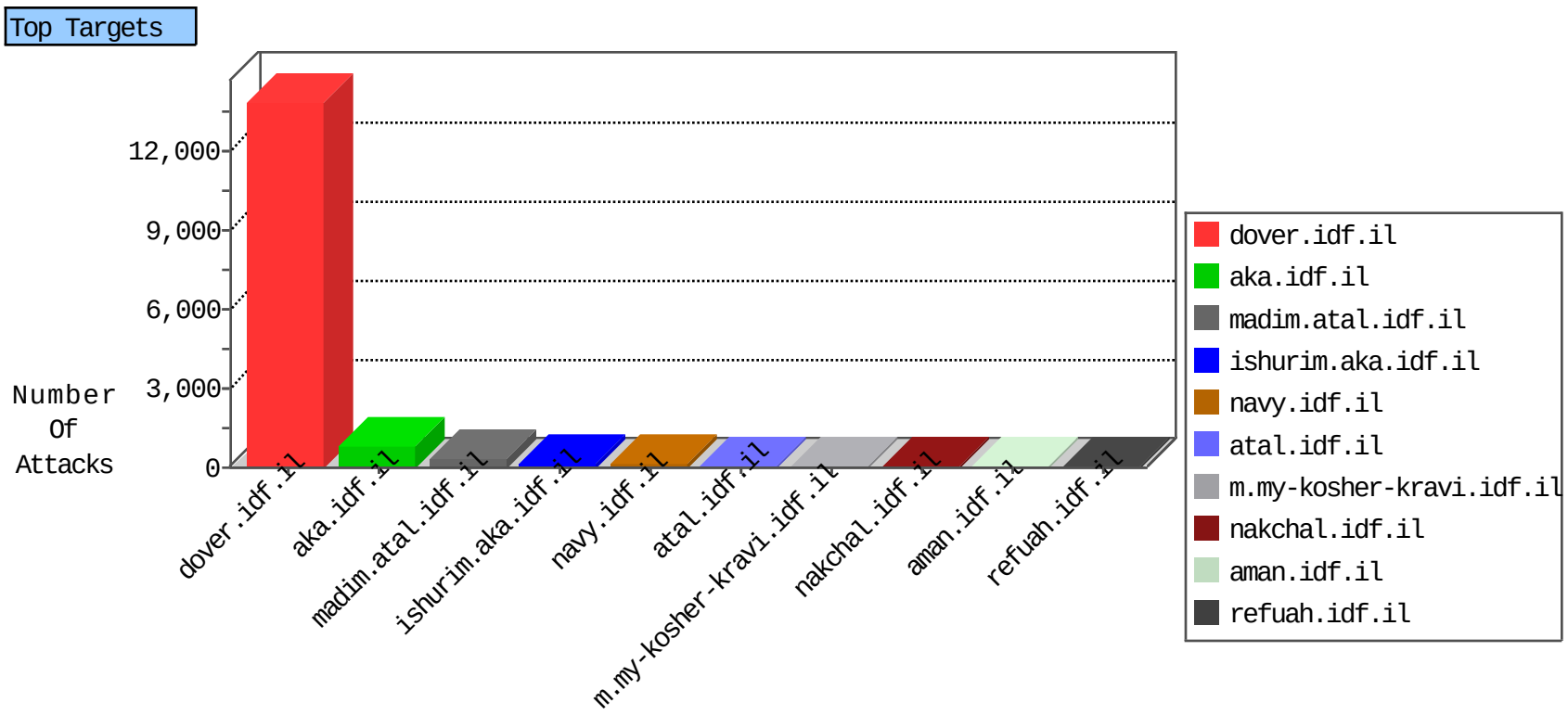
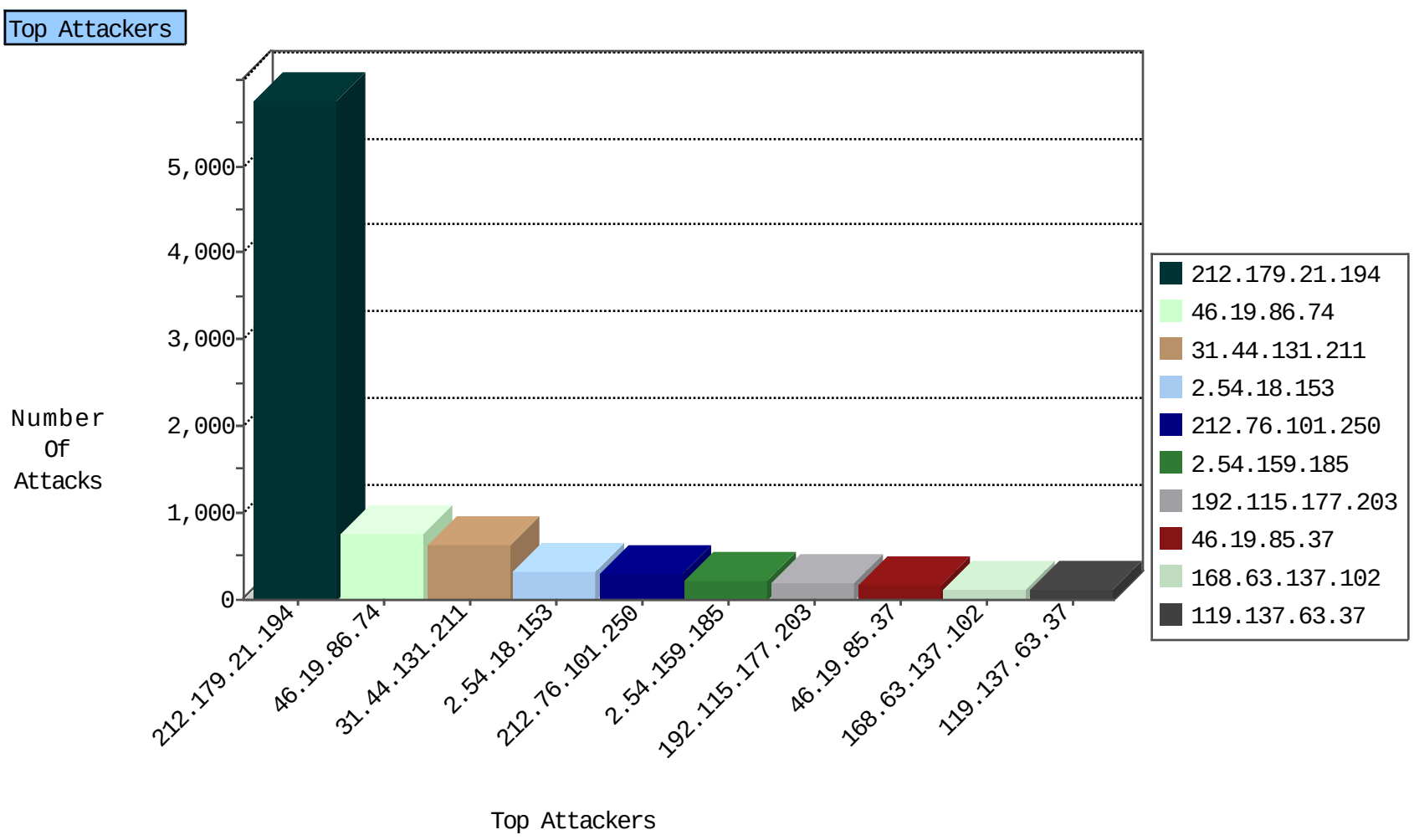
10-19-2015-14:04:00 to 10-19-2015-15:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-19-2015-14:04:00 to 10-19-2015-15:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.27.105.137	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	449
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	79
185.24.207.15	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	69
77.125.159.153	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
213.57.155.196	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
100.100.23.10		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
79.182.194.110	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	11
87.68.249.1	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
82.81.32.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.177.59.237	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
46.19.85.115	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	5
2.54.132.23	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
80.246.136.243	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
46.19.85.254	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	5
2.54.3.19	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.109.100.201	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
81.218.208.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.69.222.157	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.26.146.245	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
31.168.133.226	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
212.150.245.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.116.166.10	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
31.168.174.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.180.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
81.218.85.18	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.150.203.146	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
62.219.44.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
61.182.170.38	China	147.237.76.177	ncore.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
185.32.179.65	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
93.174.93.146	Netherlands	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
176.13.6.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
212.179.23.29	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
212.150.245.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.246.139.20	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
64.233.172.171	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.150.203.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
31.210.186.140	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
142.54.174.66	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	drop	1
82.166.134.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
79.182.201.171	Israel	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.54.180.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
93.174.93.146	Netherlands	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	1
176.13.2.223	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
80.246.136.199	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-19-2015-14:04:00 to 10-19-2015-15:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.245.1	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3

10-19-2015-14:04:00 to 10-19-2015-15:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.66.24.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.57.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.151.50.165	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
37.26.148.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.195.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.210.186.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.88.162.1	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.129.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
165.228.233.142	147.237.77.205	Australia	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
109.66.57.96	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.82.96	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.151.50.165	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
46.117.105.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.108.132.58	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.139.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.160.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.74.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-19-2015-14:04:00 to 10-19-2015-15:04:00

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	5676
46.19.86.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	757
31.44.131.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	633
2.54.18.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	325
212.76.101.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	300
46.19.85.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	170
168.63.137.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
119.137.63.37	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	118
77.126.221.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	117
192.115.177.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
46.117.63.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
195.243.181.2	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
107.6.142.117	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
87.69.197.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
46.19.85.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
37.26.147.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
147.236.138.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
109.226.21.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
76.23.52.122	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
77.126.168.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
217.66.178.124	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
212.130.119.209	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
37.26.147.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
2.54.129.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
2.54.1.243	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	44
77.125.130.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
176.13.6.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
78.40.176.178	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
2.54.132.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
80.246.136.243	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
2.54.3.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
46.117.89.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.102.8.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
82.80.135.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
2.54.19.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
31.168.201.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
109.64.9.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
62.90.107.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
176.13.6.37	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
176.106.42.93	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.52.31.33	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	30
213.57.183.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.159.185	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.159.185	Block	208
109.64.34.244	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 109.64.34.244	None	88
192.115.177.203	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1620.jpg	Block	78
37.26.149.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	78
68.180.231.61	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1072-he/nakhal.aspx	Block	76
46.120.216.135	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	52
207.46.13.141	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	26
84.108.158.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	26
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	26
168.235.198.76	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripts/ui/ui.datepicker.×²Ö³Ö´	Block	13
37.187.56.47	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/homepage	Block	13
84.108.106.23	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$chkBitulTlushim in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	13
66.249.65.239	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	13
46.117.247.21	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
132.70.66.11	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/7	Block	13
85.250.169.32	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	13
2.85.143.64	Greece	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/xmlrpc.php	Block	13
66.249.93.140	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.scrollfollow.js	Block	13
212.143.133.107	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	13
184.105.139.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	13
62.90.194.104	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
109.66.6.159	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	13
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clienthttp/1.1 200 okdate: mon, 19 oct 2015 05:40:25 gmtlast-modified: sun, 03 jun 2012 07:44:40 gmtetag:	Block	13
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/redirects/ssl-redirect.html	Block	13
207.46.13.187	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	13
46.117.247.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/https:/aka.idf.il/	Block	13
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/milnet	Block	13
87.69.231.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
5.102.212.112	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	13
212.199.112.144	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/datepicker.css	Block	13
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	13
46.19.86.104	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.scrollfollow.js	Block	13
109.67.11.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	13
2.54.159.185	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	13
84.108.226.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	13
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	13
46.120.69.178	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/https:/aka.idf.il/	Block	13
108.46.177.198	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/gg	Block	13
31.44.133.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
217.194.193.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
79.179.56.155	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	13
199.207.253.101	United States	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$chkBitulTlushim in aka.idf.il/main/sachar/registrationwizard/step3.aspx	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
46.19.86.160	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
109.226.30.78	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
85.250.147.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.250.147.57	Block	13
66.249.78.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.asp	Block	13
212.76.125.126	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.76.125.126	Block	13
147.236.28.31	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13