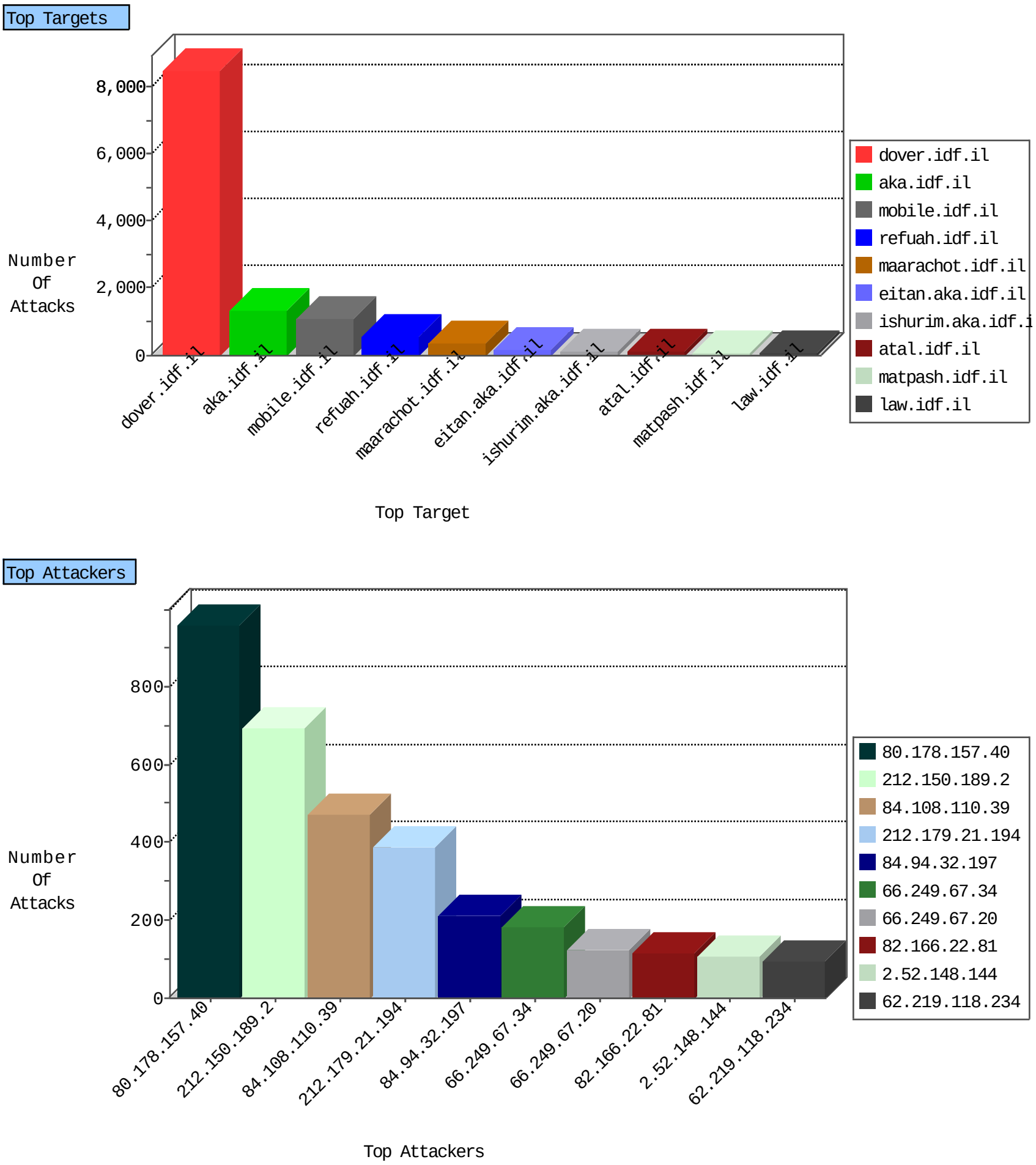
10-29-2015-10:04:04 to 10-29-2015-11:04:04

IDF Under Attack
Daily Report



10-29-2015-10:04:04 to 10-29-2015-11:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	11752
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	10012
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1571
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	1263
66.249.69.85	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	762
66.249.64.200	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	615
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	396
37.26.146.214	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	288
195.93.246.159	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	240
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	80
109.64.26.204	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	73
84.229.198.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
109.66.167.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
109.64.100.60	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	33
79.181.15.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
46.19.85.232	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	30
192.114.91.231	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
46.120.219.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
212.76.122.227	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
80.246.137.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
80.246.139.123	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
46.19.86.210	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	20
80.246.139.149	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
2.54.185.83	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
2.54.17.207	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
2.54.139.25	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
2.54.57.65	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
66.249.67.210	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	16
100.100.64.207		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
2.54.135.30	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
82.81.11.187	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
192.114.23.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
46.19.85.111	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
10.0.0.4		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
2.54.59.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
80.246.137.53	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
46.19.86.190	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 unverified cookie	drop	10
46.19.85.82	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
212.150.189.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
46.19.86.111	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
2.54.163.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
132.65.125.111	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
37.26.146.140	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
2.54.25.91	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	9
79.182.146.54	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	9
2.54.131.50	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9

10-29-2015-10:04:04 to 10-29-2015-11:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.9.134	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
84.108.110.39	Israel	147.237.76.42	refuah.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	16
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
198.20.69.74	United States	147.237.76.198	e.yohalan.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
81.218.33.77	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-29-2015-10:04:04 to 10-29-2015-11:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
192.198.151.45	147.237.72.167	Europe	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
46.19.85.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.219.67.177	147.237.0.200	Iran, Islamic Republic of	m4u.idf.il	ET SCAN NMAP -f -sS	1
2.54.11.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.117.156.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.36.62	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.76.198	United States	e.yohalan.idf.il	ET DROP Dshield Block Listed Source	1
192.116.149.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.138.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.73.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.108.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.219.67.177	147.237.0.200	Iran, Islamic Republic of	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
5.22.129.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.227.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.190.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.102.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.106.227.93	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
81.218.40.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1

10-29-2015-10:04:04 to 10-29-2015-11:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.150.189.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	681
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	334
84.94.32.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	210
2.52.148.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
62.219.118.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
46.19.86.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
213.57.42.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
62.219.232.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
82.81.11.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
212.199.57.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
46.19.85.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
37.142.106.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	57
79.183.12.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
2.54.27.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
87.255.31.90	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
195.93.246.159	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
2.54.57.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
46.19.85.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
212.179.90.106	Israel	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	46
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
5.29.108.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
79.179.104.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
176.12.144.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
212.179.46.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
213.8.241.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
212.199.69.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
2.54.14.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
2.54.163.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
79.181.166.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.120.219.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
37.26.148.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
95.149.0.6	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
46.116.75.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
109.64.2.20	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
192.114.91.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
46.19.85.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
46.19.86.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
37.26.146.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
79.181.125.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28

10-29-2015-10:04:04 to 10-29-2015-11:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.178.157.40	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	930
84.108.110.39	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	225
84.108.110.39	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/images/shared/green_tri_left.gif	Block	225
82.166.22.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	75
66.249.81.217	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	75
2.52.4.97	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	45
46.19.85.67	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	45
66.249.81.220	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	45
66.249.81.223	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	45
80.178.157.40	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	30
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/milnet	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
87.69.189.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash/home/home.asp	Block	30
66.249.64.195	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
79.180.228.10	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	30
89.138.84.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	30
79.180.228.10	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	30
77.125.12.22	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/forms.aspx	Block	30
46.19.85.31	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version deflate, sdch	Block	15
188.165.15.241	France	147.237.72.166	aka.idf.il	Unknown Parameter DocID in www.aka.idf.il/giyus/atuda/	None	15
79.180.139.115	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
94.25.132.49	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.law.idf.il/327-en/patzar.aspx	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	15
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
46.120.159.25	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	15
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/size220x0/17329.jpg	Block	15
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	15
31.168.180.13	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	15
157.55.39.39	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	15
87.69.160.97	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	15
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1275-he/atal.aspx	Block	15
80.246.136.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/ 	Block	15
46.19.85.31	Israel	147.237.76.42	refuah.idf.il	Malformed URL gzip,	Block	15
192.114.23.210	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	15
79.180.139.115	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/catalog.asp	Block	15
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	15
82.166.22.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	15
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/home/default.aspx	Block	15
209.88.157.45	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	15
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	15
157.55.39.247	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	15
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1273-he/atal.aspx	Block	15
80.246.136.228	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	15
46.19.85.31	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method : in URL gzip,	Block	15
193.106.52.34	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	15
2.54.10.199	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	15
141.212.122.64	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /x	Block	15
66.249.67.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	15

10-29-2015-10:04:04 to 10-29-2015-11:04:04