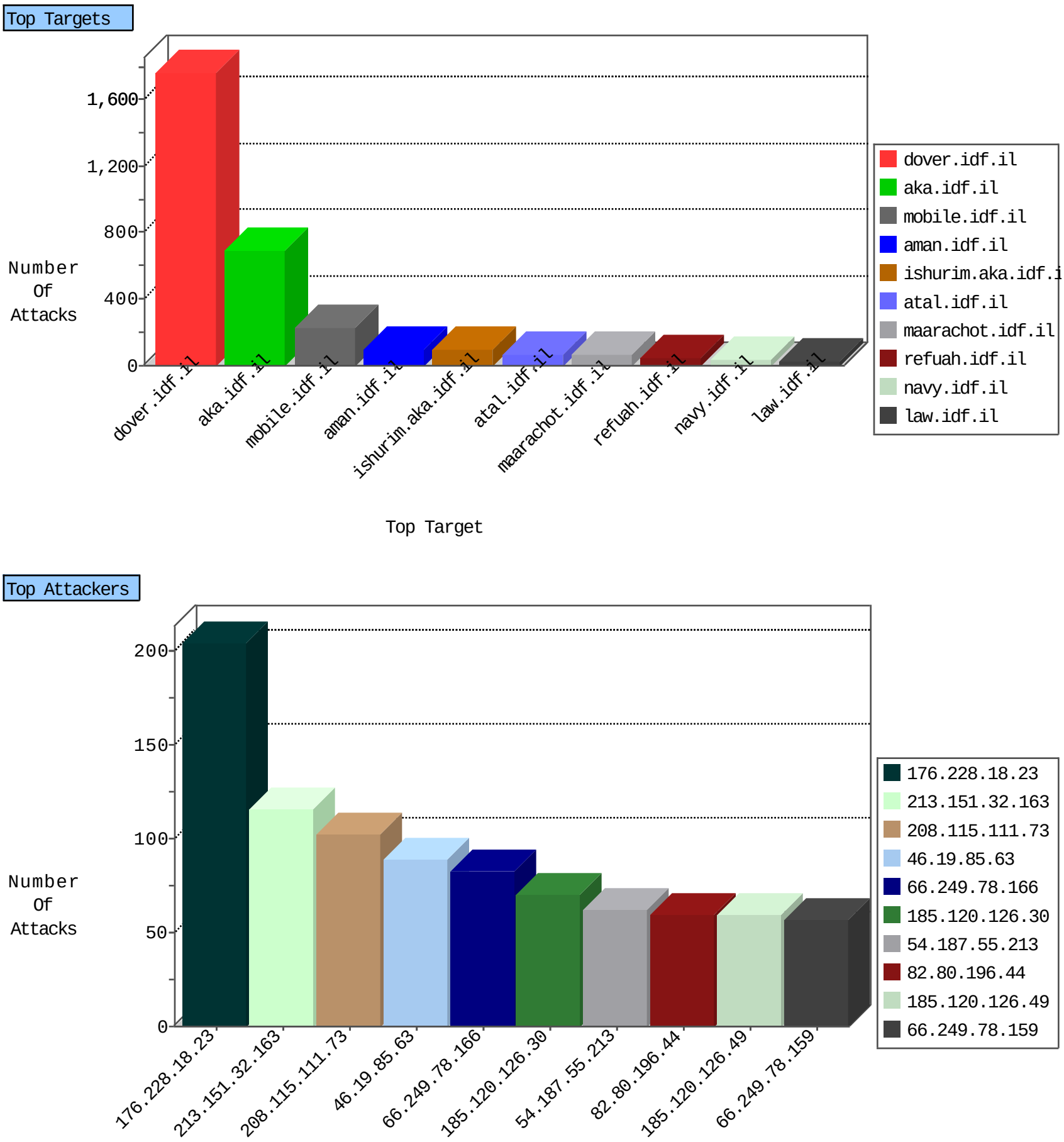
10-29-2015-07:04:01 to 10-29-2015-08:04:01

IDF Under Attack Daily Report



10-29-2015-07:04:01 to 10-29-2015-08:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.68.102	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3002
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	698
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	107
213.151.35.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	102
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	97
46.19.86.6	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	43
185.120.126.30		147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	43
185.120.126.30		147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
46.19.85.63	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	30
46.19.85.115	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
2.54.20.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
136.160.90.35	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
95.35.175.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
2.52.184.120	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	15
46.19.86.111	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
213.151.32.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
2.54.174.19	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
37.26.146.164	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.19.85.252	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	10
5.22.130.198	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.19.85.212	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	8
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
46.120.76.213	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5
79.182.102.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.120.76.213	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.136.167	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
69.126.90.169	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
66.249.78.217	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.0.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.6	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
213.186.177.173	Jordan	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.18.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.8.38.227	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.147.224	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
69.126.90.169	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
119.97.137.170	China	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
85.65.199.188	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.4.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.187.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.149.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.4.201	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.20.109	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.182.102.113	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
82.80.26.75	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.13.2.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.12.147.224	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.11.82	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-29-2015-07:04:01 to 10-29-2015-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-29-2015-07:04:01 to 10-29-2015-08:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.69.85	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
104.238.158.208	147.237.77.235		sviva.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.72.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.195	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
66.249.64.139	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
218.89.137.3	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.39	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.58.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
169.57.5.20	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
120.150.29.211	147.237.77.19	Australia	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
109.64.197.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.238.158.208	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.89.137.3	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
5.28.149.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
169.57.5.20	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.128.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.200.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
120.150.29.211	147.237.77.19	Australia	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1

10-29-2015-07:04:01 to 10-29-2015-08:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.228.18.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	205
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
46.19.85.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
67.71.135.101	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.252	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
167.114.107.51	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
31.168.84.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
213.151.35.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
174.236.0.181	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
80.246.130.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
5.22.129.221	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
185.120.126.30		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
84.228.124.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.120.126.30		147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.20.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.52.1.129	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.199	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.166.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.52.27.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.82.160		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
2.54.166.218	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
136.160.90.51	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.16.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
85.64.171.96	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
212.199.57.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.54.174.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.146.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.182.102.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.142.136.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.178.212.60	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.186.177.173	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.147.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	90
185.120.126.49		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	30
82.80.196.44	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	30
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	30
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	30
199.16.156.126	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/1/size220x0/17451.jpg	Block	30
185.120.126.49		147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	30
199.59.148.209	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/1/size220x0/17451.jpg	Block	30
2.54.39.105	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	15
68.180.229.173	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/brothers/home	Block	15
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1164-he/chinuch.aspx	Block	15
63.141.228.70	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.cloud.ph/	Block	15
157.55.39.62	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/youtube.com/idfspox1	Block	15
176.13.4.152	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	15
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/70607.pdf	Block	15
109.65.110.16	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	15
5.29.171.117	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	15
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9032-he/refuah.aspx	Block	15
66.249.67.34	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.67.34	Block	15
63.141.236.66	United States	147.237.77.235	sviva.idf.il	Distributed Unauthorized URL Access on www.cloud.ph/	Block	15
173.208.168.165	United States	147.237.0.15	kosher-kravi.idf.i	Distributed Unauthorized URL Access on www.cloud.ph/	Block	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
207.46.13.173	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	15
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=d7e41673kkkkkkk_d7e41673	Block	15
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
109.65.110.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ajax/updatestatus.php	Block	15
37.26.147.248	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
79.177.108.127	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	15
66.249.67.204	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on 147.237.77.74/templates/getfile/getfile.aspx	Block	15
192.118.48.248	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/	Block	15
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
173.208.168.165	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.cloud.ph/	Block	15
84.111.4.92	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/facebook.com/tzahalonline	Block	15
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
185.32.179.108	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	15
66.249.64.139	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	15
46.116.12.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	15
142.54.172.102	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on www.cloud.ph/	Block	15
79.183.106.218	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	15
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9067-he/atal.aspx	Block	15
66.249.64.18	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
176.12.136.167	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
85.93.91.84	Germany	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/templates/	Block	15
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/homepage/asp	Block	15
67.212.175.138	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteykatava/	Block	15
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
46.120.131.103	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15