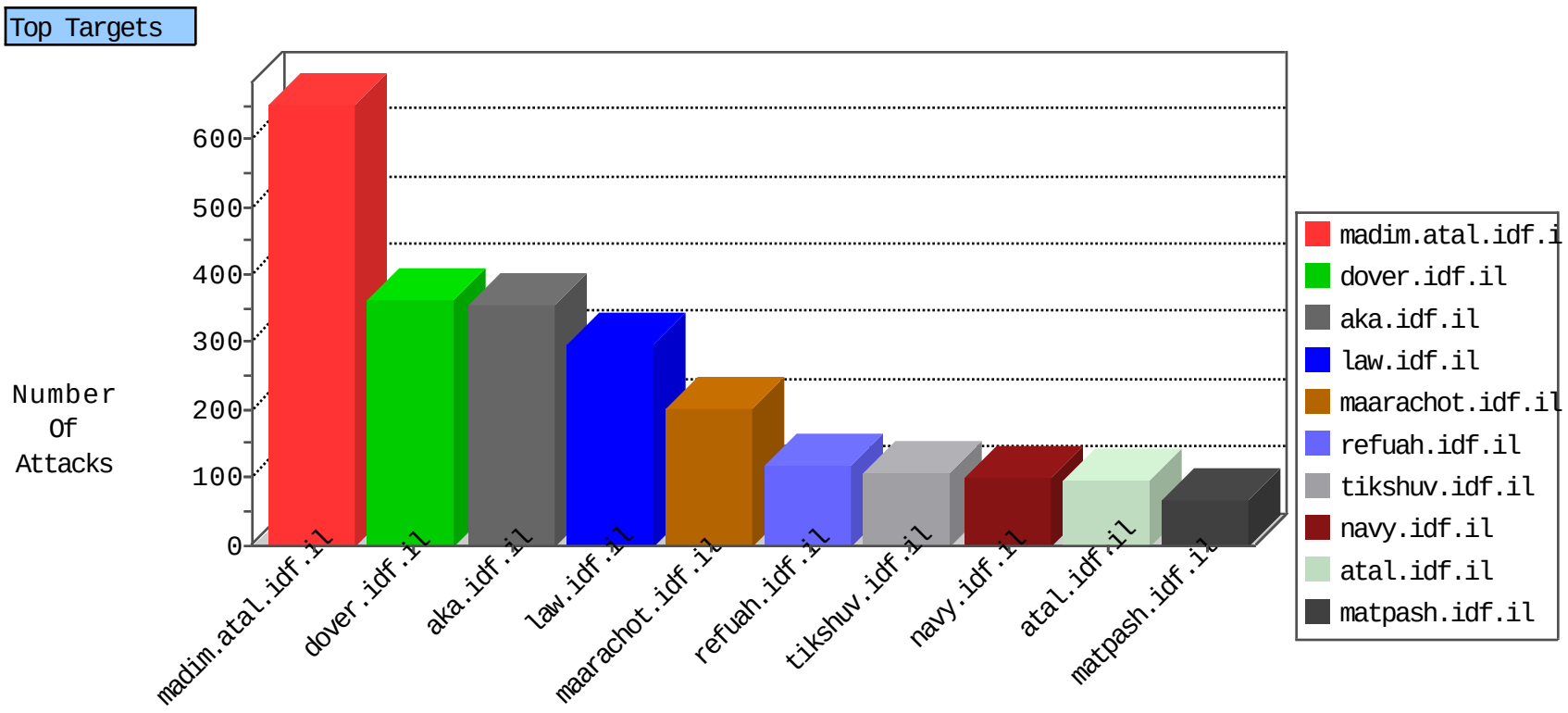
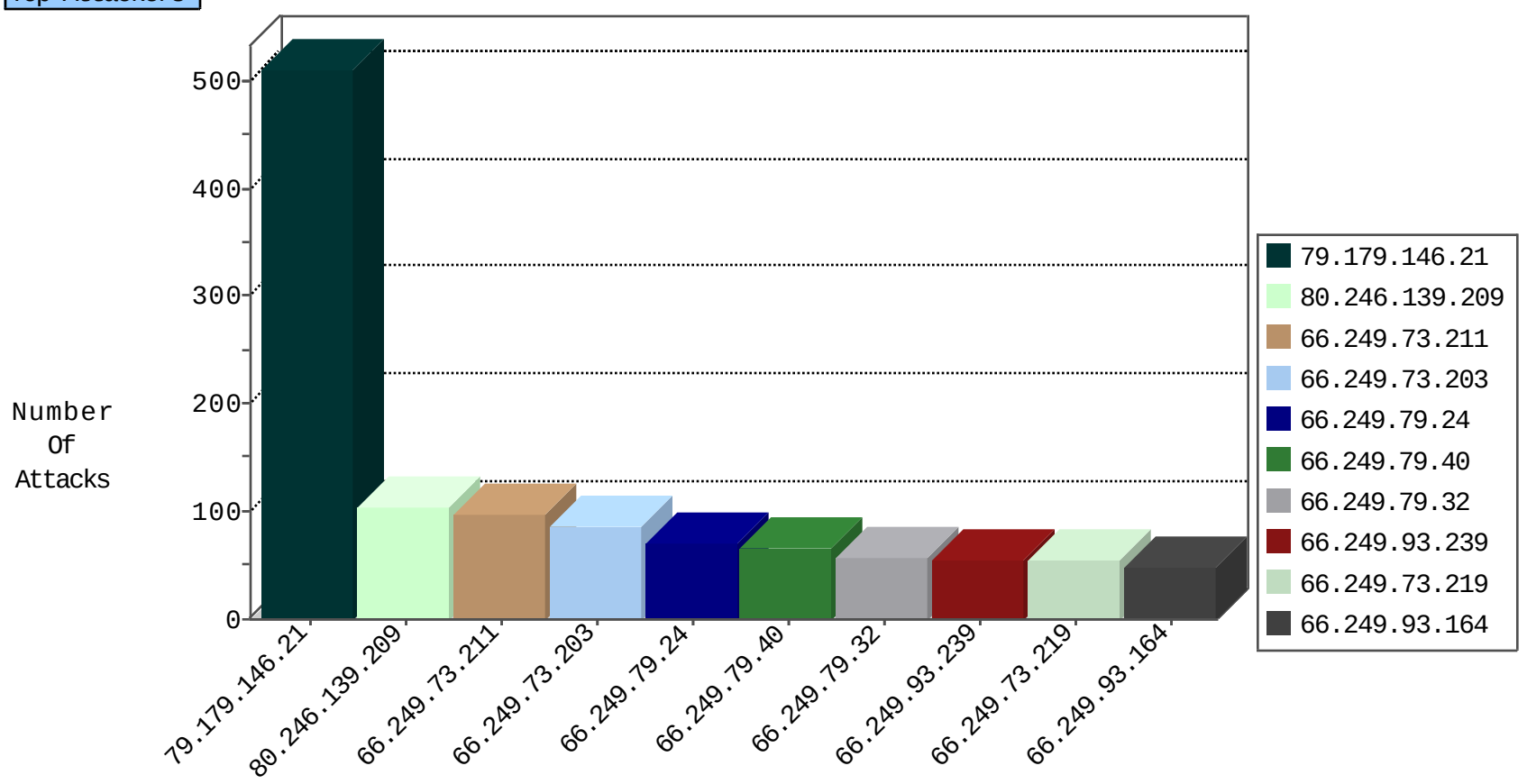
04-05-2015-22:03:03 to 04-05-2015-23:03:03

IDF Under Attack
04-05-2015-22:03:03

Top Targets



Top Attackers



04-05-2015-22:03:03 to 04-05-2015-23:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.73.211	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	97
66.249.73.203	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	87
66.249.79.24	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	70
66.249.79.40	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	65
66.249.79.32	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	57
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	54
66.249.73.219	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	54
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	49
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	45
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	43
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	41
66.249.67.73	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	41
66.249.65.199	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	32
66.249.67.81	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	29
66.249.73.187	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	27
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	26
66.249.73.233	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	26
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	26
66.249.73.129	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	25
66.249.73.195	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	25
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	24
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	23
66.249.65.191	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	23
66.249.78.144	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	22
66.249.78.130	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	21
66.249.79.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	20
66.249.79.13	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	19
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.65.195	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	18
66.249.79.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.65.143	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	18
66.249.79.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
66.249.79.34	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	16
66.249.79.157	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
66.249.78.148	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	16
66.249.73.241	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	15
66.249.78.137	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	15
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	14
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
66.249.79.50	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	13
66.249.67.37	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	12
66.249.67.131	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	12
66.249.79.5	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.141	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	10
66.249.67.29	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.78.228	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	9
66.249.73.238	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	9
66.249.80.75	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.89.85	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.79.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8

04-05-2015-22:03:03 to 04-05-2015-23:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
198.20.69.98	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.226	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
87.69.6.45	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
50.7.159.11	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
213.57.62.197	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.228.86.155	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1

04-05-2015-22:03:03 to 04-05-2015-23:03:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
177.129.79.177	Brazil	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 2048	1
177.129.79.177	Brazil	147.237.76.86	navy.idf.il	ET SCAN NMAP -f -sS	1
80.246.139.209	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
61.240.144.64	China	147.237.77.233	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
212.7.199.208	Netherlands	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.7.199.208	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.20.69.98	United States	147.237.76.148	gqcenter.aka.idf.il	ET DROP Dshield Block Listed Source	1
183.136.216.7	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
177.129.79.177	Brazil	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
113.88.130.97	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.7.199.208	Netherlands	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.51.75.164	Canada	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1

04-05-2015-22:03:03 to 04-05-2015-23:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	28
176.12.139.113	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.159.191	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.138.53	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.131.253	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
2.54.62.185	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	12
2.54.62.185	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	12
2.54.62.185	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	12
109.253.159.37	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
78.108.175.37	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
85.133.5.50	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
193.153.133.60	Spain	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.210.186.128	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
46.19.85.250	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	SAM rule	drop	drop	5
31.210.186.128	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
93.152.214.216	Bulgaria	147.237.76.44	e.refuah.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
209.193.89.213	United States	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
209.193.89.213	United States	147.237.76.44	e.refuah.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
105.210.180.197	South Africa	147.237.77.216	dover.idf.il	SAM rule	drop	drop	4
209.193.89.213	United States	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
209.193.89.213	United States	147.237.76.201	e.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
188.120.148.201	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
209.193.89.213	United States	147.237.76.197	e.himush.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
8.37.227.68	Anonymous Proxy	147.237.77.233	atal.idf.il	Response out of state	Block HTTP Non Compliant	monitor	4
46.116.113.151	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
209.193.89.213	United States	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
209.193.89.213	United States	147.237.76.198	e.yohalan.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
70.39.186.218	Satellite Provide	147.237.77.233	atal.idf.il	Response out of state	Block HTTP Non Compliant	monitor	3
79.176.12.236	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
79.176.12.236	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
209.193.89.213	United States	147.237.76.176	test.ncore.idf.il	SAM rule	drop	drop	2
46.19.86.144	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
61.135.190.70	China	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
209.193.89.213	United States	147.237.76.177	ncore.idf.il	SAM rule	drop	drop	2
192.115.83.5	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
209.193.89.213	United States	147.237.76.200	eitan.aka.idf.il	SAM rule	drop	drop	2
209.193.89.213	United States	147.237.76.86	navy.idf.il	SAM rule	drop	drop	2
46.19.85.192	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
192.115.83.5	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
209.193.89.213	United States	147.237.76.147	chinuch.aka.idf.il	SAM rule	drop	drop	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
209.193.89.213	United States	147.237.76.148	gqcenter.aka.idf.i	SAM rule	drop	drop	2
69.159.54.155	Canada	147.237.77.74	law.idf.il	SAM rule	drop	drop	2
8.37.227.69	Anonymous Proxy	147.237.77.233	atal.idf.il	Response out of state	Block HTTP Non Compliant	monitor	2
93.152.214.216	Bulgaria	147.237.76.34	yohalan.idf.il		drop	drop	2
209.193.89.213	United States	147.237.76.34	yohalan.idf.il		drop	drop	2
52.4.217.116	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
162.209.98.69	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.85.64	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.179.146.21	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.179.146.21	Block	511
80.246.139.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	104
46.19.86.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	26
46.116.24.65	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	10
149.88.148.96	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.66.117.147	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.64.157.94	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
54.172.21.120	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/questionnaire/default.aspx#/tabs/2/mitham/1295	Block	2
109.66.129.208	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
79.183.206.250	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
167.114.64.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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
79.176.12.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
209.193.89.213	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
91.109.10.133	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
84.109.56.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.138.17.205	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
75.61.131.100	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/alnajah/alnajah.stm	Block	1
37.52.206.211	Ukraine	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
189.90.150.229		147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1
87.69.220.108	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.31.253.156	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
79.176.24.211	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
109.253.140.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
93.152.214.216	Bulgaria	147.237.76.30	himush.idf.il	Distributed Unauthorized URL Access on //tmunblock.cgi	Block	1
84.228.19.32	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
188.165.15.66	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/656-he/patzar.aspx	Block	1
75.119.222.136	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1129-2.stm	Block	1
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
199.16.128.43	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
89.138.60.98	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
178.120.104.216	Belarus	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
70.167.8.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalanmain/main.asp	Block	1
109.253.142.39	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.152.214.216	Bulgaria	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on //tmunblock.cgi	Block	1
84.228.86.155	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.198	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.198	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.177.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
203.133.169.157	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
89.139.163.216	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-20127-he/kkkkkkk=bc69e9b3kkkkkkk_bc69e9b3	Block	1
70.196.67.215	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
149.88.0.172	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
98.138.81.164	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
85.64.144.252	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
188.165.15.198	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1110-4.stm	Block	1
77.127.196.30	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$rbSearchSites in aka.idf.il/main/sachar/	None	1

04-05-2015-22:03:03 to 04-05-2015-23:03:03