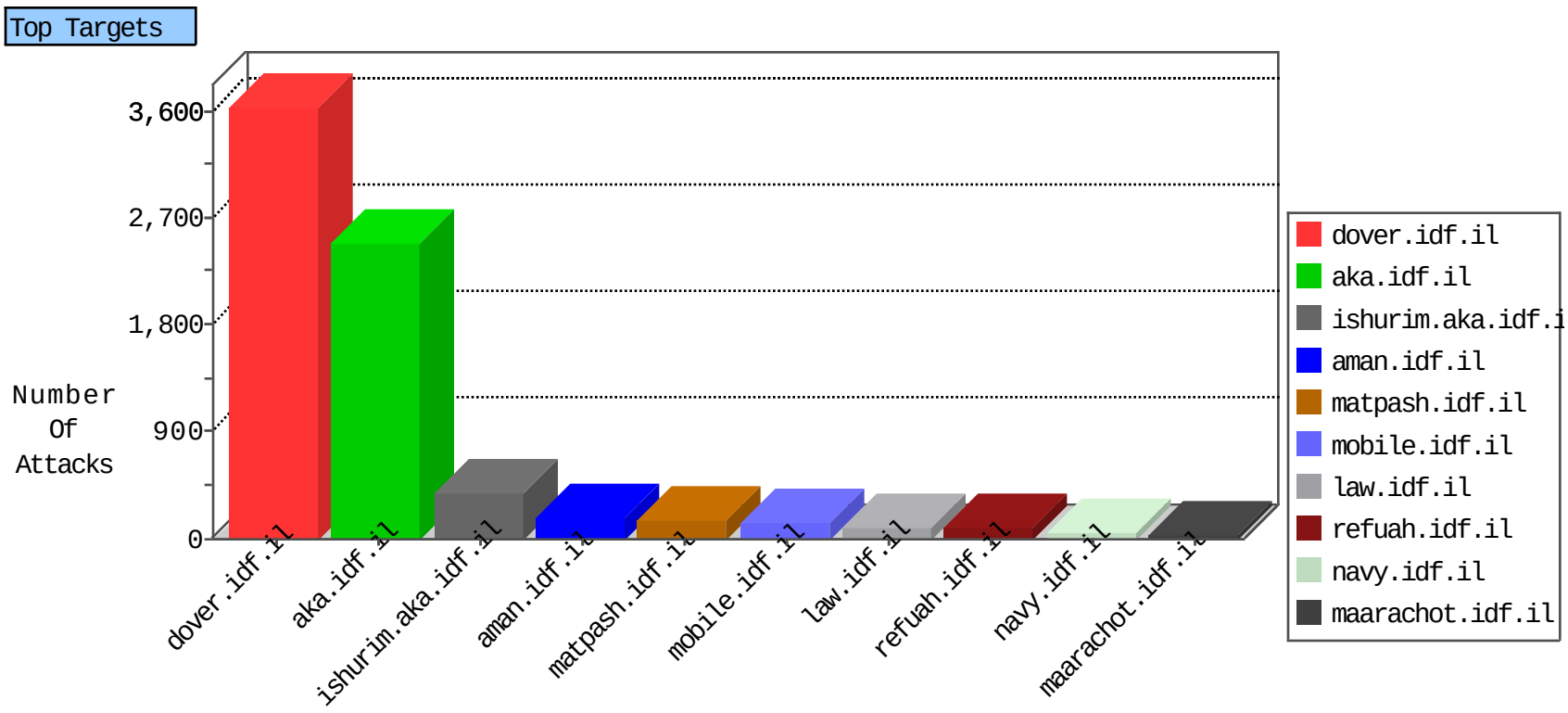
10-26-2015-16:04:06 to 10-26-2015-17:04:06

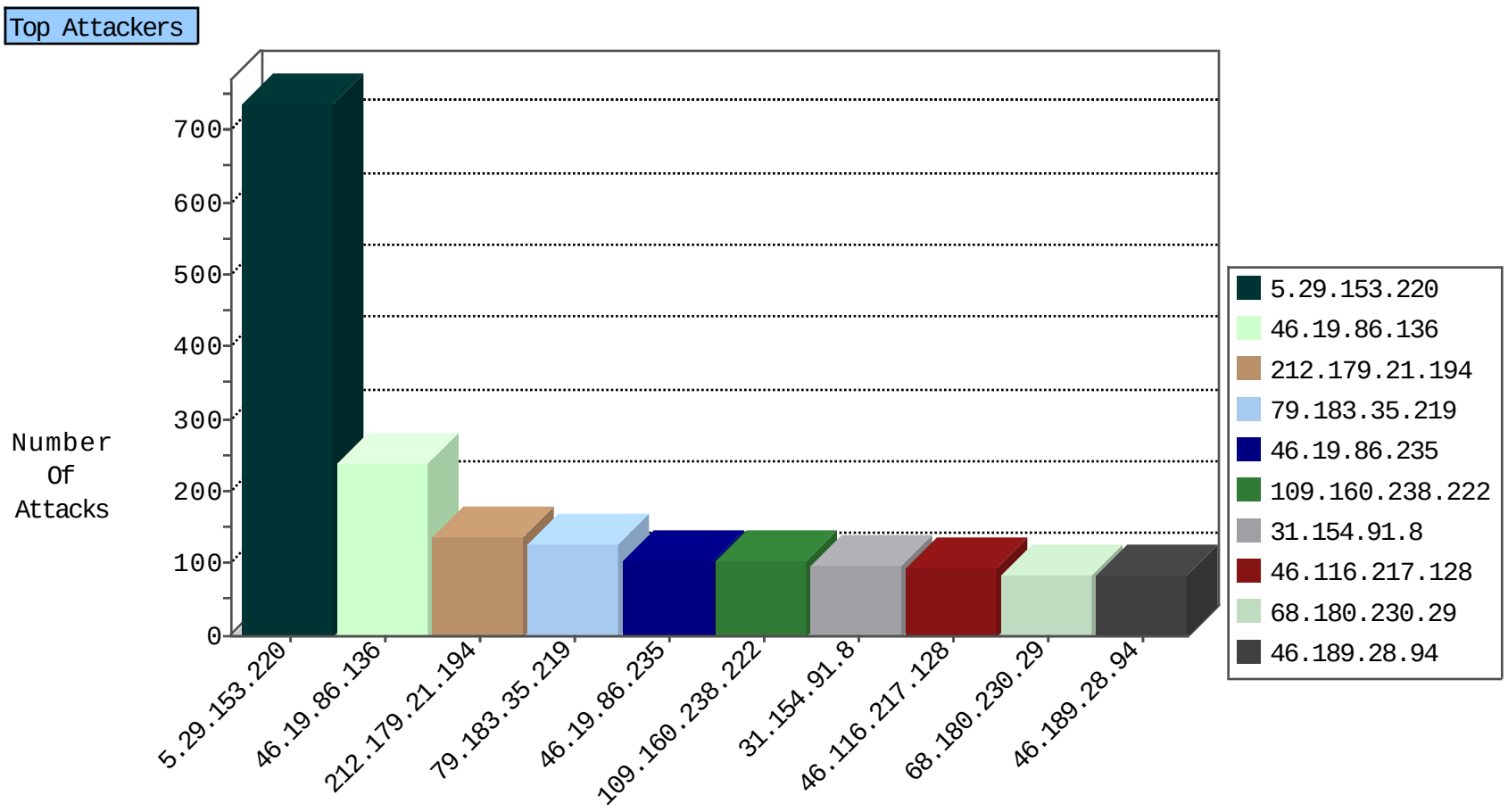
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-26-2015-16:04:06 to 10-26-2015-17:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3623
5.29.153.220	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	3578
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	518
46.19.85.231	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	170
79.177.118.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	52
185.32.179.87	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	39
89.138.247.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
2.54.182.182	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	32
79.178.102.151	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
212.143.231.38	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
79.181.198.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
98.248.47.127	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
212.179.57.174	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
46.19.85.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
188.122.86.211	Netherlands	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
62.90.131.82	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
212.179.147.178	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
84.228.11.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
5.29.182.51	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
37.26.146.177	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
87.68.49.114	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
77.125.150.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.121.159.4	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
80.246.139.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
81.218.208.46	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
109.186.141.191	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
2.54.182.182	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
80.56.30.232	Netherlands	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
89.139.22.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.65.126.221	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.19.85.155	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
176.13.20.193	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.121.29.35	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
185.32.179.9	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
67.194.236.234	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
109.64.183.213	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
176.13.13.213	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
194.9.253.238	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
5.22.131.228	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.111.126.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.32.179.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
62.219.190.26	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
132.70.66.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
5.28.138.9	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.10.165	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.106.226.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.121.29.35	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
46.19.85.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5

10-26-2015-16:04:06 to 10-26-2015-17:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
203.171.41.47	New Zealand	147.237.77.74	law.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	20
50.59.103.190	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
98.19.222.133	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
81.218.198.54	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
89.148.240.68	Russian Federation	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
178.94.229.176	Ukraine	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
97.88.205.32	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
98.19.222.133	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1

10-26-2015-16:04:06 to 10-26-2015-17:04:06

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	22
98.19.222.133	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	5
77.127.153.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
84.110.110.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.247.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.17.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.166.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.159	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.131.132	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

10-26-2015-16:04:06 to 10-26-2015-17:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.86.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
109.160.238.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
46.19.86.235	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
46.116.217.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	90
46.189.28.94	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
159.53.46.141	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
132.74.58.90	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	66
46.19.85.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
46.19.86.136	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
46.19.85.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
82.81.17.28	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
93.172.109.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
37.142.197.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	50
46.19.86.190	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
46.19.86.214	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
46.19.86.111	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
5.29.196.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
12.148.2.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
79.179.175.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
100.100.85.101		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
100.100.111.121		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
37.142.165.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	37
31.154.234.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
70.197.227.113	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
212.179.147.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.102.8.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
81.218.130.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
46.116.145.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
194.9.253.238	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.54.182.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
95.86.112.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
80.179.23.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
109.66.147.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.181.198.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.26.149.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
79.177.108.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.102.8.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
185.32.179.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.102.8.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
79.178.102.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.102.8.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
176.106.226.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
147.235.236.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
195.239.199.146	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21

10-26-2015-16:04:06 to 10-26-2015-17:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.35.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.183.35.219	Block	112
31.154.91.8	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.154.91.8	Block	84
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	84
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
80.246.136.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
201.141.134.66	Mexico	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	28
84.109.1.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
79.176.57.158	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	28
213.57.224.151	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	28
46.19.85.16	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	28
80.74.101.7	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	28
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/band	Block	14
147.235.236.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	14
46.19.85.133	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
89.138.237.125	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7	Block	14
213.57.34.82	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
181.225.231.173	Cuba	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	14
67.212.175.138	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/yohalan/main/main.asp	Block	14
109.186.185.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl07.x in www.aka.idf.il/main/sachar/payslips.aspx	None	14
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/mainfs.asp	Block	14
77.127.147.244	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	14
149.78.43.146	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	14
46.19.85.151	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	14
94.73.145.90	Turkey	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	14
79.183.35.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	14
213.57.199.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	14
188.138.1.218	Germany	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
109.186.185.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl39.x in www.aka.idf.il/main/sachar/payslips.aspx	None	14
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
31.154.91.8	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	14
207.46.13.83	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/unitfs.asp	Block	14
176.12.136.170	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	14
94.73.145.90	Turkey	147.237.72.166	aka.idf.il	Multiple signatures from 94.73.145.90	Block	14
46.19.85.232	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	14
80.74.101.7	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.74.101.7	Block	14
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8687-he/refuah.aspx	Block	14
109.186.185.87	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20236-he/idfgdover.aspx	Block	14
84.109.113.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
79.176.159.144	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	14
178.62.209.185	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/getfile/getfile.aspx?filename=xhbyb3nly3v0aw9ulwrvy3ncyxzpcm90x3nhbwltxgktmtu4ltaylnbkzg==&infocenteritem=true	Block	14
99.238.130.114	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash/login/default.asp	Block	14
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	14
188.165.15.241	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/list.asp	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
132.74.58.90	Israel	147.237.72.156	aman.idf.il	XSS - Basic 3	Block	14

10-26-2015-16:04:06 to 10-26-2015-17:04:06