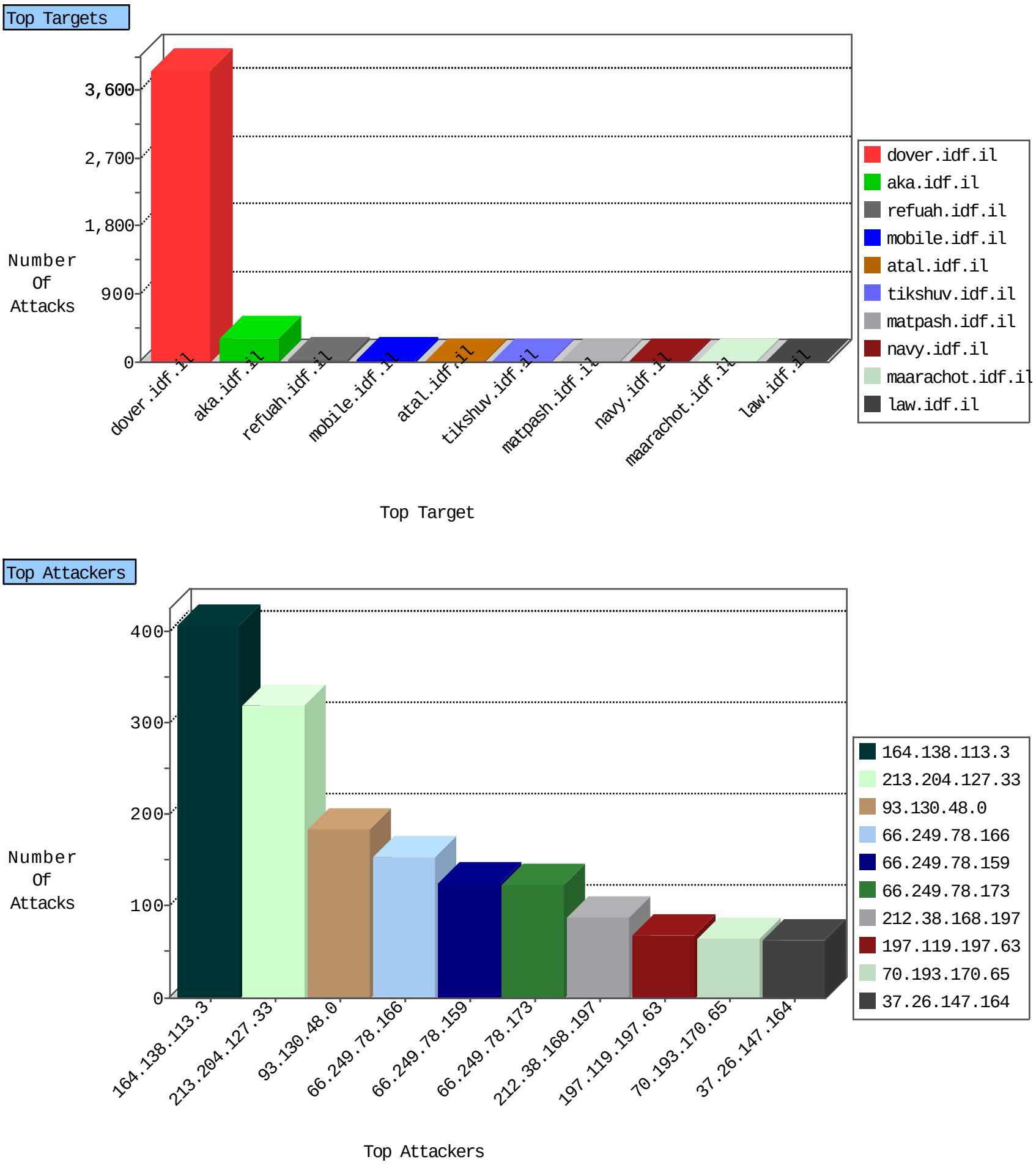
04-15-2015-23:03:05 to 04-16-2015-00:03:05

IDF Under Attack
04-15-2015-23:03:05



04-15-2015-23:03:05 to 04-16-2015-00:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
213.204.127.33	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	107
197.35.3.184	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	17
46.19.86.154	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
79.180.2.68	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	4
2.54.176.135	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
84.109.125.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
41.142.12.98	Morocco	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
10.0.0.1		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.86.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
124.232.142.220	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
212.179.61.122	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.246.140.175	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.86.154	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
124.232.142.220	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
70.45.59.237	Puerto Rico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
188.120.148.245	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
70.91.91.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
84.228.161.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
61.90.69.85	Thailand	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
2.54.150.251	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-15-2015-23:03:05 to 04-16-2015-00:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	26
46.19.85.39	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.81	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.117.32.161	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.70.114	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	2
79.179.119.87	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
5.29.229.61	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
188.138.9.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	2
66.240.236.119	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.196	e.sviva.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
85.25.103.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	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
198.20.69.98	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
79.181.164.183	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	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.200	eitan.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
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
84.228.194.243	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
149.88.38.142	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1

04-15-2015-23:03:05 to 04-16-2015-00:03:05

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	4
212.29.224.69	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
85.250.20.150	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
59.175.148.68	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
117.78.1.200	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
59.41.39.125	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
111.13.30.109	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
46.19.86.190	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
91.217.90.19	Ukraine	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.79.106	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.240.144.65	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
59.175.148.68	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
59.175.148.68	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
111.13.30.109	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
59.41.39.125	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
91.217.90.19	Ukraine	147.237.76.148	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
70.193.170.65	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

04-15-2015-23:03:05 to 04-16-2015-00:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
164.138.113.3	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	408
213.204.127.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	316
93.130.48.0	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	180
212.38.168.197	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	88
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	70
197.119.197.63	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	68
37.26.147.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	64
109.65.108.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
2.54.153.25	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
77.127.170.100	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
70.193.170.65	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
85.214.34.246	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
93.173.152.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
199.243.180.67	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
46.19.85.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
77.127.246.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
46.19.86.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
80.246.133.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
207.46.13.77	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
178.2.219.71	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
176.12.151.93	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
46.117.112.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.87.83.50	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
46.19.86.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
46.117.32.161	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	22
66.249.81.218	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
79.181.167.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
66.249.93.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
66.249.93.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
70.45.59.237	Puerto Rico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
84.109.125.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
31.186.228.89	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	18
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
76.68.233.45	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	41
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	29
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	27
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
95.86.64.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	3
213.204.127.33	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
84.109.180.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
87.68.87.59	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
46.117.67.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.182.136.221	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
98.168.171.234	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.178	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
80.246.130.135	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.127	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
31.44.135.252	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
178.254.50.101	Germany	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 178.254.50.101	Block	1
109.65.124.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
85.250.155.132	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
77.126.213.235	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
58.22.77.143	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp/trackback/	Block	1
157.55.39.206	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chamatz/home/d...sp	Block	1
66.249.79.74	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8497-he/navy.aspx	Block	1
94.136.40.100	United Kingdom	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/blog/wp-admin/	Block	1
66.249.67.32	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/×'×™×œ ×™××• ××ª	Block	1
84.108.123.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9746-he/refuah.aspx	Block	1
37.8.10.236	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
178.254.50.101	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp/wp-admin/	Block	1
66.249.79.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
109.67.165.74	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/iturim/iturim.aspx	None	1
85.250.155.132	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
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-8021-he/dover.aspx	Block	1
66.249.64.48	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//scriptresource.axd	Block	1
213.251.182.110	France	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/test/wp-admin/	Block	1
79.176.157.180	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
2.54.21.105	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/default.stm	Block	1
176.10.104.227	Switzerland	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.10.104.227	Block	1
66.249.79.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/iturim/asp/displayallsoldiers.asp	Block	1
66.249.67.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0518-1.stm	Block	1
68.180.228.59	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
46.117.32.161	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
198.20.69.74	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
109.253.141.67	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.58	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8283-he/navy.aspx	Block	1
66.249.78.134	Israel	147.237.76.30	himush.idf.il	Unknown Parameter &SortDir in www.chimush.atal.idf.il/938-he/himush.aspx	None	1
66.249.64.56	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	1
79.179.165.238	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.154.119	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1