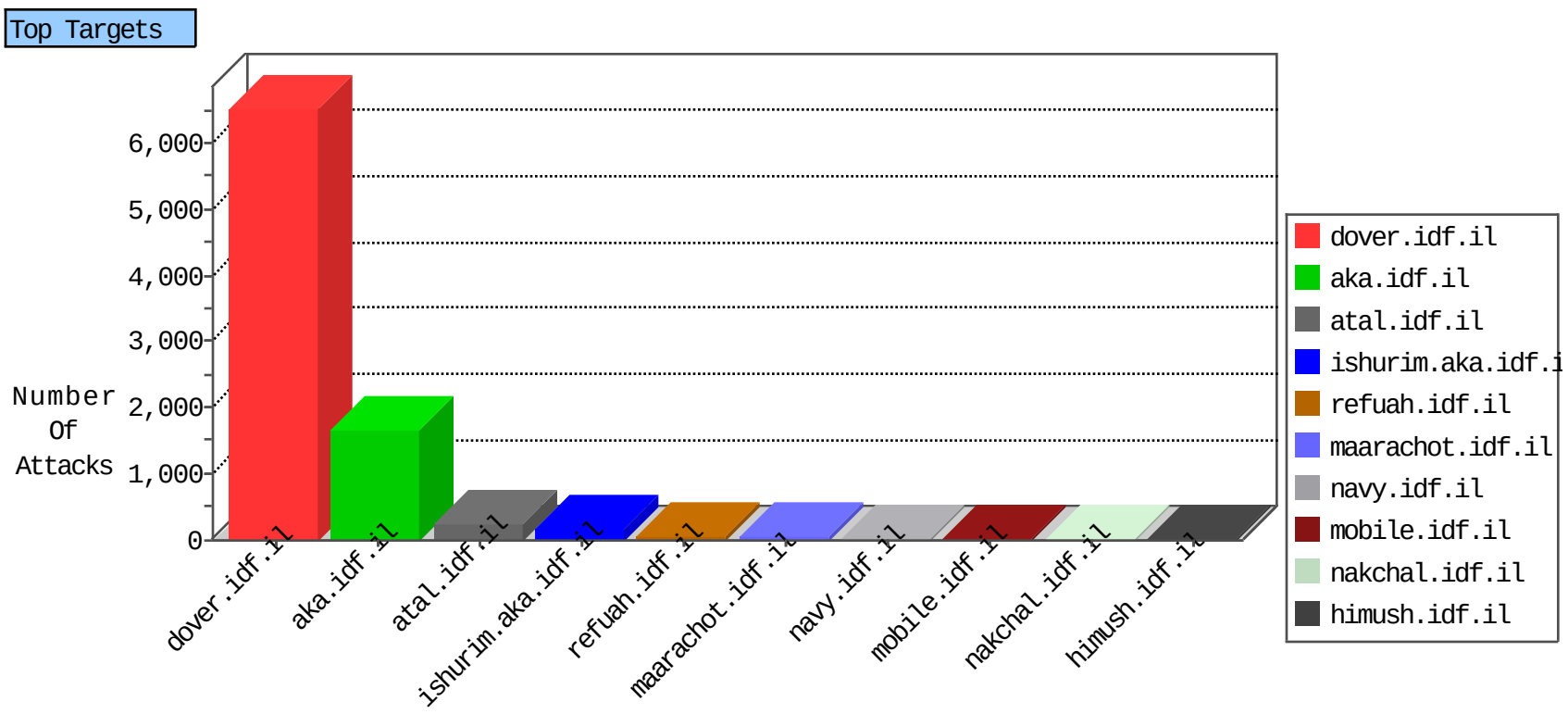
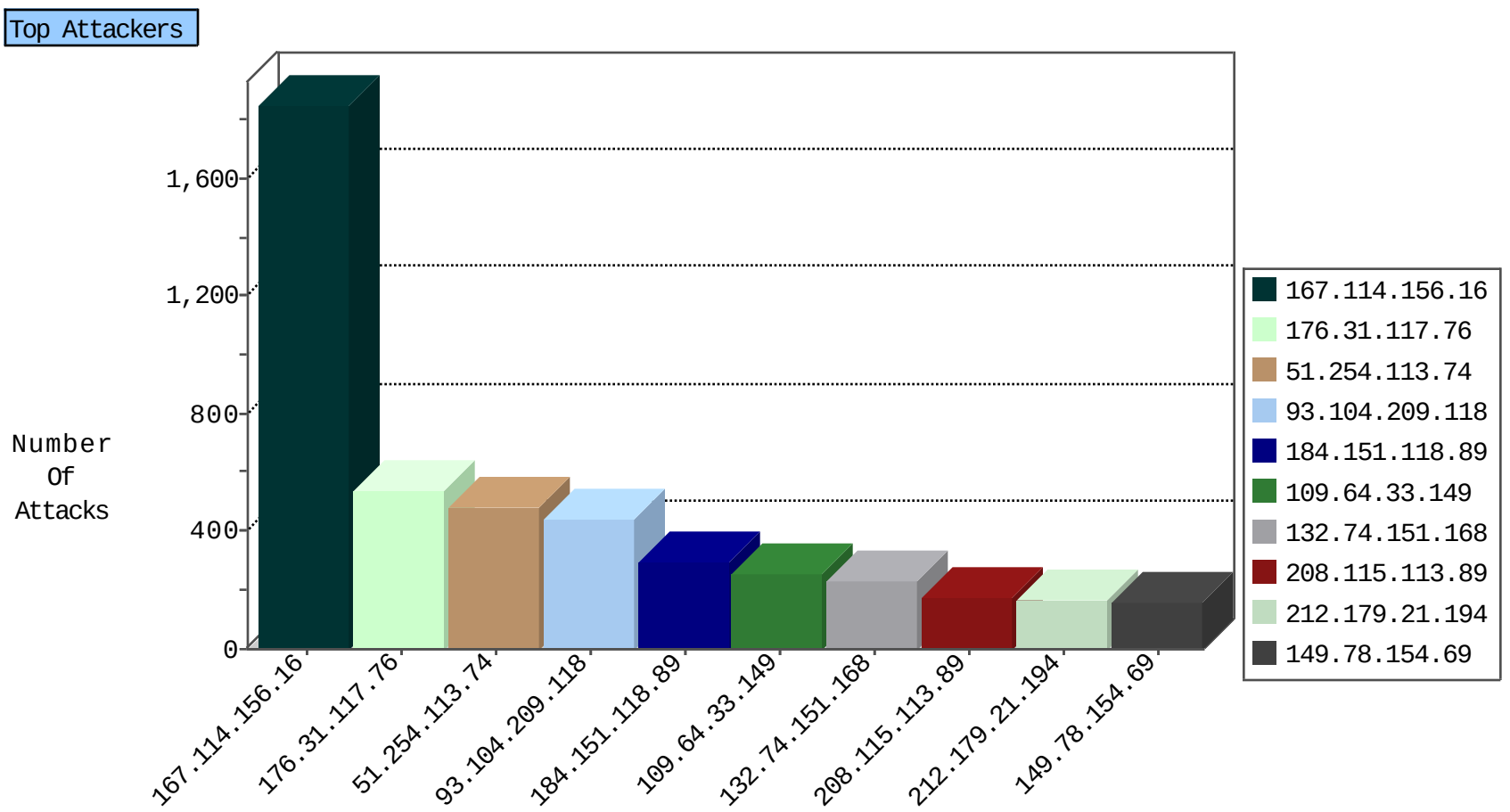
11-04-2015-08:04:00 to 11-04-2015-09:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-04-2015-08:04:00 to 11-04-2015-09:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	5475
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4914
51.254.113.74	United Kingdom	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3135
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2900
176.31.117.76	France	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2620
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2231
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2167
198.58.103.115	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1753
208.115.113.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1743
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1580
184.151.118.89	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1534
66.249.69.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1453
37.26.146.151	Israel	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	1451
143.229.240.219	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1430
66.249.67.227	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1400
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1161
66.249.69.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1056
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	960
207.232.36.181	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	912
66.249.69.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	550
123.125.71.76	China	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	406
205.203.135.1	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	229
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	198
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	193
176.13.3.150	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	58
183.56.172.222	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	20
81.218.97.114	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
93.104.209.118	Germany	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8
31.210.187.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
80.178.24.52	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
109.64.217.141	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
213.57.82.58	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	6
109.163.234.4	Romania	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
31.210.187.163	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
193.105.199.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	4
2.54.40.4	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
176.13.5.189	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
222.186.34.48	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
176.12.136.228	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.88	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
212.47.246.21	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
107.128.212.205	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
222.186.56.42	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
119.97.202.161	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2

11-04-2015-08:04:00 to 11-04-2015-09:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.145.63	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
198.20.69.74	United States	147.237.76.199	e.nakchal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

11-04-2015-08:04:00 to 11-04-2015-09:04:00

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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
122.204.139.210	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
119.97.202.161	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.155	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
2.52.2.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.107.16.206	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.82.201.17	147.237.77.216		dover.idf.il	ET DOS SSL Bomb DoS Attempt	1
176.13.3.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
119.97.202.161	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
119.90.138.214	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
85.64.52.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.19.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.102.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.114.146.227	147.237.72.167	Israel	ishurim.aka.idf.i	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
193.107.16.206	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.13.17.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

11-04-2015-08:04:00 to 11-04-2015-09:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.31.117.76	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	531
51.254.113.74	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	476
93.104.209.118	Germany	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	434
184.151.118.89	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	276
109.64.33.149	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	256
132.74.151.168	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	210
212.179.21.194	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	161
208.115.113.89	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	160
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	155
46.19.86.13	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	137
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	66
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
212.25.102.63	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
54.72.73.168	Ireland	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	47
168.63.139.43	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
2.54.28.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
193.105.199.65	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
66.249.69.34	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
149.78.251.205	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
31.210.187.163	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
46.19.86.51	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
66.249.69.42	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.69.26	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
219.74.148.42	Singapore	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
109.65.54.3	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
77.126.190.239	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
66.249.69.26	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
220.255.98.6	Singapore	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
46.120.157.148	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
84.229.134.55	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
66.249.69.34	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
81.218.251.250	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
198.50.145.72	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
132.74.151.168	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
185.58.201.28	Lebanon	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
219.74.38.145	Singapore	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
109.67.197.133	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
2.54.40.4	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
219.74.38.178	Singapore	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
183.79.223.173	Japan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
176.13.3.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
212.76.96.109	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
46.19.85.147	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	2
85.64.52.176	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
209.133.77.165	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/.	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2430.jpg	Block	1
2.54.171.204	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.14.175	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.180.49.140	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.67.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
217.69.133.223	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/17471.jpg	Block	1
46.19.85.176	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	1
84.228.220.148	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
66.249.74.108	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/112282.pdf	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.76.96.109	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
5.29.226.97	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
183.79.223.173	Japan	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
81.218.251.251	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/68320.doc	Block	1
46.19.86.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.132.201	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.52	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
5.29.226.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/pniotfindanswer.aspx	Block	1
192.115.83.5	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
82.166.22.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.79	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/×œ ×§×©×¨ ×œ×—×œ×§ ×©×ž×¡×‘×™×¨ ×¢×œ ×–×”	Block	1
46.121.133.80	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.160.191	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
109.64.108.28	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.41	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
212.199.57.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
8.37.70.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/894-he/navy.aspx&usg=alkjrhhcfxax-mo6-rrcesiii5ar-y bvlw	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res ources/images/innerpage/goback.gif	Block	1
84.228.220.148	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/news/<a href=	Block	1
54.219.117.34	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19020-he/dov	Block	1
2.54.33.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
132.74.151.168	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
77.237.154.221	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/71558.pdf	Block	1
217.69.133.220	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/69385.pdf	Block	1
194.114.146.227	Israel	147.237.72.167	ishurim.aka.idf.i	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.103	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.220.148	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.220.148	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1