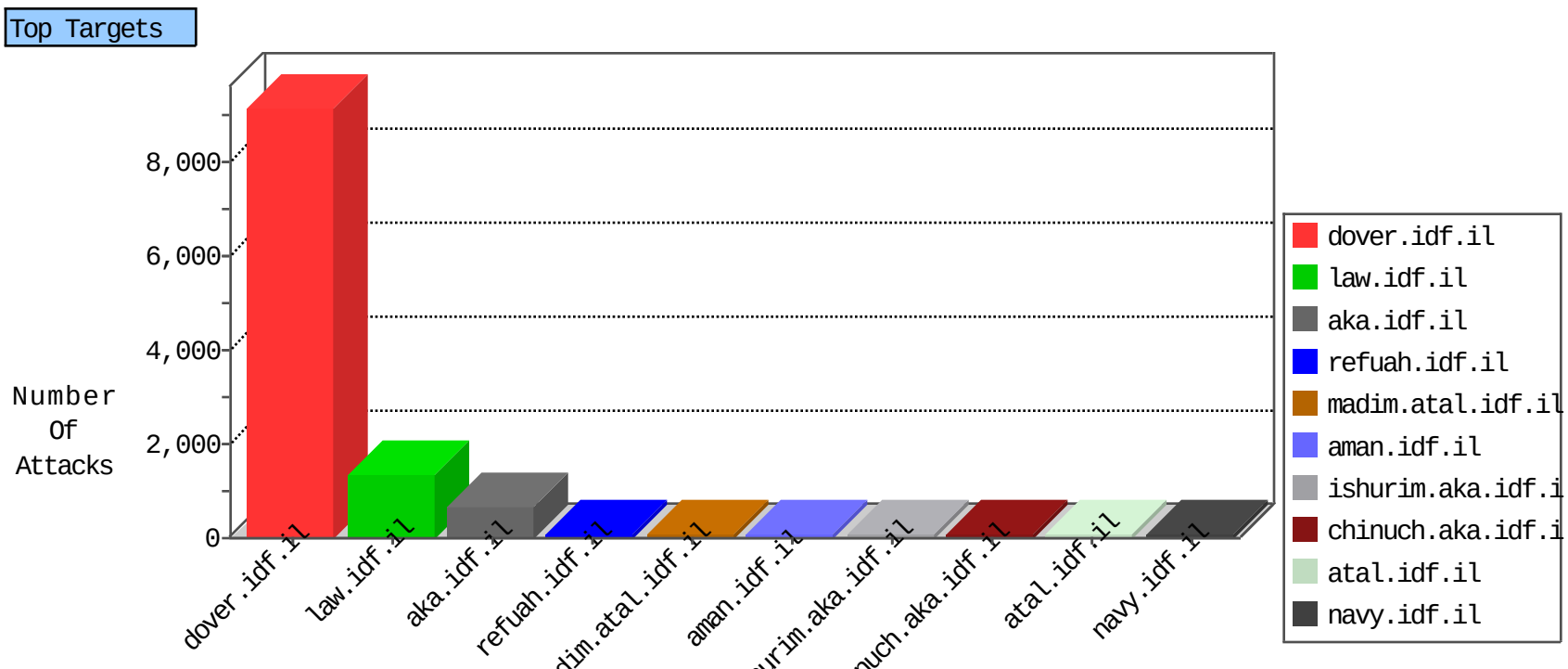
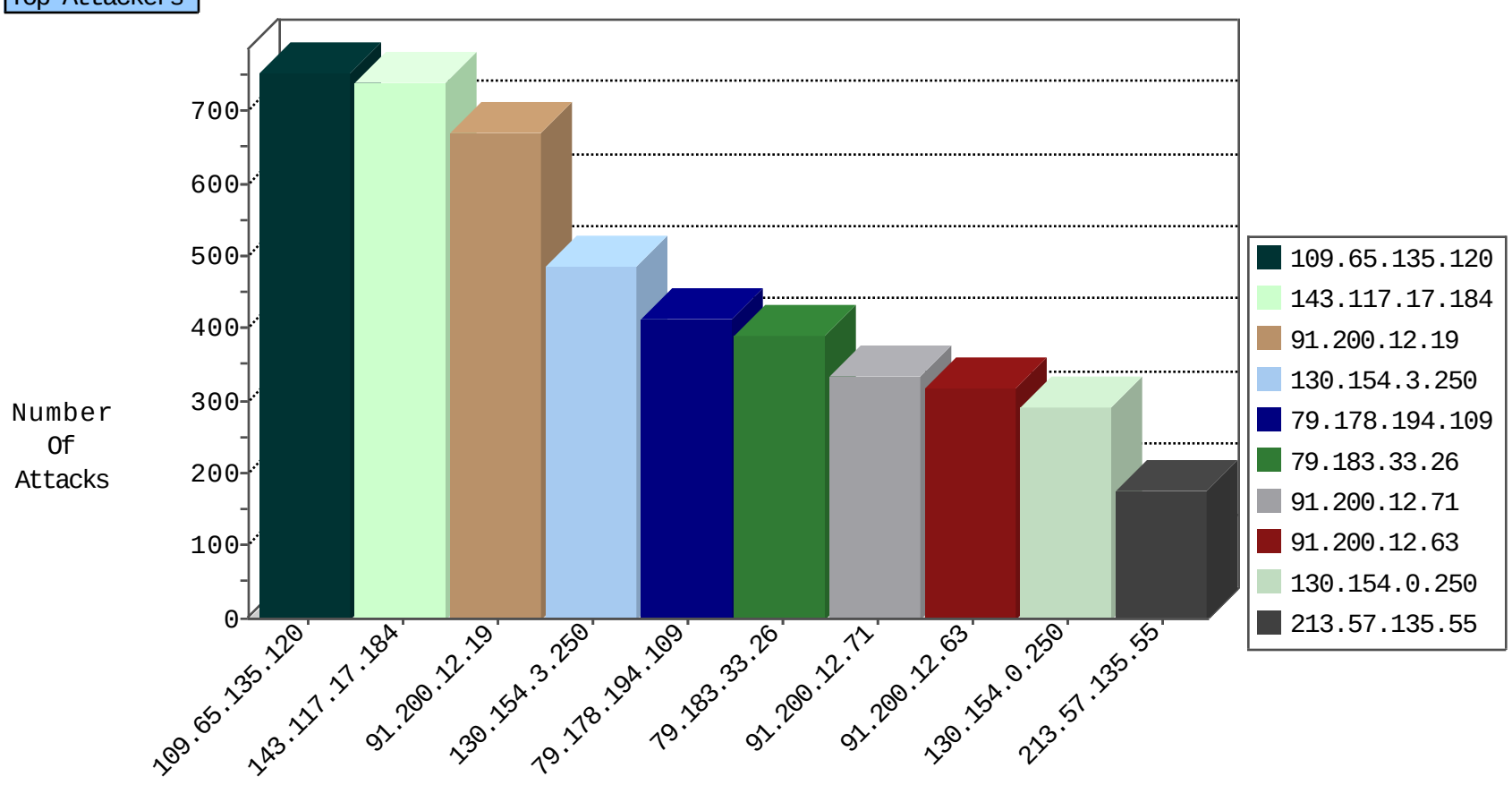
10-21-2015-22:04:09 to 10-21-2015-23:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-21-2015-22:04:09 to 10-21-2015-23:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.88.91	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	530
66.249.67.235	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	60
46.19.85.224	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	56
197.157.131.21	Rwanda	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
84.111.36.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
212.117.154.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
214.4.253.121	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
31.154.91.87	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
79.183.33.26	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
100.100.90.111		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
83.130.99.243	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.142.177.111	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	2
46.19.85.99	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.88.81	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.76.204.174	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
212.143.156.33	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
149.78.80.252	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
37.76.204.174	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.176.214.87	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
93.174.93.100	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

10-21-2015-22:04:09 to 10-21-2015-23:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.151.50.148	Israel	147.237.77.216	dover.idf.il	C1000098: Block - dns poisoning	Block	1

10-21-2015-22:04:09 to 10-21-2015-23:04:09

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	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
58.253.96.122	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 2048	1
46.19.85.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
43.229.53.89	147.237.0.34	Japan	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
183.0.6.245	147.237.76.44	China	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
43.229.53.89	147.237.0.15	Japan	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
124.122.74.66	147.237.0.34	Thailand	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.78.159	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
62.210.25.83	147.237.0.200	France	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
61.182.170.38	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 3072	1
58.253.96.122	147.237.0.33	China	idf.il	ET SCAN NMAP -f -sS	1
43.229.53.89	147.237.0.200	Japan	m4u.idf.il	ET SCAN Potential SSH Scan	1
43.229.53.89	147.237.0.19	Japan	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
176.13.15.20	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
85.250.218.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.210.25.83	147.237.0.200	France	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
62.210.25.83	147.237.0.200	France	m4u.idf.il	ET SCAN NMAP -f -sS	1
61.182.170.38	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

10-21-2015-22:04:09 to 10-21-2015-23:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.135.120	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	754
143.117.17.184	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	739
130.154.3.250	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	487
79.178.194.109	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	415
79.183.33.26	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	388
130.154.0.250	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	283
213.57.135.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	175
105.198.242.170	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	156
85.181.135.97	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	150
168.63.139.43	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	144
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	143
207.244.70.35	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	141
79.181.120.187	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	136
141.0.15.26	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	102
143.117.17.186	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	88
84.228.11.173	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	84
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	80
24.237.158.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	78
31.44.139.237	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	75
87.195.251.73	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	68
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	67
12.249.99.202	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	66
79.180.24.5	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	59
86.56.80.26	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	59
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
5.22.129.138	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
46.43.72.102	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
185.19.220.197	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
185.24.76.152	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
176.13.18.97	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
197.246.213.57	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
188.247.74.76	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
70.193.103.81	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
151.80.31.115	Italy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
185.120.126.51		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
66.249.88.81	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
212.106.89.195	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
67.191.35.57	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
212.179.21.194	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
37.142.190.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36
93.172.184.58	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
109.173.57.80	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
2.54.61.22	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
85.65.67.168	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
134.99.174.12	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34

10-21-2015-22:04:09 to 10-21-2015-23:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.200.12.19	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	336
91.200.12.19	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 91.200.12.19	Block	322
91.200.12.63	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	165
91.200.12.71	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 91.200.12.71	Block	154
91.200.12.63	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 91.200.12.63	Block	154
91.200.12.71	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	84
91.200.12.71	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	84
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	70
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
84.228.11.173	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	42
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	42
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	42
84.228.11.173	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEntrance in madim.atal.idf.il/1088-he/meretz.aspx	Block	41
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	28
65.55.210.90	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	28
85.250.94.175	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
131.253.25.227	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	28
212.117.154.242	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	14
176.13.22.90	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
77.127.167.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
94.159.214.77	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	14
31.154.91.201	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	14
80.246.136.151	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
194.90.83.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_text.asp	Block	14
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
46.116.169.8	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	14
212.199.57.205	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	14
176.13.23.226	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
79.177.57.119	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	14
109.66.108.76	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pniasubmittedsuccessfully.aspx	None	14
37.26.148.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
80.246.136.151	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	14
207.46.13.48	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	14
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	14
62.219.134.244	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	14
213.151.50.148	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	14
84.229.28.13	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	14
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	14
79.178.155.242	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	14
38.111.147.84	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 38.111.147.84	Block	14
91.200.12.19	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/592-4071-en/index.php	Block	14
84.108.170.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
207.46.13.119	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/klali.aspx	Block	14
176.13.3.214	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	14
180.153.180.111	China	147.237.72.166	aka.idf.il	URL is Above Root Directory www.aka.idf.il/../resources/scripts/site.js	Block	14
79.180.122.119	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	14
46.116.81.222	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14

10-21-2015-22:04:09 to 10-21-2015-23:04:09