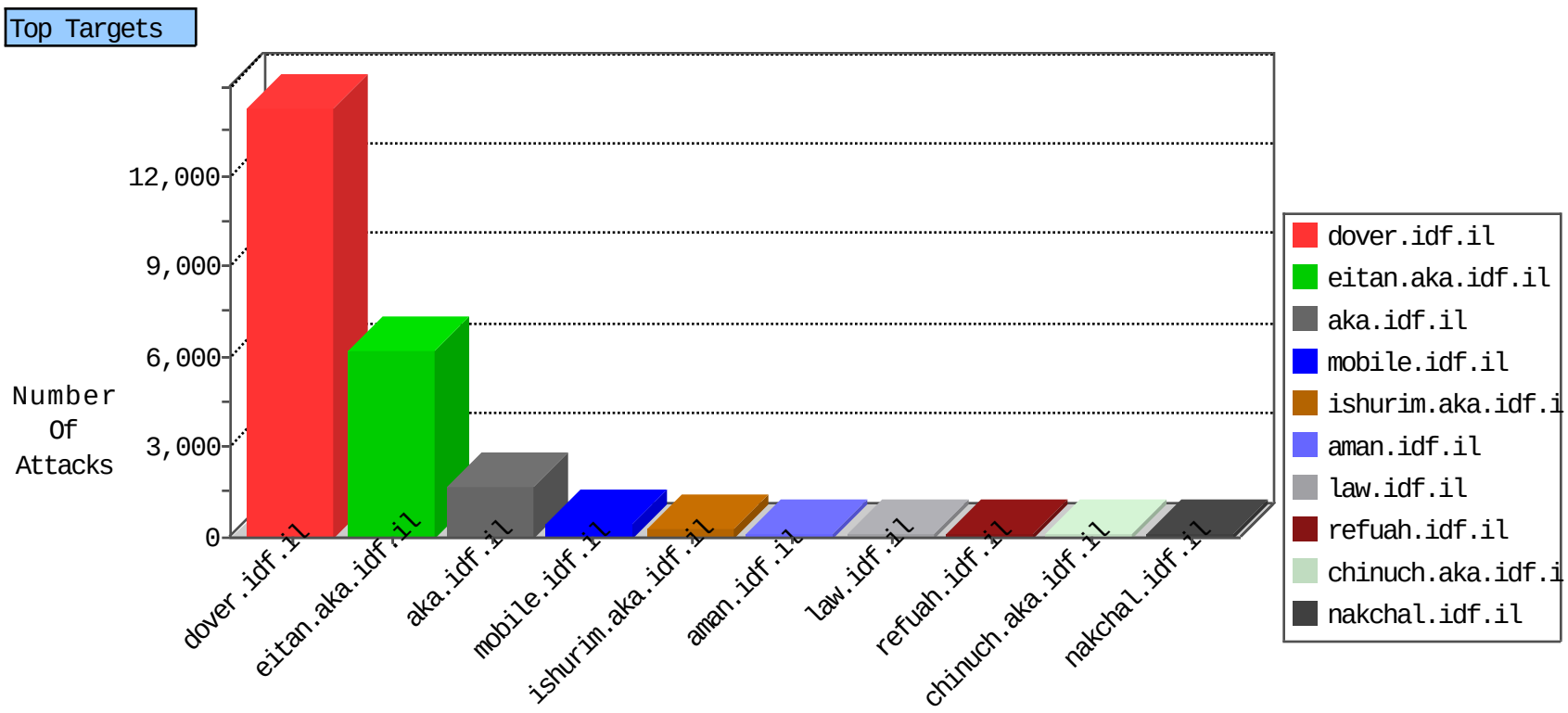
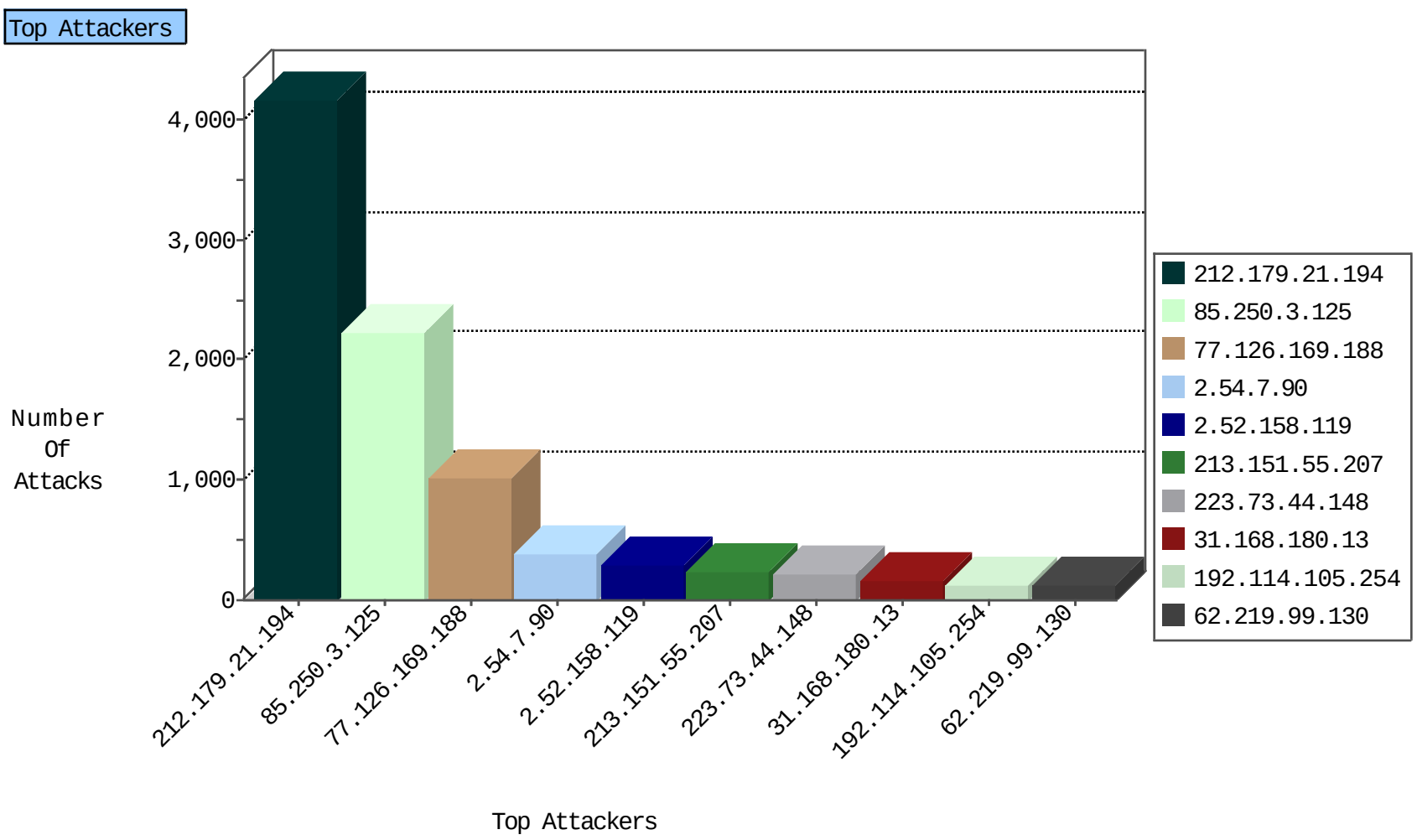
10-29-2015-09:04:09 to 10-29-2015-10:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-29-2015-09:04:09 to 10-29-2015-10:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1430
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	1334
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	684
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	481
66.249.67.210	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	325
66.249.69.77	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	228
79.182.147.34	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	139
46.19.86.160	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	129
2.54.17.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	82
46.19.85.41	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	77
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	42
46.19.86.249	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	42
185.13.195.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	41
213.151.48.39	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	41
8.37.70.125	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36
50.87.144.145	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33
85.250.166.165	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	33
176.12.146.74	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31
2.52.34.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
79.181.149.56	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
77.126.169.188	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	27
84.110.146.111	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
80.74.97.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
185.32.179.67	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
176.12.142.215	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
176.12.146.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
62.219.99.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
37.26.149.165	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	21
176.12.146.74	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
79.178.17.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
176.12.142.215	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
46.19.85.168	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
79.179.149.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
176.13.9.73	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
213.151.48.39	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
185.32.179.17	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
79.180.215.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
138.134.102.16	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
79.182.1.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
194.90.105.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
185.32.179.240	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
62.219.99.130	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
79.182.106.93	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.13.17.233	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.13.22.17	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
2.52.4.99	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
149.88.117.207	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	9

10-29-2015-09:04:09 to 10-29-2015-10:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
223.73.44.148	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	24
223.73.44.148	China	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	9
79.180.54.197	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

10-29-2015-09:04:09 to 10-29-2015-10:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.229.154.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.118.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.21.196	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.176.58.122	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.63.180	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	portscan: TCP Distributed Portscan	1
210.50.197.147	147.237.76.197	Australia	e.himush.idf.il	ET SCAN NMAP -f -sS	1
24.232.250.138	147.237.72.217	Argentina	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
194.90.167.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.139.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
138.134.102.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.163.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.21.196	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.177.116.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.109.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.246	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sA (2)	1
210.50.197.147	147.237.76.197	Australia	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
37.8.94.192	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
207.232.27.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.34.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.106.227.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.137.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
110.20.10.117	147.237.77.216	Australia	dover.idf.il	portscan: TCP Distributed Portscan	1

10-29-2015-09:04:09 to 10-29-2015-10:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.126.169.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1017
2.54.7.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	388
2.52.158.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	293
213.151.55.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	242
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	156
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	118
62.219.99.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
109.64.97.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
46.19.86.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
223.73.44.148	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
37.26.146.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
37.26.148.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
79.177.116.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
211.197.243.76	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
46.19.85.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
213.151.48.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
109.160.221.191	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	62
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
194.90.105.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
37.26.147.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
174.144.114.162	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
31.168.13.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
81.218.251.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
212.117.140.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
176.12.142.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	48
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
2.54.17.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
85.250.241.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
212.143.110.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
79.182.147.34	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
213.8.118.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
80.74.97.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
192.114.23.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.93.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
195.250.33.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
54.244.22.103	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
192.114.23.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
80.246.139.41	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3990
85.250.3.125	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2220
176.13.4.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	90
192.114.1.131	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	75
31.168.180.13	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	75
31.168.180.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	75
149.88.26.241	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	60
223.73.44.148	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 223.73.44.148	Block	60
40.77.167.44	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	30
185.32.179.29	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	30
223.73.44.148	China	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	30
2.54.177.84	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	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
37.26.148.218	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	30
149.88.26.241	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	30
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
80.179.8.14	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	24
81.218.251.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
40.77.167.43	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	15
66.249.75.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/2616.jpg	Block	15
2.54.18.192	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	15
109.64.31.117	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/990-he/patzar.aspx	Block	15
93.85.219.2	Belarus	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/modules/mod_twit/mod_twit.php	Block	15
66.249.64.195	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.195	Block	15
184.105.247.196	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	15
176.13.3.180	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	15
85.93.91.84	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
62.219.163.248	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
37.23.249.41	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	15
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/milnet	Block	15
217.118.78.95	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/modules/mod_mapsapi/mod_mapsapi.php	Block	15
66.249.67.196	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	15
188.163.73.101	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	15
95.59.198.117	Kazakstan	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	15
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.131	Block	15
176.103.215.24	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/modules/mod_mapsgoogle/mod_mapsgoogle.php	Block	15
91.189.129.90	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/modules/mod_rssemailer/mod_rssemailer.php	Block	15
82.80.28.123	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	15
157.55.39.142	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	15
66.249.93.139	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	15
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17396.jpg	Block	15
2.54.150.167	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/personaldetails	Block	15
109.124.3.241	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	15
93.159.219.35	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	15
66.249.64.195	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus×• ×'×—×¨×•	Block	15
66.199.231.242	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/chinuch/klali/	None	15
37.23.249.41	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/modules/mod_media_style/mod_media_style.php	Block	15
141.0.13.136	Norway	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	15
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/2414.jpg	Block	15