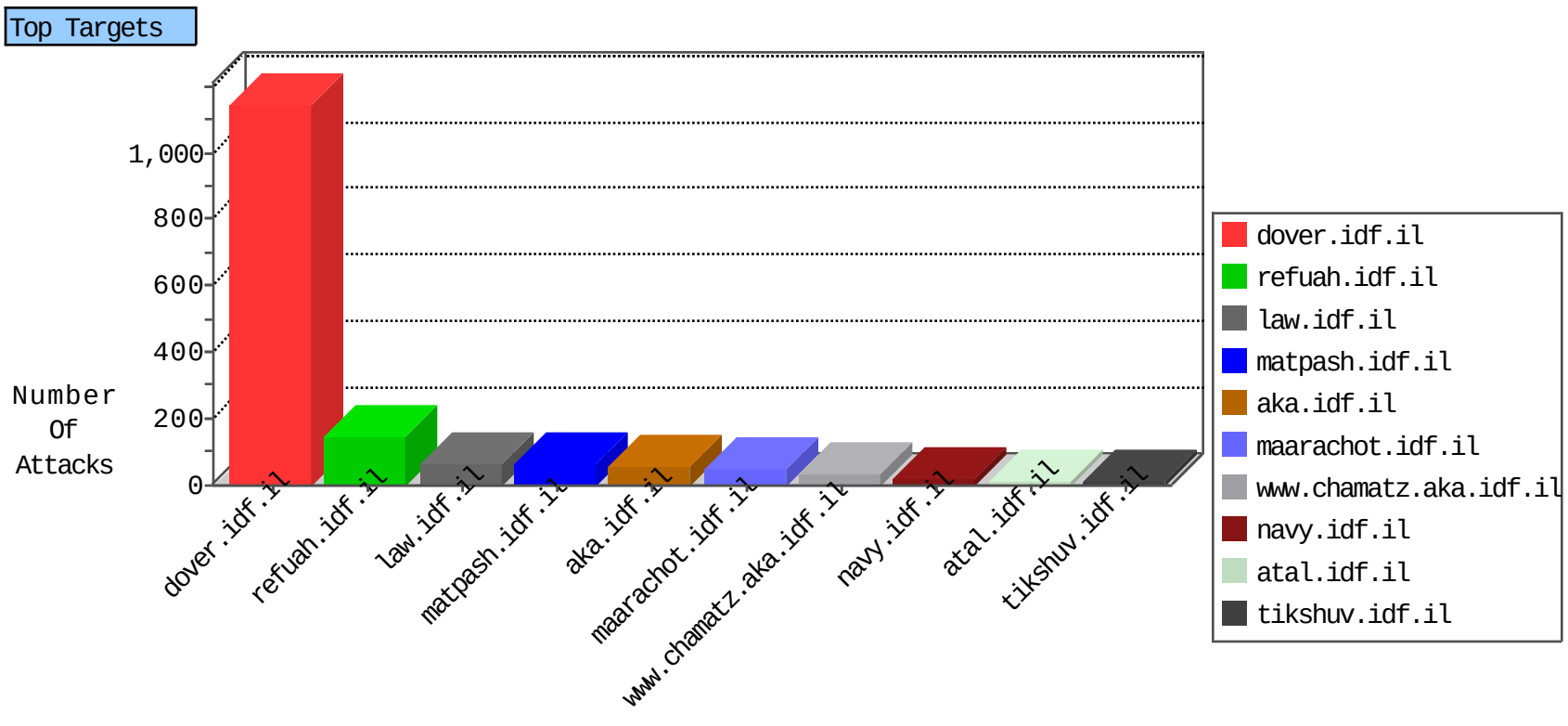
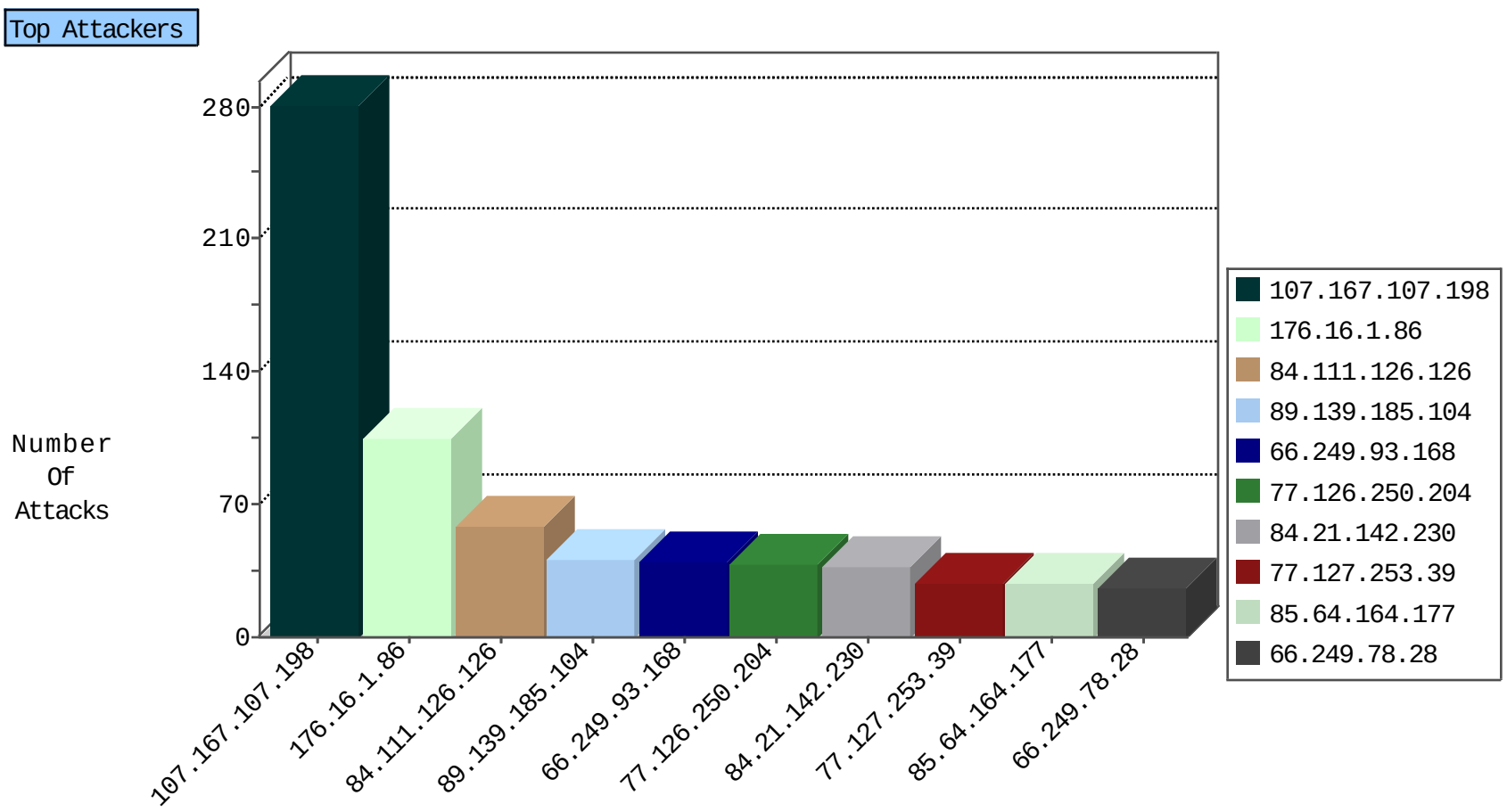
04-10-2015-08:03:05 to 04-10-2015-09:03:05

IDF Under Attack
04-10-2015-08:03:05

Top Targets



Top Attackers



04-10-2015-08:03:05 to 04-10-2015-09:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	26
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	26
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	19
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	18
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	18
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	17
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	16
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.93.176	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.78.45	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	14
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	13
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	13
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	13
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	13
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	9
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	8
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.15	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.64.79	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	7
66.249.65.196	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	6
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.64.125	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.64.147	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	5
66.249.64.4	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5
66.249.89.105	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
201.92.191.130	Brazil	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	5
66.249.64.169	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	4
66.249.78.29	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	4
66.249.64.187	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	4
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	4
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	4
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	4
66.249.64.129	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	4
66.249.69.128	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	4
66.249.78.18	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	4
66.249.78.236	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	4

04-10-2015-08:03:05 to 04-10-2015-09:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	26
46.19.85.192	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-10-2015-08:03:05 to 04-10-2015-09:03:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	24
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
93.190.92.127	Germany	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	1
89.248.171.162	Netherlands	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.21.142.230	United Kingdom	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
113.59.33.61	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.56.231	Netherlands	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
89.248.171.162	Netherlands	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.171.162	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.21.142.230	United Kingdom	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	1
113.59.33.61	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1

04-10-2015-08:03:05 to 04-10-2015-09:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
107.167.107.198	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	281
176.16.1.86	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	105
84.111.126.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
77.126.250.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
85.64.164.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
77.127.253.39	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
109.253.141.72	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.157.8	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
84.111.85.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
87.69.154.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
109.66.162.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.253.146.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
184.53.38.107	United States	147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	9
61.3.216.192	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
46.19.86.92	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
5.22.129.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
109.253.144.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
180.250.197.98	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
73.185.134.74	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
84.21.142.230	United Kingdom	147.237.77.74	law.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	7
77.127.6.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
84.21.142.230	United Kingdom	147.237.77.74	law.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
157.55.39.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.253.157.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
2.90.37.146	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
99.102.174.194	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
85.130.187.90	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.144.72	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
89.139.185.104	Israel	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	6
176.12.144.137	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
75.168.168.248	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
149.88.30.15	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
109.253.157.129	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
84.21.142.230	United Kingdom	147.237.77.176	matpash.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	4
84.21.142.230	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
104.33.1.197		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.14.243.78	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
77.125.215.143	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	3
46.19.86.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigation.asp	Block	2
213.61.227.39	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
87.68.55.40	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
149.78.60.170	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
84.21.142.230	United Kingdom	147.237.77.216	dover.idf.il	Multiple signatures from 84.21.142.230	Block	1
175.42.91.134	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/3/3593.pdf/trackback/	Block	1
89.139.185.104	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 89.139.185.104	Block	1
2.52.35.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
184.173.183.173	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1175-he/refuah.aspx&usg=alkjrhgwavjkcz07afvujil0dvm9fs0pra	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
84.94.74.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/	None	1
50.97.52.131	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1253-he/refuah.aspx&usg=alkjrhil9eog2e280qbrz9t0sazc42dptg	Block	1
184.53.38.107	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
93.190.92.127	Germany	147.237.77.176	matpash.idf.il	Multiple signatures from 93.190.92.127	Block	1
84.21.142.230	United Kingdom	147.237.77.74	law.idf.il	Multiple signatures from 84.21.142.230	Block	1
5.29.109.163	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.241	Block	1
84.109.4.146	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
54.153.14.125	United States	147.237.76.39	mobile.meitav.idf.il	Suspicious Response Code	Block	1
184.53.38.107	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
93.190.92.127	Germany	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
84.21.142.230	United Kingdom	147.237.77.74	law.idf.il	PHP Attempt	Block	1
5.29.109.163	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0914-1b.stm	Block	1
157.55.39.143	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
84.111.23.128	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
184.173.183.170	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1250-he/refuah.aspx&usg=alkjrhhwsbbck5i-bc-21dvmmjhkpqpkfa	Block	1
109.253.67.234	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
84.21.142.230	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
184.173.183.173	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 184.173.183.173	Block	1

04-10-2015-08:03:05 to 04-10-2015-09:03:05