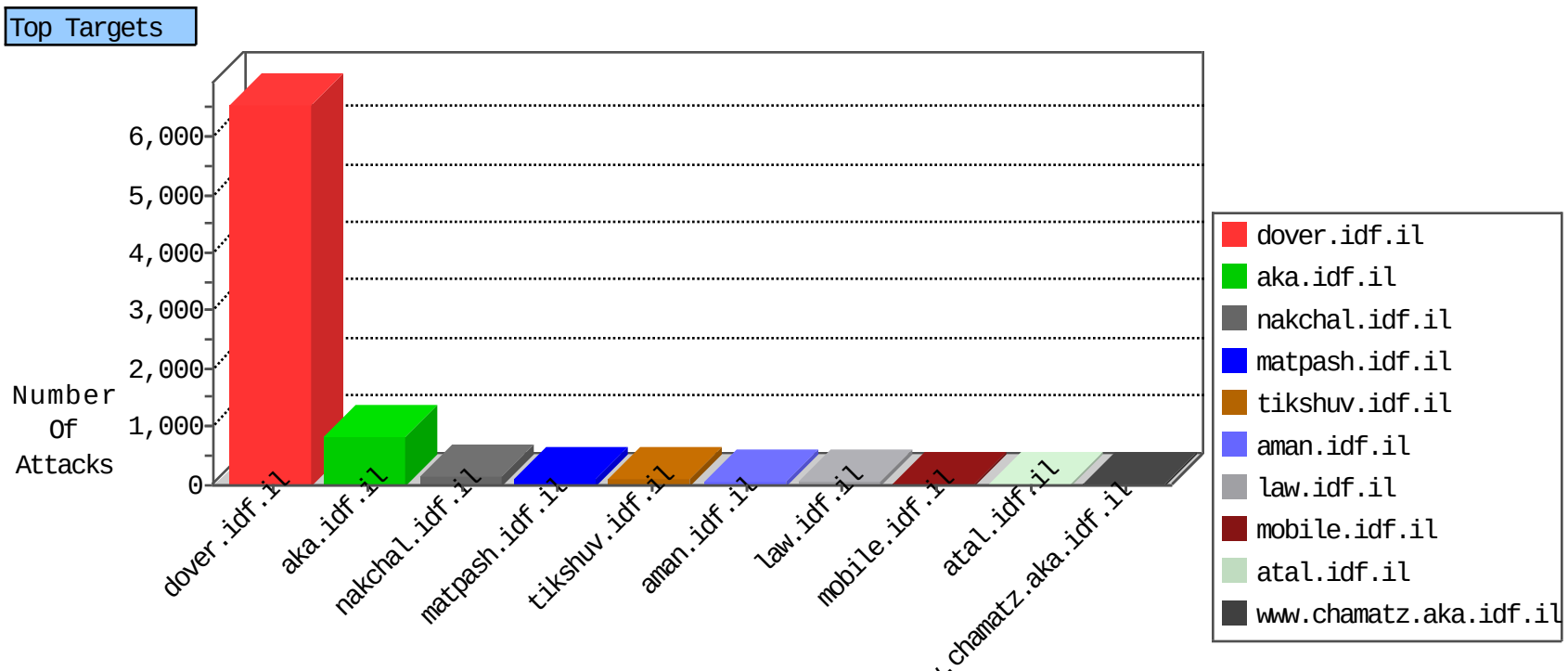
10-21-2015-19:04:08 to 10-21-2015-20:04:08

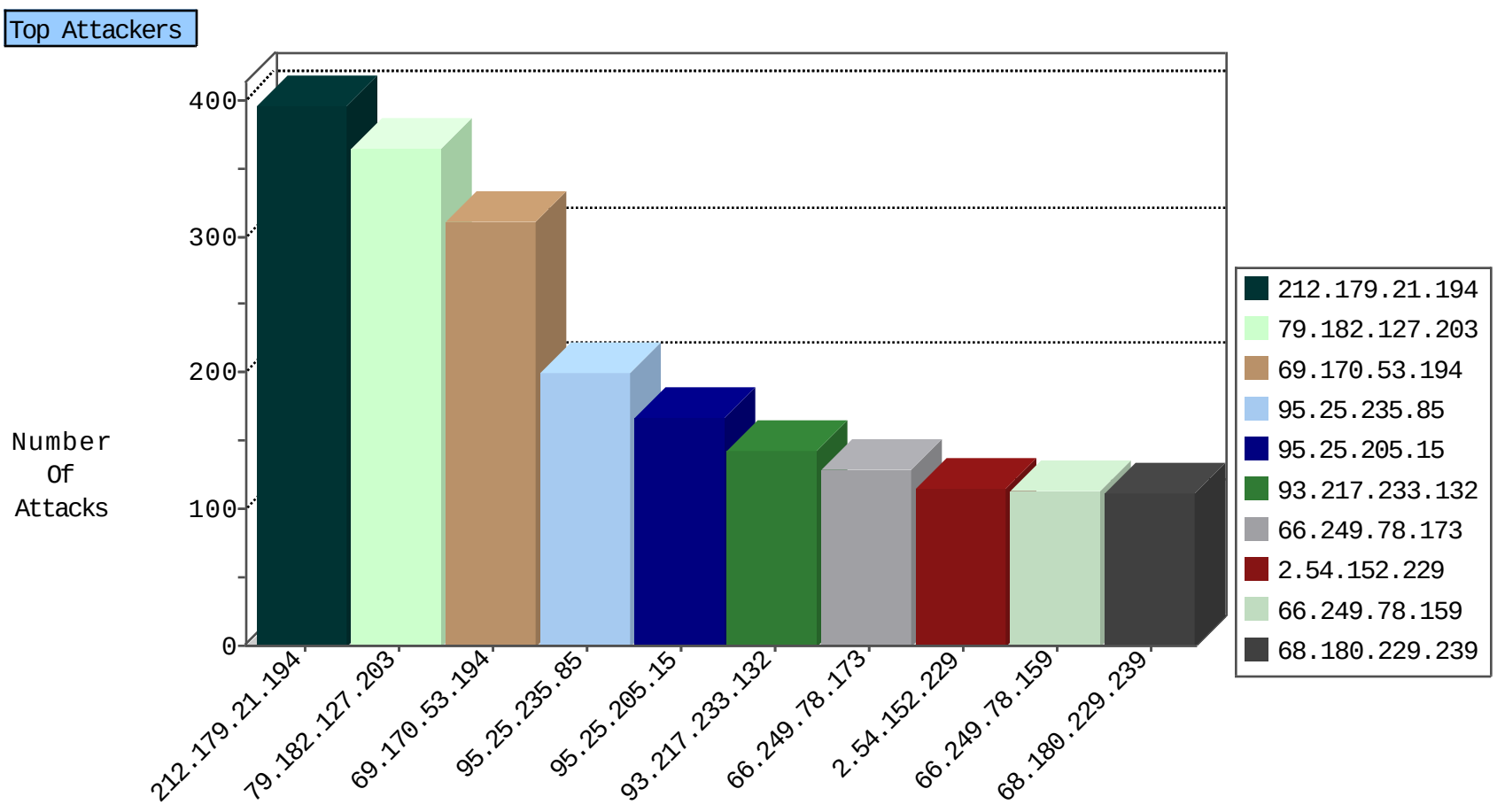
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-21-2015-19:04:08 to 10-21-2015-20:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.140.249	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	89
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
46.116.252.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
31.154.86.105	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
95.86.87.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
84.228.18.212	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
5.28.172.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
66.249.67.59	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
84.94.48.157	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
94.191.188.6	Denmark	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.87	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
80.82.78.169	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.162	China	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.37	China	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
80.82.78.169	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
197.0.26.167	Tunisia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
71.6.135.131	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.37	China	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
109.67.121.84	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
180.97.106.161	China	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.37	China	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1

10-21-2015-19:04:08 to 10-21-2015-20:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.136.48	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.121.41.19	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

10-21-2015-19:04:08 to 10-21-2015-20:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
61.149.161.186	147.237.77.235	China	sviva.idf.il	GPL SCAN nmap TCP	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
41.109.13.146	147.237.77.216	Algeria	dover.idf.il	portscan: TCP Distributed Portscan	1
175.136.225.229	147.237.76.30	Malaysia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
39.32.251.196	147.237.77.216	Pakistan	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.178.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.222.203	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1
27.75.168.255	147.237.76.200	Vietnam	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
79.182.59.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
27.75.168.255	147.237.76.34	Vietnam	yohalan.idf.il	ET SCAN Potential SSH Scan	1
79.179.55.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
27.75.168.255	147.237.8.46	Vietnam	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
79.143.180.44	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
27.75.168.255	147.237.0.15	Vietnam	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
66.249.78.166	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.44.140	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.165.239.212	147.237.76.201	Germany	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
192.118.11.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.92.220	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1
37.142.132.140	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.112.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.79.104	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
27.75.168.255	147.237.76.42	Vietnam	refuah.idf.il	ET SCAN Potential SSH Scan	1
79.181.155.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
27.75.168.255	147.237.72.167	Vietnam	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
79.177.160.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
27.75.168.255	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN Potential SSH Scan	1
78.95.176.116	147.237.77.216	Romania	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.163.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-21-2015-19:04:08 to 10-21-2015-20:04:08

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.i	drop	First packet isn't SYN	drop	397
79.182.127.203	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	366
69.170.53.194	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	311
95.25.235.85	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	201
95.25.205.15	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	167
93.217.233.132	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	143
2.54.152.229	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	116
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	106
37.26.146.193	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	96
185.71.143.45	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	84
54.244.22.103	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	79
82.166.22.13	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	74
141.0.14.145	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	72
130.193.165.119	Iraq	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	67
66.249.78.159	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
66.249.78.173	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	55
94.191.188.6	Denmark	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	55
46.185.141.11	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	54
176.13.6.183	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
176.193.101.153	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
93.184.12.14	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
37.26.146.141	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
2.54.190.225	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
105.109.43.124	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
185.76.33.113		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
92.241.50.64	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
37.142.96.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	40
66.249.78.173	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
93.172.184.58	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
183.79.221.75	Japan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
151.80.31.115	Italy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
82.145.221.245	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
46.60.35.32	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
66.249.84.166	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
95.26.69.130	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
5.28.172.65	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
66.249.78.159	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
66.249.78.166	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.78.173	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
100.100.115.178		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
109.186.51.15	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28

10-21-2015-19:04:08 to 10-21-2015-20:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	98
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
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1100-he/nakhal.aspx	Block	84
2.54.142.89	Israel	147.237.0.34	tikshuv.idf.il	Redundant HTTP Headers from 2.54.142.89	Block	56
176.65.16.128	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22777-ar/dover.aspx)	Block	28
84.108.250.74	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	28
188.165.15.89	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
46.120.112.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
109.65.211.30	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	14
79.181.175.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	14
212.116.169.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
157.55.39.11	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	14
46.19.85.158	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	14
85.65.203.61	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
197.134.255.73	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22777-ar/dover.aspx)	Block	14
66.249.64.210	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/robots.txt	Block	14
5.29.31.33	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in aka.idf.il/main/sachar/tfasim.aspx	None	14
109.66.80.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
79.181.195.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sechar	Block	14
66.249.93.149	Israel	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx	Block	14
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.143.3.44	Block	14
176.13.2.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
46.116.238.100	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 46.116.238.100	Block	14
85.250.31.107	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/forgotpassword.aspx parameter	None	14
79.177.108.36	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	14
66.249.64.215	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/robots.txt	Block	14
207.46.13.48	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
5.29.74.149	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	14
109.66.188.17	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
80.246.136.26	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	14
46.117.74.181	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	14
2.54.54.26	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	14
79.177.185.254	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	14
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
207.46.13.119	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
31.154.156.0	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	14
149.78.242.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
180.109.236.14	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	14
46.120.62.233	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	14
2.54.142.89	Israel	147.237.0.34	tikshuv.idf.il	Redundant HTTP Headers Referer	Block	14
93.173.26.91	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
79.181.32.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	14
149.78.251.49	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	14
37.46.39.120	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/adguard-ajax-api/api	Block	14
84.229.160.86	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/421-2258-he/patzar.aspx	Block	14
93.173.8.215	Israel	147.237.72.156	aman.idf.il	Cross-site scripting on parameter ctl00$ctl00$cphMain$CPHMainContent$ctl77$ctl01$ctl03$txtField in www.aman.idf.il/modiin/questionnaires.aspx	Block	12

10-21-2015-19:04:08 to 10-21-2015-20:04:08