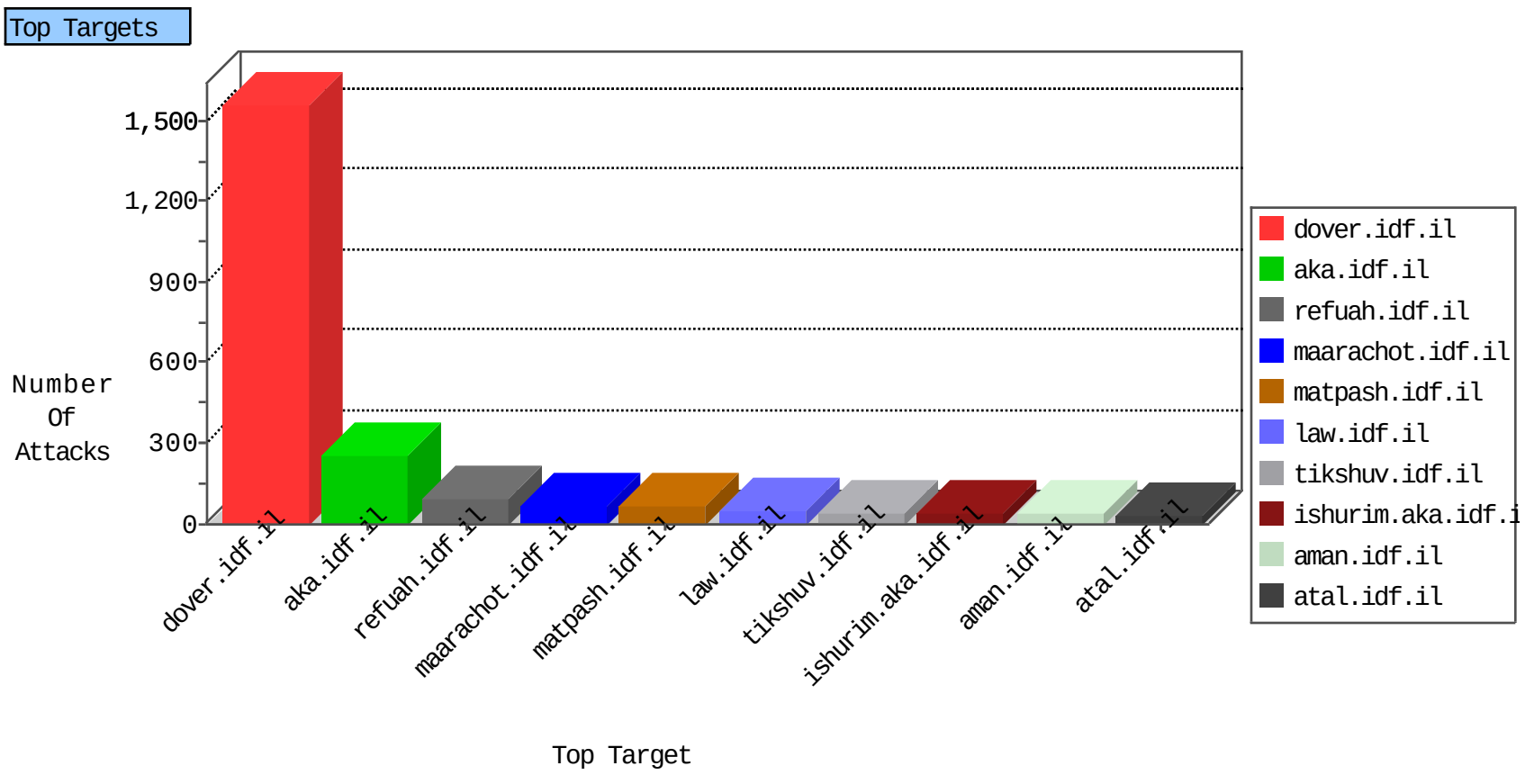
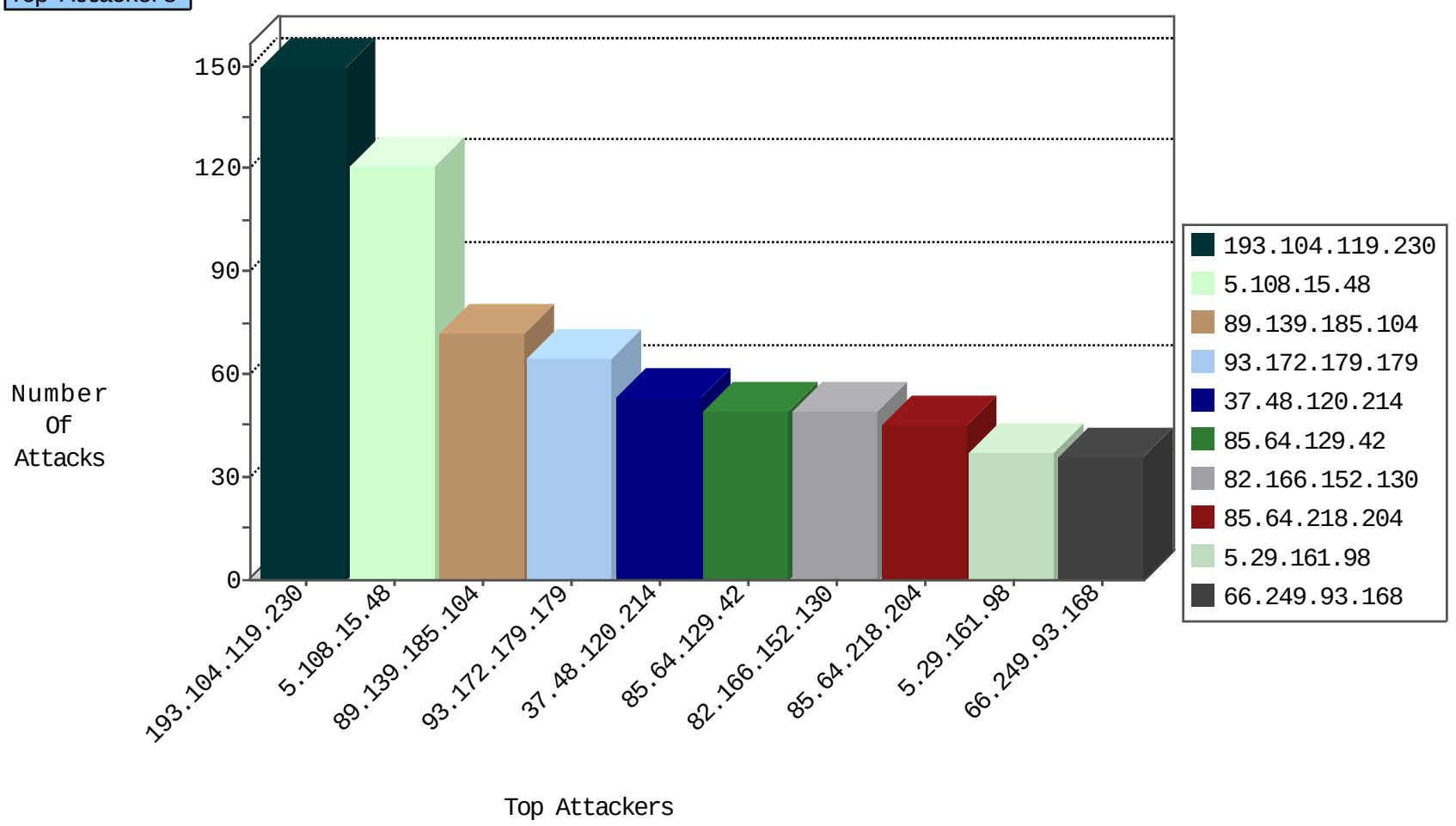
04-10-2015-10:03:00 to 04-10-2015-11:03:00

IDF Under Attack
04-10-2015-10:03:00

Top Targets



Top Attackers



04-10-2015-10:03:00 to 04-10-2015-11:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
5.102.212.116	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	259
87.68.30.35	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
80.246.139.42	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	34
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	26
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	25
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	24
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	23
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	21
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	18
77.127.43.206	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	17
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	16
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	15
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	15
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	15
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	14
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.69.101	United States	147.237.72.166	aka.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
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	13
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.69.128	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	10
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.69.97	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	10
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	9
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.65.155	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	8
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	8
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	8
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	7
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	7
66.249.69.90	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.93.246	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.81.146	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	6
66.249.93.240	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.64.41	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	6
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.64.87	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	5
66.249.65.186	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	5
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.69.113	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	5
66.249.64.55	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	5

04-10-2015-10:03:00 to 04-10-2015-11:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.109.9.83	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.219	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
213.57.45.159	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.183	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.76.198	e.yohalan.idf.i	DVRep_B-N_60_100	Block	1
94.159.210.166	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.116.92.21	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
192.116.177.146	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
83.240.211.34	Portugal	147.237.72.156	aman.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
213.57.45.159	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-10-2015-10:03:00 to 04-10-2015-11:03:00

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
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
213.57.45.159	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.213	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
209.126.230.72	United States	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	Russian Federation	147.237.77.205	prisha.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
221.235.188.213	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
176.12.139.77	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.213	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
152.157.46.21	United States	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1

04-10-2015-10:03:00 to 04-10-2015-11:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
193.104.119.230	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	150
5.108.15.48	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	121
89.139.185.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	72
93.172.179.179	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	65
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
85.64.129.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
82.166.152.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
85.64.218.204	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
109.253.156.20	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
94.197.121.23	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
5.29.161.98	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
37.231.42.125	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
141.14.238.112	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
185.23.124.119	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
82.213.16.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
94.159.210.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
79.176.32.68	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
150.183.45.253	Korea, Republic of	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
46.19.85.238	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	12
176.12.140.91	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
77.75.77.32	Czech Republic	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
74.248.241.189	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
84.228.23.234	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
157.55.39.114	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
132.64.31.11	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
216.223.27.56	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
157.55.39.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
37.142.200.54	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
112.134.49.117	Sri Lanka	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
80.246.138.99	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	8
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
213.8.46.1	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
109.253.146.184	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
80.246.138.99	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
80.246.138.99	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	8
78.5.138.92	Italy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
80.246.137.141	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	7
79.182.151.49	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
68.180.228.117	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
80.246.137.141	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
80.246.137.141	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	7

04-10-2015-10:03:00 to 04-10-2015-11:03:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.29.161.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
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
46.19.85.139	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	2
77.126.37.247	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.186.185.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
5.255.253.99	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/1381.pdf	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/eurl.axd/73879113e5ed344fa80d3b2b3f38c361/	Block	1
157.55.39.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/archive_2002.stm	Block	1
85.65.63.105	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	1
2.52.12.153	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
188.40.28.160	Germany	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
112.111.188.90	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/brothers/skira/default.asp/trackback/	Block	1
77.125.150.176	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0217-2.stm	Block	1
174.29.187.98	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
89.209.249.10	Ukraine	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
54.153.14.125	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
2.52.31.7	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
188.165.15.75	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9589-he/refuah.aspx	Block	1
113.110.182.150	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/window.location.href	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
178.135.80.0	Lebanon	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
92.222.181.1	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
62.210.124.129	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
190.107.176.148	Chile	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
123.237.163.218	India	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/14-en/patzar.aspx	Block	1
79.178.137.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.152.88.35	Spain	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
180.76.4.12	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
101.22.191.97	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/113198.pdf/trackback/	Block	1
70.167.8.42	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/276-he/sb_item_lev2	Block	1
5.79.16.135	United Kingdom	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.114	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.114	Block	1
79.181.117.240	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
39.48.25.179	Pakistan	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
188.40.28.160	Germany	147.237.77.216	dover.idf.il	Distributed Extremely Long HTTP Request	Block	1

04-10-2015-10:03:00 to 04-10-2015-11:03:00