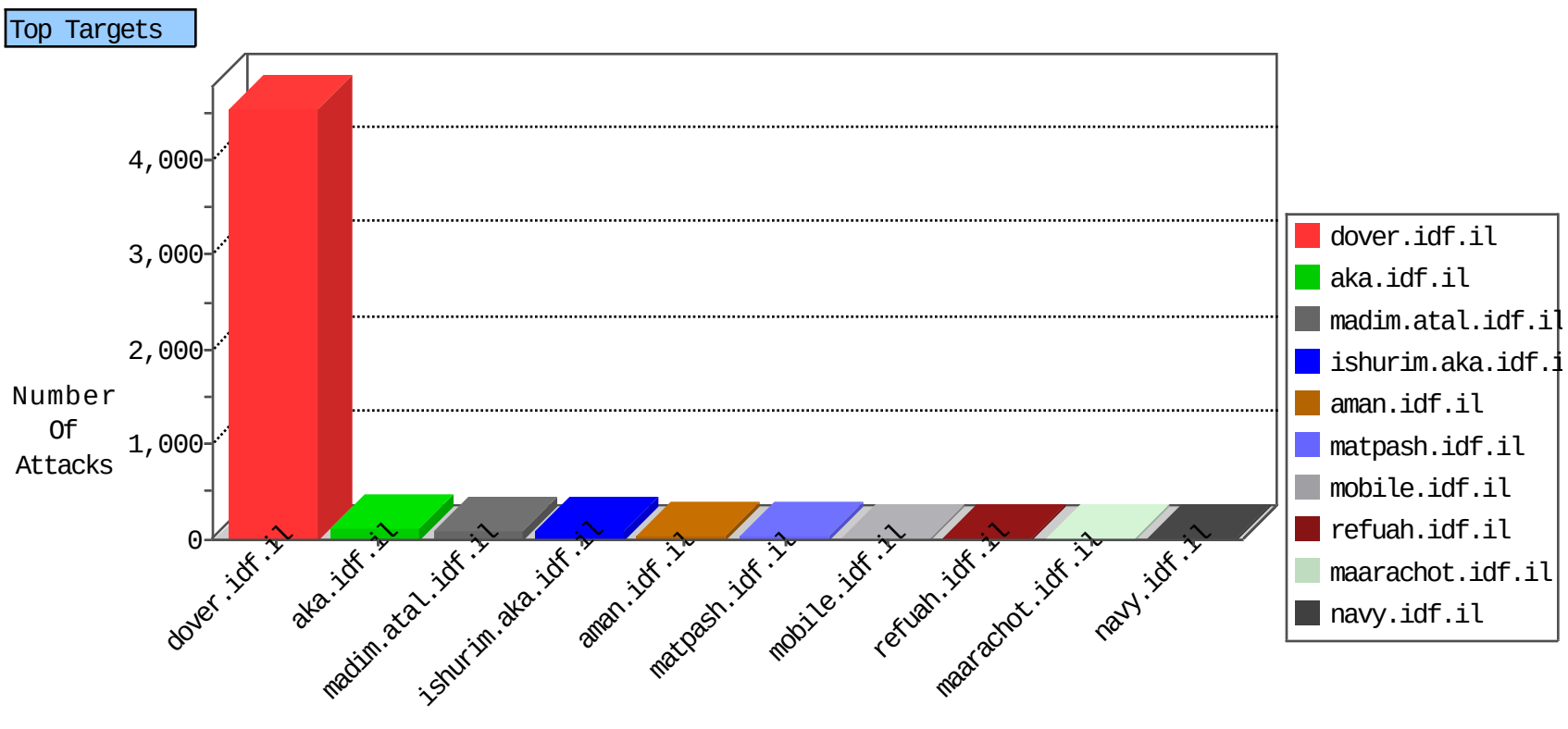
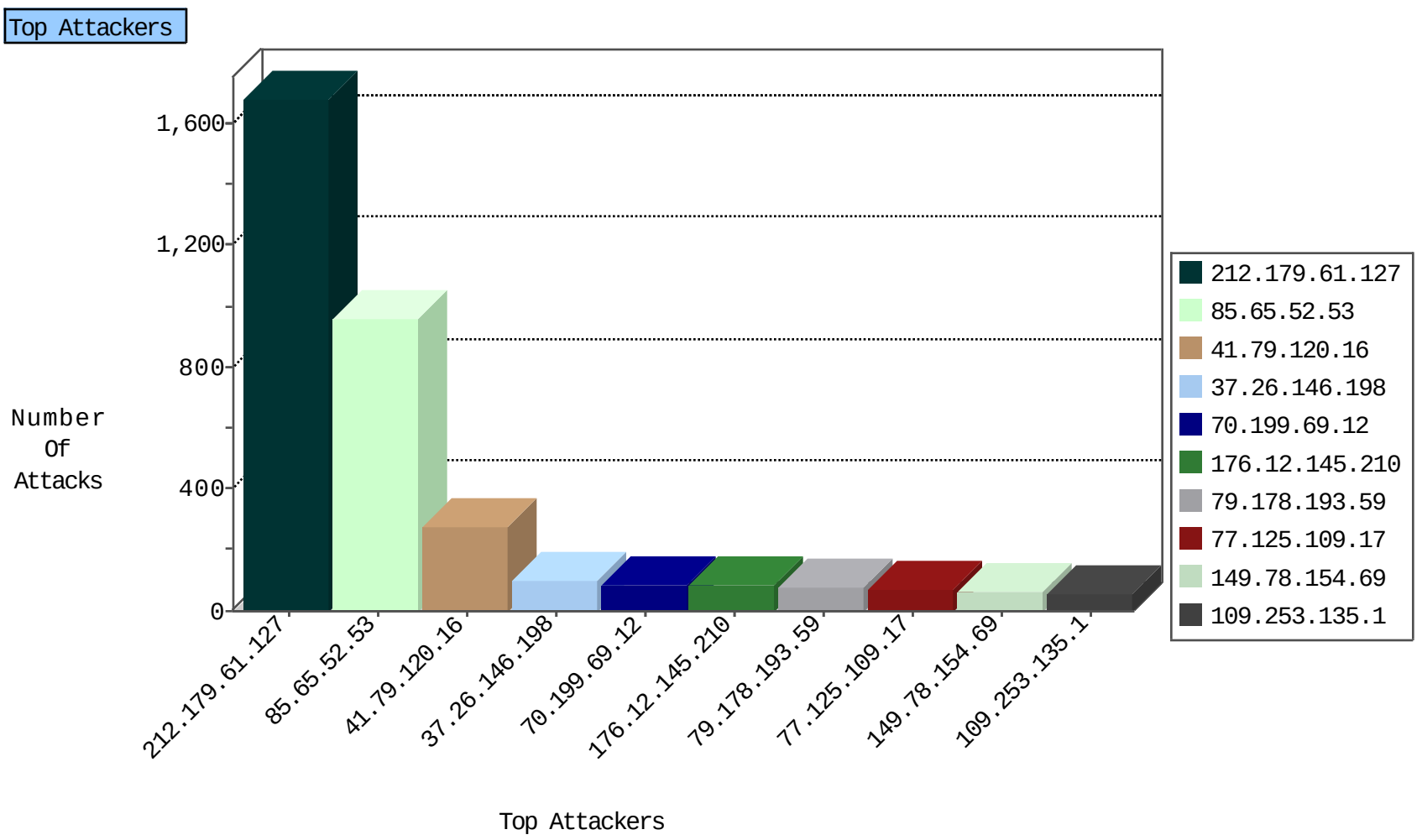
05-08-2015-10:03:08 to 05-08-2015-11:03:08

IDF Under Attack
05-08-2015-10:03:08

Top Targets



Top Attackers



05-08-2015-10:03:08 to 05-08-2015-11:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.152	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	633
77.125.109.17	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	586
213.57.248.78	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195
66.249.67.126	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	179
84.109.165.19	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	7
77.127.173.230	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
109.186.27.105	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
212.150.174.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
93.172.27.130	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.64.106.206	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
111.202.66.66	China	147.237.77.74	law.idf.il	L4 Source or Dest Port Zero	drop	1

05-08-2015-10:03:08 to 05-08-2015-11:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
106.185.44.134	Japan	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	5
5.29.119.201	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	2
222.185.140.2	China	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
66.240.192.138	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
113.191.249.253	Vietnam	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.199	e.nakchal.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
31.7.57.198	Switzerland	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.21	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
5.29.112.24	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	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
109.64.100.183	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.72.167	ishurim.aka.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

05-08-2015-10:03:08 to 05-08-2015-11:03:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
109.186.27.105	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.93.243	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.242	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
80.82.78.27	Netherlands	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.27	Netherlands	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.167.194	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.240.144.67	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
121.88.5.177	Korea, Republic of	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.135.1	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
58.97.2.66	Thailand	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.130		147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
93.158.215.110	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
212.18.232.63	United Kingdom	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
92.47.29.12	Kazakstan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
200.83.155.37	Chile	147.237.8.27	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.82.78.27	Netherlands	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.51	Germany	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
67.159.16.2	United States	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
144.0.0.60	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
121.88.5.177	Korea, Republic of	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
121.88.5.177	Korea, Republic of	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
60.169.78.79	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
37.26.148.220	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
93.158.215.110	Netherlands	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
212.18.232.63	United Kingdom	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
93.158.215.110	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
212.18.232.63	United Kingdom	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1

05-08-2015-10:03:08 to 05-08-2015-11:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1682
85.65.52.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	958
41.79.120.16	N/A	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	278
37.26.146.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	102
70.199.69.12	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	82
79.178.193.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	78
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
109.253.135.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
46.19.86.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
93.172.139.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
212.179.46.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
192.241.245.200	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
62.219.118.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
82.80.17.163	Israel	147.237.72.156	aman.idf.il	SAM rule	drop	drop	26
77.127.217.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
94.159.183.141	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
109.160.253.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
80.246.137.63	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
5.29.110.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
109.203.125.100	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
5.29.24.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
178.234.243.44	Russian Federation	147.237.77.176	matpash.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	13
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
79.182.188.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
82.166.146.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
69.114.227.252	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
79.178.26.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
5.28.172.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
46.120.129.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
84.228.129.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
80.246.133.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
62.219.110.173	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
179.178.174.77	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
79.182.100.49	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.116.123.65	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
79.182.207.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
46.121.62.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.64.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
79.178.141.86	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.145.210	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.145.210	Block	82
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	5
93.172.27.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
114.215.133.202	China	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	5
31.44.136.66	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
2.54.175.6	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
213.57.28.139	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
5.248.238.78	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	3
106.185.44.134	Japan	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/ftb.imagegallery.aspx	Block	2
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.67.171.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.228.50.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	2
79.183.233.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
37.26.147.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
66.249.67.75	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1111-he/nakhal.aspx	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sachar/forms/downloadform.asp	Block	1
80.246.137.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.121.108.84	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
176.194.5.74	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/	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
66.249.67.218	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.119.201	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/reserve	Block	1
46.121.108.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
178.54.242.223	Ukraine	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
2.52.177.179	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.171.74	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/history/iaffirst.stm	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.139	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-he/×¦×”	Block	1
93.172.20.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
52.6.169.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/alnajah/alnajah.stm	Block	1
178.234.243.44	Russian Federation	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 178.234.243.44	Block	1
113.191.249.253	Vietnam	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
2.54.17.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
74.82.47.2	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
176.12.138.148	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
2.54.174.61	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1

05-08-2015-10:03:08 to 05-08-2015-11:03:08