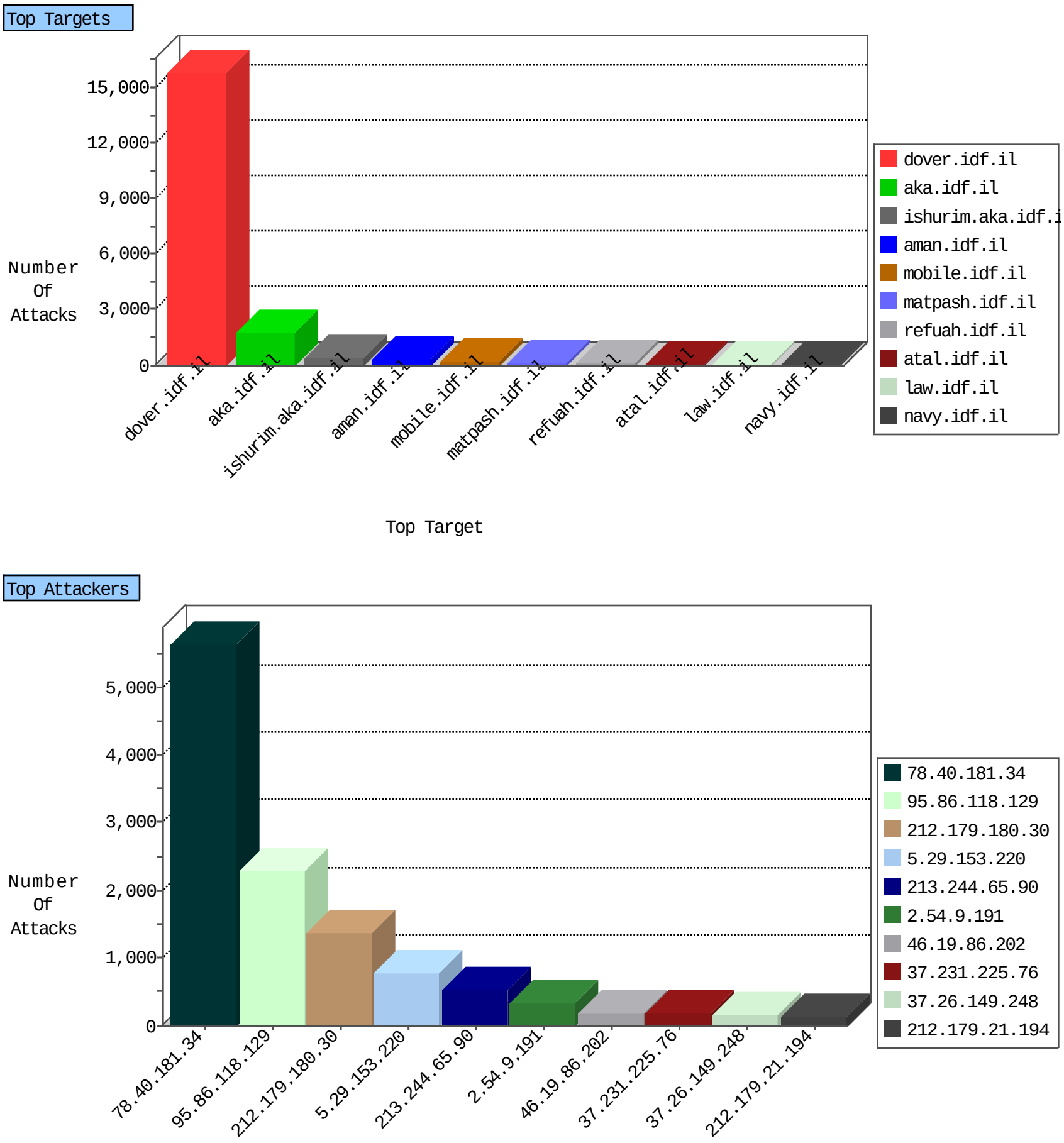
10-26-2015-15:04:02 to 10-26-2015-16:04:02

IDF Under Attack Daily Report



10-26-2015-15:04:02 to 10-26-2015-16:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.153.220	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	3574
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	462
2.84.83.162	Greece	147.237.72.167	ishurim.aka.idf.il	TCP handshake violation, first packet not syn	drop	452
64.233.172.171	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	448
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	423
2.52.170.156	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	154
79.181.15.195	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	135
109.160.219.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	74
2.54.182.13	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	57
85.130.221.188	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
82.80.38.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
84.108.48.68	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
37.142.68.52	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
185.32.179.87	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
85.250.250.55	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
37.26.149.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
46.19.86.92	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
2.54.191.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
84.111.38.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
176.12.139.9	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
176.12.143.51	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
176.13.23.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
46.19.86.41	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
31.168.6.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
176.12.147.206	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
77.127.153.20	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
85.250.145.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.12.143.41	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
176.12.137.110	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
62.0.42.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
193.104.77.4	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
84.110.54.128	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
109.66.10.27	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.54.159.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
46.19.85.243	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
109.66.106.212	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
46.19.85.203	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.26.149.134	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.67.170.54	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.120.152.228	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.32.179.224	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.5.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.94.57.172	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
31.154.175.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
199.203.172.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.61.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.52.138.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4

10-26-2015-15:04:02 to 10-26-2015-16:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
178.240.160.206	Turkey	147.237.77.74	law.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

10-26-2015-15:04:02 to 10-26-2015-16:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.29.153.220	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sS window 1024	58
79.178.109.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.107.16.206	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.240.155.234	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
113.223.152.207	147.237.8.14	China	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.2.197.181	147.237.8.14	Romania	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
109.66.31.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.61.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.139.169.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.191.224	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
223.4.174.30	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
84.108.10.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
77.125.95.248	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.107.16.206	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.29.153.220	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.191.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.2.197.181	147.237.72.166	Romania	aka.idf.il	ET SCAN Potential SSH Scan	1
109.66.139.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.115.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.186.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
223.4.174.30	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.109.156.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
223.4.174.30	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

10-26-2015-15:04:02 to 10-26-2015-16:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
78.40.181.34	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5644
95.86.118.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2301
212.179.180.30	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1365
213.244.65.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	529
2.54.9.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	335
46.19.86.202	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	192
37.231.225.76	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	177
37.26.149.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	120
95.86.77.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	119
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
46.19.86.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
46.19.85.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
192.114.91.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
73.149.108.198	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
46.19.86.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
137.54.44.157	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
2.54.56.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
46.19.86.127	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
46.19.86.129	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
82.102.170.201	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	54
83.244.113.182	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
188.247.72.186	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
46.19.85.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
46.19.86.100	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
46.19.86.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
46.19.86.232	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
162.157.109.136	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
87.101.137.122	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
213.57.221.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
193.104.77.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
220.227.161.85	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
37.142.237.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	31
195.160.240.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
37.26.149.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
93.173.233.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.86.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.54.49.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
81.218.48.37	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	29
37.142.218.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	28

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.6.178	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.13.6.178	Block	84
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2110-he/cogat.aspx	Block	56
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	56
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	42
176.12.151.168	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	39
79.176.173.32	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	28
176.106.40.81	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	28
109.66.176.138	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	28
82.80.222.116	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	28
178.62.209.185	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/general.aspx?catid=61230	Block	28
91.231.192.149	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 91.231.192.149 (Unknown SSL Session)	None	14
46.19.85.108	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/clientscripts/scroller/jqueryhttp/1.1 200 okdate: mon, 26 oct 2015 05:21:11 gmtlast-modified: tue, 10 sep 2013 13:49:33 gmtetag:	Block	14
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17396.jpg	Block	14
46.120.177.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
109.65.211.30	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	14
5.34.120.197	Kazakstan	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/forums/forums.asp	Block	14
80.246.136.167	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
66.249.64.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
147.236.254.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/faq.aspx	None	14
91.231.192.149	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	14
46.19.86.3	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	14
2.54.148.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
79.177.80.144	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	14
176.13.6.178	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus.com	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
46.121.146.12	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	14
31.44.137.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
168.235.194.234	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 168.235.194.234	Block	14
66.249.67.196	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	14
93.172.53.226	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	14
46.19.86.31	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTTARGET in www.aka.idf.il/main/giyus/pniotfindanswer.aspx	None	14
2.54.171.79	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
79.178.109.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/mailbox.aspx	Block	14
176.13.8.246	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12801-h	Block	14
46.121.146.12	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
109.186.40.122	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	14
84.111.83.70	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	14
37.26.149.233	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	14
77.61.196.13	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	14
178.240.160.206	Turkey	147.237.77.74	law.idf.il	PHP Attempt	Block	14
168.235.194.234	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shipt	Block	14
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
109.65.63.191	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	14
46.19.86.85	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
2.54.176.81	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
79.181.112.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
176.13.9.137	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	14
62.210.88.201	France	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	14