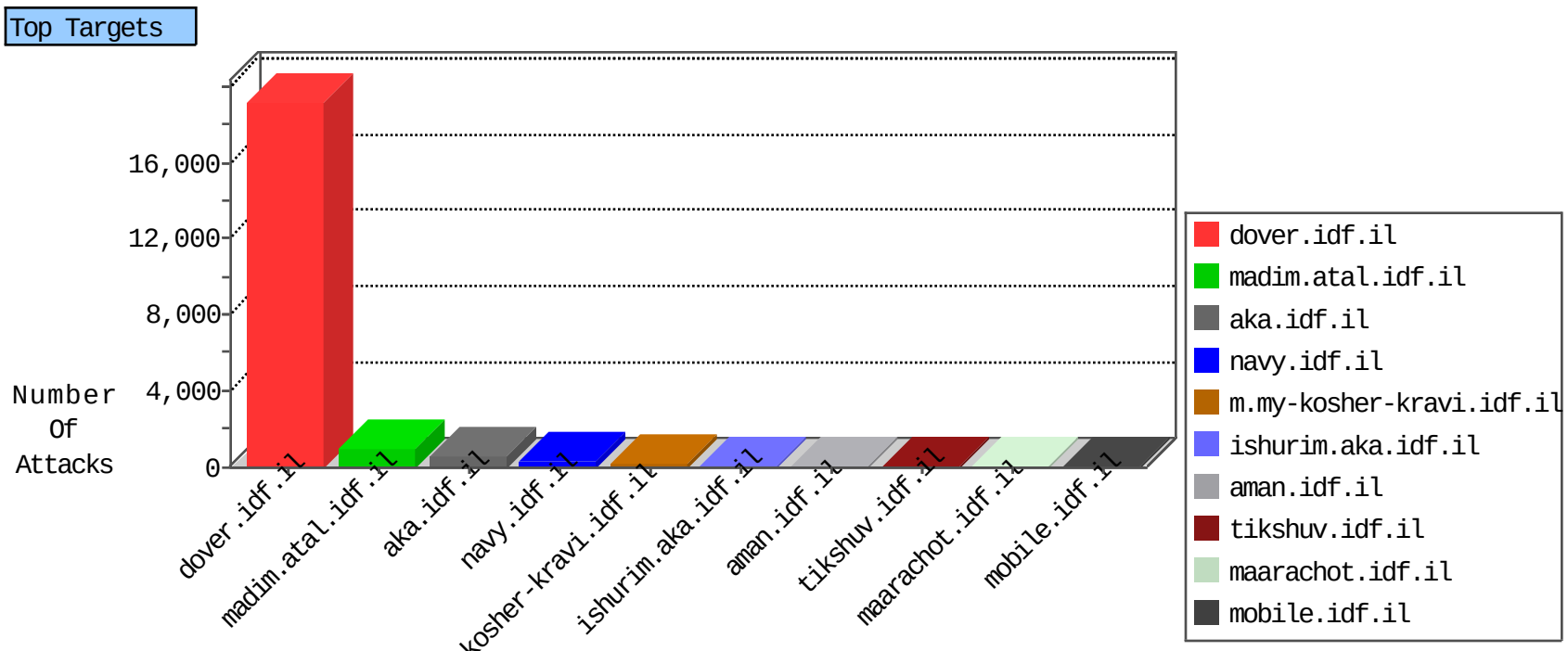
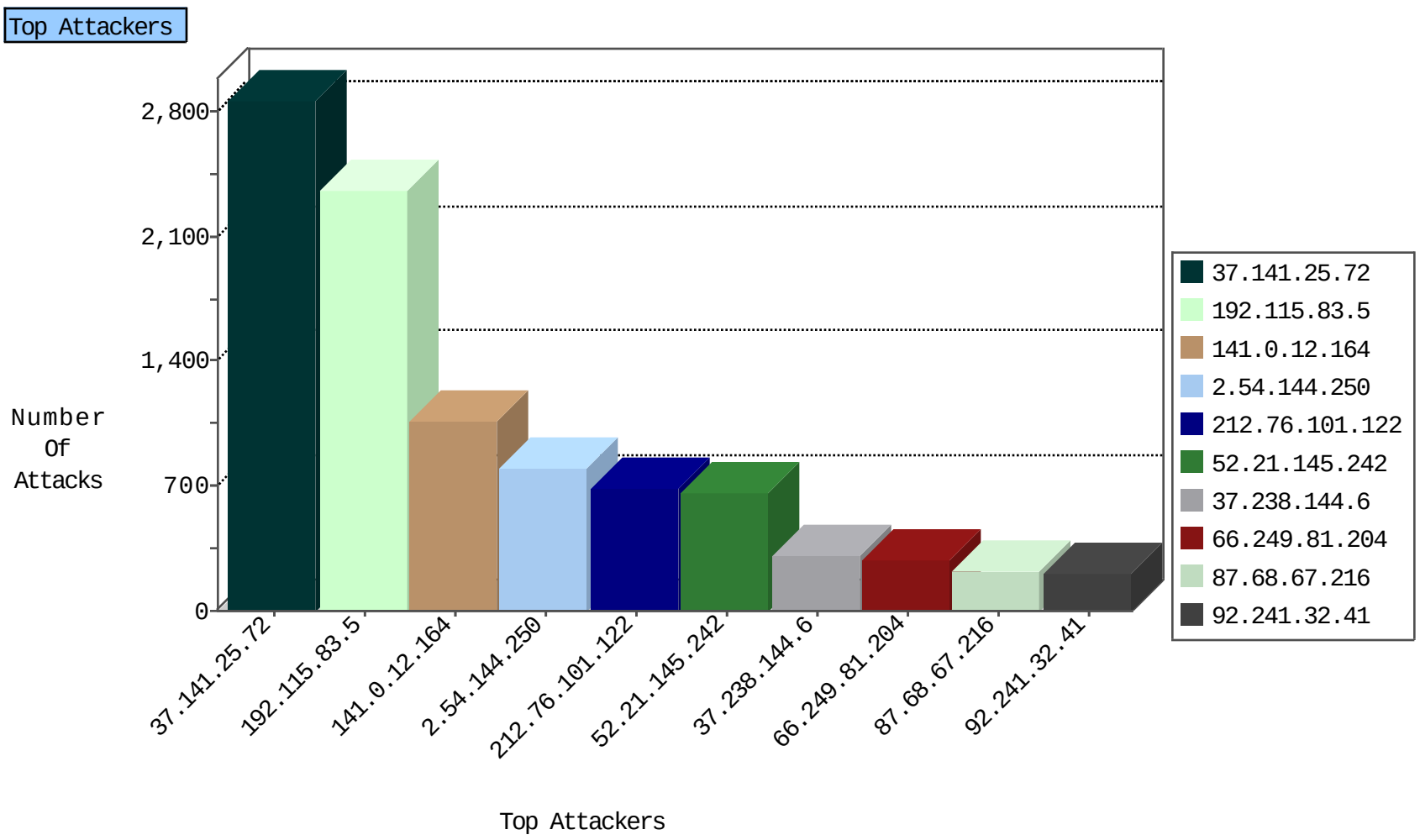
10-21-2015-10:04:00 to 10-21-2015-11:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-21-2015-10:04:00 to 10-21-2015-11:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	53
46.19.85.118	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	36
79.180.32.3	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	33
212.76.101.85	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
31.154.10.106	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
178.2.156.220	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
185.24.76.158	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
109.67.133.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
2.54.0.45	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	5
87.69.127.100	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
197.15.66.237	Tunisia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
209.88.198.1	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.178.66.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
86.46.127.45	Ireland	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
95.86.93.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.185.223	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
89.237.149.237	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.43.111.197	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.46	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
84.158.228.3	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.144.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.85.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
192.114.105.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.144.255	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.85.233	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
82.102.210.254	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.176	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
41.130.67.66	Egypt	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
85.64.126.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.186.141.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
82.205.41.63	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.150.11	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.141.25.72	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
130.193.254.122	Iraq	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
212.156.70.118	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.60.31.67	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
31.218.55.17	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.15.0	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
146.185.60.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
62.209.14.7	Bahrain	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.26.147.199	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	2
176.13.20.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
166.170.51.44	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
5.41.90.29	Romania	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.75.214.125	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
89.248.172.98	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
2.54.135.179	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
173.208.168.165	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
95.172.79.244	United Kingdom	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
196.219.224.69	Egypt	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-21-2015-10:04:00 to 10-21-2015-11:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.86.107.145	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
192.116.127.113	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
195.110.40.7	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
41.46.88.56	Egypt	147.237.77.216	dover.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	1
94.23.46.192	France	147.237.77.74	law.idf.il	C1000106: HTTP: majestic bot	Block	1

10-21-2015-10:04:00 to 10-21-2015-11:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.81.204	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	286
176.13.6.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.65.165.215	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
111.93.198.54	147.237.8.14	India	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
80.246.136.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.251.13.167	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.54.150.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.108.132.58	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.12.79	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.0.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
111.93.198.54	147.237.8.14	India	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
93.172.27.228	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.151.55.40	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.207.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.148.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.225.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-21-2015-10:04:00 to 10-21-2015-11:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.141.25.72	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2865
192.115.83.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2367
141.0.12.164	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1065
212.76.101.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	684
52.21.145.242	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	658
37.238.144.6	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	309
92.241.32.41	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	214
193.188.136.30	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	201
84.158.228.3	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	194
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	177
5.244.85.190	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	157
5.246.170.111	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	143
103.26.198.126	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	130
105.95.227.245	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	128
212.156.70.118	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	127
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	117
46.19.86.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
213.204.127.27	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
188.161.181.129	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	114
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	113
41.34.201.163	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
79.182.195.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	109
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
82.205.237.166	United Arab Emirates	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
89.34.235.222	Moldova, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
37.26.148.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
188.247.74.199	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
5.11.41.227	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
5.46.116.88	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
213.130.112.178	Qatar	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
81.10.98.241	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
46.19.85.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
37.8.84.205	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
109.84.3.192	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
46.19.85.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
87.6.58.140	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
80.12.59.28	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
149.88.27.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
31.223.176.62	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
138.134.102.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
77.125.147.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
105.47.210.41	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.144.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	800
87.68.67.216	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 87.68.67.216	None	164
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	143
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.200	Block	52
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	39
87.68.67.216	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Parameter Type Violation on m.my-kosher-kravi.idf.il/templates/login.aspx parameter ctl00$ContentPlaceHolder1$txtPassword	Block	39
91.90.191.135	Poland	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	26
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	26
212.150.215.254	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 212.150.215.254	Block	26
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.208	Block	26
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.192	Block	26
82.166.61.61	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	26
176.13.11.208	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Email in mobile.idf.il/sachar/createaccount	Block	26
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
2.54.143.87	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	25
199.203.100.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	13
46.19.85.153	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	13
137.226.113.7	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	13
2.54.9.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	13
85.65.224.4	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	13
69.58.178.58	United States	147.237.77.170	maarachot.idf.il	URL is Above Root Directory www.maarachot.idf.il/../	Block	13
217.194.207.24	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	13
66.249.64.249	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	13
176.28.17.231	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/old/wp-admin/	Block	13
24.228.80.141	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	13
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/	None	13
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/oref/	Block	13
46.19.85.153	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method sdch in URL	Block	13
85.250.110.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
79.180.194.213	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	13
184.105.247.196	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	13
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	13
91.198.47.105	Portugal	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp/wp-admin/	Block	13
37.26.146.226	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	13
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/main/home/default.aspx	None	13
46.19.86.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
147.236.113.1	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	13
2.54.144.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
80.179.10.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
192.116.200.220	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
109.65.182.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
37.26.148.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
212.150.215.254	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/111838.pdf	Block	13
66.249.67.253	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	13
87.68.67.216	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	13
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	13
199.203.100.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	13
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	13
109.66.179.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
37.128.186.113	United Kingdom	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/blog/wp-admin/	Block	13