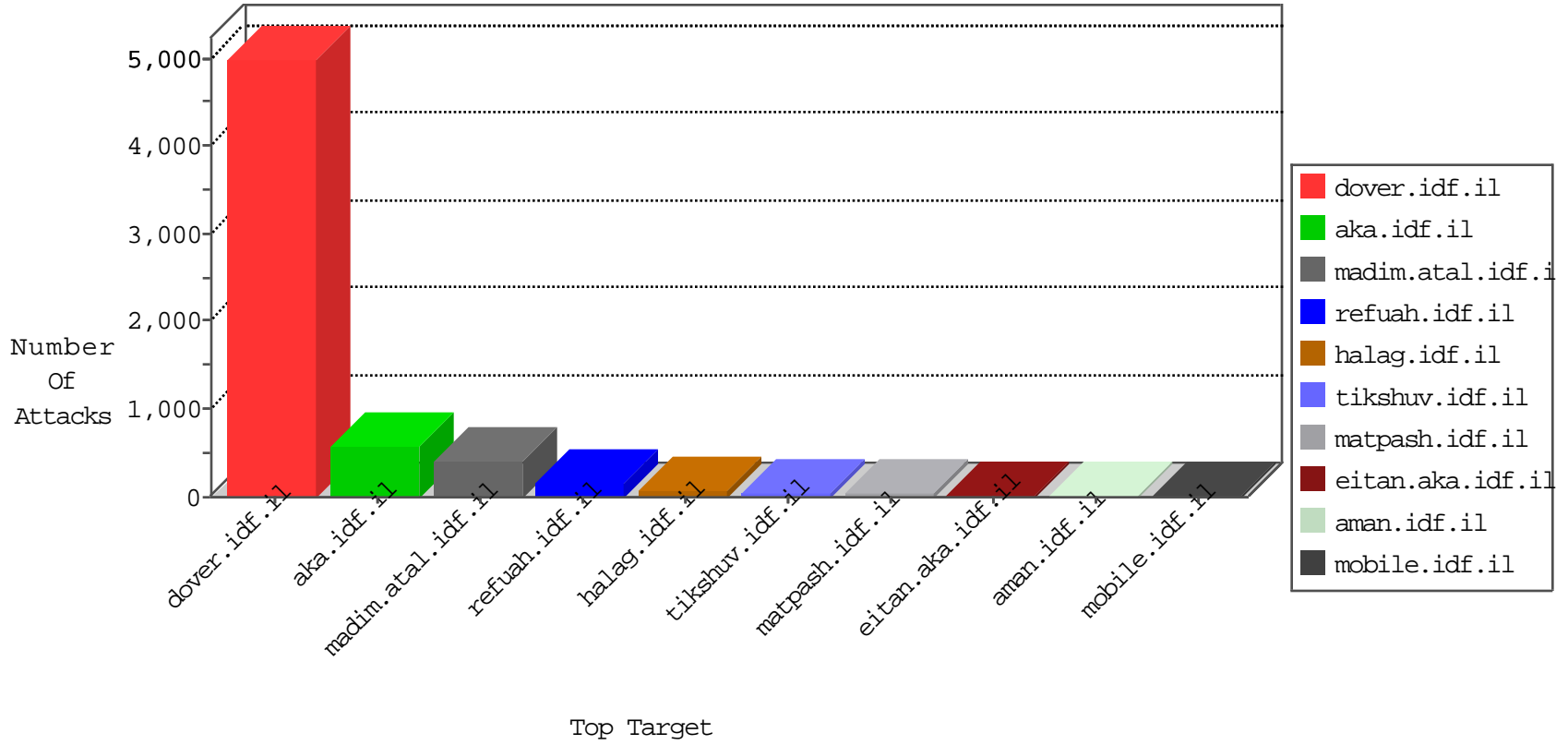


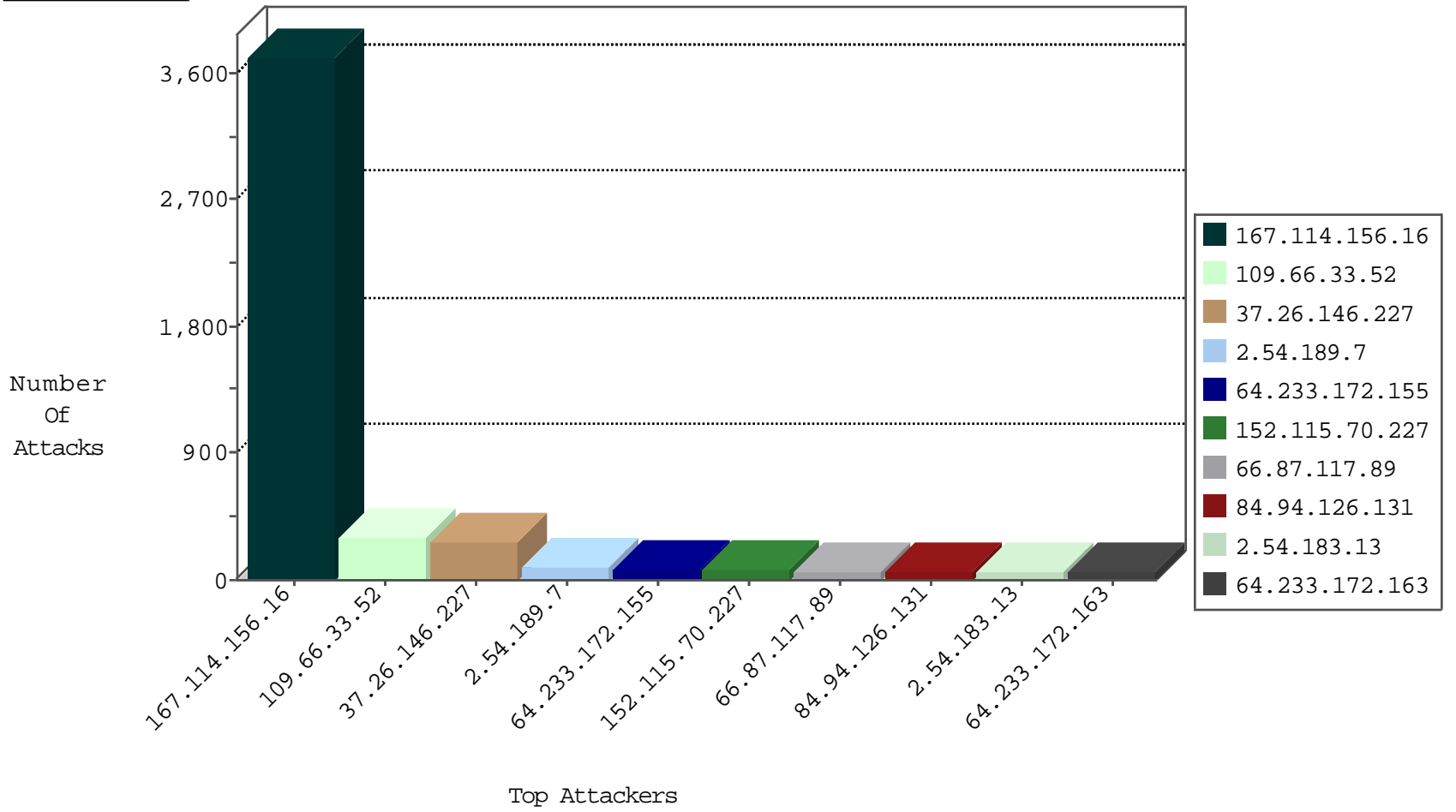
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	2651
154.97.165.190	Sudan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
152.115.70.227	147.237.76.42	Denmark	refuah.idf.il	SQL Injection - Select From	72
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.19.85.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
222.186.56.38	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.56.38	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
199.101.186.178	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 3072	1
61.130.145.216	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.38	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.56.38	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
199.101.186.178	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.195	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1

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	1886
37.26.146.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	273
2.54.189.7	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	83
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
66.87.117.89	United States	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	62
84.94.126.131	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	59
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
170.235.218.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
5.175.26.46	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	31
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
100.100.123.154		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.142.181.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
52.34.179.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
2.54.183.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
46.19.85.197	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
173.252.88.244	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
5.102.254.53	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.73.165		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
31.154.92.78	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.233.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
188.161.50.241	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
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
100.100.43.82		147.237.76.200	eitan.aka.idf.	drop	First packet isn't SYN	drop	11
213.57.128.207	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
154.97.165.190	Sudan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.85.197	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
87.203.98.130	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
100.100.110.121		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
93.63.227.234	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.183.13	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.183.13	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
46.121.120.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
100.100.43.82		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.54.183.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.121.120.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.183.13	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
129.195.0.205	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
183.60.244.24	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.33.52	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.66.33.52	Block	156
109.66.33.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	138
46.19.86.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
46.19.85.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
2.54.6.53	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 2.54.6.53	Block	31
79.183.224.202	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	13
46.19.85.109	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
109.67.111.211	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	4
77.127.169.22	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
5.28.142.179	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	4
84.111.66.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.15.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.107.229	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewihkyrb4anjahvhp4khwumbaqgfggimaa&sig=43pu9patudqyoofftjptaa&usg=afqjcnhcvyvg7wlcq-yhd5_ammzoyodtwa	Block	3
79.183.224.202	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.183.224.202	Block	3
5.29.176.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.10.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.42.187	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
2.54.1.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.209.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.250.138.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.67.213.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
60.51.9.245	Malaysia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
87.169.99.127	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
197.35.237.250	Egypt	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
31.154.170.198	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
79.179.114.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.43.182	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
77.237.138.202	Czech Republic	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
109.64.34.217	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
46.116.199.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.152.90	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
176.13.3.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.6.53	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method undefined in URL www.aka.idf.il/main/giyus/api/api/professiondescription/5357	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1361-he/dover.aspx	Block	1
95.86.120.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewjax5fz7knjahxnvhikhr62d70qfggbmai&usg=afqjcnhcvyvg7wlcq-yhd5_ammzoyodtwa	Block	1
217.132.32.207	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
41.237.106.25	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
80.246.137.160	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.2.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.64.73	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed PHP Attempt	Block	1
79.181.184.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.178.234	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1086-en/dover.aspx	Block	1
89.139.29.182	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
212.143.139.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
87.68.78.164	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.120.126.33		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
14.102.31.145	India	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
79.176.61.146	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
109.64.131.189	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/xmlrpc.php	Block	1