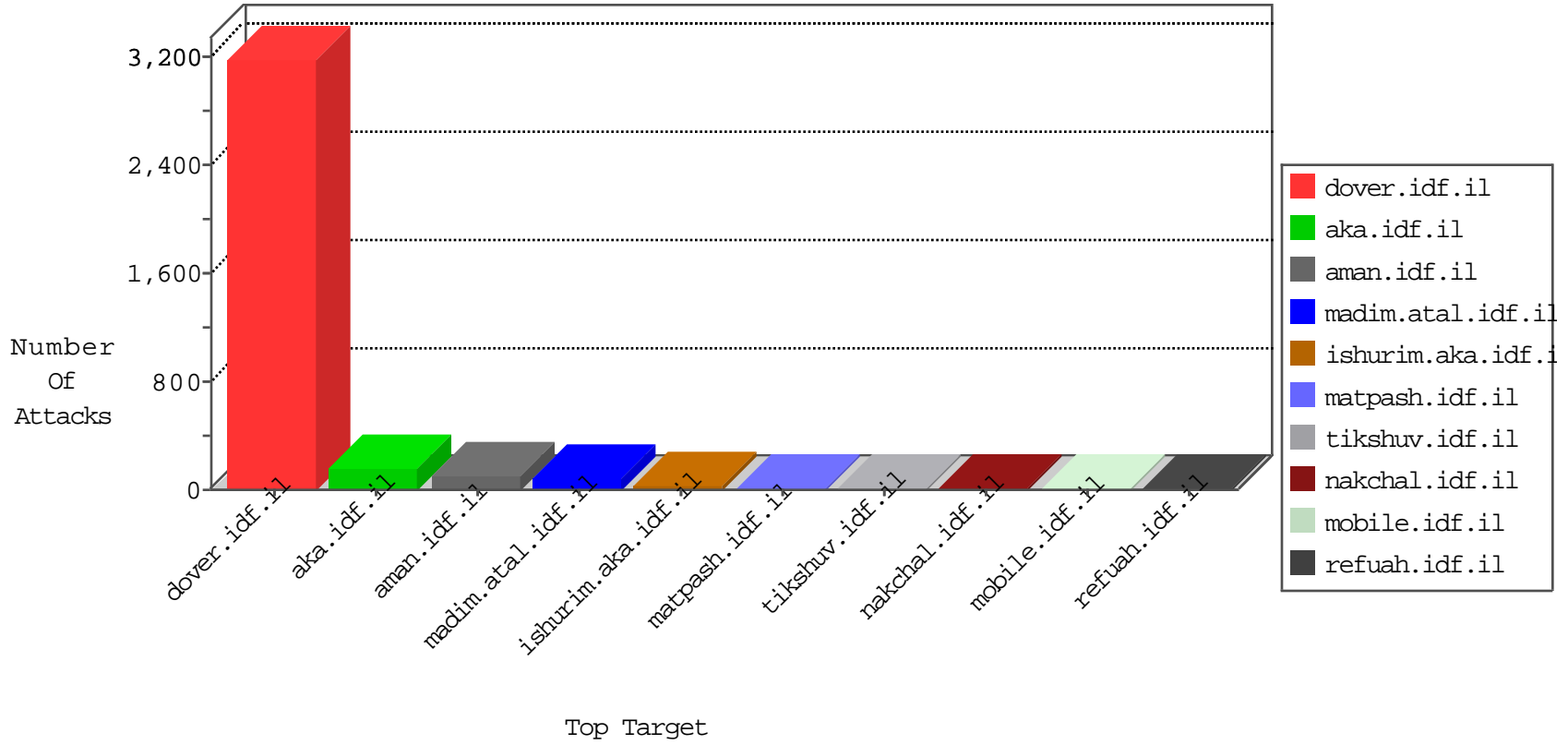
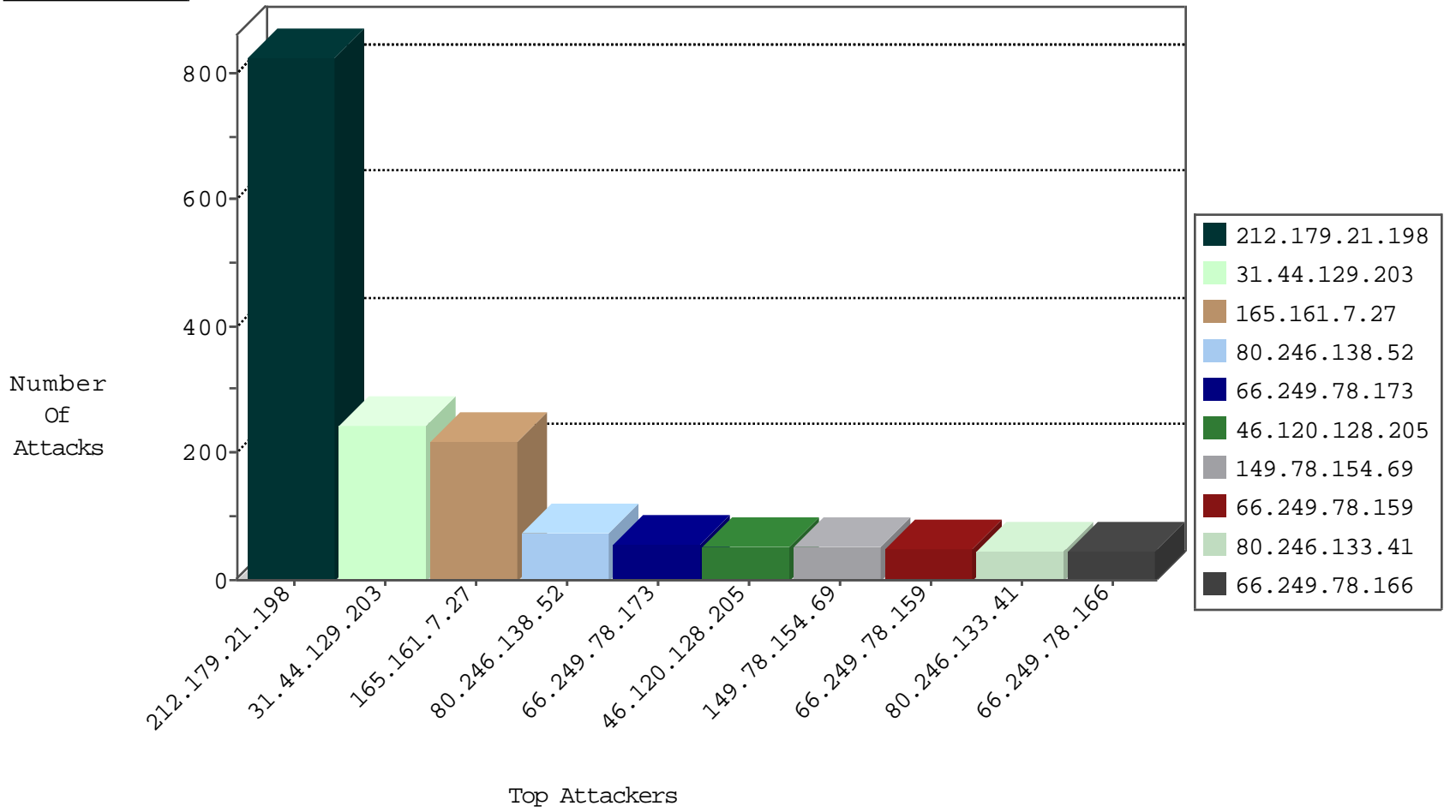




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
46.120.128.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	618
79.179.2.10	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	264
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	222
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	157
37.26.146.142	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	36
85.65.133.1	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
84.109.117.53	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
212.116.164.9	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
89.139.43.176	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
10.0.0.210		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
84.109.117.53	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.179.183.221	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
79.176.103.250	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
84.109.119.190	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.176.103.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
89.139.184.184	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
71.6.216.40	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
79.179.183.221	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
1.33.82.124	Japan	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
89.139.184.184	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
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
81.218.150.120	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	2
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.135.131	United States	147.237.76.176	test.ncoore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.177	ncoore.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
66.240.236.119	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.46	e.chinuch.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
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.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
94.23.172.110	Czech Republic	147.237.72.166	aka.idf.il	Cl000106: HTTP: majestic bot	Block	1
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.121	e.navy.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	147.237.76.39	mobile.meitav.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	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
46.117.160.26	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
89.139.43.176	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
85.250.125.204	Israel	147.237.77.216	dover.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
109.65.122.95	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
104.155.200.187		147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
104.155.200.187		147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
91.224.132.118	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.21.135	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.240.144.66	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	United States	147.237.77.243	mobile.idf.il	ET DROP Dshield Block Listed Source	1
61.240.144.64	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
151.226.160.107	United Kingdom	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
121.88.5.177	Korea, Republic of	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.115	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
104.167.118.60		147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 4096	1
104.155.200.187		147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
101.226.2.99	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
79.176.197.18	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
202.71.25.29	India	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
121.88.5.177	Korea, Republic of	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
46.121.108.249	Israel	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
212.179.21.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	826
31.44.129.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	245
165.161.7.27	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	216
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
31.154.18.65	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
80.246.133.41	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
172.56.37.186	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
46.19.85.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
79.178.219.207	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
46.19.85.132	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
66.249.93.160	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
157.55.39.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
217.27.219.230	Hungary	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
36.48.159.218	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
37.26.146.142	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
177.32.92.153	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
66.249.93.164	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
79.183.96.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
109.65.2.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
192.114.23.208	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
2.52.44.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
76.15.212.34	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
216.162.93.194	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
50.200.116.246	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
212.14.242.36	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
46.19.85.100	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
2.54.32.61	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
80.179.225.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
77.126.250.83	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
109.253.141.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
176.12.150.171	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
87.68.228.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
134.191.232.70	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
134.191.232.71	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
84.108.250.142	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
85.130.246.101	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	11
157.55.39.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
84.94.83.164	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
80.246.138.52	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.138.52	Block	74
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	10
157.55.39.4	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	5
109.66.114.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	4
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
185.32.176.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
93.204.241.73	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	3
79.181.182.155	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
95.86.116.200	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
85.64.158.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.182.165.108	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
192.116.92.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
62.90.122.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.19.85.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
2.54.25.223	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.12.147.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/sachar	Block	2
195.154.181.152	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/manager/	Block	2
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-6447-he/patzar.aspx	Block	1
213.151.58.171	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/×××××××××××××\$	Block	1
109.67.50.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.193.69	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19916-he/idfgdover.aspx	Block	1
192.114.91.249	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
157.55.39.81	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/links/	Block	1
80.179.54.68	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 80.179.54.68	Block	1
46.19.85.125	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
149.78.149.184	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
66.249.75.42	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/mobile/	Block	1
198.20.69.74	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
46.121.108.84	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//https://www.aman.idf.il/	Block	1
185.32.179.191	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
84.110.2.102	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	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/69-he/patzar.aspx	Block	1
109.67.185.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
85.250.9.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https://www.aka.idf.il/	Block	1
66.249.67.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/print_text.asp	Block	1
192.116.92.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.116.92.57	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
80.246.136.127	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
79.118.23.73	Romania	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//	Block	1
66.249.75.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/modules/forums/forum.aspx	Block	1
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.121.108.84	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https://www.aka.idf.il/	Block	1
185.61.138.244		147.237.0.34	tikshuv.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0102-1.stm	Block	1
138.134.192.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1