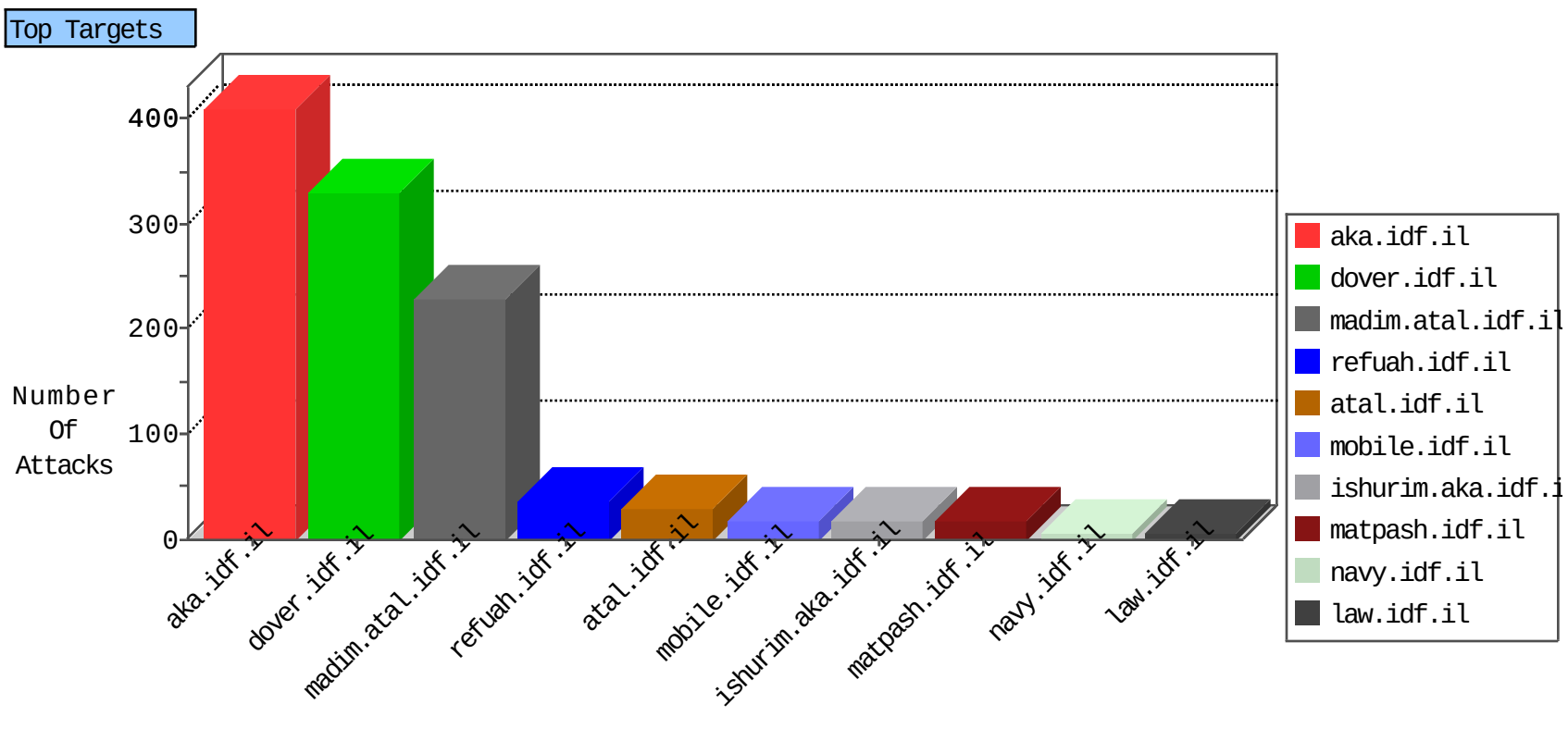
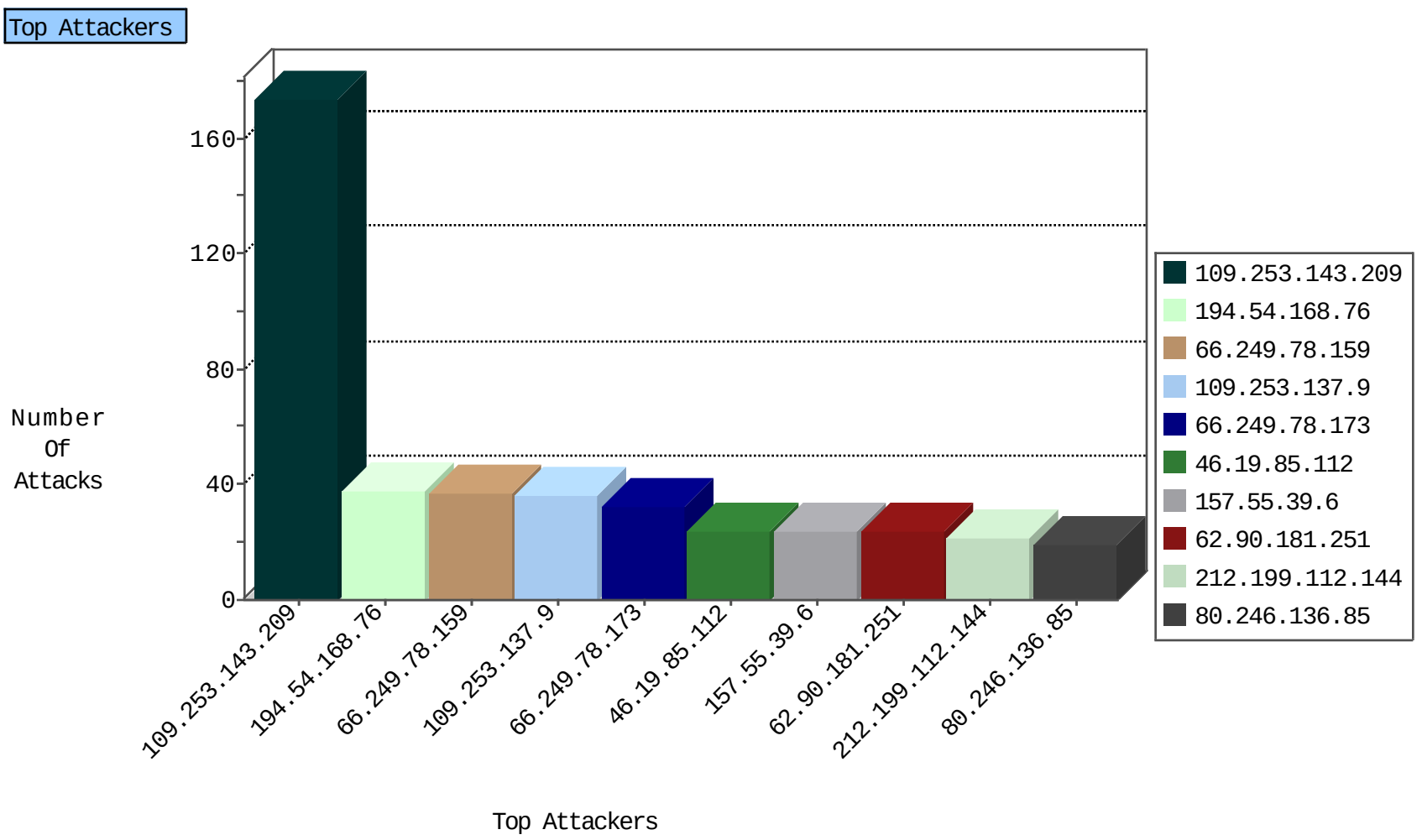
03-29-2015-15:03:07 to 03-29-2015-16:03:07

IDF Under Attack
03-29-2015-15:03:07

Top Targets



Top Attackers



03-29-2015-15:03:07 to 03-29-2015-16:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
194.54.168.76	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	356
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	151
95.86.123.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
66.249.78.159	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	8
82.196.10.104	Netherlands	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	7
52.16.5.197	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	6
46.244.75.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	6
144.76.43.70	Germany	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
41.79.120.29	N/A	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
64.228.143.96	Canada	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
82.220.1.199	Switzerland	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	4
185.7.123.176	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	4
207.46.13.16	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
188.161.150.6	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	4
157.55.39.137	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	4
157.55.39.67	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	3
188.161.150.6	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
194.165.146.149	Jordan	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
188.165.15.148	France	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	3
157.55.39.6	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
24.90.136.188	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
157.55.39.42	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
92.17.166.79	United Kingdom	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
82.145.223.2	Europe	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
66.249.78.160	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	2
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	2
31.186.228.25	United Kingdom	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	2
82.205.51.150	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	2
173.192.238.44	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
63.249.66.212	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
37.140.141.37	Russian Federation	147.237.77.74	law.idf.il	unblock-sp-traf1	forward	1
108.59.253.71	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
87.139.65.203	Germany	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
81.164.228.23	Belgium	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	1
157.55.39.137	United States	147.237.72.167	ishurim.aka.idf.il	unblock-sp-traf1	forward	1
31.186.228.59	United Kingdom	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
82.205.51.150	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
182.169.230.49	Japan	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.204	United States	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	1
157.55.39.67	United States	147.237.77.226	www.chamatz.aka.idf.il	unblock-sp-traf1	forward	1
115.64.99.243	Australia	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
91.21.182.138	Germany	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
157.55.235.59	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
54.72.0.55	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1

03-29-2015-15:03:07 to 03-29-2015-16:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
93.109.158.28	Cyprus	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

03-29-2015-15:03:07 to 03-29-2015-16:03:07

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	3
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
109.253.157.145	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.91.1	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.61.216	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.72.56	United States	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
77.126.29.156	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.72.56	United States	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.72.56	United States	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
31.154.8.68	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
193.107.16.206	Russian Federation	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.86.116	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
116.121.137.5	Korea, Republic of	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
116.121.137.5	Korea, Republic of	147.237.76.42	refuah.idf.il	ET SCAN NMAP -f -sS	1
222.186.42.11	China	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
88.249.106.23	Turkey	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
213.8.46.1	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.72.56	United States	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.67	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.72.56	United States	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
41.79.120.29	N/A	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
27.50.132.61	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.16.206	Russian Federation	147.237.76.199	e.nakchal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
118.69.174.89	Vietnam	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
116.121.137.5	Korea, Republic of	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

03-29-2015-15:03:07 to 03-29-2015-16:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
62.90.181.251	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	23
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
109.253.137.41	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
188.139.224.44	Syrian Arab Republic	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	18
31.186.228.92	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	14
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
31.186.228.64	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	12
176.12.139.41	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
216.223.27.25	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	8
31.186.228.61	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	7
80.246.136.85	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
46.19.85.7	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	6
176.12.146.114	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.186.228.24	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.91	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.112	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	alert	6
109.253.128.121	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
81.218.77.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
80.246.136.85	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
31.186.228.170	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.112	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	6
31.186.228.67	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
31.186.228.94	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
80.246.136.85	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
31.186.228.90	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.95	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	5
85.64.87.240	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
46.19.86.230	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
46.19.85.44	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	5
31.210.186.129	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
31.186.228.68	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	5
31.186.228.28	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
194.90.239.2	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
80.246.136.223	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
31.186.228.58	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
109.253.157.91	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
31.186.228.29	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.7	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
31.186.228.96	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.87	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
109.253.158.228	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
31.186.228.88	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
80.246.138.21	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
109.253.129.198	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
31.186.228.31	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
80.246.138.21	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.143.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	171
109.253.137.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	36
109.253.136.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
109.253.135.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	4
66.249.78.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/search.asp	Block	4
46.117.29.80	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	4
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	4
164.138.122.11	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
109.253.143.209	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/mobile/shared/ajax/updatemakatqauntity.aspx	Block	3
217.132.94.246	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
207.46.13.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.16	Block	3
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	3
109.253.129.54	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.142.252.53	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
79.177.149.198	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	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
157.55.39.2	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il//captcha.ashx	Block	2
85.69.29.243	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.186.153.203	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.131.134	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
87.68.247.101	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1564	Block	2
80.246.136.223	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
63.217.168.125	United States	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTARGUMENT in aka.idf.il/main/sachar/	None	1
176.12.140.110	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.132.220	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
37.46.39.209	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
149.88.58.73	United States	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTTARGET in www.aka.idf.il/main/sachar/	None	1
84.228.193.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
79.176.151.69	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.57.34.49	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
66.249.78.159	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1105-2.stm	Block	1
194.54.168.76	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
91.135.102.191	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.60.42.57	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin/view/javascript/fckeditor/editor/filemanager/connectors	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/122403-2.stm	Block	1
115.25.81.71	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
81.218.182.85	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
2.54.60.229	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/armored1.stm	Block	1
212.76.111.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
63.217.168.125	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/payslips.aspx	None	1
185.32.178.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.132.220	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
155.254.245.94		147.237.77.74	law.idf.il	PHP Attempt	Block	1
85.65.177.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
109.253.156.171	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.129.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.56.3	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.96.159	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1