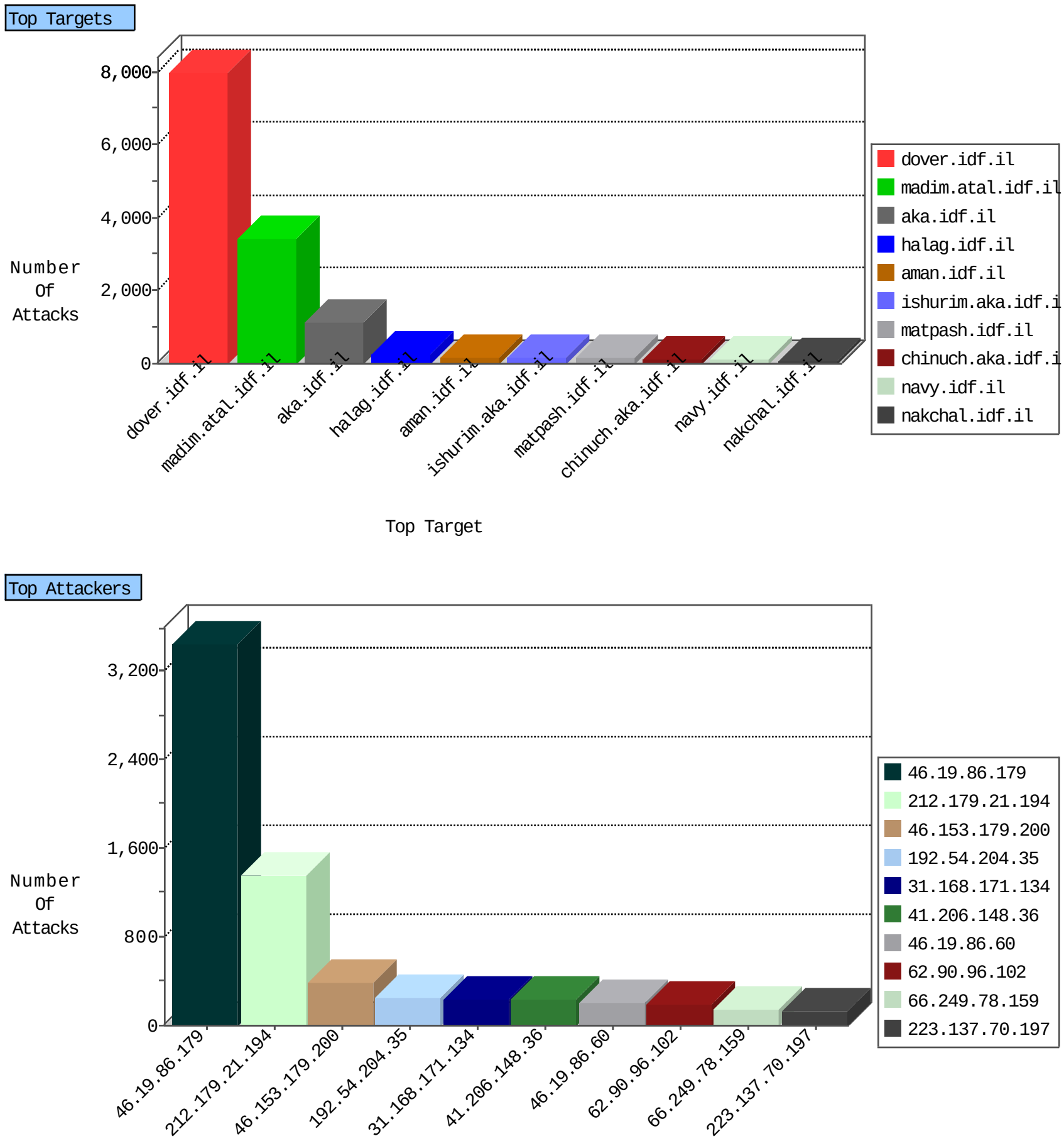
10-22-2015-11:04:04 to 10-22-2015-12:04:04

IDF Under Attack Daily Report



10-22-2015-11:04:04 to 10-22-2015-12:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.4.82	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2619
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	157
2.54.169.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	85
79.182.174.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
91.194.4.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
46.19.86.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
176.12.149.247	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
2.54.41.178	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
46.19.86.27	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
213.8.129.144	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
2.54.4.82	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
2.52.59.171	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
2.52.59.171	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
185.120.126.26		147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.105.134.129	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.95.251.240	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	5
2.54.153.249	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	5
87.68.47.86	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.179.180.30	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.182.121.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.57.215.214	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
178.76.237.234	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.7.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.146.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.85.222	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.12.138.241	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.19.140	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.147.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
222.186.21.180	China	147.237.0.35	akaws.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
2.52.38.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
183.128.178.216	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
109.67.24.233	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
81.218.174.17	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
49.89.188.41	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
5.8.66.69	Russian Federation	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
142.54.187.42	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
89.248.172.98	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
66.102.8.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
116.29.82.196	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
213.151.32.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
58.152.130.4	Hong Kong	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
37.26.147.202	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
162.213.152.192	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
121.34.161.137	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
60.166.151.89	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
162.213.152.192	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
107.150.56.166	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
142.54.172.106	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
89.248.172.98	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

10-22-2015-11:04:04 to 10-22-2015-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.251.250	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
213.151.48.44	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

10-22-2015-11:04:04 to 10-22-2015-12:04:04

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	2
185.120.126.40	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
73.1.42.67	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
41.140.253.9	147.237.76.198	Morocco	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
37.26.149.216	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.176.122	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.194.193.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.18.200.82	147.237.72.217	Russian Federation	e.idf.il	ET SCAN NMAP -sS window 3072	1
176.12.144.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.106.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.137.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.187.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.44.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

10-22-2015-11:04:04 to 10-22-2015-12:04:04

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	1337
46.153.179.200	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	383
31.168.171.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	231
41.206.148.36	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	224
46.19.86.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	204
62.90.96.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	190
223.137.70.197	Taiwan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	136
46.117.180.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
41.218.182.151	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
85.140.0.28	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
37.26.148.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
194.114.146.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
194.55.26.7	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
189.203.217.170	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
46.19.86.61	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
194.55.26.8	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
37.142.101.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	56
212.25.83.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
81.149.206.22	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
46.163.68.109	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
46.19.86.175	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
2.54.21.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
194.55.30.7	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
213.57.21.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
87.68.153.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
79.176.169.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
148.177.129.213	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
194.55.30.8	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
176.12.144.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
86.108.12.231	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
100.100.65.49		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	35
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
2.54.155.180	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
46.19.86.227	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	33
37.26.146.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
37.26.146.145	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
2.54.183.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
79.179.167.30	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
46.19.86.229	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30

10-22-2015-11:04:04 to 10-22-2015-12:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.179	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.179	Block	3447
192.54.204.35	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 192.54.204.35	Block	238
93.173.0.24	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	112
188.143.232.11	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.11	Block	70
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	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
212.179.159.253	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 212.179.159.253	Block	42
37.237.143.173	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	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
193.34.56.101	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/undefined	Block	28
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	28
212.179.245.207	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	28
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
84.95.251.240	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	28
212.179.15.202	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	27
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	14
185.82.201.17		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php/admin	Block	14
113.91.150.18	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	14
82.213.48.225	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	14
192.54.204.35	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/1/size338x0/1531.jpg	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	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
176.13.2.134	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	14
31.13.97.104	Ireland	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
87.69.81.241	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
77.237.138.51	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	14
212.179.159.253	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	14
141.212.122.96	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to /x	Block	14
46.19.86.237	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	14
84.55.42.31	Lithuania	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/print_bottom.asp	Block	14
66.249.65.99	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
176.13.14.130	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	14
31.168.79.54	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	14
87.69.105.237	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
79.178.168.129	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
188.143.232.11	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/900-he/	Block	14
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
167.114.64.100	Canada	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	14
52.23.156.32	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	14
84.95.251.240	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
203.133.168.83	Korea, Republic of	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	14
184.105.247.195	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	14
93.172.47.16	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
79.180.114.245	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
188.143.232.24	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	14
176.12.143.227	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	14
62.219.141.247	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14

10-22-2015-11:04:04 to 10-22-2015-12:04:04