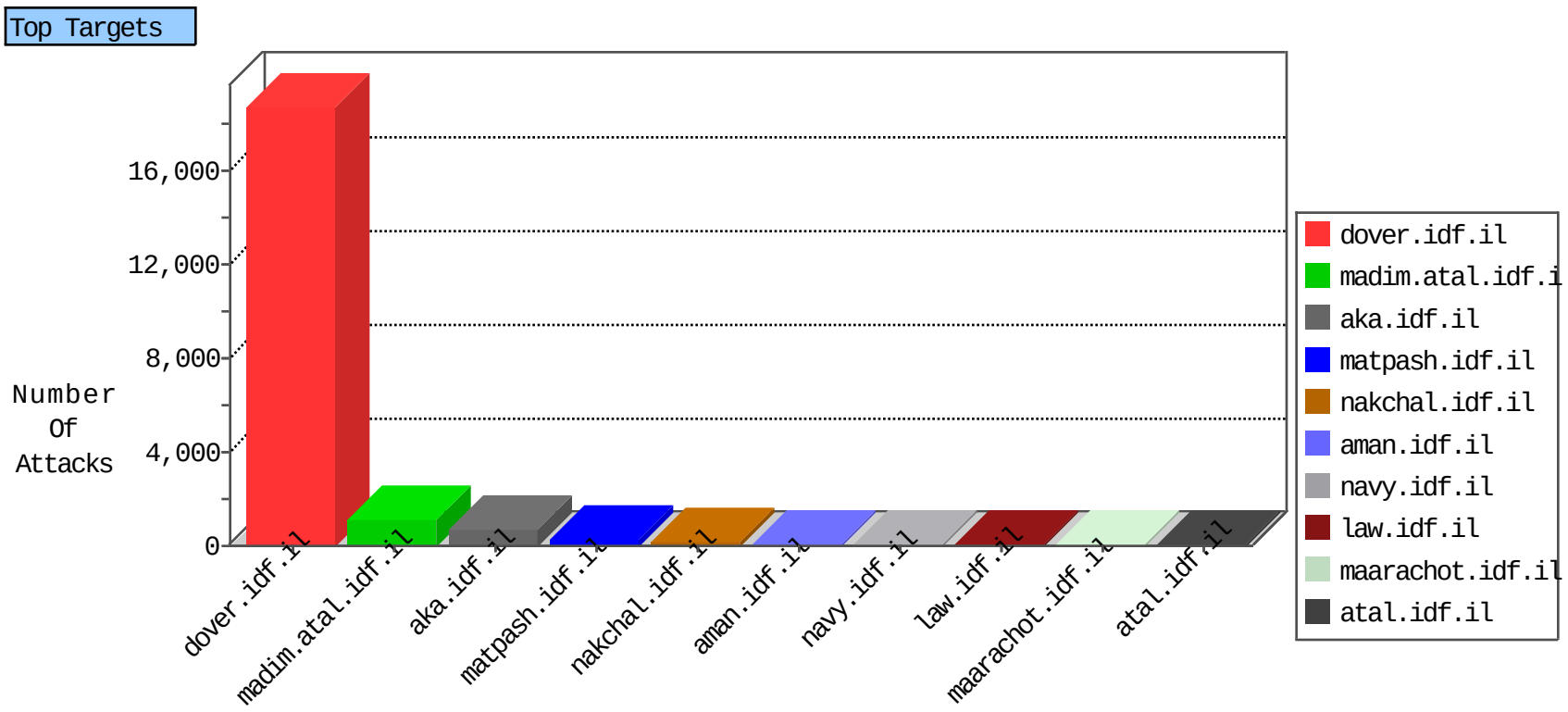
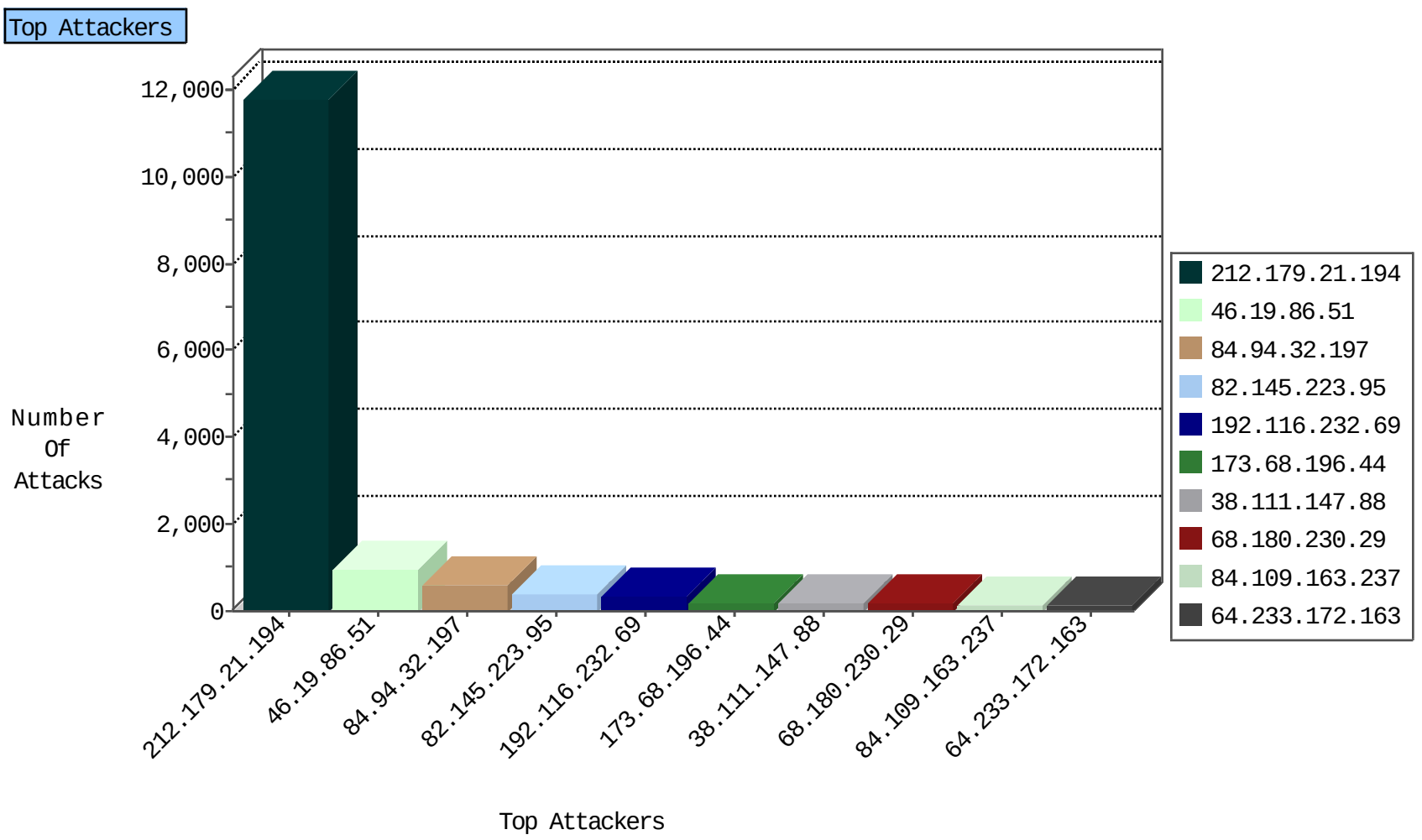
10-25-2015-17:04:01 to 10-25-2015-18:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-25-2015-17:04:01 to 10-25-2015-18:04:01

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.i	TCP handshake violation, first packet not syn	drop	2541
46.19.85.223	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
212.179.197.122	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	67
0.0.0.0		147.237.77.216	dover.idf.i	SYN Flood full table	drop	59
213.57.15.150	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	36
192.116.232.69	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	35
79.179.32.202	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	27
176.106.227.36	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	19
79.181.9.165	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	16
84.109.3.143	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	12
79.178.14.84	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	12
5.29.176.224	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	11
66.102.8.152	United States	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
212.179.21.194	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
79.180.22.197	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
46.19.86.18	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
149.88.127.27	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	8
213.57.15.150	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	8
65.189.12.158	United States	147.237.77.216	dover.idf.i	SYN Flood full table	drop	8
213.151.32.163	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	7
87.69.231.127	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
199.203.215.1	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
46.60.54.142	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
95.86.96.163	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
2.54.146.216	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
31.168.3.26	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
79.178.49.202	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
46.19.86.43	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	5
99.226.181.87	Canada	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
46.19.86.51	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
93.172.137.17	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
46.19.85.247	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
37.142.129.106	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
67.83.76.38	United States	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
46.116.226.75	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
149.78.41.25	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
176.13.22.156	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	3
79.177.29.165	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	3
192.118.132.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
95.86.121.65	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	3
192.117.138.210	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	2
84.94.66.27	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	2
37.26.147.239	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	2
80.246.136.190	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	2
107.77.160.19	United States	147.237.77.216	dover.idf.i	SYN Flood full table	drop	2
192.116.108.151	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	2
85.250.139.231	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	2
38.111.147.88	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2
46.19.85.239	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	2

10-25-2015-17:04:01 to 10-25-2015-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
96.224.6.115	United States	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

10-25-2015-17:04:01 to 10-25-2015-18:04:01

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	4
66.249.67.59	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
82.80.147.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.151.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.53	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
61.182.170.38	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
52.21.145.242	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
109.67.141.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.12.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.33.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.182.170.38	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
59.106.108.116	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	1
50.87.144.145	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.15.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.108.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

10-25-2015-17:04:01 to 10-25-2015-18:04:01

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	11794
84.94.32.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	577
82.145.223.95	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	402
173.68.196.44	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	201
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	181
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	123
46.19.86.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
149.255.232.16	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
77.126.213.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
177.32.176.138	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
82.166.37.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
79.177.10.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
69.125.162.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
79.181.24.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
79.18.240.254	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
89.13.1.19	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
5.102.254.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
2.54.184.0	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
185.33.169.99	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
81.218.251.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
46.210.162.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
192.117.138.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
192.117.138.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
2.54.176.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
66.102.8.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
108.233.242.170	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
66.102.8.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
109.222.72.70	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
2.54.10.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
66.249.67.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
2.54.14.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
85.250.139.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
199.221.15.225	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
213.57.15.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
93.172.137.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.102.7.226	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.102.7.240	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
81.184.114.204	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
164.138.125.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	952
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	280
84.109.163.237	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	126
79.182.25.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	112
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2061-he/cogat.aspx	Block	84
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	84
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	82
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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1111-he/nakhal.aspx	Block	28
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	28
176.13.23.178	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1072-he/nakhal.aspx	Block	28
212.235.31.125	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	28
198.204.249.34	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	28
46.60.54.142	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	28
212.199.84.42	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/14-he/patzar.aspx	Block	25
176.10.104.234	Switzerland	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	25
79.180.28.66	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14
66.249.69.33	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	14
176.13.23.182	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 119 cookies	Block	14
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Malformed URL __atuvs=562cf3f872fd368e000;	Block	14
46.117.135.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$passwordUpdate$txtPassword in www.aka.idf.il/main/giyus/faq.aspx	None	14
203.67.9.75	Taiwan	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method	Block	14
37.26.147.179	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	14
151.80.31.124	Italy	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	14
212.199.84.42	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/965-he/patzar.aspx	Block	14
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 0%2C0%7C41%2C0%7C42%2C1%7C43; in URL __atuvs=562cf3f872fd368e000	Block	14
2.52.156.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
85.65.77.232	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	14
46.121.102.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
203.67.9.75	Taiwan	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in Method	Block	14
37.142.68.108	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
81.209.177.189	Europe	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	14
212.235.31.125	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.235.31.125	Block	14
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/mailthis.gif	Block	14
46.19.86.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
2.54.54.243	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	14
109.65.159.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	14
79.177.149.33	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	14
203.67.9.75	Taiwan	147.237.77.74	law.idf.il	Illegal Byte Code Character in Method	Block	14
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	14
81.218.198.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
192.117.12.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/rabanut/scriptresource.axd	None	14
2.54.181.131	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
109.160.219.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
79.179.192.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in aka.idf.il/main/sachar/viewpniot.aspx	None	14
176.13.23.178	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1119-he/nakhal.aspx	Block	14
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_id.20.8afc=f5647cdeb6631c91.1433970942.3.1445786618.1445786618.; _pk_ses.20.8afc=*	Block	14