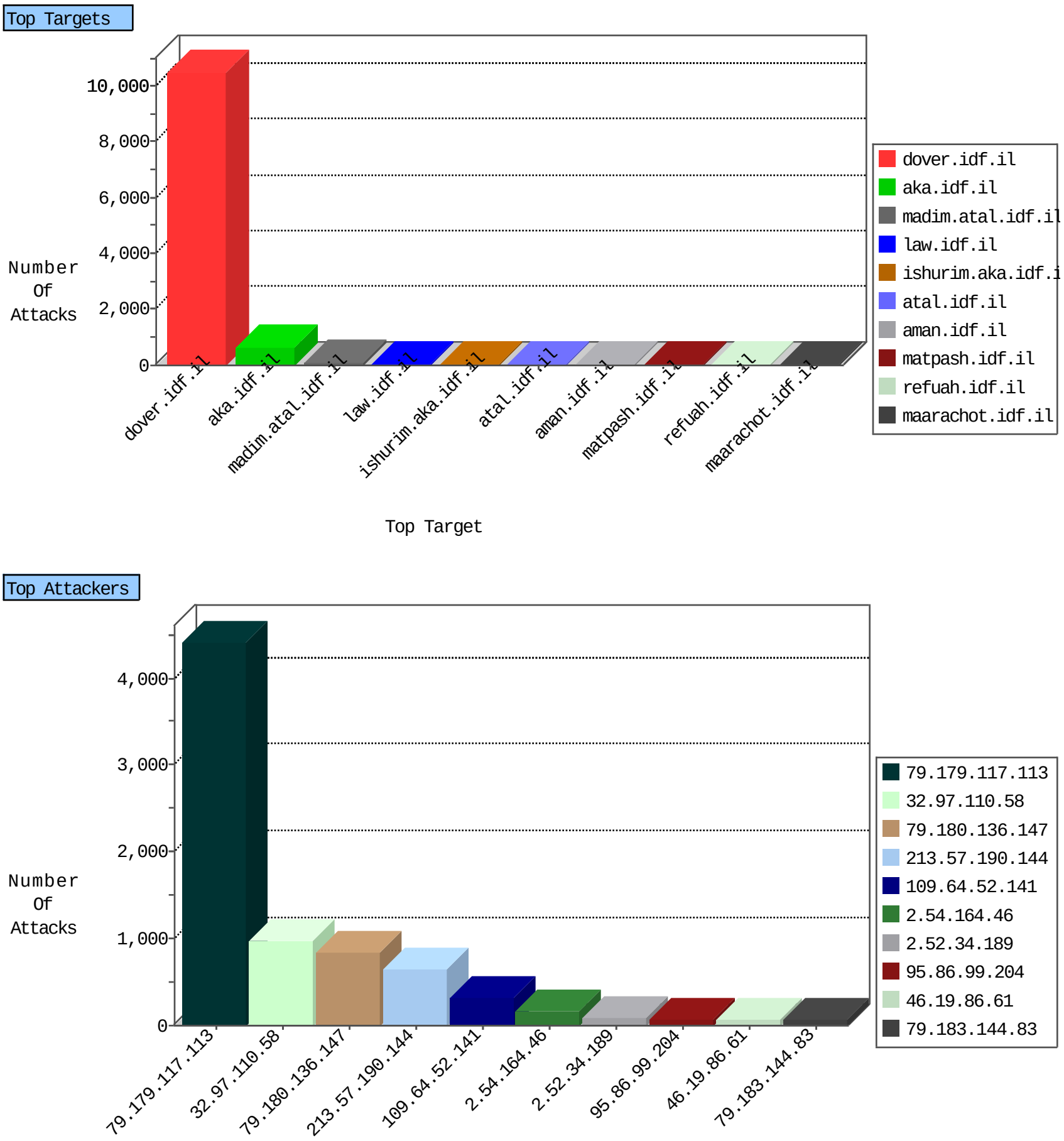
04-28-2015-23:03:05 to 04-29-2015-00:03:05

IDF Under Attack
04-28-2015-23:03:05



04-28-2015-23:03:05 to 04-29-2015-00:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.116	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1057
220.181.108.95	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	256
46.117.20.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	189
66.249.64.68	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	111
220.181.108.163	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	93
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
85.65.49.98	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
204.13.200.28	United States	147.237.72.166	aka.idf.il	Frk_Under_Attack_Con_Https	drop	2
91.238.134.42	Poland	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
10.0.0.20		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
52.74.47.48	United States	147.237.0.35	akaws.idf.il	Invalid TCP Flags	drop	1
23.253.32.88	United States	147.237.0.15	kosher-kravi.idf.il	Invalid L4 Header Length	drop	1
52.74.49.82	United States	147.237.76.42	refuah.idf.il	Invalid L4 Header Length	drop	1
37.26.147.177	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-28-2015-23:03:05 to 04-29-2015-00:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.52.141	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	323
5.22.135.245	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
94.159.169.56	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
41.226.77.23	Tunisia	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
155.133.78.74	Poland	147.237.77.170	maarachot.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	2
89.139.167.139	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.109.194.225	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
69.199.224.222	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
93.172.182.56	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-28-2015-23:03:05 to 04-29-2015-00:03:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.67.84	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	35
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
91.195.154.34	Sweden	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
190.106.66.54	Costa Rica	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
199.119.180.110	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
5.22.130.59	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
195.211.167.193	United Kingdom	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
192.169.217.96	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
50.63.174.137	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.67.116	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.68	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
155.133.78.74	Poland	147.237.77.170	maarachot.idf.il	Tehila - Perl LWP with fake user agent	2
46.120.136.190	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
216.69.179.127	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
43.255.191.165	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.165	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
176.53.115.114	Turkey	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
113.59.33.61	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
113.59.33.61	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.165	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
104.167.109.15		147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
208.184.217.221	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.165	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.167.109.15		147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
208.184.217.221	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.165	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.165	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	United States	147.237.77.227	e.hamaz.idf.il	ET DROP Dshield Block Listed Source	1
43.255.191.165	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
61.183.128.6	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
60.18.162.244	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
113.59.33.61	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.186.180.230	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.165	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
104.167.109.15		147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
208.184.217.221	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.165	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

04-28-2015-23:03:05 to 04-29-2015-00:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
79.179.117.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4157
32.97.110.58	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	952
79.180.136.147	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	839
213.57.190.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	655
2.54.164.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	157
95.86.99.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	70
46.19.86.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	66
79.183.144.83	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	64
77.125.129.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	60
46.116.150.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
190.247.167.48	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
2.54.142.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
2.52.161.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
195.95.183.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
212.150.174.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
194.90.37.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
79.182.140.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
46.120.164.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
176.12.140.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
79.181.149.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
79.177.35.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
166.137.139.57	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
79.176.51.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
109.67.154.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
37.26.147.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
37.250.169.82	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
80.246.138.161	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
165.123.243.167	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
176.12.147.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
2.54.59.151	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
37.26.147.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
93.173.140.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
82.81.128.59	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	26
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
207.158.41.206	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	21
79.178.39.205	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
46.19.86.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
2.54.136.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
109.186.16.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
205.142.59.245	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
70.208.73.221	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
82.102.248.38	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
82.80.79.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
37.142.204.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.52.34.189	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.34.189	Block	77
79.177.114.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
92.253.36.81	Jordan	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	3
85.65.46.211	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
149.78.243.71	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 149.78.243.71	Block	3
149.78.243.71	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/2042	Block	3
199.119.180.110	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&amp	Block	3
91.195.154.34	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&amp	Block	3
80.3.244.107	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
80.246.138.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.59.151	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
149.78.74.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.12.151.110	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0616-2.stm	Block	1
174.102.54.158	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.228.254.148	Russian Federation	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method COOK in URL www.cogat.idf.il/901-10677-en/cogat.aspx	Block	1
213.57.37.250	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
185.32.176.62	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.143.217	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.176.182.132	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
149.78.224.177	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.64.78	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
2.52.34.189	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
199.119.180.110	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
91.195.154.34	Sweden	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.195.154.34	Block	1
178.137.19.143	Ukraine	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/hovot/templates/main.asp	Block	1
176.12.137.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.172.182.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
37.115.187.54	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
213.57.215.239	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.134.218.126	Hungary	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
186.202.153.185	Brazil	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
176.12.143.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.92	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
199.119.180.110	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.119.180.110	Block	1
91.195.154.34	Sweden	147.237.77.216	dover.idf.il	Multiple signatures from 91.195.154.34	Block	1
178.137.166.68	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
80.246.141.182	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
70.167.8.42	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/726-en/sb_item_lev2_s	Block	1
176.12.138.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.146.147	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
46.117.104.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
217.12.202.39	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
89.138.11.75	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie _pk_ref.322.9cd2: Expected ["","",1430248768,"https://web.whatsapp.com/"], Observed ["","",1430254239,"https://web.whatsapp.com/"]	None	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1012-2.stm	Block	1
176.12.146.218	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.178.147.182	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
199.119.180.110	United States	147.237.77.216	dover.idf.il	Multiple signatures from 199.119.180.110	Block	1

04-28-2015-23:03:05 to 04-29-2015-00:03:05