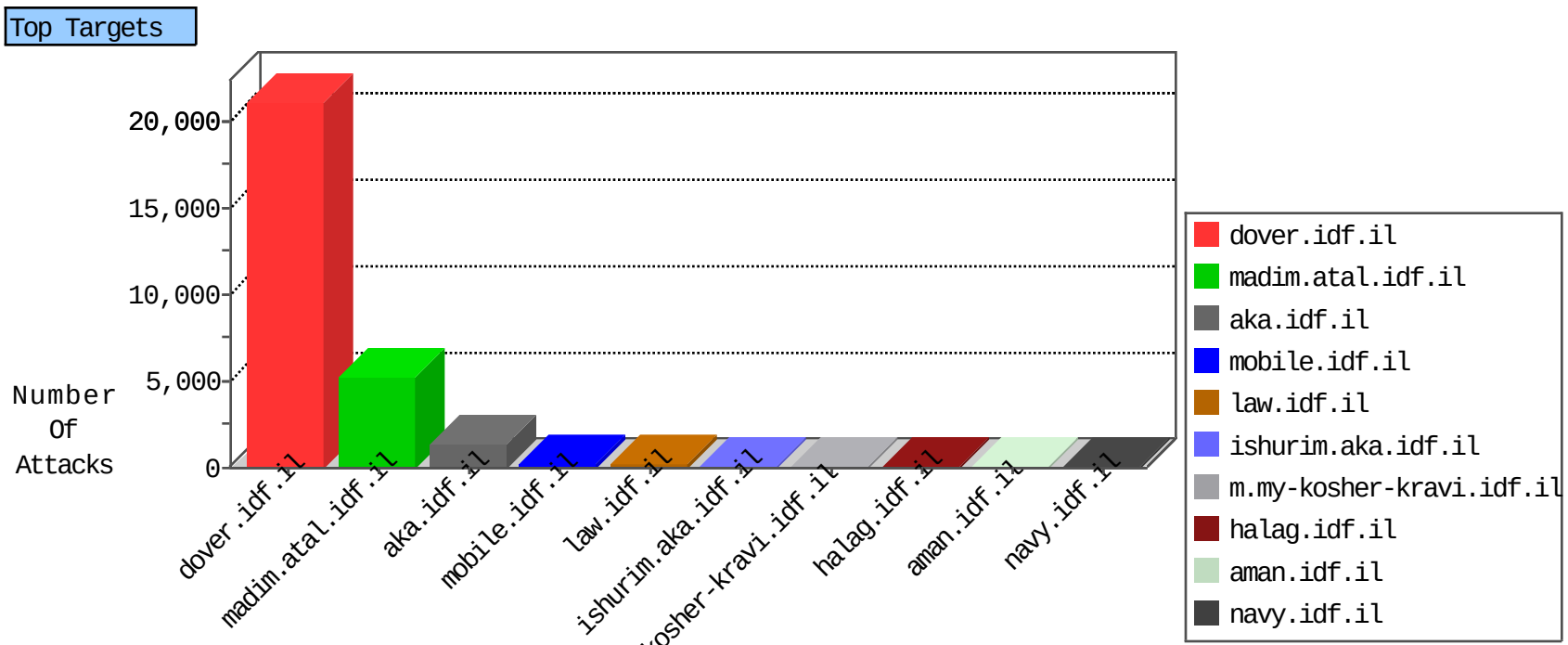
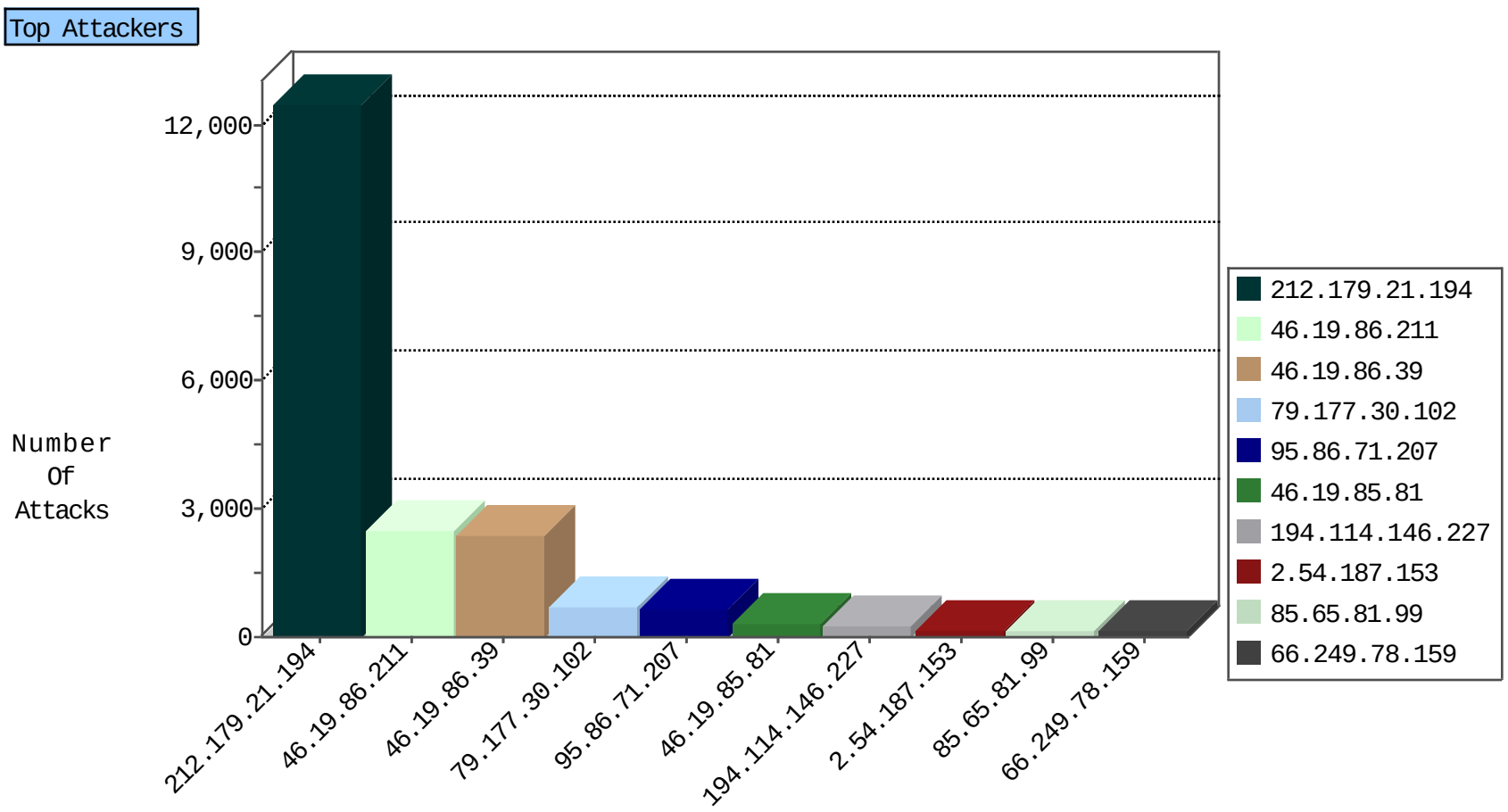
10-18-2015-17:04:00 to 10-18-2015-18:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-18-2015-17:04:00 to 10-18-2015-18:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2785
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	611
2.54.36.35	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	89
109.66.21.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	42
193.17.74.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
93.173.250.183	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
5.29.89.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	21
109.67.207.201	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
37.26.148.215	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
176.12.145.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
79.183.229.209	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
46.121.68.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
79.180.195.252	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
2.54.180.105	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
176.106.227.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
89.139.163.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
84.39.5.250	Netherlands	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
109.64.163.136	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
46.19.85.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
46.19.86.237	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
79.177.229.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
2.54.11.68	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
91.208.129.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.179.98.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
87.68.151.56	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
46.19.86.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
87.68.151.56	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
46.19.86.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
37.26.149.193	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	7
37.26.146.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
85.65.167.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
213.8.58.170	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
109.65.212.251	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
37.26.149.193	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
82.145.211.94	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
79.183.226.55	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
2.54.57.19	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
84.228.225.161	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.19.85.210	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
46.121.118.82	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.228.213.33	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
85.64.224.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.139.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.228.225.161	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	6
109.67.4.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.177.60	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
80.178.189.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
195.228.141.162	Hungary	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.65.181.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.53.252	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.16	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.94.165.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5

10-18-2015-17:04:00 to 10-18-2015-18:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.86.100.253	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.120.170.50	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-18-2015-17:04:00 to 10-18-2015-18:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
139.162.155.48	147.237.8.46	Netherlands	e.chinuch.idf.i	ET SCAN Potential SSH Scan	1
37.26.149.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.184.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.129.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.71.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.154.8.76	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.166	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.159.103	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
197.44.62.78	147.237.77.235	Egypt	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.85.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.160.178.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.4.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.69.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.173.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.214.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
197.44.62.78	147.237.77.235	Egypt	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

10-18-2015-17:04:00 to 10-18-2015-18:04:00

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.il	drop	First packet isn't SYN	drop	12450
79.177.30.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	693
95.86.71.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	645
2.54.187.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	166
46.19.85.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
46.19.85.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
37.26.149.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
66.102.8.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
2.54.61.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
79.178.61.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
46.19.86.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
46.19.85.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.102.8.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
87.68.151.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
212.26.4.140	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
66.102.8.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
46.19.85.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
84.108.33.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
66.249.78.166	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
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	43
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
62.219.244.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
100.100.77.1		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	40
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
46.19.86.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
46.19.86.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
94.230.86.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
2.54.180.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
5.28.157.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	37
46.19.86.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
176.12.144.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
2.54.168.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
199.203.123.201	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	34
46.19.86.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
62.219.160.128	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
37.26.149.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
194.114.146.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
86.140.2.124	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
79.182.147.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
204.93.58.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.54.46.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2368
46.19.86.211	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.211	Block	2065
46.19.86.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	410
46.19.85.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	316
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	234
85.65.81.99	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.81.99	Block	143
93.172.149.54	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	39
87.69.87.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Parameter Type Violation on m.my-kosher-kravi.idf.il/templates/training/training.aspx parameter ctl00$ContentPlaceHolder1$txtAreaRemarks	Block	39
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	39
204.12.251.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	39
162.144.98.244	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	39
162.144.98.244	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.php	Block	26
85.250.88.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	26
62.128.48.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	26
79.177.147.96	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	26
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	26
79.183.145.90	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	26
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
149.78.94.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	26
109.66.146.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	26
85.64.254.77	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 85.64.254.77	Block	13
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	13
46.116.154.53	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	13
84.94.37.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
5.29.26.12	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	13
109.67.19.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
79.182.150.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
66.249.93.145	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx	Block	13
213.57.254.229	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	13
192.114.3.241	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1806.jpg	Block	13
84.111.227.100	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	13
80.179.22.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58609&docid=72568	Block	13
46.19.86.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
149.88.194.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
2.52.17.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
213.151.55.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
85.64.254.77	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	13
212.199.218.190	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	13
46.116.154.53	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.116.154.53	Block	13
173.252.73.117	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
84.108.17.71	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
37.142.138.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
109.67.155.152	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
77.125.121.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
213.57.254.229	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method [[#23]][[#3]][[#3]][[#3]][[#0]]()nÂˆÂ¡Â‡[[#27]]Â?Ã½2DÃ°QÃ¦Ã¶pÂ¥[[#22]]:?Â“Â…Ã?Ã?,GÃšÂ¡+pÂ?Ãƒ	Block	13
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	13
81.218.197.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
162.144.98.244	United States	147.237.77.74	law.idf.il	Admin Blocking	Block	13
2.52.53.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13