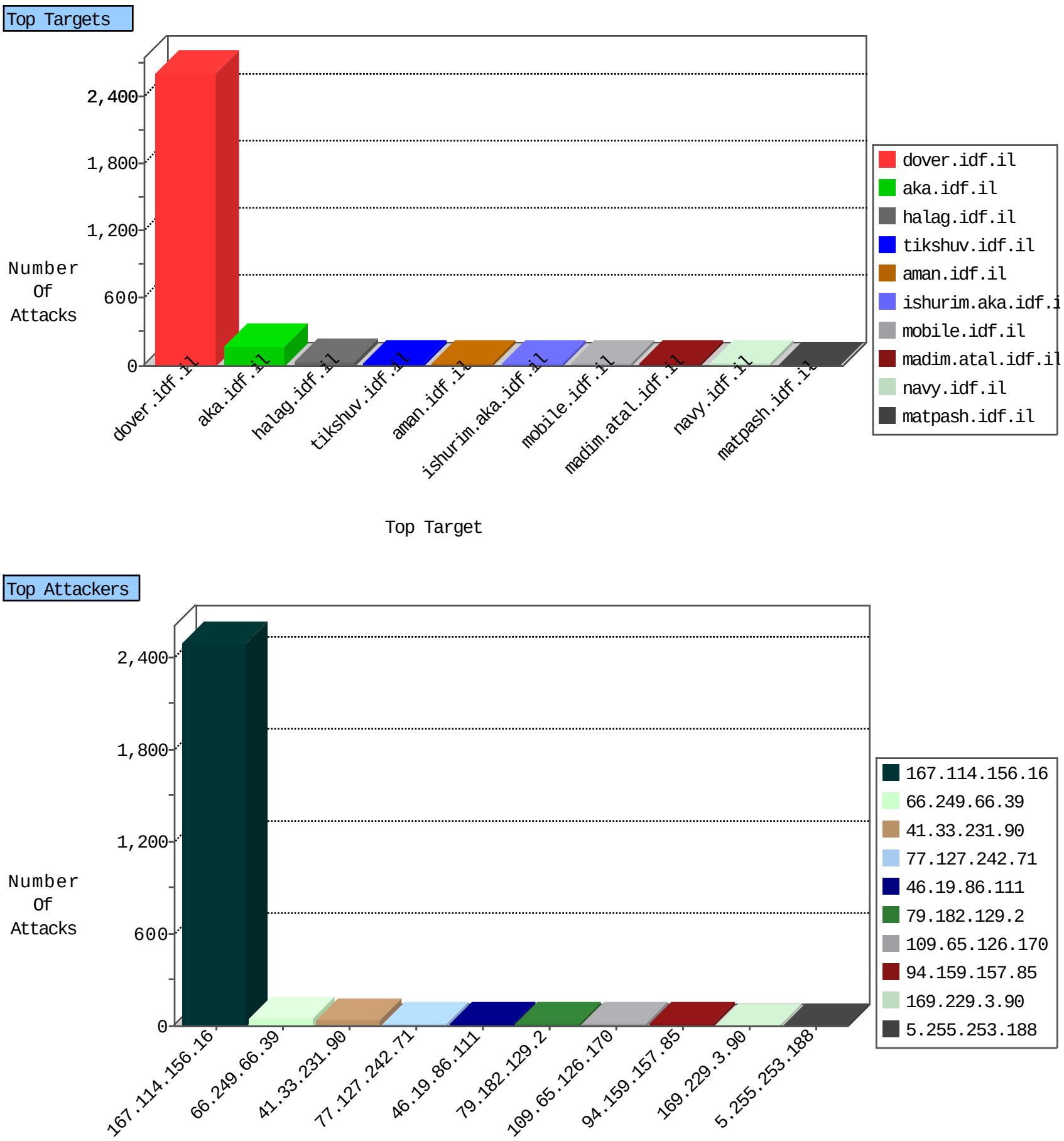
12-11-2015-16:04:10 to 12-11-2015-17:04:10

IDF Under Attack
Daily Report



12-11-2015-16:04:10 to 12-11-2015-17:04:10

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	3341
107.150.55.52	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
107.150.55.54	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	drop	1
89.248.160.229	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
107.150.55.53	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1
89.248.160.229	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
107.150.55.53	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
89.248.160.229	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.229	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
107.150.55.53	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
89.248.160.229	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

12-11-2015-16:04:10 to 12-11-2015-17:04:10

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.153	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1

12-11-2015-16:04:10 to 12-11-2015-17:04:10

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
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
185.106.94.16	147.237.77.178		e.matpash.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.16	147.237.76.177		ncore.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.16	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
116.72.166.83	147.237.76.147	India	chinuch.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.195	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
85.251.84.161	147.237.76.31	Spain	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.39.222.253	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
185.106.94.16	147.237.77.235		sviva.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.16	147.237.77.170		maarachot.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.16	147.237.72.156		aman.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.16	147.237.0.200		m4u.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.77.179	Ukraine	e.mazi.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
190.83.138.97	147.237.72.14	Trinidad and Tobago	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

12-11-2015-16:04:10 to 12-11-2015-17:04:10

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.111	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	19
79.182.129.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
94.159.157.85	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
192.118.11.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.181.11.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
185.3.146.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.31.23.79	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
80.246.139.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.65.126.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.65.126.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.102.254.160	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.127.23.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.212	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.176.183.186	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.102.254.144	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.64.113.66	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
176.13.22.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.98.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
87.68.248.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.7.97	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.139.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.67.27.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.139.163.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.142.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.53.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.0.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.125.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.107.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
40.77.167.89	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
178.26.138.233	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
94.230.86.174	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.227.254.119	Germany	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
188.120.148.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.66.93	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.220	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
207.46.13.155	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2

12-11-2015-16:04:10 to 12-11-2015-17:04:10

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
94.230.86.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.227.254.119	Germany	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
149.88.80.245	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.88.80.245	Block	4
176.12.151.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
149.88.80.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
176.13.2.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.3.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
194.90.240.221	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
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	2
46.19.85.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.57.61.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.0.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/6255.jpg	Block	1
79.180.123.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.127.242.71	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 77.127.242.71	Block	1
40.77.167.45	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/coordinationgaza	Block	1
77.127.242.71	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Value at 3 for	Block	1
128.232.110.29	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
84.94.91.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8879-he/refuah.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
77.127.255.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.68.153	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
176.45.22.160	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
5.29.178.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.90.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.242.71	Israel	147.237.72.166	aka.idf.il	Malformed URL ×žÃ»(hÂ¢[[#17]][[#5]]5[[#3]]ÂŒt×'ÂŽÂŒ[[#5]]×¨\e`â€ ¡×¢rËœÂ¸iÖ±Ö³]â€¦]×?@u× Ö¿[[#11]]"ljÂ¹×?[[#5]]Â¹Â®h[[#14]][[#17]]Â§z×' Âµ[[#5]]Ã»•â€™!×?×ªÂŽ	Block	1
77.127.242.71	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name Â›Ã¹xÂ±yÃ‹SÃ´hkÃ¿=Ã§s[[#1]]Ã	Block	1
217.42.198.230	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	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
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/size220x0/17672.jpg	Block	1
79.180.123.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.242.71	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 77.127.242.71	Block	1
40.77.167.94	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/â€Ž	Block	1
77.127.242.71	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Query String Â?Ã?[[#3]]×¡Â f[[#24]]Ö²Â¢Â´â€ ¦Â?hÂ¶P×‚â€¢}[[#22]][[#4]]Â«Â³,>JÖ²Â¬Jâ€žâ€™×–×›[[#11]]]×§9×‚ [[#4]][[#6]]× Ö²[[#5]]ÃŸ[[#11]] =Ã?[[#21]]B8qÂ²Â?Â¬â€?[[#19]]eUÂ°% L7A×°*×Ÿ5×?×¤r×˜ÂŽR	Block	1
149.88.80.245	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.88.80.245	Block	1
84.109.69.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.96.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
176.45.22.160	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
46.246.124.92	Sweden	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
37.26.146.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
157.55.39.231	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.242.71	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 77.127.242.71	Block	1
77.127.242.71	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
217.55.88.46	Egypt	147.237.77.170	maarachot.idf.il	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/1133-22461-he/dover.aspx.	Block	1
66.249.66.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1