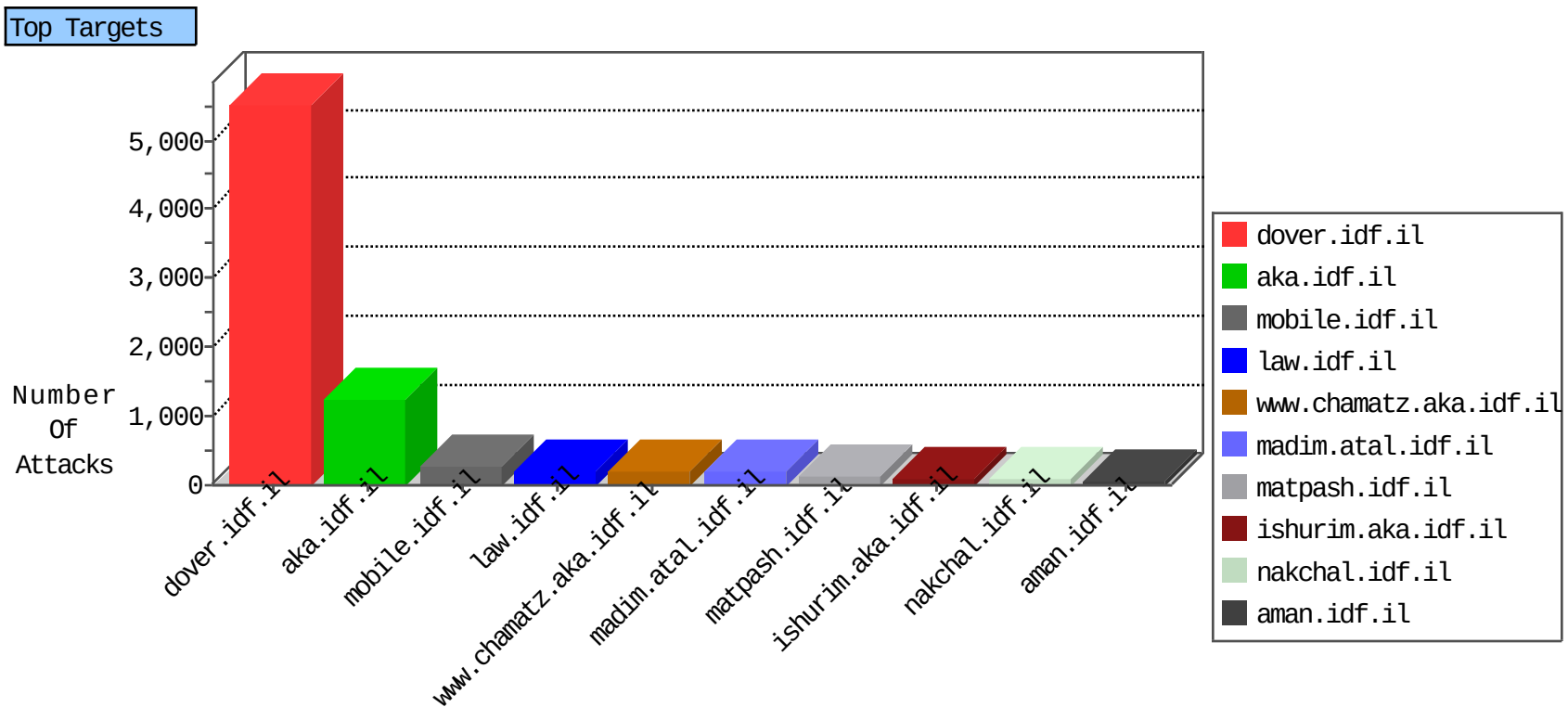
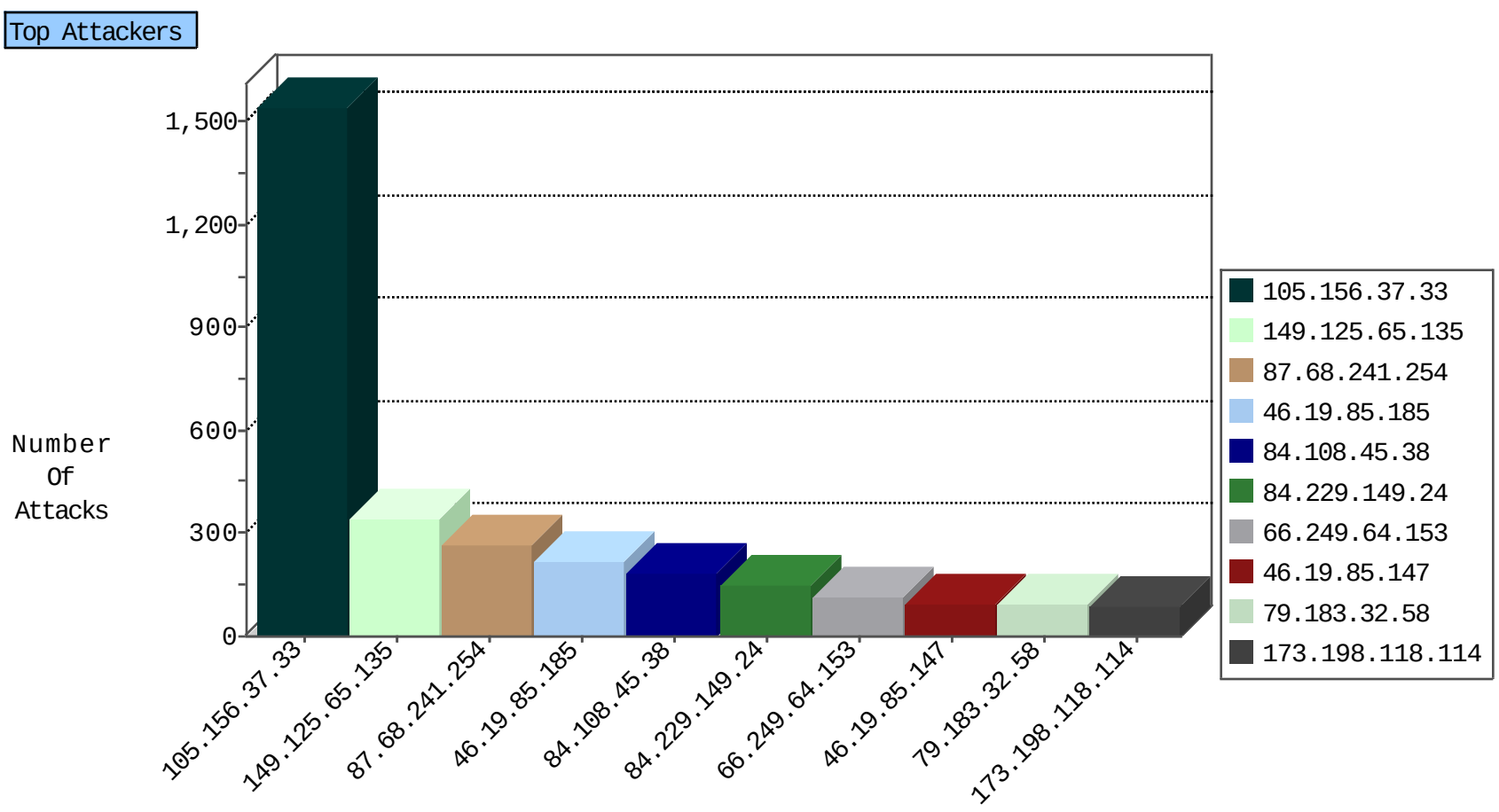
10-28-2015-20:04:05 to 10-28-2015-21:04:05

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-28-2015-20:04:05 to 10-28-2015-21:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.153	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	8602
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5053
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3822
66.249.64.159	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	3285
41.29.77.248	South Africa	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2283
66.249.69.85	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1750
66.249.69.8	United States	147.237.77.234	halag.idf.il	TCP handshake violation, first packet not syn	drop	1179
54.244.22.103	United States	147.237.0.19	madim.atal.idf.il	TCP handshake violation, first packet not syn	drop	1068
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	848
66.249.67.216	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	778
149.125.65.135	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	681
66.249.69.69	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	426
66.249.67.194	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	361
66.249.69.77	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	334
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	302
92.81.100.160	Romania	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	288
66.249.81.218	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	215
64.233.172.163	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	199
46.244.95.186	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	186
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	122
66.249.81.212	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	83
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	79
37.26.146.242	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	71
37.26.146.183	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	47
66.249.67.208	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	34
87.68.241.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
79.183.32.58	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
79.183.32.58	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
80.179.9.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.183.32.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
84.108.43.246	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.12.140.161	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
217.194.198.104	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
84.228.204.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
5.29.117.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
87.69.68.182	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
66.249.69.16	United States	147.237.77.234	halag.idf.il	TCP handshake violation, first packet not syn	drop	8
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
2.52.178.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.182.16.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.66.51.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
147.236.30.46	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.180.193.73	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
2.52.178.162	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
46.121.235.74	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
217.194.198.104	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
92.97.142.249	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5

10-28-2015-20:04:05 to 10-28-2015-21:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.172.186.255	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5

10-28-2015-20:04:05 to 10-28-2015-21:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
79.180.193.73	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
176.193.147.182	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.241.209.114	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.182.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
169.57.5.20	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
77.127.227.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
169.57.5.20	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.67.240	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
149.78.97.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
43.229.53.89	147.237.0.33	Japan	idf.il	ET SCAN Potential SSH Scan	1
118.189.208.107	147.237.76.31	Singapore	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
109.64.13.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.8.66.110	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN Potential SSH Scan	1
93.173.178.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.8.66.110	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Potential SSH Scan	1
84.111.224.123	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.166.62.68	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
5.8.66.110	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
176.13.1.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.164.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
169.57.5.20	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.173	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.224.248	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.232	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
149.78.80.9	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.33.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.8.66.110	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
95.17.54.146	147.237.76.30	Spain	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.8.66.110	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Potential SSH Scan	1
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.120.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.8.66.110	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
192.116.96.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.166.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-28-2015-20:04:05 to 10-28-2015-21:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.156.37.33	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1269
149.125.65.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	331
46.19.85.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	218
84.108.45.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	185
173.198.118.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
79.181.63.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
24.190.175.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
37.26.146.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
79.183.32.58	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	53
87.68.241.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
109.66.31.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
141.0.14.98	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
41.100.29.68	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
37.142.197.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
89.139.183.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
46.117.220.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
37.142.132.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	33
100.100.107.138		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	33
176.13.22.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
138.16.113.205	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
46.19.85.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
141.0.13.130	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
72.82.230.99	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
208.218.238.20	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
74.101.114.16	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
2.54.23.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
66.102.8.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
209.112.135.62	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.142.99.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
37.142.241.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
84.108.209.186	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
37.142.204.198	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
37.142.255.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
77.125.76.120	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	15
82.166.22.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.54.158.16	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.156.37.33	Morocco	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.156.37.33	Block	272
87.68.241.254	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	195
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	90
84.229.149.24	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	75
84.229.149.24	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	75
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	45
46.120.142.167	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	30
176.12.138.166	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
84.108.146.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	30
2.54.23.95	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
95.86.101.22	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	30
2.54.177.118	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
79.177.174.67	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	30
5.22.129.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	30
79.177.174.67	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	30
84.108.146.196	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	30
66.249.69.32	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	15
2.54.22.224	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	15
85.64.103.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.13	Block	15
212.116.166.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	15
79.183.166.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
31.154.25.42	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	15
141.212.122.128	United States	147.237.72.167	ishurim.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	15
66.249.67.224	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	15
95.45.254.122	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	15
63.141.226.242	United States	147.237.77.235	sviva.idf.il	Distributed Unauthorized URL Access on www.cloud.ph/	Block	15
188.165.15.205	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5737-he/patzar.aspx	Block	15
79.176.119.73	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	15
46.19.86.192	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
149.78.232.117	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	15
107.150.56.165	United States	147.237.0.15	kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.cloud.ph/	Block	15
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	15
85.64.175.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	15
217.194.198.104	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	15
54.175.209.193	United States	147.237.0.34	tikshuv.idf.il	URL is Above Root Directory www.tikshuv.idf.il/../shared/clientscripts/jquery.plugins/jquery.charts.js	Block	15
176.12.140.161	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	15
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
37.26.148.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
141.212.122.128	United States	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	15
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.232	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	15
84.108.209.186	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	15
63.141.226.245	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.cloud.ph/	Block	15
204.12.251.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/shared/usercontrols/headerupper/	Block	15
79.176.119.73	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ajax/updatestatus.php	Block	15
46.19.86.192	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
157.55.39.82	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	15
107.150.56.166	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.cloud.ph/	Block	15