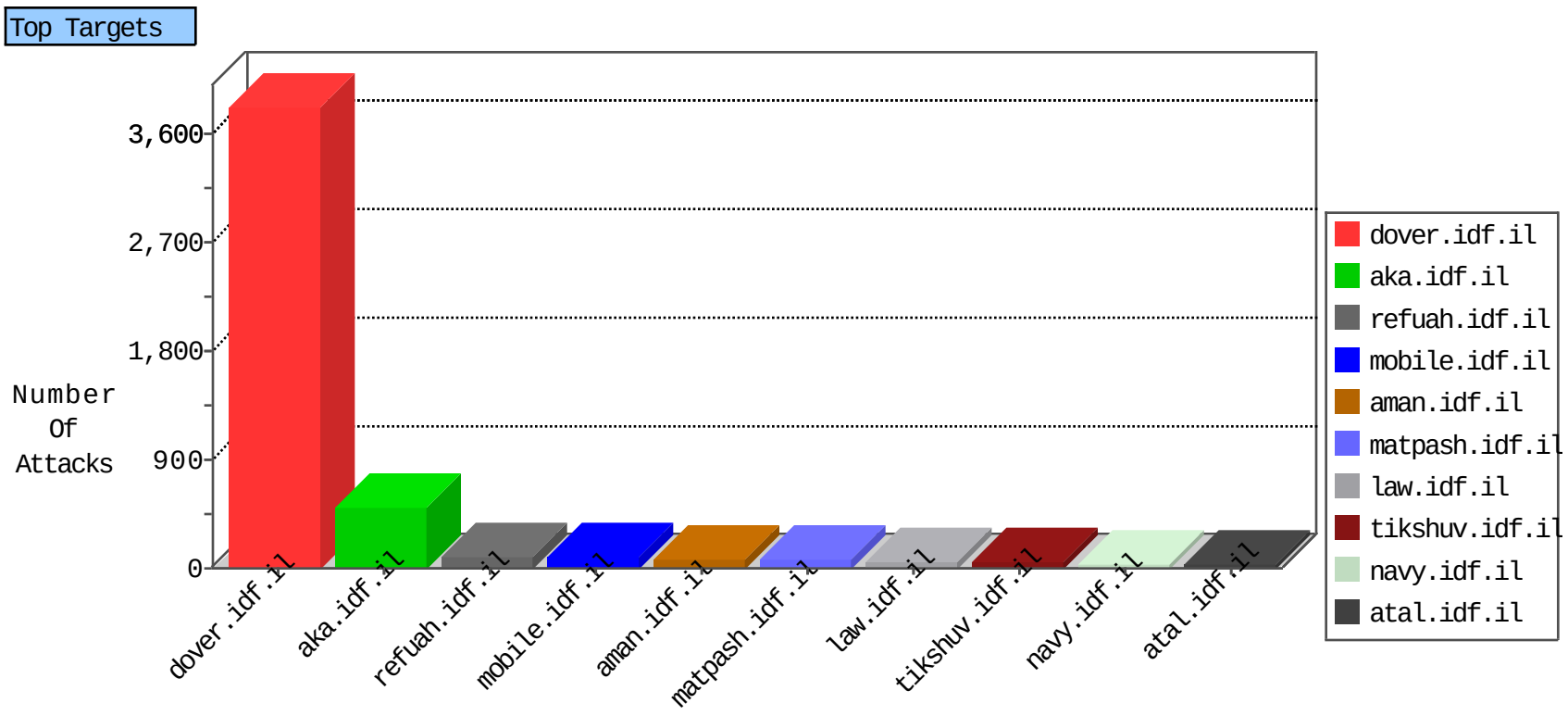
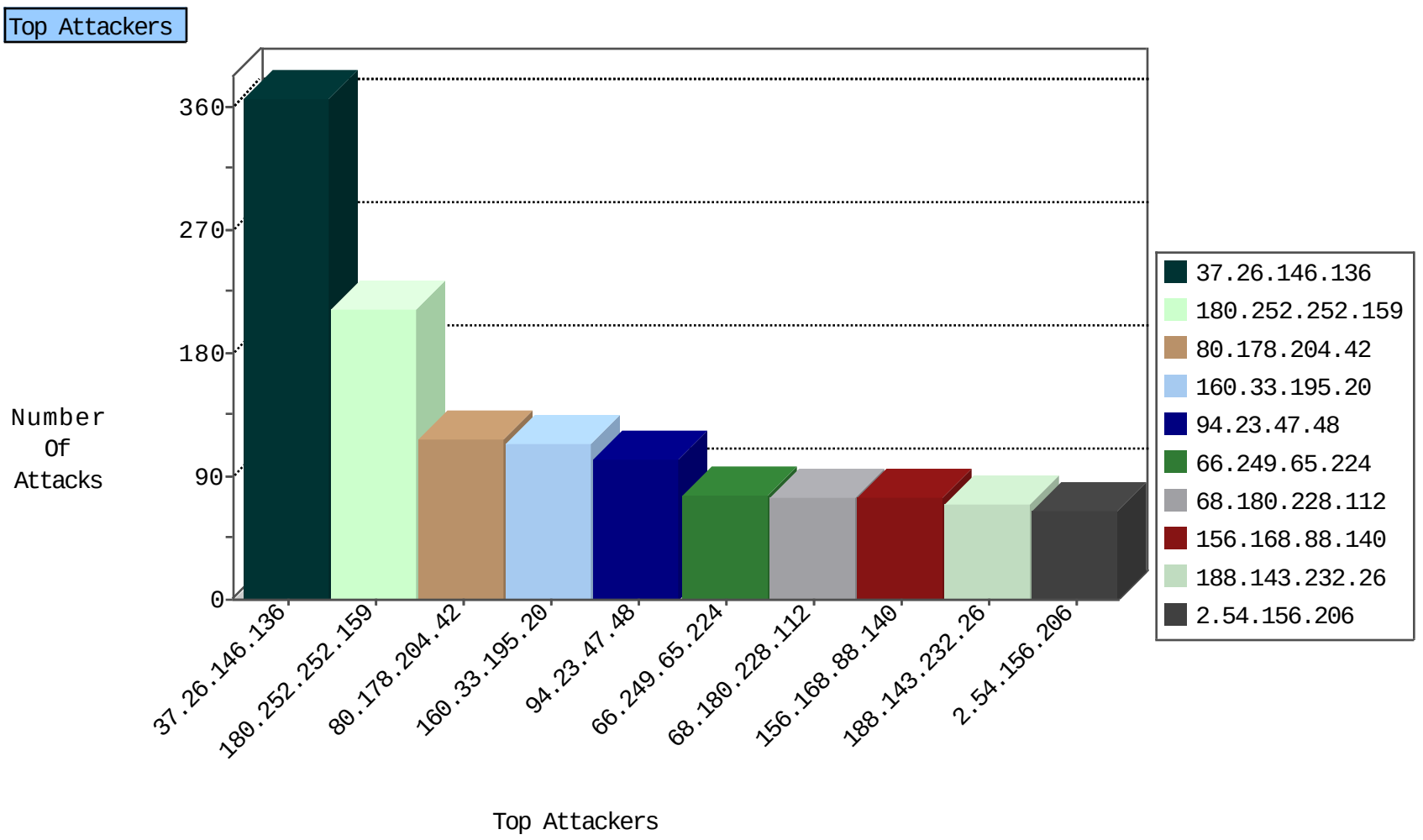
10-23-2015-16:04:00 to 10-23-2015-17:04:00

IDF Under Attack Daily Report





10-23-2015-16:04:00 to 10-23-2015-17:04:00

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	123
46.121.153.49	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	40
212.76.115.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	21
83.4.101.251	Poland	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
2.54.42.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
149.88.242.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
2.54.166.166	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
78.53.226.50	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
93.173.245.172	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
79.182.222.141	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
93.173.173.31	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
77.127.242.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
89.139.181.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
93.172.175.73	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
79.176.109.57	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
109.64.111.62	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.168.63	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
37.26.146.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.178.127.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
85.250.0.95	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.64.111.62	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
176.106.227.106	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.228.31.65	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
2.52.191.43	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
73.149.108.198	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.228.31.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.228.31.65	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
79.180.16.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.228.223.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
41.140.171.99	Morocco	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.166.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
187.174.83.35	Mexico	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.0.192	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
80.178.204.42	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
5.28.147.104	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
192.168.127.119		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
109.64.111.62	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
93.173.173.31	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.26.147.189	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.166.166	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
109.64.101.12	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
82.244.125.77	France	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
31.154.169.142	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.131.109	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
79.181.120.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
69.248.86.176	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
45.32.68.116		147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
173.208.168.166	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-23-2015-16:04:00 to 10-23-2015-17:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

10-23-2015-16:04:00 to 10-23-2015-17:04:00

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	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
107.150.19.109	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
218.108.132.58	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.17.72	147.237.76.38	Seychelles	e.e.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
107.150.19.109	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
95.220.165.95	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.142.64.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.34.158	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.180.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-23-2015-16:04:00 to 10-23-2015-17:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	367
180.252.252.159	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	212
80.178.204.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
160.33.195.20	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	114
156.168.88.140		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
2.54.156.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
46.43.116.49	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
5.22.129.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
85.65.32.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
173.208.155.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
111.199.77.78	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
188.143.232.26	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
37.8.27.117	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
84.228.113.55	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	40
176.12.144.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
105.198.243.243	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
212.143.85.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
77.127.242.84	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.54.170.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
143.229.245.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.92	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
2.54.168.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
109.173.23.91	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
194.165.134.162	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
84.94.84.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
37.142.249.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
213.86.221.35	United Kingdom	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	16
84.228.58.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.46.220.30	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
37.26.147.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
87.68.149.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.178.127.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
93.173.245.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
109.65.168.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.23.47.48	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.23.47.48	Block	98
2.52.22.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	42
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
79.181.165.18	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	28
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	28
146.185.234.48	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 146.185.234.48	Block	28
185.24.207.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$hiddenUpdateQuestion in www.aka.idf.il/main/giyus/faq.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
109.64.154.134	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
64.251.27.99	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /robots.txt	Block	14
84.228.5.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
212.143.139.72	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	14
77.127.29.113	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.231	Block	14
152.62.109.206	Europe	147.237.72.166	aka.idf.il	Unknown Parameter _ in www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	None	14
85.64.168.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
46.19.85.67	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
79.183.204.8	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	14
188.143.232.26	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	14
109.65.52.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.52.146	Block	14
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
84.228.58.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
77.127.242.84	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	14
213.57.199.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	14
157.55.39.200	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	14
93.172.137.246	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	14
46.116.128.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	14
81.223.254.34	Austria	147.237.77.233	atal.idf.il	Unauthorized URL Access to /robots.txt	Block	14
188.143.232.26	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1133-he/dover.aspx	Block	14
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
109.65.52.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9	Block	14
84.228.243.62	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
79.176.28.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
176.106.226.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
93.172.171.237	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	14
64.251.27.99	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to /robots.txt	Block	14
84.111.138.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
207.46.13.82	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	14
66.249.79.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	14
85.64.76.147	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
79.181.165.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
182.118.70.88	China	147.237.77.170	maarachot.idf.il	URL is Above Root Directory maarachot.idf.il/../shared/clientscripts/jquery/jcarousellite_1.0.1.pack.js	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	14
64.251.27.99	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to /robots.txt	Block	14
84.228.5.119	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	14
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1133-ar/dover.aspx	Block	14