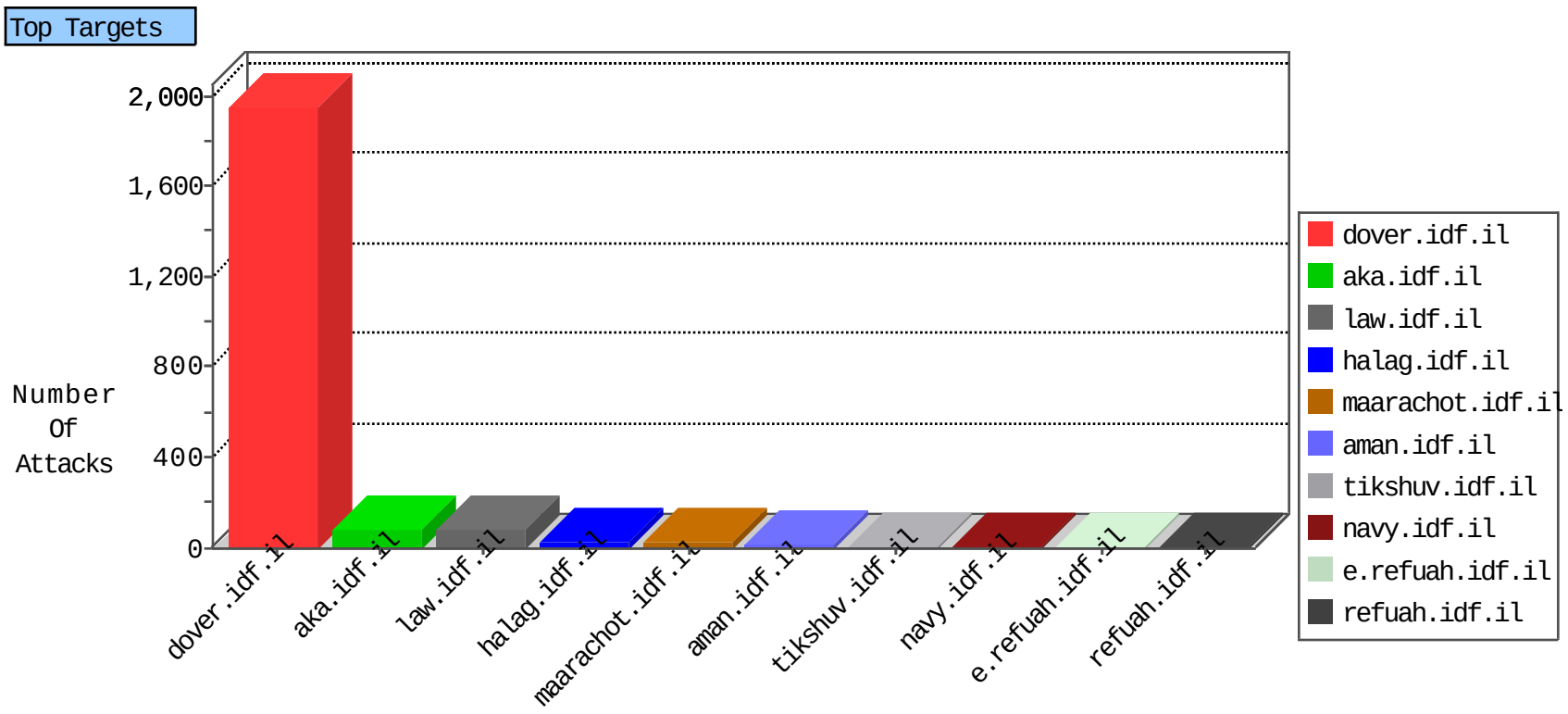
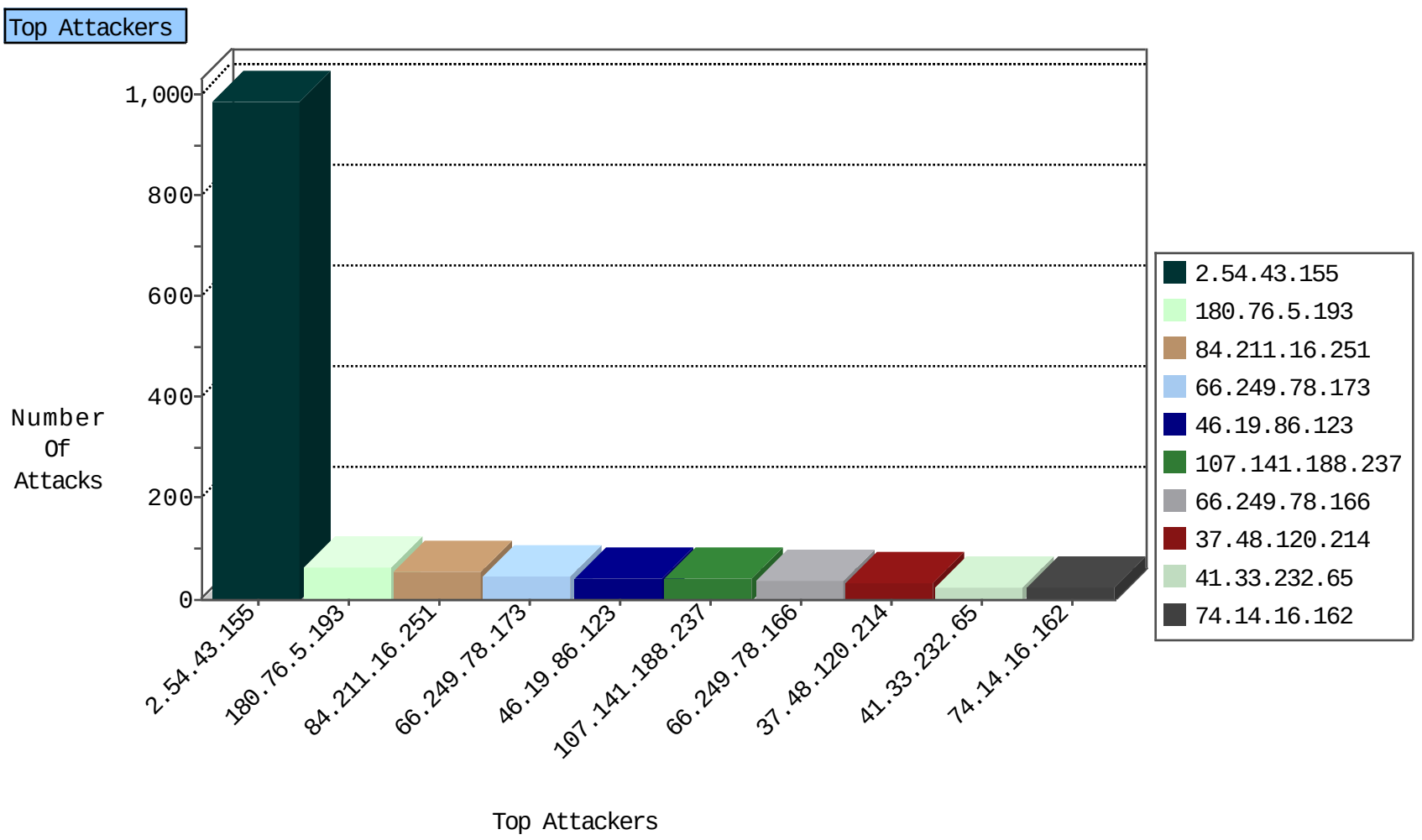
04-30-2015-01:03:07 to 04-30-2015-02:03:07

IDF Under Attack
04-30-2015-01:03:07

Top Targets



Top Attackers



04-30-2015-01:03:07 to 04-30-2015-02:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.84	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2568
66.249.67.92	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	957
220.181.108.181	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	171
93.173.2.75	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
220.181.108.84	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	29
84.109.100.201	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
189.125.130.2	Brazil	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
58.176.206.178	Hong Kong	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
41.21.200.142	South Africa	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
104.192.0.20		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
41.21.200.142	South Africa	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
195.37.190.86	Germany	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
41.21.200.142	South Africa	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
151.236.58.222	United Kingdom	147.237.76.200	eitan.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	1
195.37.190.86	Germany	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
41.21.200.142	South Africa	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
151.236.58.222	United Kingdom	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Http	drop	1

04-30-2015-01:03:07 to 04-30-2015-02:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	63
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	4
188.138.9.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
203.77.161.228	Australia	147.237.77.234	halag.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
66.240.236.119	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
5.22.130.153	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	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
46.117.7.236	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.25.103.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.35	akaws.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
66.240.192.138	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	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1

04-30-2015-01:03:07 to 04-30-2015-02:03:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.67.108	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
109.67.29.227	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.119.217	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.222.104	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.229.33.168	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
63.141.250.99	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
46.162.115.130	Sweden	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
46.162.115.130	Sweden	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
96.56.250.243	United States	147.237.77.233	atal.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
91.224.132.118	Russian Federation	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	Turkey	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.253.29.62	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
61.183.128.6	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
46.162.115.130	Sweden	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.72.166	aka.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
96.56.250.243	United States	147.237.77.233	atal.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Cookie	1
91.224.132.118	Russian Federation	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
80.253.29.62	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1

04-30-2015-01:03:07 to 04-30-2015-02:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.43.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	966
84.211.16.251	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
46.19.86.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
107.141.188.237	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
74.14.16.162	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
217.87.116.120	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
95.35.50.140	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.160.188.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
184.155.2.219	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
46.19.85.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
109.65.222.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
77.125.15.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
82.166.20.17	Israel	147.237.77.170	maarachot.idf.il	Invalid sequence number	Bad TCP sequence	monitor	12
80.246.130.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
41.33.231.86	Egypt	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	11
81.218.66.107	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
189.125.130.2	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
176.12.138.89	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
98.14.138.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.176	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
77.127.253.66	Israel	147.237.77.170	maarachot.idf.il	Invalid sequence number	Bad TCP sequence	monitor	9
66.249.64.76	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	9
195.10.194.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.10	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
46.116.251.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
2.54.43.155	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	8
2.54.43.155	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
46.19.85.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
207.46.13.92	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
2.54.43.155	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	8
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
94.230.86.172	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
70.133.153.193	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
109.65.52.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.137	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
99.244.200.254	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.142.234.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	10
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	10
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	9
2.54.24.43	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
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
91.200.12.127	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.177.112.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.79.74	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
188.120.152.94	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.64.91	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
115.25.81.70	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//aman	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
199.30.24.47	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	1
66.249.67.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
84.228.231.236	Bulgaria	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.241	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.79.135	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
188.120.152.94	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1
66.249.67.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/webresource.axd	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar	Block	1
207.46.13.108	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
176.12.138.89	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/983-he/atal.aspx	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.79.157	Israel	147.237.72.166	aka.idf.il	Unknown Parameter sOpenLinkIn in www.aka.idf.il/eitan/pratim/pirteychayal/	None	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//templates/sendtofriend/sendtofriend.aspx	Block	1
188.165.15.95	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9712-he/refuah.aspx	Block	1
66.249.67.62	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/869-4426-he/patzar.aspx	Block	1
157.55.39.72	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//	Block	1
76.64.3.161	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
66.249.79.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20439-he/kkkkkkk=b218ad86kkkkkkk_b218ad86	Block	1
66.249.78.13	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
95.35.50.140	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17474-en/dover.aspxhttp:/	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
188.165.15.195	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0108-5.stm	Block	1
66.249.67.70	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/14-en/patzar.aspx	Block	1
79.176.201.53	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
37.239.140.110	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qar/	Block	1
66.249.79.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/chinuch/news/default.asp	Block	1
180.76.6.231	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/geut/english/	Block	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1