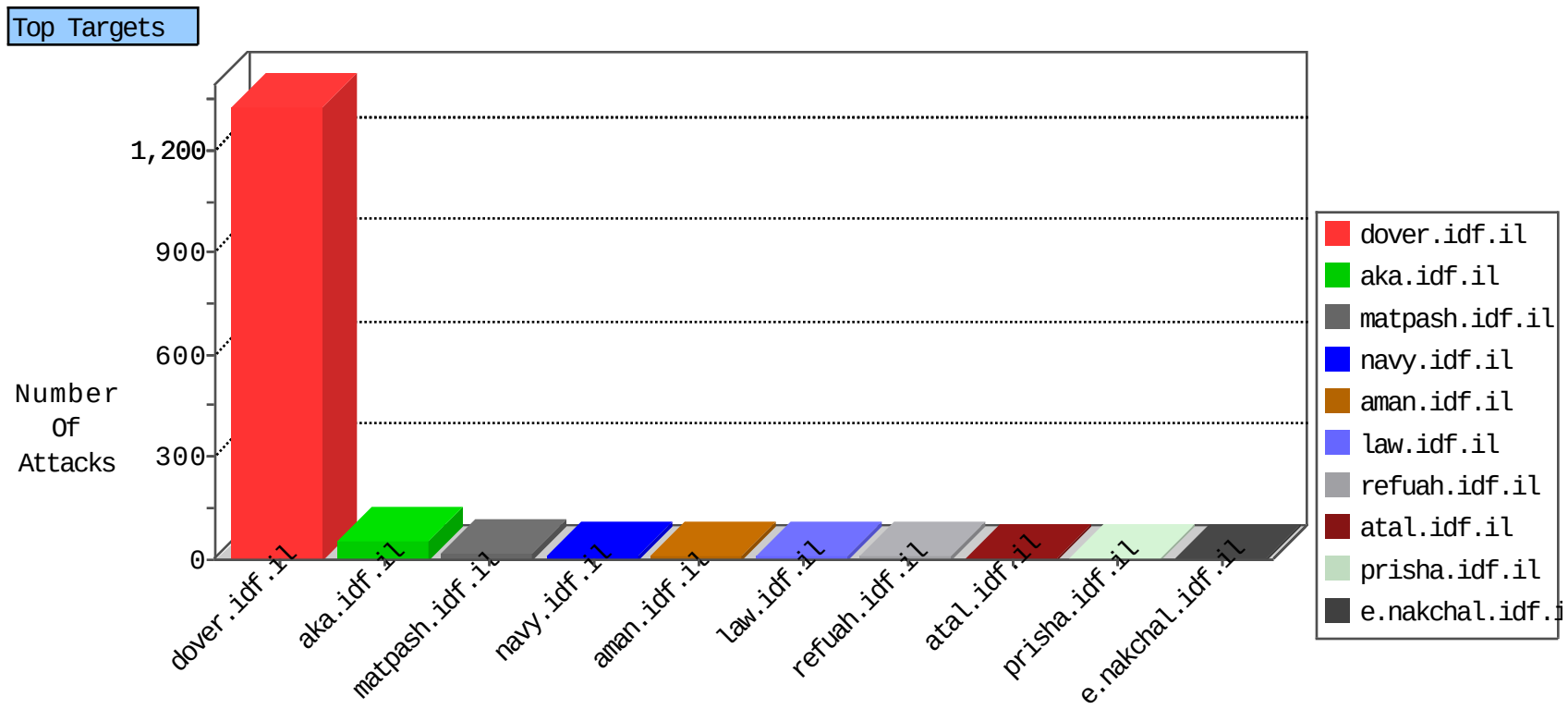
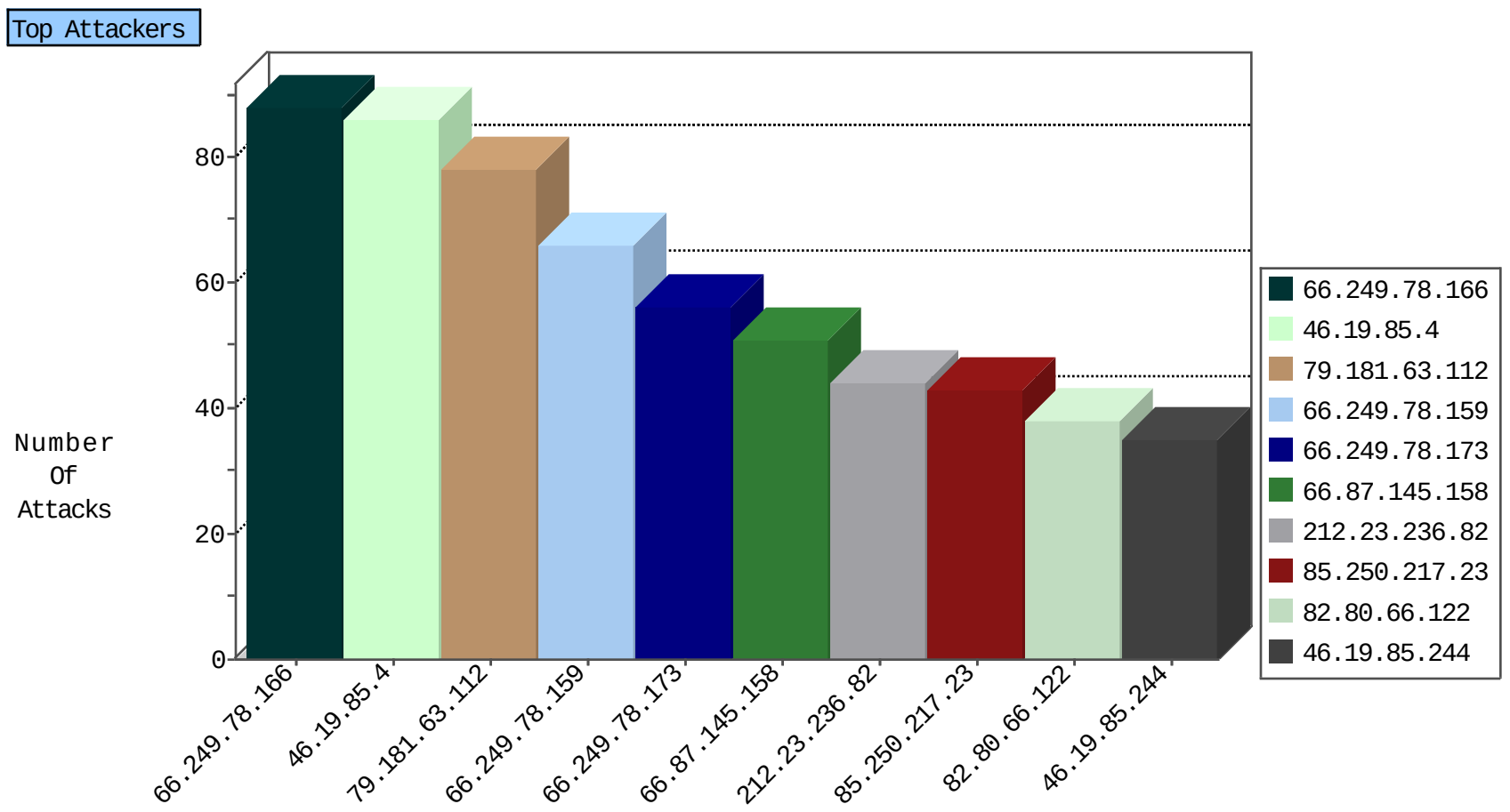
04-17-2015-08:03:02 to 04-17-2015-09:03:02

IDF Under Attack
04-17-2015-08:03:02

Top Targets



Top Attackers



04-17-2015-08:03:02 to 04-17-2015-09:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.118	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	3321
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	722
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	319
85.64.79.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
108.211.78.223	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
185.32.177.11	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
220.247.187.119	Japan	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
192.187.115.212	United States	147.237.77.205	prisha.idf.il	JLM_Purple_Con_Limit_Http	drop	1
108.211.78.223	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
209.88.157.240	Israel	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

04-17-2015-08:03:02 to 04-17-2015-09:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
190.17.51.210	Argentina	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
81.218.251.252	Israel	147.237.76.86	navy.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.216	dover.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
93.120.27.62	Romania	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1

04-17-2015-08:03:02 to 04-17-2015-09:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	6
46.43.106.159	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.147	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
221.235.188.210	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
199.68.196.126	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
31.7.57.198	Switzerland	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	Russian Federation	147.237.77.176	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
221.235.188.210	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
111.13.30.109	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
221.235.188.210	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
199.68.196.126	United States	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
199.68.196.125	United States	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
31.7.57.198	Switzerland	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	Russian Federation	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
111.13.30.109	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
221.235.188.210	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
85.250.217.23	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

04-17-2015-08:03:02 to 04-17-2015-09:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.85.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	82
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	80
79.181.63.112	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	78
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	62
66.87.145.158	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
212.23.236.82	Switzerland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
85.250.217.23	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
82.80.66.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
46.19.85.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
108.211.78.223	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
46.19.86.109	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
46.240.35.232	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
109.253.128.11	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.64.74	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
188.247.79.33	Jordan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
109.253.138.81	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
94.159.174.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
66.249.64.76	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
77.126.249.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
66.249.64.72	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
176.12.137.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
85.64.201.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
109.253.143.213	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
109.253.158.91	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
176.12.146.158	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
157.55.39.33	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
46.121.193.38	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
79.183.37.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
46.19.86.246	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
46.43.106.159	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
37.26.147.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
84.111.110.90	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
109.67.178.139	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
46.19.85.175	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
37.26.147.153	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
77.126.15.48	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
84.228.29.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
109.253.134.54	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
207.46.13.77	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
81.218.251.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
77.126.249.233	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	5
77.126.249.233	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.127.95.191	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
46.43.106.159	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
46.43.106.159	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 46.43.106.159	Block	3
149.210.150.228	Netherlands	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/noex/ist1234.htmlabc	Block	3
91.200.12.139	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
192.117.166.147	Israel	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
91.200.12.139	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	2
157.55.39.33	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.33	Block	1
77.126.41.245	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
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
46.43.106.159	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
188.165.15.78	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/november/6.stm	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/034.stm	Block	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/list.aspx	None	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info10.stm	Block	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.179	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
141.212.122.66	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
213.57.159.166	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.65.178	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
167.160.103.112		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
79.176.163.226	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/nakhal/foreword.stm	Block	1
216.218.206.68	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.67.5	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.5	Block	1
174.129.237.157	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.64.201.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/feburary/10.stm	Block	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.77	Block	1
46.43.106.159	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.125.245.31	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl59 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.67.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1236-he/atal.aspx	Block	1
2.54.19.50	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
188.165.15.43	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9180-he/refuah.aspx	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
52.4.217.78	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/homas/scriptresource.axd	None	1

04-17-2015-08:03:02 to 04-17-2015-09:03:02