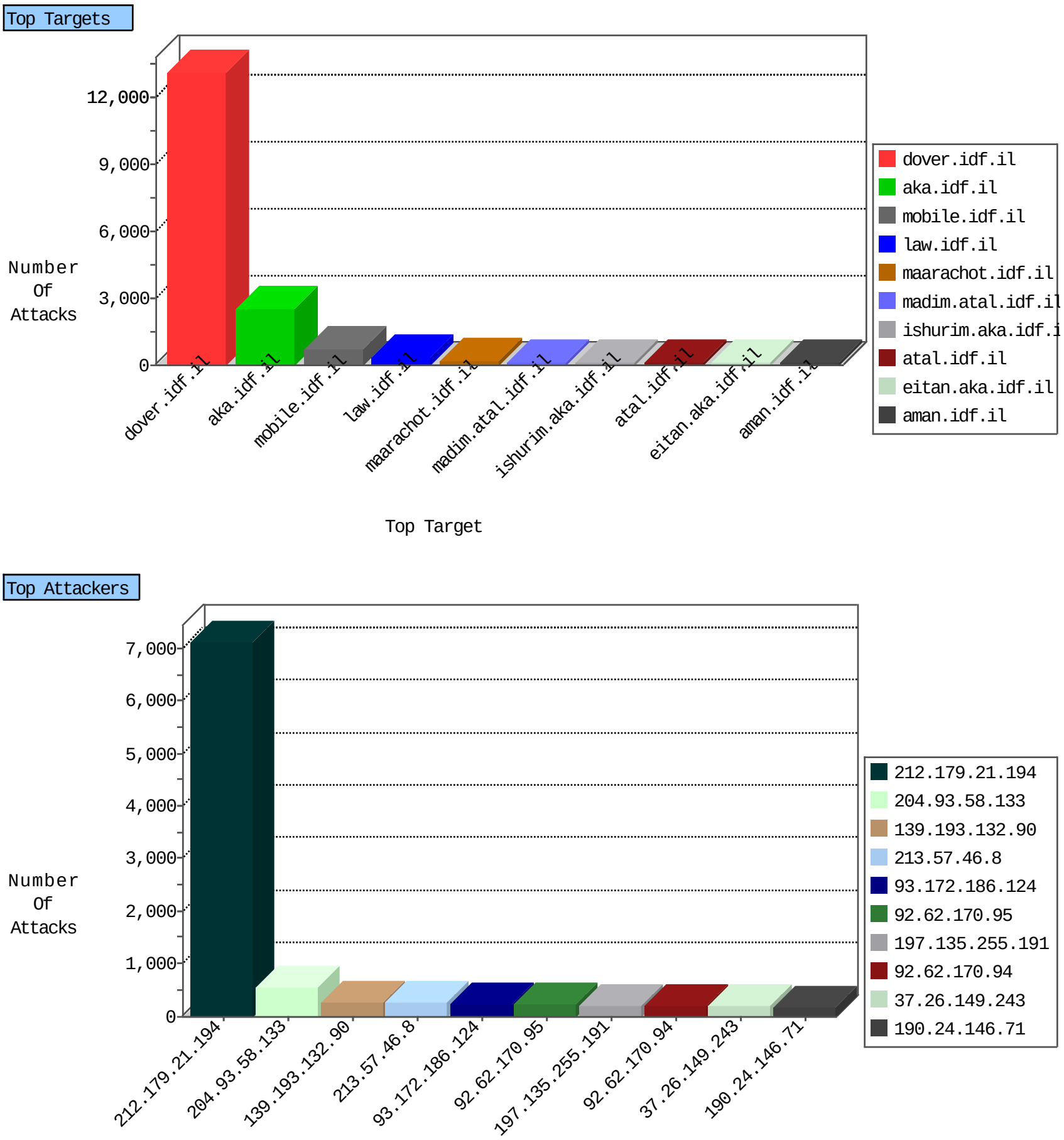
10-29-2015-15:04:05 to 10-29-2015-16:04:05

IDF Under Attack Daily Report



10-29-2015-15:04:05 to 10-29-2015-16:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1416
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	545
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	308
66.249.69.34	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	243
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	159
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	67
5.29.161.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	42
46.19.85.45	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	33
84.108.246.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	32
84.108.74.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
132.65.251.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
93.172.186.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	26
212.235.116.69	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
2.54.149.22	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
80.246.139.158	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	22
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	19
2.52.159.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
46.19.85.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
66.249.67.202	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	13
85.130.219.89	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.13.4.230	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
194.90.83.233	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.179.210.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.178.61.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
66.249.69.77	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	6
217.194.199.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
46.19.85.7	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
132.65.251.130	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
2.52.47.19	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
212.235.113.234	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
31.168.171.81	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.18.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
66.249.75.60	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5
46.19.85.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.9.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
78.160.189.5	Turkey	147.237.72.166	aka.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
213.57.46.8	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
109.64.213.89	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.64.213.89	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
46.19.85.234	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
5.102.214.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.85	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
87.68.156.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.76.107.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.234	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
149.78.224.228	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.26.146.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.235.113.234	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
66.102.8.237	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3

10-29-2015-15:04:05 to 10-29-2015-16:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.179.19.55	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
81.110.84.149	United Kingdom	147.237.77.74	law.idf.il	C1000106: HTTP: majestic bot	Block	1
216.221.146.186	United States	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
78.160.189.5	Turkey	147.237.72.166	aka.idf.il	10767: HTTP: Acunetix Security Scanner	Block	1

10-29-2015-15:04:05 to 10-29-2015-16:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.84	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
185.32.179.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.53.247.3	147.237.8.14	Macau	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
128.199.95.16	147.237.72.166	Singapore	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
84.229.30.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.60	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
210.211.99.242	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
176.12.145.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.116.239	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.35.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.97.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.27	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
66.249.64.55	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.59.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.101.186.159	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1

10-29-2015-15:04:05 to 10-29-2015-16:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7092
204.93.58.133	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	552
213.57.46.8	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	254
92.62.170.95	Lebanon	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	224
197.135.255.191	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	214
92.62.170.94	Lebanon	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	202
190.24.146.71	Colombia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	165
85.17.24.66	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	165
92.62.170.83	Lebanon	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	160
110.168.33.117	Thailand	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	130
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	84
46.19.85.45	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	78
79.183.11.174	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	74
46.19.85.7	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	72
64.233.172.171	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	71
64.233.172.155	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	66
192.38.10.38	Denmark	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
46.19.85.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	54
31.154.169.41	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
212.179.28.215	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
2.52.159.37	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
100.100.51.107		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	45
94.159.228.136	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
46.19.85.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
64.233.172.163	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
100.100.3.186		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	39
54.244.22.103	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
109.64.213.89	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
84.228.70.123	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
46.19.85.162	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
156.184.112.136		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
31.168.171.81	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
93.172.186.124	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
2.54.149.22	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
46.19.86.123	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
79.181.108.212	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
84.108.246.120	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
5.29.161.162	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
79.181.137.114	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
97.78.183.46	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
213.57.88.74	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
151.80.31.112	Italy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
176.13.4.230	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24

10-29-2015-15:04:05 to 10-29-2015-16:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.243	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	195
139.193.132.90	Indonesia	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Header Value from 139.193.132.90	Block	125
139.193.132.90	Indonesia	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in Header Value from 139.193.132.90	Block	121
46.19.85.133	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	90
176.13.4.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	75
213.8.90.204	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/ajax/updatestatus.php	Block	60
93.172.186.124	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/ajax/updatestatus.php	Block	60
46.19.85.156	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	60
149.88.136.175	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	60
149.88.136.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	60
213.8.90.204	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	60
93.172.186.124	Israel	147.237.0.19	madim.atal.idf.il	PHP Attempt	Block	60
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	45
176.13.18.114	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	45
176.13.3.106	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
64.41.200.104	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.104 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	45
176.13.5.47	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	45
66.249.64.195	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.195	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
79.178.175.207	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	30
213.8.91.133	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	30
93.172.186.124	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	30
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	30
193.169.70.108	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	30
66.249.93.208	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
93.172.186.124	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	30
66.249.93.212	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
46.19.86.170	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	30
81.218.163.76	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/61192.pdfÂ	Block	30
37.142.195.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	30
66.249.64.200	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.200	Block	30
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	30
79.178.175.207	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	30
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international-training	Block	15
128.199.95.16	Singapore	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/l27.zip	Block	15
199.203.215.1	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	15
2.54.130.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
79.182.219.59	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	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
176.12.151.18	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
149.78.10.14	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	15
37.26.149.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
109.66.143.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.64.233	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	15
212.143.138.230	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	15
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/mailthis.gif	Block	15
64.41.200.104	United States	147.237.77.243	mobile.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.104 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	15
157.55.39.148	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/iturim/asp/displayonesoldier.asp	None	15
66.249.79.119	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1777	Block	15

10-29-2015-15:04:05 to 10-29-2015-16:04:05