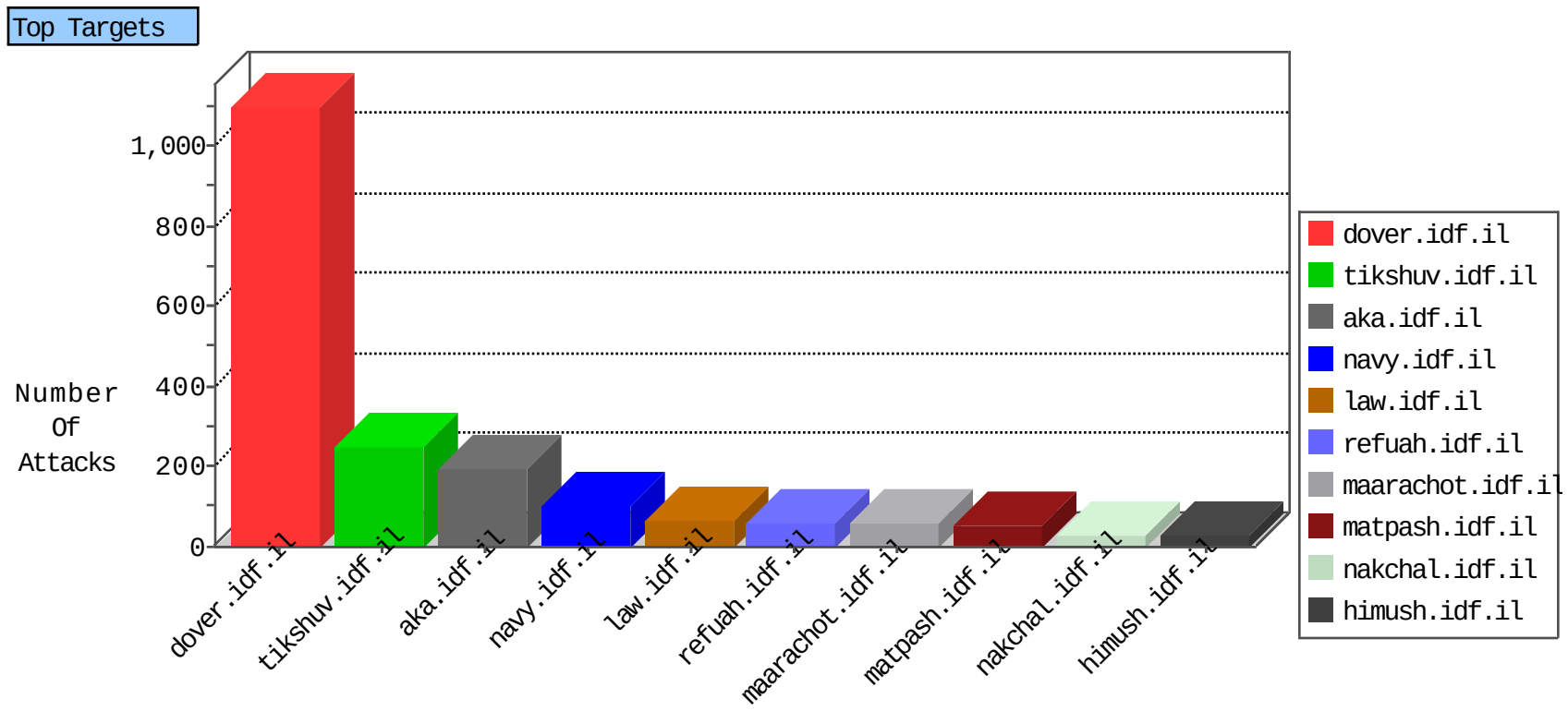
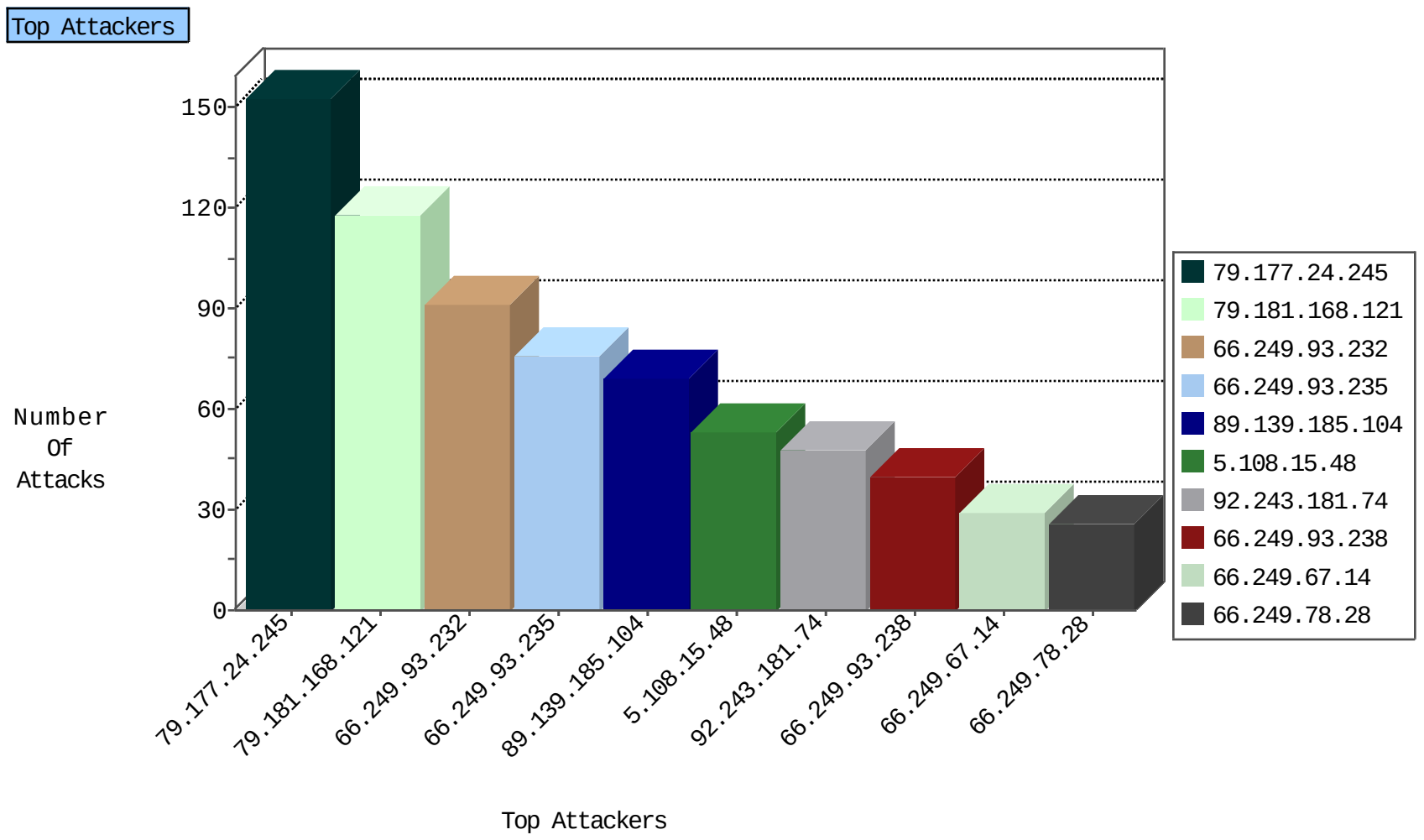
04-10-2015-11:03:03 to 04-10-2015-12:03:03

IDF Under Attack
04-10-2015-11:03:03

Top Targets



Top Attackers



04-10-2015-11:03:03 to 04-10-2015-12:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
79.181.168.121	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	587
220.181.108.116	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	126
66.249.93.232	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	91
66.249.93.235	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	76
66.249.93.238	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	40
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	29
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	26
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	25
66.249.69.109	United States	147.237.72.166	aka.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	22
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	22
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	21
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	21
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	21
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	20
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	19
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	17
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	17
66.249.93.158	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	15
66.249.69.101	United States	147.237.72.166	aka.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	15
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	14
66.249.78.15	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.65.155	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	13
66.249.69.16	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	13
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	13
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.65.147	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	10
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.69.93	United States	147.237.72.166	aka.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
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.64.59	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	7
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	7
66.249.64.55	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.64.83	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.21	United States	147.237.76.42	refuah.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	6
66.249.81.206	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.64.55	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	5
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	5
66.249.64.79	United States	147.237.76.31	nakchal.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
66.249.69.8	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	5

04-10-2015-11:03:03 to 04-10-2015-12:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.138.47.2	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
2.52.173.58	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.140	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.120.27.62	Romania	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
5.29.164.40	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
149.78.109.77	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
182.73.13.118	India	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.65.87.214	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-10-2015-11:03:03 to 04-10-2015-12:03:03

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	26
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	7
109.66.117.106	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.138.80.106	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
58.20.54.249	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.74	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.73	United States	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.56	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.56	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.56	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.56	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
81.200.91.2	Russian Federation	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
222.186.34.56	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
81.200.91.2	Russian Federation	147.237.77.235	sviva.idf.il	ET SCAN NMAP -f -sS	1
222.186.34.56	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.75	United States	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.73	United States	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.72	United States	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.56	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.56	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.56.231	Netherlands	147.237.8.14	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.34.56	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.56	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
81.200.91.2	Russian Federation	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
222.186.34.56	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.56	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

04-10-2015-11:03:03 to 04-10-2015-12:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
79.177.24.245	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	152
79.181.168.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	116
89.139.185.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	69
5.108.15.48	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
92.243.181.74	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
37.26.147.190	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
79.181.173.67	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
85.250.170.119	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
182.73.13.118	India	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.67.160.88	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
37.26.146.182	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
2.54.29.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
109.160.235.32	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
109.253.135.119	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
197.9.82.116	Tunisia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
109.253.145.231	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
116.212.202.46	Australia	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
80.246.130.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
109.66.170.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
80.229.45.203	United Kingdom	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	6
149.78.224.205	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
176.12.145.160	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.206	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
149.78.54.19	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
79.183.112.143	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
109.253.158.63	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.210.179.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
50.8.177.115	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
149.78.133.144	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
110.175.242.57	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
212.199.11.78	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
46.19.85.140	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
84.228.144.163	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
157.55.39.114	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
46.19.85.11	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
176.12.147.5	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
81.218.80.226	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
46.19.86.113	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
46.19.85.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
94.230.86.241	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	4
176.12.147.178	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
46.19.86.117	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
93.173.146.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.186.32.114	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.186.32.114	Block	16
79.183.119.242	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 79.183.119.242	Block	5
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	3
81.218.8.170	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
85.65.87.214	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	2
79.176.169.56	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
31.13.112.120	Ireland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/1081-he	Block	1
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
109.186.32.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/function (a, b) { return this.indexof(a, b) != -1	Block	1
84.110.1.161	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
64.19.78.241	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
209.126.230.75	United States	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_SERVER_HELLO)	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/barak/litani.stm	Block	1
2.54.138.149	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
89.186.184.12	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.183.119.242	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/homepage/6_s3_	Block	1
37.16.72.139	France	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.79	Block	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/6880031/english/main_index.stm	Block	1
84.228.67.14	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
216.218.206.67	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
68.180.228.167	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.4.149	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
5.29.129.125	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
109.186.32.114	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
79.183.119.242	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 79.183.119.242	Block	1
37.142.22.60	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0318-3.stm	Block	1
188.138.17.205	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
5.29.164.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
109.186.32.114	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding www.aka.idf.il/main/giyus/function () { var c = math.round(this[2] / 100 * 255); if (this[1] == 0) { return [c, c, c]; } else { var a = this[0] r 360; var e = a e 60; var g = math.round((this[2] * (100 this[1])) / 10000 * 255); var d = math.round((this[2] * (6000 - this[1] * e)) / 600000 * 255); var b = math.round((this[2] * (6000 - this[1] * (60 - e))) / 600000 * 255); switch (math.floor(a / 60)) { case 0: return b, g];	Block	1
37.142.22.60	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
209.126.230.73	United States	147.237.76.39	mobile.meitav.idf.i	Multiple Untraceable SSL Sessions from 209.126.230.73 (Protocol violation (SSL_CONN_SERVER_HELLO))	None	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/pakar5.stm	Block	1
85.250.170.119	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0102-2.stm	Block	1
5.102.254.66	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
84.108.246.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
46.121.248.255	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
209.126.230.73	United States	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_SERVER_HELLO)	None	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim.	Block	1
89.138.2.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1