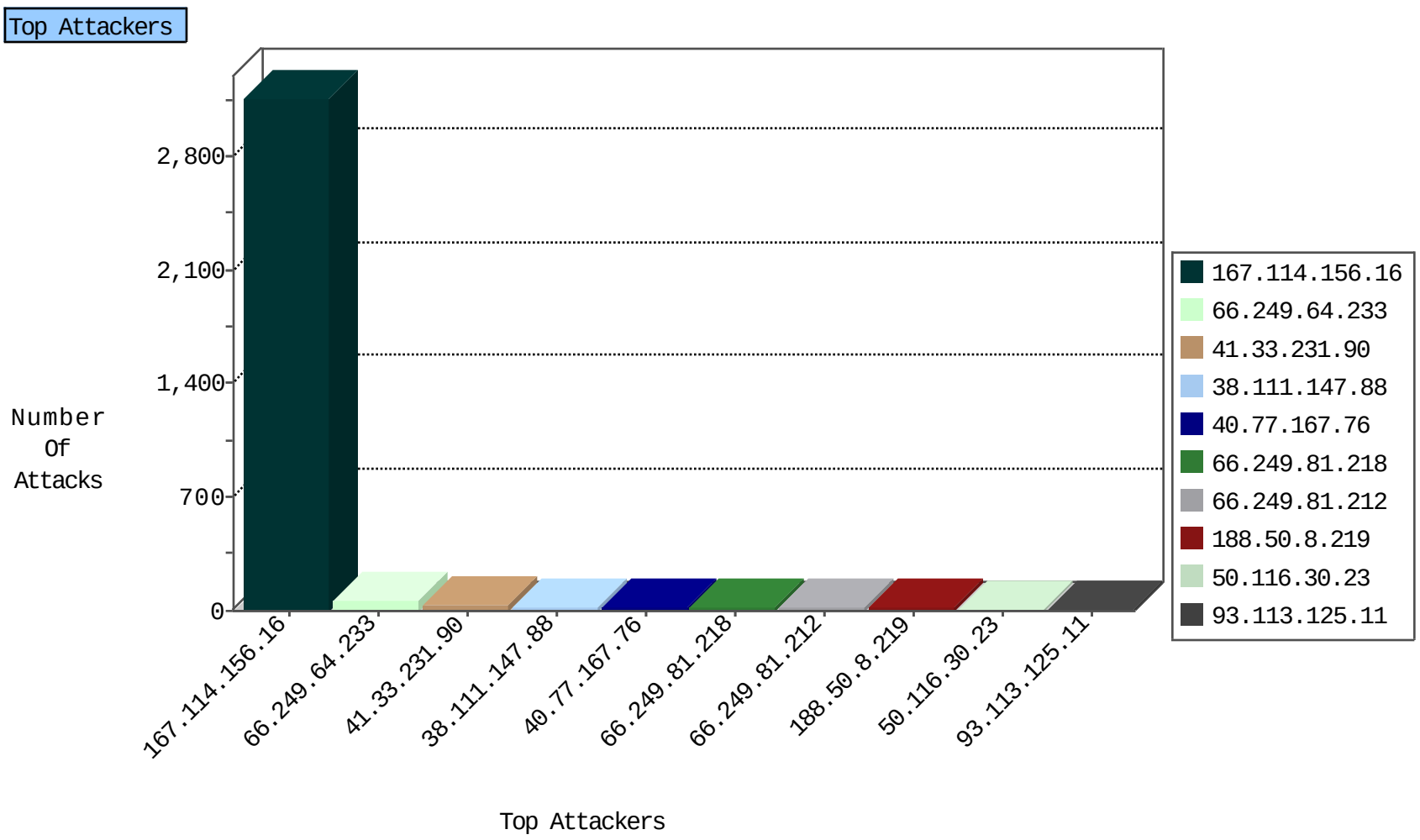
11-25-2015-02:04:04 to 11-25-2015-03:04:04

IDF Under Attack Daily Report





11-25-2015-02:04:04 to 11-25-2015-03:04:04

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	3029
66.249.78.82	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3026
66.249.66.96	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	81

11-25-2015-02:04:04 to 11-25-2015-03:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-25-2015-02:04:04 to 11-25-2015-03:04:04

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
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.155.48.126	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.115	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.0.33	Germany	idf.il	ET SCAN NMAP -sS window 1024	1
165.255.4.143	147.237.0.19		madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
5.230.141.115	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
119.73.228.130	147.237.76.201	Singapore	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
5.230.141.115	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
113.59.33.61	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
93.113.125.11	147.237.0.15	Romania	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
71.177.22.76	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
222.186.56.115	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.155.48.126	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 2048	1
222.186.56.115	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.155.48.126	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -f -sS	1
31.6.71.154	147.237.76.176	Poland	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
165.255.4.143	147.237.0.19		madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.230.141.115	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
119.73.228.130	147.237.76.201	Singapore	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
113.59.33.61	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
74.117.209.135	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
71.177.22.76	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
222.186.56.115	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.67.232	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
222.186.56.115	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

11-25-2015-02:04:04 to 11-25-2015-03:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1041
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	64
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
40.77.167.76	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	19
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
188.50.8.219	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
219.74.38.243	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
220.255.97.4	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
203.127.58.236	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.115	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.218.202.198	Spain	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.144.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
119.73.253.4	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.217	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
99.199.73.91	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
157.55.39.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
93.113.125.11	Romania	147.237.0.15	kosher-kravi.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
87.68.248.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	3
109.64.143.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.182.20.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.34.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
91.200.12.137	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.172	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
73.140.244.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
37.26.148.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
91.200.12.137	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	2
157.55.39.226	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
150.70.97.86	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
137.116.71.170	United States	147.237.0.35	akaws.idf.il	drop		drop	1
101.6.30.81	China	147.237.76.34	yohalan.idf.il	drop		drop	1
185.3.144.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.169	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
122.226.77.226	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
93.113.125.11	Romania	147.237.0.33	idf.il	drop		drop	1

11-25-2015-02:04:04 to 11-25-2015-03:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
38.111.147.88	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
87.218.202.198	Spain	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
98.71.195.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.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
61.135.190.71	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
141.212.122.160	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
93.44.33.138	Italy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
46.116.73.204	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/×™×•×″×œ×Ÿ	Block	1
77.125.156.188	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
175.136.61.24	Malaysia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.67.232	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.121.208.233	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
41.218.170.239	Egypt	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 41.218.170.239	Block	1
87.68.248.28	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
77.125.156.188	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
150.70.173.52	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
93.113.125.11	Romania	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /readme_for_decrypt.txt	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
5.175.26.46	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
77.125.156.188	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on www.atal.idf.il/xmlrpc.php	Block	1
175.136.61.24	Malaysia	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.121.208.233	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
109.64.143.181	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
41.238.217.99	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
77.125.156.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
150.70.173.52	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
31.193.51.59	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
83.166.234.95	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
180.76.15.11	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
61.135.190.69	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
109.66.210.43	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
89.138.69.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
41.238.217.99	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
77.125.156.188	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.129	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1

11-25-2015-02:04:04 to 11-25-2015-03:04:04