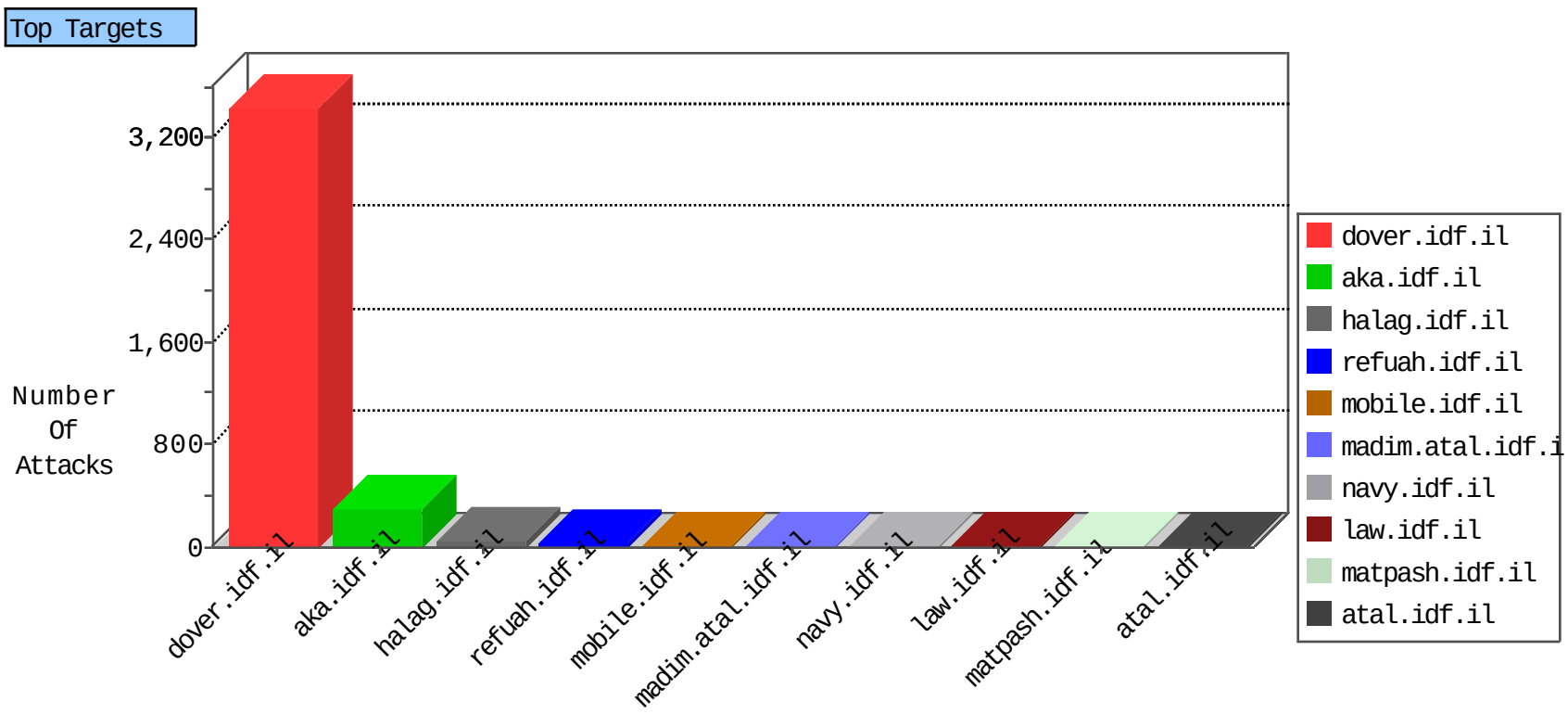
04-18-2015-13:03:08 to 04-18-2015-14:03:08

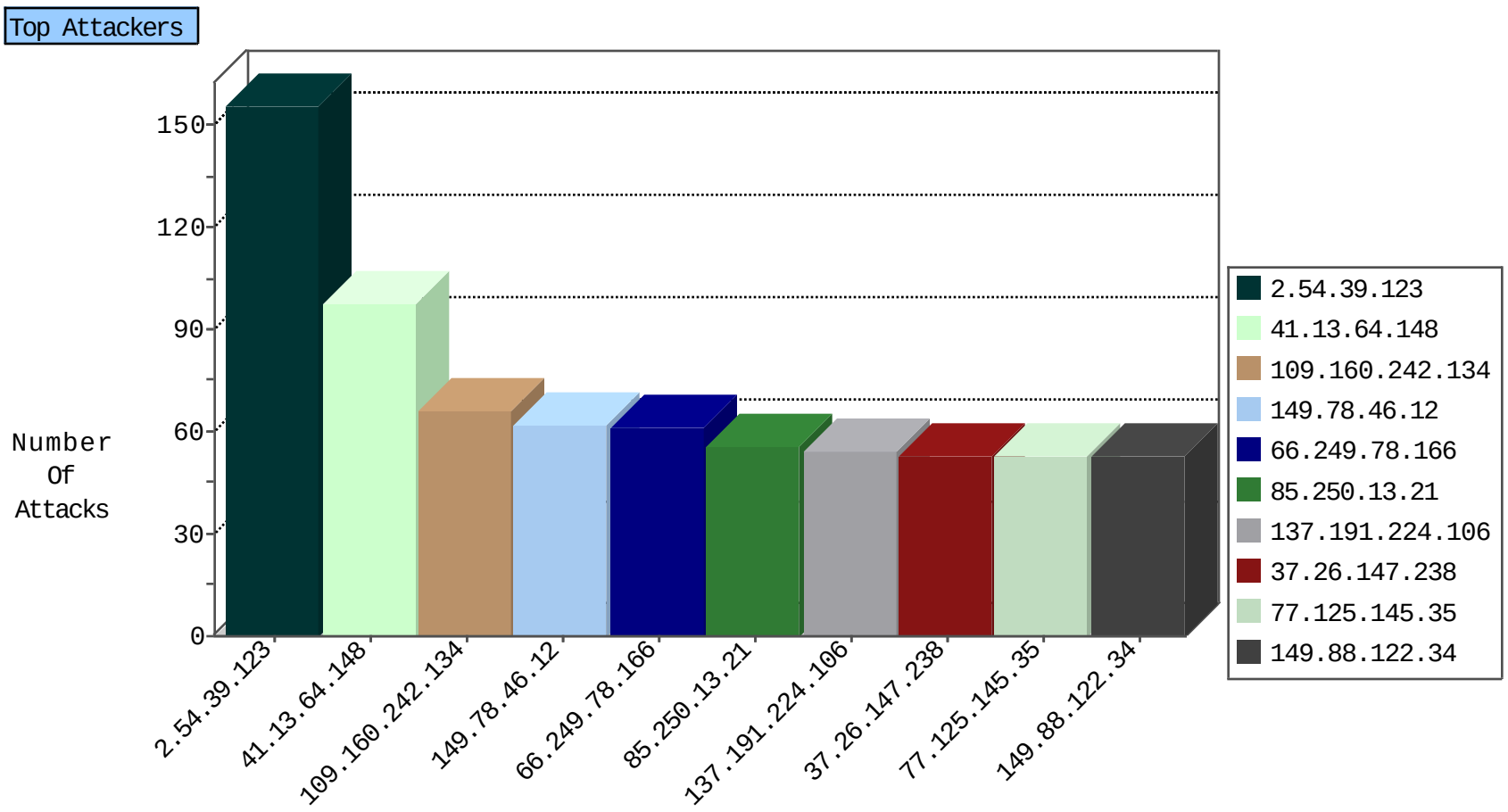
IDF Under Attack
04-18-2015-13:03:08

Top Targets



Top Target

Top Attackers



Top Attackers

04-18-2015-13:03:08 to 04-18-2015-14:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.224	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
203.147.10.65	Thailand	147.237.76.197	e.himush.idf.il	L4 Source or Dest Port Zero	drop	3
109.67.179.148	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
124.122.22.22	Thailand	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
82.12.112.233	United Kingdom	147.237.77.216	dover.idf.il	ID-OpenSSL-Heartbeat-ex1	dest-reset	1

04-18-2015-13:03:08 to 04-18-2015-14:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.181.198.139	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.117.251.140	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.250.52.95	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.250.140.186	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.139.189.81	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
194.117.2.100	Portugal	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
188.138.9.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
79.177.168.156	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
84.229.177.71	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.28	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.177	ncore.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
198.20.69.98	United States	147.237.77.212	e.dover.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
46.19.86.179	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1

04-18-2015-13:03:08 to 04-18-2015-14:03:08

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
66.249.78.204	United States	147.237.77.176	matpash.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
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
104.167.117.197		147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
122.228.207.76	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
101.71.71.167	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
122.228.207.76	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
101.71.71.167	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
122.228.207.76	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
92.50.82.18	Germany	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
218.77.79.43	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.200	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
122.228.207.76	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.200	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
111.69.193.38	New Zealand	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
104.167.117.197		147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
101.71.71.167	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
122.228.207.76	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
92.50.82.18	Germany	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
218.77.79.43	China	147.237.77.74	law.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
122.228.207.76	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
205.209.123.22	United States	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.228.207.76	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.200	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
66.249.64.12	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
122.228.207.76	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
115.238.240.59	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1

04-18-2015-13:03:08 to 04-18-2015-14:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.39.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	156
41.13.64.148	South Africa	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	98
109.160.242.134	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	66
85.250.13.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
137.191.224.106	Ireland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
149.88.122.34	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
37.26.147.238	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
77.125.145.35	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
84.108.145.199	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
46.120.112.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
85.65.59.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
77.127.150.196	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
31.51.200.8	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
80.179.118.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
83.130.125.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
109.186.42.5	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
212.71.237.205	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
80.230.124.193	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
176.12.137.47	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
46.19.85.40	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
149.78.46.12	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
190.114.248.77	Peru	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
109.253.131.167	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
46.19.85.5	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
31.168.78.49	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
79.177.124.160	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
109.253.128.157	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
5.41.43.170	Romania	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
2.54.12.78	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
213.57.88.193	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
176.12.151.117	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
212.199.218.50	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
46.19.85.128	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
149.78.46.12	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
109.65.99.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
176.228.215.187	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
46.120.90.143	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
109.64.6.164	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
66.249.93.164	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
176.12.148.115	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
212.41.73.140	Switzerland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
66.249.78.51	United States	147.237.77.234	halag.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
41.13.78.17	South Africa	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.141.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
176.12.149.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
5.28.169.235	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 5.28.169.235	Block	5
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
176.12.149.79	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
89.106.244.18	Belgium	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
79.176.163.177	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/108502.pdf/	Block	2
151.236.44.13	United Kingdom	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
80.87.240.42	Bosnia and Herzegovina	147.237.72.166	aka.idf.il	Distributed PHP Attempt	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
188.93.78.243	Spain	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
37.140.192.97	Russian Federation	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
66.249.64.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
31.168.79.114	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
151.236.44.13	United Kingdom	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
80.87.240.42	Bosnia and Herzegovina	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
194.117.2.100	Portugal	147.237.76.42	refuah.idf.il	Admin Blocking	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam.	Block	1
46.117.194.172	Israel	147.237.76.30	himush.idf.il	Suspicious Response Code	Block	1
5.200.7.28	Netherlands	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
37.140.192.97	Russian Federation	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
194.117.2.100	Portugal	147.237.76.42	refuah.idf.il	PHP Attempt	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
176.12.136.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
46.210.126.134	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
93.172.44.150	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
79.177.168.156	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.67.33	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/kkkkkkk=3f79fe5ekkkkkkk_3f79fe5e	Block	1
157.55.39.4	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.140.192.97	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
84.108.181.233	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
207.46.13.35	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/panmaz/havai2.stm	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/statistics/chief of staff.stm	Block	1
176.12.136.65	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.12	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
95.173.171.236	Turkey	147.237.77.226	www.chamatz.aka.idf.il	Illegal HTTP Version	Block	1
79.180.206.253	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/5/4525/pdf	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1361-10624-he/dover.aspx	Block	1
188.93.78.243	Spain	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.140.192.97	Russian Federation	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	1
84.109.107.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
5.28.169.235	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1294-he/â€?â€ ?internet explorer	Block	1
207.46.13.51	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/memorial/pages/nisimtraves.aspx	Block	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter newsItem in www.aka.idf.il/megurim/news/	None	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1119-1.stm	Block	1