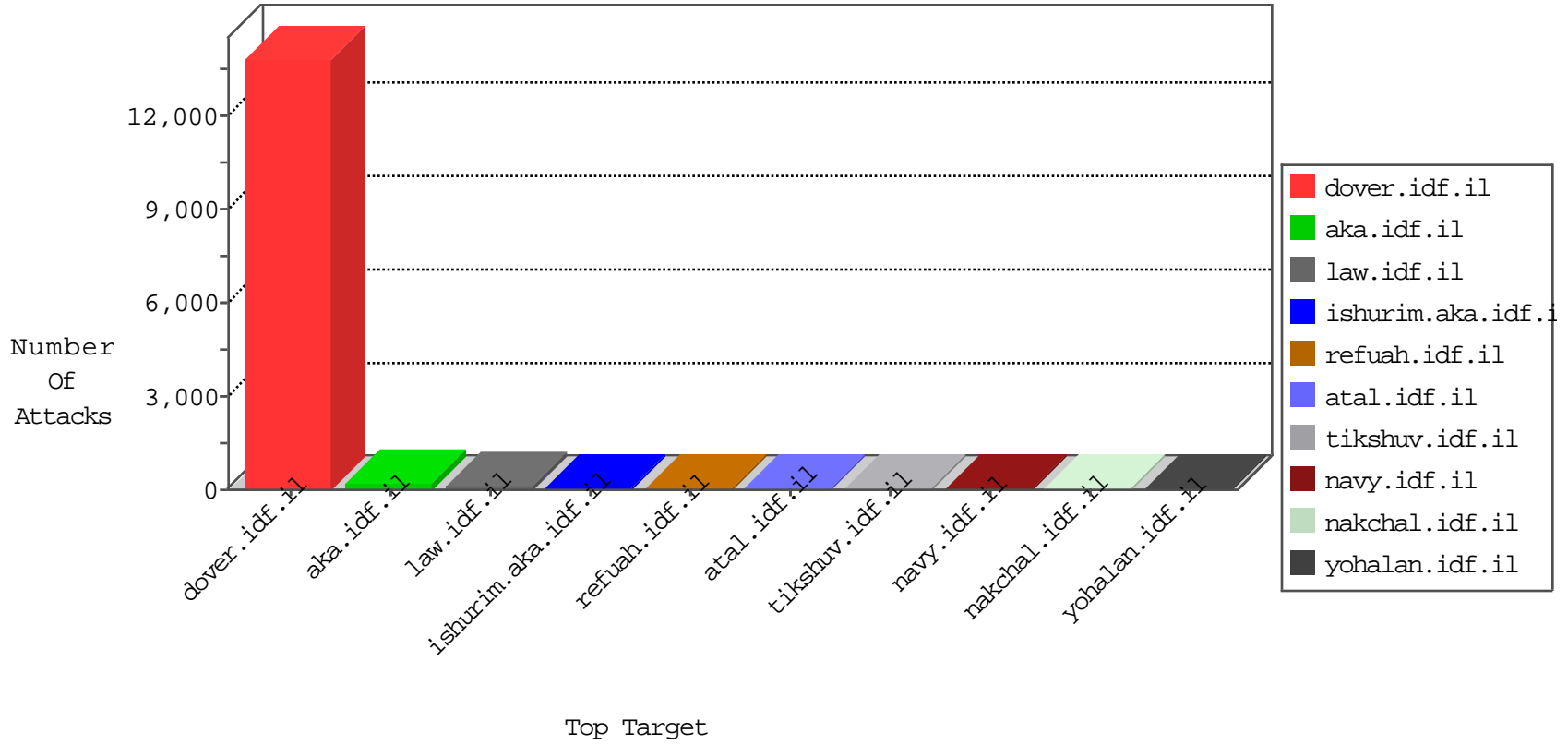
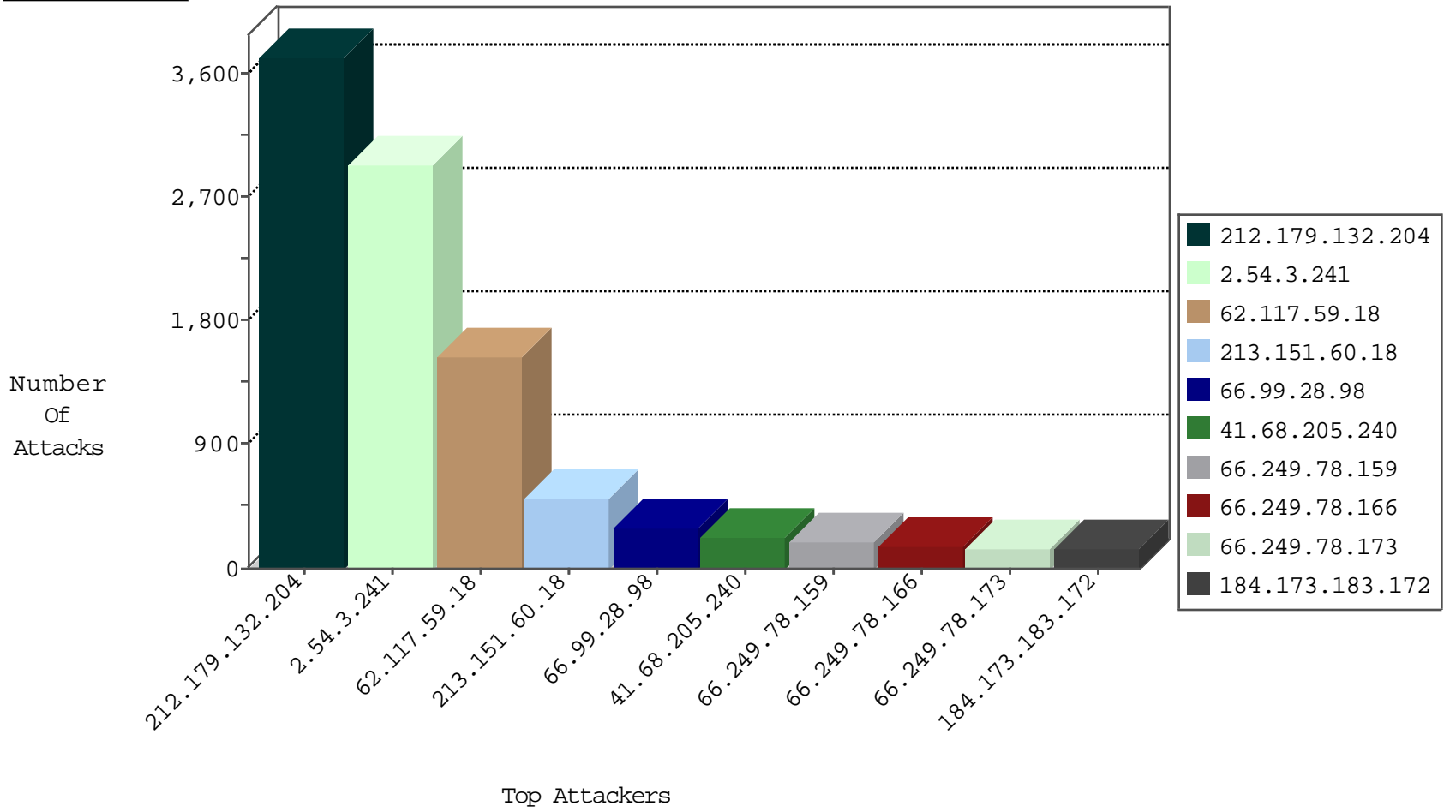


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
79.176.144.5	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	689
190.24.128.254	Colombia	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	63
46.19.85.167	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	25
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
91.199.69.254	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
109.66.164.149	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
213.175.183.170	Lebanon	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
5.22.129.179	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
192.114.91.244	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.79.5	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
41.68.205.240	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.167.142	United States	147.237.76.34	ychalan.idf.il	Block_Udp_All_Nets	drop	1
109.253.139.180	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	142
46.19.86.219	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
66.240.236.119	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	2
84.108.96.73	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.103.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
195.88.208.250	Russian Federation	147.237.76.34	yohalan.idf.il	DVRep_P-N_40-59	Permit	1
46.19.85.208	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.66.80.112	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	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.34	yohalan.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
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
109.67.104.159	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.0.19	madim.atal.idf.il	7610: IP Reputation	Block	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.166	aka.idf.il	7610: IP Reputation	Block	1
66.240.236.119	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
2.54.138.114	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.64.125.239	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	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
213.151.38.196	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
147.226.221.87	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	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	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.2	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
79.179.136.145	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.217	e.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
188.138.9.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.167	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1

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	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
84.94.76.177	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
201.27.104.209	Brazil	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
60.169.77.174	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
199.68.196.123	United States	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
60.169.77.174	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
120.132.70.61	China	147.237.8.46	e.chimuch.idf.il	ET SCAN Potential SSH Scan	1
2.52.133.132	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
120.132.70.61	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
84.109.163.35	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.235.69	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.175.77	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.143	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
222.69.94.13	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
199.68.196.125	United States	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
60.169.77.174	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.117.110.20	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
120.132.70.61	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
95.86.110.30	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.151	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.132.204	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3727
2.54.3.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2854
62.117.59.18	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1539
213.151.60.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	516
66.99.28.98	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	291
41.68.205.240	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	230
213.175.183.170	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	104
84.95.229.132	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	94
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	88
109.64.126.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	78
164.138.119.36	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	77
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	70
46.19.86.128	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	65
46.19.85.39	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
66.249.78.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
172.56.6.121	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
89.138.197.32	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
5.29.134.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
84.108.34.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
79.7.129.220	Italy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
176.58.68.193	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
80.184.27.246	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
134.126.227.96	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
109.66.171.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
69.248.82.82	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
109.253.130.93	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
109.253.133.181	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
46.19.85.231	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
70.209.203.83	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
207.46.13.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
109.253.142.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
176.12.138.204	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
37.26.148.170	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.133.188	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
157.55.39.146	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
70.199.196.14	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
2.54.3.241	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	30
2.54.3.241	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	30
157.55.39.33	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
2.54.3.241	Israel	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	30
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
37.26.147.148	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.183.180.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	29
212.76.99.24	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
31.44.136.209	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
46.19.86.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
95.86.93.239	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
46.120.137.229	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.79.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
80.246.130.69	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	2
109.67.194.170	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.59.43.170	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.133	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.125.132.32	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
109.253.137.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.206	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.79.36	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/gyius/gyius/general.aspx	Block	1
66.249.78.34	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
84.228.116.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyius	Block	1
78.129.148.101	United Kingdom	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
188.138.17.205	France	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
149.78.214.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9703-he/refuah.aspx	Block	1
85.130.255.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/gyius/miyun/miyunprocessquestionnaire.aspx	None	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
66.249.65.186	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
207.46.13.78	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.230.72.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
46.19.85.71	Israel	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method Only in URL	Block	1
157.150.192.237	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
68.180.228.59	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.79.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI in www.aka.idf.il/main/gyius/general.aspx	None	1
109.64.48.73	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.64.213.212	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	1
212.199.107.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.177.7.127	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	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
195.144.71.107	Belgium	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
149.88.8.231	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
66.249.79.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8818-he/refuah.aspx	Block	1
89.139.187.96	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.78.201	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/default.asp	Block	1
66.249.67.49	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
207.46.13.78	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/home.asp/info.asp	Block	1
164.138.123.35	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.79.49	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 66.249.79.49	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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
213.175.183.170	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
79.180.33.6	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/gyius/authenticationservice.aspx/getuserdetails	Block	1