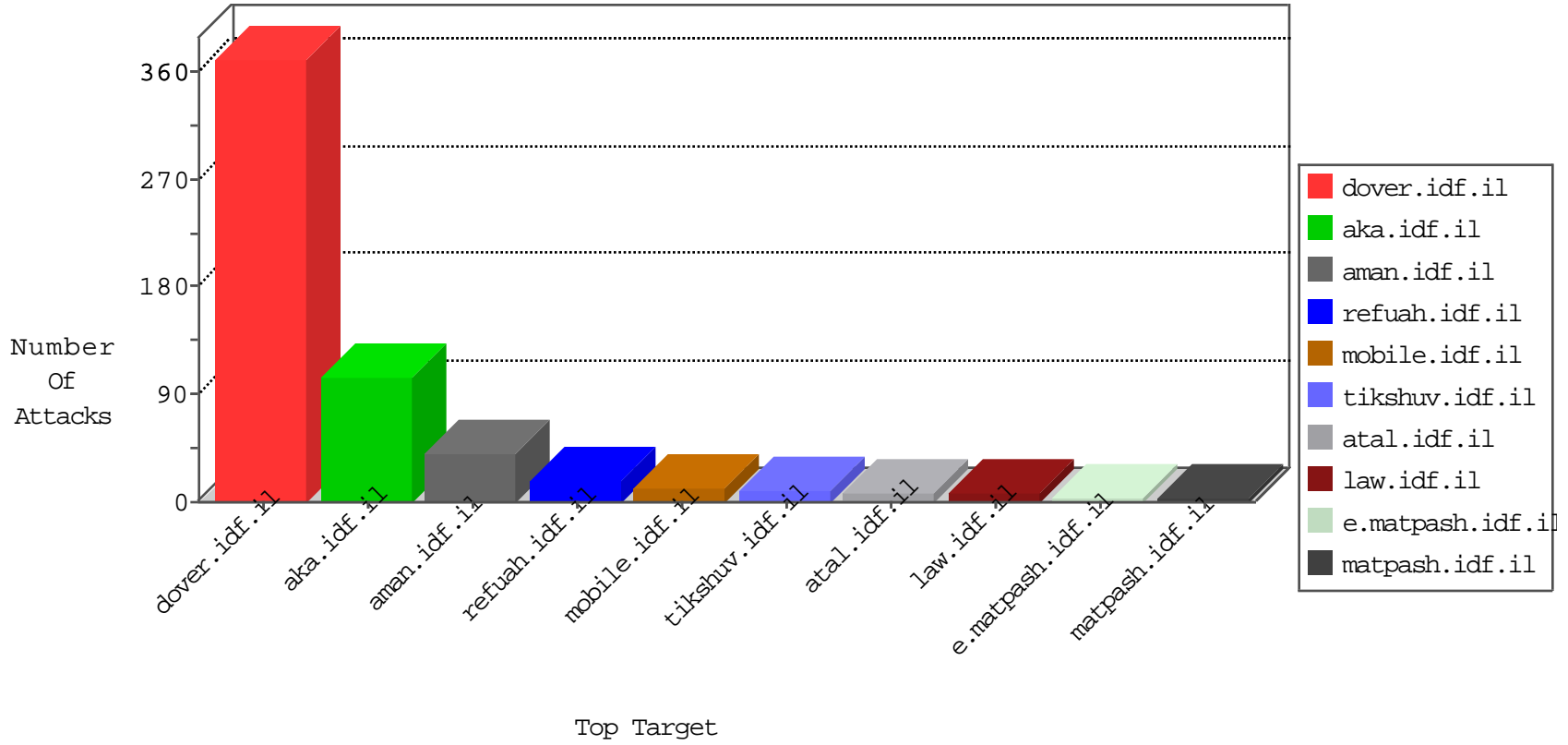
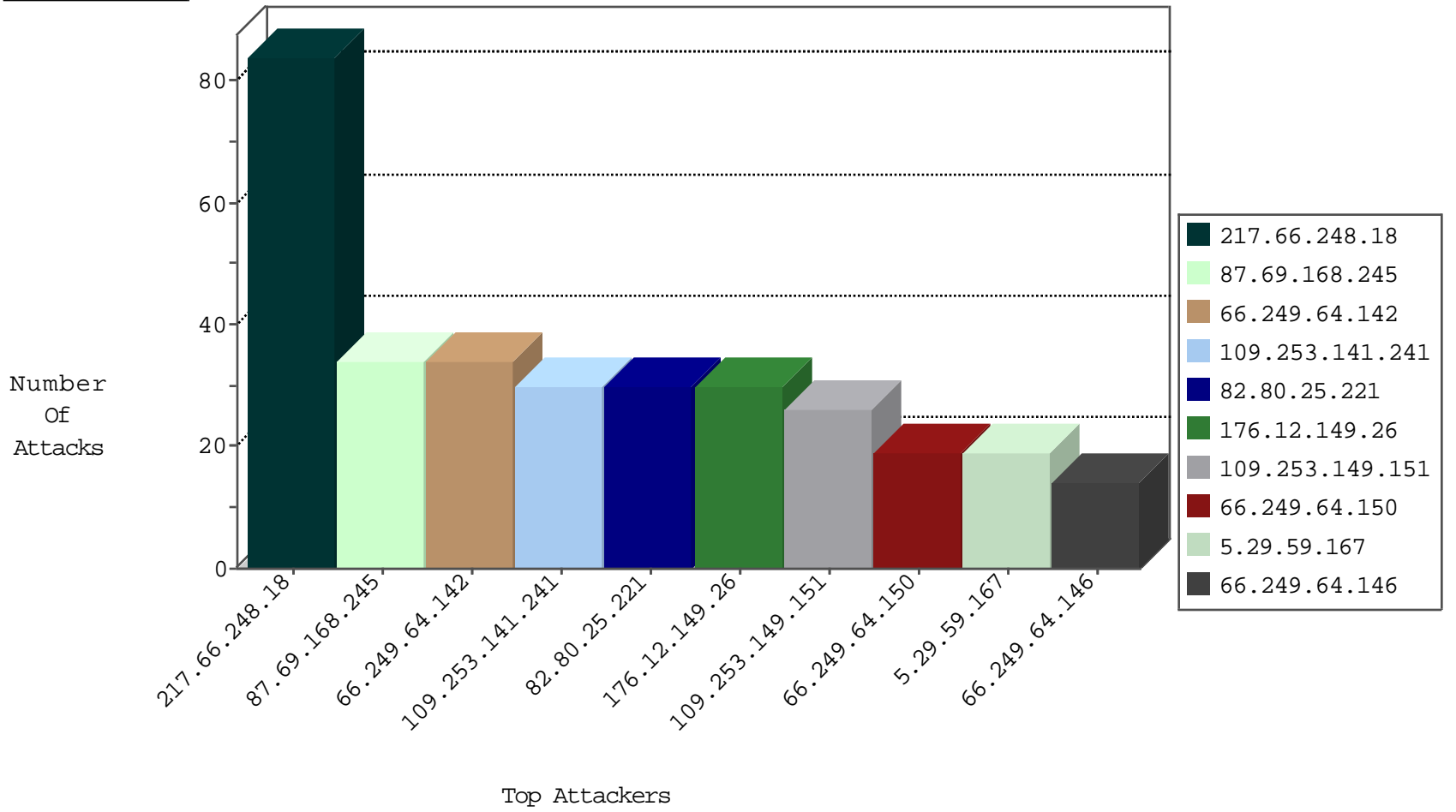




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
217.66.248.18	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	942
87.69.168.245	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	309
146.185.239.100	Russian Federation	147.237.76.86	navy.idf.il	block-sp-trafl	drop	1
71.6.216.35	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.49	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
149.88.14.39	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.0	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
2.54.42.24	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.64.191.89	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	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
23.254.132.78	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
85.25.103.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
63.138.4.238	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	30
217.66.248.18	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.78.45	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
37.26.147.167	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.146	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
37.142.235.230	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.84	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
2.54.13.155	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
116.30.168.181	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
116.30.168.181	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
116.30.168.181	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
208.39.68.33	United States	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
208.39.68.33	United States	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
60.3.0.201	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
43.255.191.163	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
116.30.168.181	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
116.30.168.181	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
116.30.168.181	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -f -sS	1
91.238.134.92	Poland	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
217.66.248.18	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.163	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
217.11.61.195	Germany	147.237.8.50	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
208.39.68.33	United States	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
198.154.60.27	United States	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
116.30.168.181	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
109.253.141.241	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.149.26	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.149.151	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.64.146	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
176.12.139.72	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
84.110.112.180	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
109.253.149.72	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.149.183	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.159.112	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
94.230.86.194	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
5.102.254.165	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
77.127.189.36	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	5
192.116.158.40	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
77.127.189.36	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	5
5.22.130.171	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
188.120.148.201	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
37.239.138.233	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.229	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
87.69.92.15	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
94.230.86.194	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
188.120.148.145	Israel	147.237.77.74	law.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
31.186.228.96	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
31.186.228.26	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
31.186.228.68	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
31.186.228.27	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
31.186.228.86	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
31.186.228.57	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
31.186.228.88	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
31.186.228.60	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
5.102.254.197	Israel	147.237.76.39	mobile.meitav.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
31.186.228.95	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
31.186.228.25	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
2.54.188.145	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
46.19.85.195	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
31.186.228.64	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
109.253.130.42	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
84.109.81.79	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
141.212.122.73	United States	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.198	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
128.199.90.112	Singapore	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
5.144.50.225	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
79.179.110.232	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.120.148.145	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
2.54.28.113	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.19.86.246	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.47	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
37.142.156.237	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
84.109.81.79	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.29.59.167	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.29.59.167	Block	16
132.68.114.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	5
66.249.64.146	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.146	Block	4
197.134.127.249	Egypt	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	4
46.120.140.187	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	4
203.133.169.208	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 203.133.169.208	Block	3
176.12.136.249	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	2
37.236.66.179	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qar/	Block	2
87.69.92.15	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
41.36.184.48	Egypt	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
66.249.78.22	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
46.121.197.104	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
109.226.15.5	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/history/darom.stm	Block	1
87.68.255.64	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cphMain\$cphSachar\$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
77.127.188.4	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
176.12.142.244	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1607-15301-he/dover.aspx	Block	1
93.173.248.240	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
37.142.30.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.152.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/gyius/authentication-service.aspx/getuserdetails	Block	1
195.238.168.13	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
84.94.192.12	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/gyius/atuda/asmachta.aspx	None	1
176.12.138.1	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.51	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
46.150.97.73	Ukraine	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
109.253.135.15	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.59.167	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyius/[object object]	Block	1
212.76.118.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.69.73.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
77.127.189.36	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
176.12.144.83	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/faq.asp	Block	1
95.86.117.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
2.54.182.192	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.108.69.216	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
176.12.141.72	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	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
52.4.217.90	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en/matpash.aspx"	Block	1
109.253.140.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.129.77	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
79.181.162.67	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/gyius/atuda/asmachta.aspx	None	1
176.12.146.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0211-2.stm	Block	1
109.65.135.238	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.59.167	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
85.65.106.120	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/gyius/authentication-service.aspx/getuserdetails	Block	1