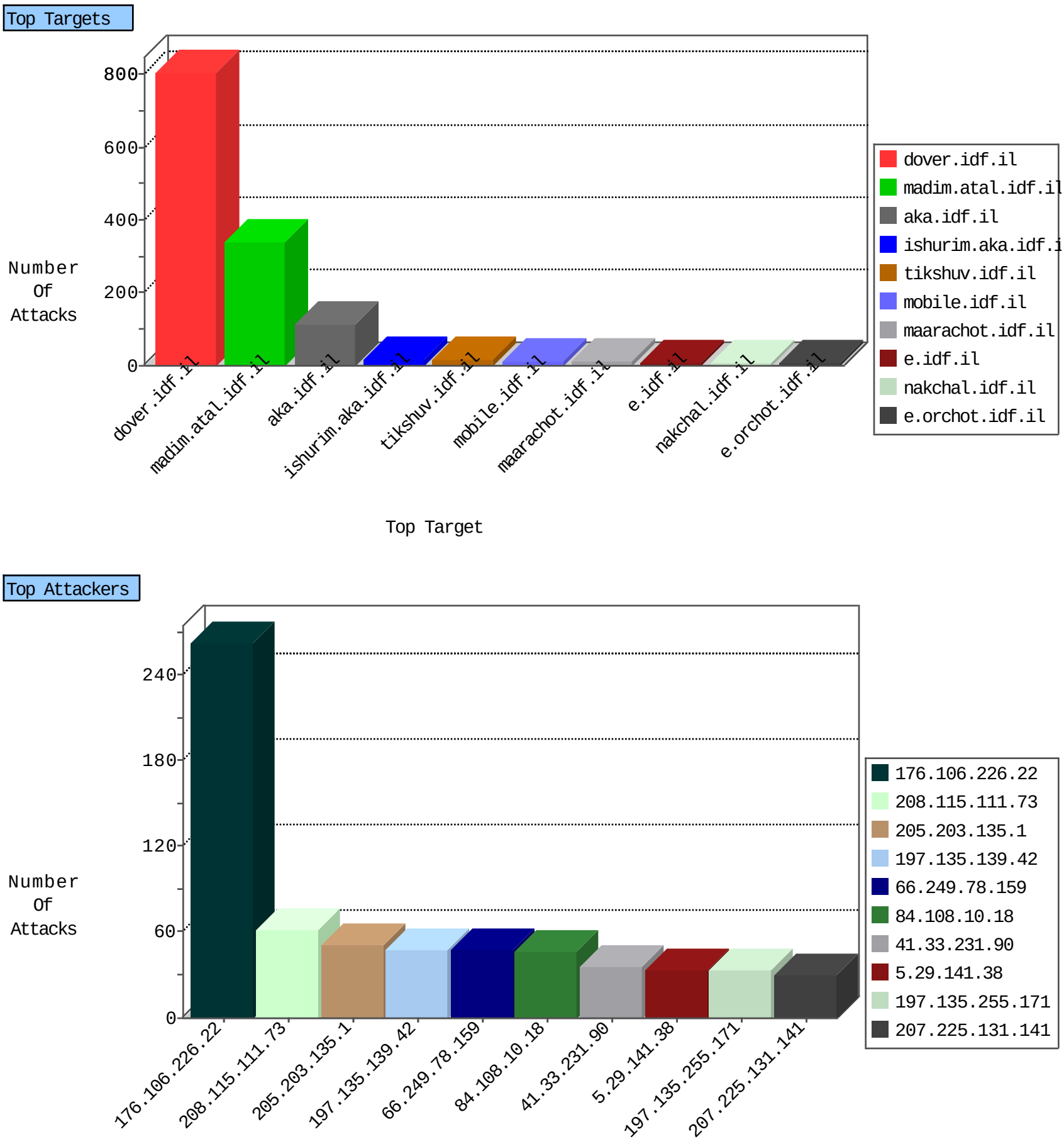
11-22-2015-00:04:06 to 11-22-2015-01:04:06

IDF Under Attack
Daily Report



11-22-2015-00:04:06 to 11-22-2015-01:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1019
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	35
79.183.9.84	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
192.168.1.103		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
192.168.0.100		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
46.116.238.253	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.166.188.68	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
61.147.103.92	China	147.237.0.33	idf.il	Frk_Under_Attack_Con_Tcp	drop	1
115.231.222.40	China	147.237.0.34	tikshuv.idf.il	Frk_Under_Attack_Con_Http	drop	1
31.210.186.172	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-22-2015-00:04:06 to 11-22-2015-01:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.171.21.74	Malaysia	147.237.77.216	dover.idf.i	12634: HTTP: JS LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	6

11-22-2015-00:04:06 to 11-22-2015-01:04:06

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
66.249.64.200	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
203.197.205.118	147.237.77.226	India	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
175.175.56.195	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
159.122.238.133	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
141.105.71.68	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
74.117.209.135	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
23.227.196.29	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
159.122.238.133	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
144.76.155.8	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

11-22-2015-00:04:06 to 11-22-2015-01:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
197.135.139.42	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
84.108.10.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
5.29.141.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
197.135.255.171	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
207.225.131.141	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
45.216.87.156	Uruguay	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
100.100.106.201		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
183.171.21.74	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
100.100.78.218		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.67.144.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
178.152.65.162	Qatar	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
122.109.7.134	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
157.55.39.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
185.20.4.143	United Kingdom	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	9
79.176.57.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.224	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
149.78.29.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.135.111.195	Hungary	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
52.33.66.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
93.202.98.97	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.29.214.119	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
70.211.7.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.127.57.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.159.207.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.116.142.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.116.238.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.29.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
122.109.7.134	Australia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.247.36.108	Netherlands	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
122.109.7.134	Australia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
37.247.36.116	Netherlands	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
66.249.64.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
122.109.7.134	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
122.109.7.134	Australia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.14.184	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
149.78.246.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

11-22-2015-00:04:06 to 11-22-2015-01:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.106.226.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	147
176.106.226.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	116
46.121.242.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
85.250.128.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
109.160.176.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
89.138.213.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
79.180.199.127	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	4
77.127.127.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
5.29.110.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.186.131.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.183.130.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.181.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
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	2
46.19.86.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.29.110.130	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.54.184.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.28.122.202	Moldova, Republic of	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL / 200	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8943-he/refuah.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.228.123.145	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
185.16.40.143	United Kingdom	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/sites/klali/default.asp	None	1
66.249.93.230	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/4/4454.Ø¨Ø¯Ù?	Block	1
46.121.101.175	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl72.y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.131	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.228.123.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.120.126.23		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.93.233	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/4454.Ø¨Ø¯Ù?	Block	1
95.86.67.136	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 95.86.67.136	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.198	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
176.126.163.232	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	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
46.19.86.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
46.166.186.224	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.201.154.173	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.142.223.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.67.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.101	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.232.15.43	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18863-en/dover.aspx.http:/www.idf.il/1283-18863-en/dover.aspx./a/p	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.121.84.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.147.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.68.48.202	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.68.48.202	Block	1

11-22-2015-00:04:06 to 11-22-2015-01:04:06