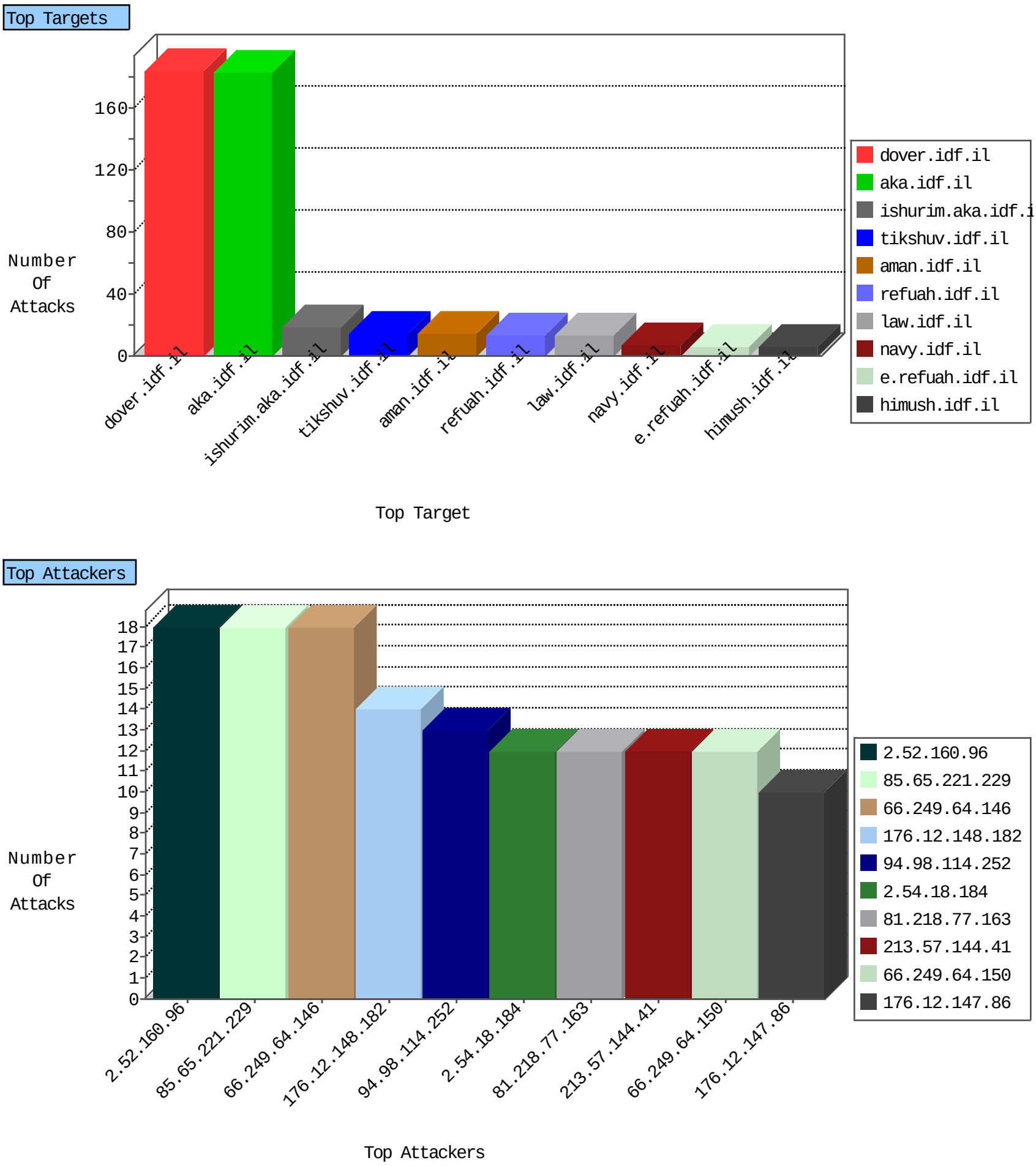
04-01-2015-13:03:04 to 04-01-2015-14:03:04

IDF Under Attack
04-01-2015-13:03:04



04-01-2015-13:03:04 to 04-01-2015-14:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
85.65.221.229	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
213.57.144.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
89.248.172.57	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
60.241.188.182	Australia	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
107.154.64.10	United States	147.237.0.15	kosher-kravi.idf.il	L4 Source or Dest Port Zero	drop	1
81.218.77.162	Israel	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
31.168.152.92	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
46.28.204.46	Switzerland	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

04-01-2015-13:03:04 to 04-01-2015-14:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.176.111.102	Israel	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	5
68.115.73.95	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.65.200.194	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.25.103.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	2
212.179.46.19	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.181.26.64	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
81.17.27.234	Switzerland	147.237.72.166	aka.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
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.44	e.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
84.109.163.109	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
84.109.163.109	Israel	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	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.200	eitan.aka.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
66.240.192.138	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1

04-01-2015-13:03:04 to 04-01-2015-14:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
80.246.141.35	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	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	2
109.66.53.110	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.108.239	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.25.208	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
107.167.181.107	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.74.58	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.122.195	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.162.228	Netherlands	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.89	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.229.148.189	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.50.165	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.77.162	Israel	147.237.77.74	law.idf.il	GPL SCAN nmap TCP	1
128.61.240.66	United States	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.142.228	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.11.31	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.98.237	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
107.167.181.107	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.67	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
95.129.1.131	Lebanon	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.50.166	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.226	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.172.160	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
84.108.56.70	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.36.80	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.77.163	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
162.232.20.147	United States	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 3072	1

04-01-2015-13:03:04 to 04-01-2015-14:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.64.146	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.148.182	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
94.98.114.252	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.147.86	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
89.138.12.19	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	10
109.253.145.240	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
216.223.27.58	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	9
15.195.185.76	Europe	147.237.0.34	tikshuv.idf.i	First packet isn't SYN	drop	drop	8
2.52.160.96	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
176.12.149.83	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
2.52.160.96	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
81.218.77.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
176.12.141.196	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
2.52.160.96	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
46.19.86.90	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
176.12.146.244	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.75.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
81.218.77.163	Israel	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	5
17.142.152.110	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
2.54.18.184	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
2.54.185.32	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
2.54.18.184	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	4
80.246.137.145	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
2.54.18.184	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
46.19.86.46	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
2.54.185.32	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
46.19.85.72	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
80.178.138.115	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.85.2	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
46.19.85.57	Israel	147.237.72.166	aka.idf.il	illegal header format detected: Malformed HTTP protocol name in response	Block HTTP Non Compliant	monitor	3
46.19.85.2	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.86.90	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
2.52.130.7	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
46.19.85.175	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
109.111.112.111	Andorra	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.12.140.22	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
95.129.1.162	Lebanon	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
213.57.141.166	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
89.187.220.4	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.49	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
176.12.140.22	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.79	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
95.129.1.162	Lebanon	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
2.52.130.7	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
2.52.130.7	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
5.29.135.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
66.249.64.142	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.142	Block	3
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	3
37.60.47.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
89.138.243.231	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×'×™×• ×¡main/home/default.aspx	Block	2
192.116.48.28	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.60.47.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
212.199.57.203	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/2042	Block	2
176.12.149.13	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
89.139.58.171	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
84.109.120.149	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
79.183.50.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.86.86.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
188.116.35.36	Poland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	2
80.246.137.145	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	1
176.12.142.29	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
54.87.107.232	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
80.178.212.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
77.127.110.67	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/f	Block	1
109.253.135.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.106	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
81.218.70.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.178.11.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
77.125.79.167	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
54.147.176.220	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/589-he/patzar.aspx=	Block	1
80.179.118.129	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.241.237.223	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
77.237.138.51	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
66.249.69.10	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.253.141.183	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/popups/markivsachar.aspx	None	1
79.183.27.90	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
216.185.39.24	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/home.aspx	None	1
77.125.79.167	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/default.aspx	None	1
180.76.4.73	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
94.23.30.222	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
80.179.209.105	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/terms.aspx	None	1
212.29.211.62	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/homas/site/homasformphase4.aspx	None	1
77.237.138.51	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
66.249.69.122	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.253.144.107	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.23	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
85.250.0.85	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
184.105.139.68	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
77.125.79.167	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
66.249.67.65	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
80.246.133.83	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
212.29.211.62	Israel	147.237.72.166	aka.idf.il	Unknown Parameter count in www.aka.idf.il/homas/site/resources/services/wsmaterials.asmx/getmaterialpossiblenamesbynamestart	None	1
79.140.3.154	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/navy/submarin.stm	Block	1