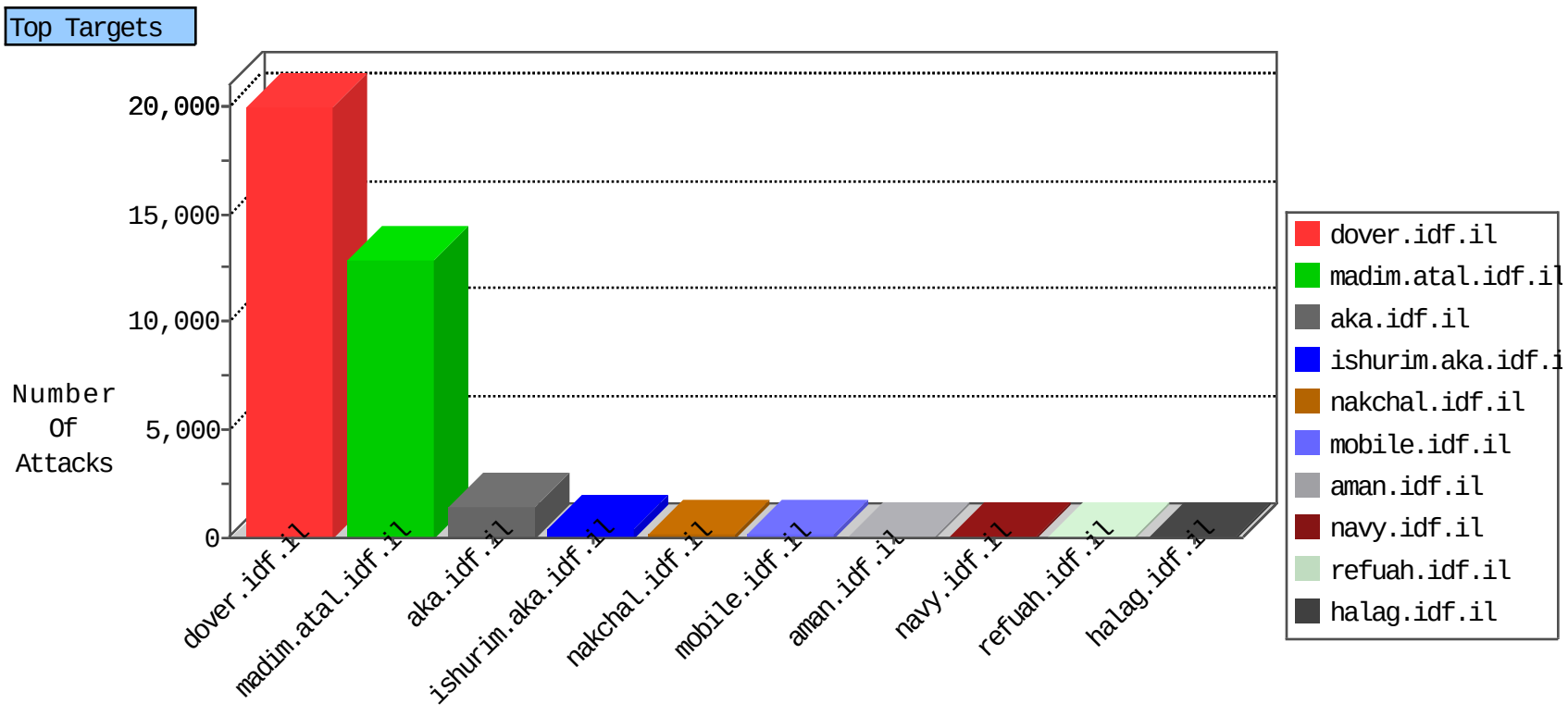
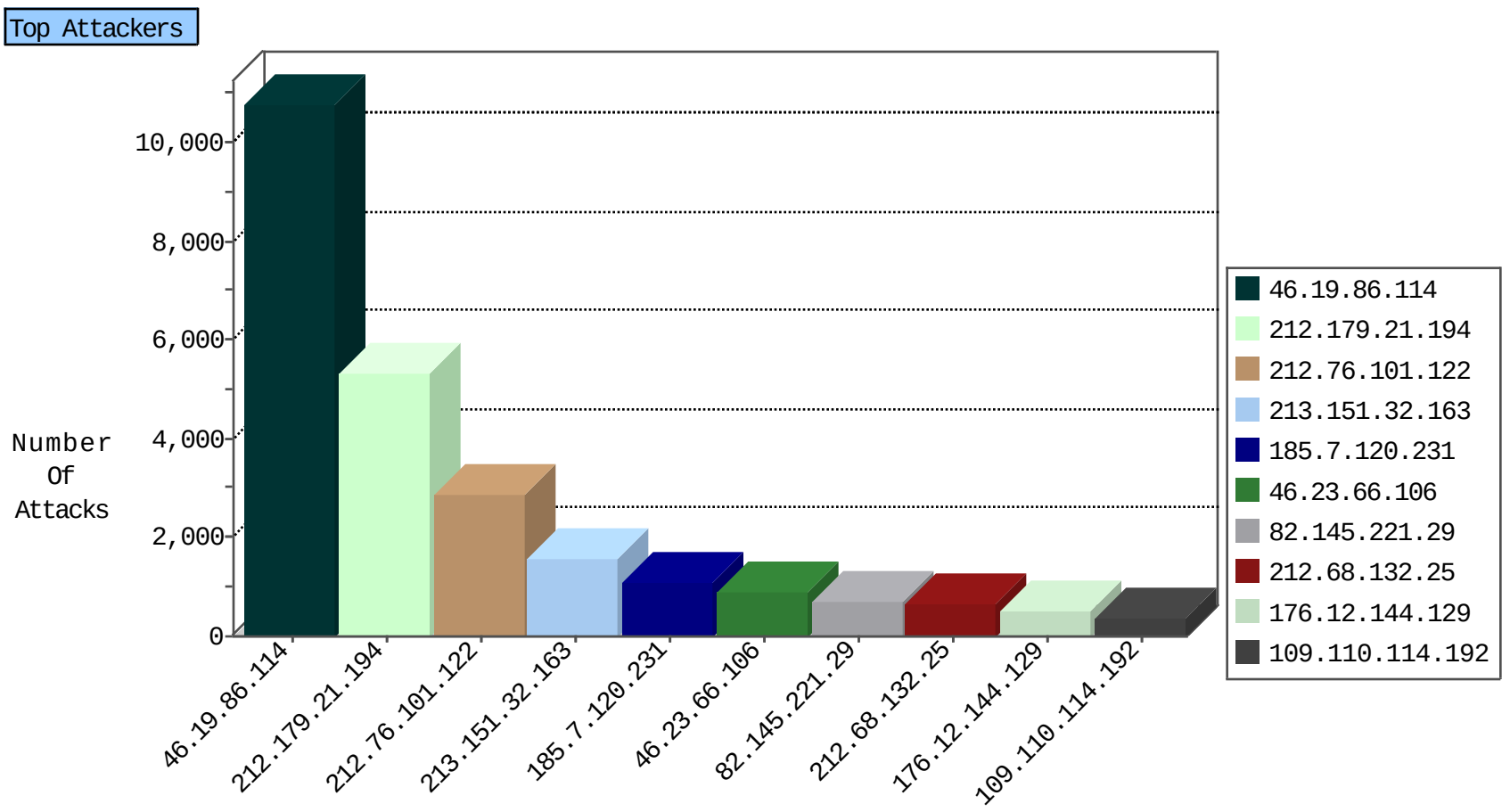
10-21-2015-11:04:03 to 10-21-2015-12:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-21-2015-11:04:03 to 10-21-2015-12:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.7.120.231	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3022
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	346
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	225
79.181.20.52	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	130
37.26.149.164	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	116
176.13.9.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	54
176.13.4.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	51
37.26.149.150	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	46
79.182.106.104	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	42
212.143.39.125	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
95.86.127.142	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
85.64.188.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
176.12.147.117	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
37.26.147.212	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
212.199.11.202	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
77.125.135.230	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
77.125.0.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
109.64.12.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
185.32.179.37	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
37.26.148.195	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
178.255.171.57	Czech Republic	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
176.12.136.4	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
41.43.57.57	Egypt	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
2.54.38.183	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
176.13.3.192	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.23.66.106	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
176.13.20.102	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
212.143.147.142	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.182.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.186.172.88	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.65.3.241	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
31.154.10.105	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
41.248.252.89	Morocco	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.76.101.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
89.167.129.96	Spain	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.228.205.187	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.181.103.92	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.154.50	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.174.209	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
213.8.99.17	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
149.78.249.224	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
81.218.89.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
197.161.80.109	Egypt	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
86.108.85.209	Jordan	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
178.168.121.8	Moldova, Republic of	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.183.141.50	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.65.123.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.15.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.140.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3

10-21-2015-11:04:03 to 10-21-2015-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.118.126	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12

10-21-2015-11:04:03 to 10-21-2015-12:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
59.46.193.114	147.237.0.16	China	my-kosher-kravi.idf.il	GPL SCAN nmap TCP	2
218.24.171.223	147.237.0.16	China	my-kosher-kravi.idf.il	GPL SCAN nmap TCP	2
80.179.90.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.209.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.220	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
54.169.6.18	147.237.8.14	Singapore	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.199	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
5.39.222.253	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
213.151.61.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.35.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.27.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.175.50	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.219.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
68.180.228.112	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
37.107.238.113	147.237.77.216	Saudi Arabia	dover.idf.il	portscan: TCP Distributed Portscan	1
24.228.17.207	147.237.76.86	United States	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.54.175.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
197.162.235.157	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.30.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
108.61.220.143	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1

10-21-2015-11:04:03 to 10-21-2015-12:04:03

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	5334
212.76.101.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2861
185.7.120.231	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1102
46.23.66.106	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	903
82.145.221.29	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	690
212.68.132.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	636
109.110.114.192	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	357
141.0.14.168	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	317
141.0.14.241	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	296
103.26.198.126	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	195
82.81.17.28	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	186
66.171.228.56	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	175
82.81.193.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	138
83.103.25.60	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	120
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	119
188.161.65.162	Palestinian Territory, Occupied	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	103
176.65.18.118	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
185.120.126.40		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
194.56.215.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
188.161.115.36	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
124.124.48.36	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
209.95.33.208	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
66.249.67.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
197.158.248.192	Seychelles	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
66.249.67.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
37.141.160.92	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
77.126.82.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
197.34.237.251	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
176.13.17.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.249.67.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
46.19.85.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
169.253.194.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
66.249.67.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
81.218.48.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
62.90.243.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
2.54.9.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
176.13.4.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
2.89.204.62	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
46.52.68.19	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
188.48.21.250	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10789
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1556
176.12.144.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	503
84.108.82.194	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.82.194	Block	234
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	234
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.208	Block	88
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1110-he/nakhal.aspx	Block	78
80.246.139.109	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	65
46.19.85.142	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	52
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	52
176.12.147.2	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	39
2.54.5.126	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	39
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.192	Block	39
95.86.127.142	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	39
82.213.13.186	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	39
147.251.43.20	Czech Republic	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 147.251.43.20	Block	39
2.52.23.27	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
46.19.85.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
176.12.144.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	25
84.108.82.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/[object object]	Block	13
64.41.200.103	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.103 (Unsupported Legacy SSL Version)	None	13
37.120.66.193	Germany	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
182.118.54.167	China	147.237.77.170	maarachot.idf.il	URL is Above Root Directory www.maarachot.idf.il/../shared/clientscripts/jquery/jquery-ui.js	Block	13
81.218.179.41	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	13
147.251.43.20	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1589-	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
132.64.25.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	13
46.116.122.251	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	13
216.218.206.67	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	13
82.166.20.36	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /	Block	13
5.175.25.171	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	13
137.226.113.7	Germany	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	13
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	13
89.138.194.157	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	13
64.41.200.103	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	13
182.118.54.181	China	147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/../shared/clientscripts/jquery/global.js	Block	13
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/favicon.ico	Block	13
176.12.136.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
69.171.230.112	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/1919.jpg	Block	13
132.69.198.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
82.166.235.55	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	13
62.90.131.54	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1119-he/nakhal.aspx	Block	13
79.182.127.62	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
15.203.178.12	France	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/sachar/scriptresource.axd	None	13
176.13.11.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
141.212.122.64	United States	147.237.76.31	nakchal.idf.il	Malformed URL proxytest.zmap.io:80	Block	13
64.41.200.103	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	13
185.32.179.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
81.218.251.252	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/×?	Block	13