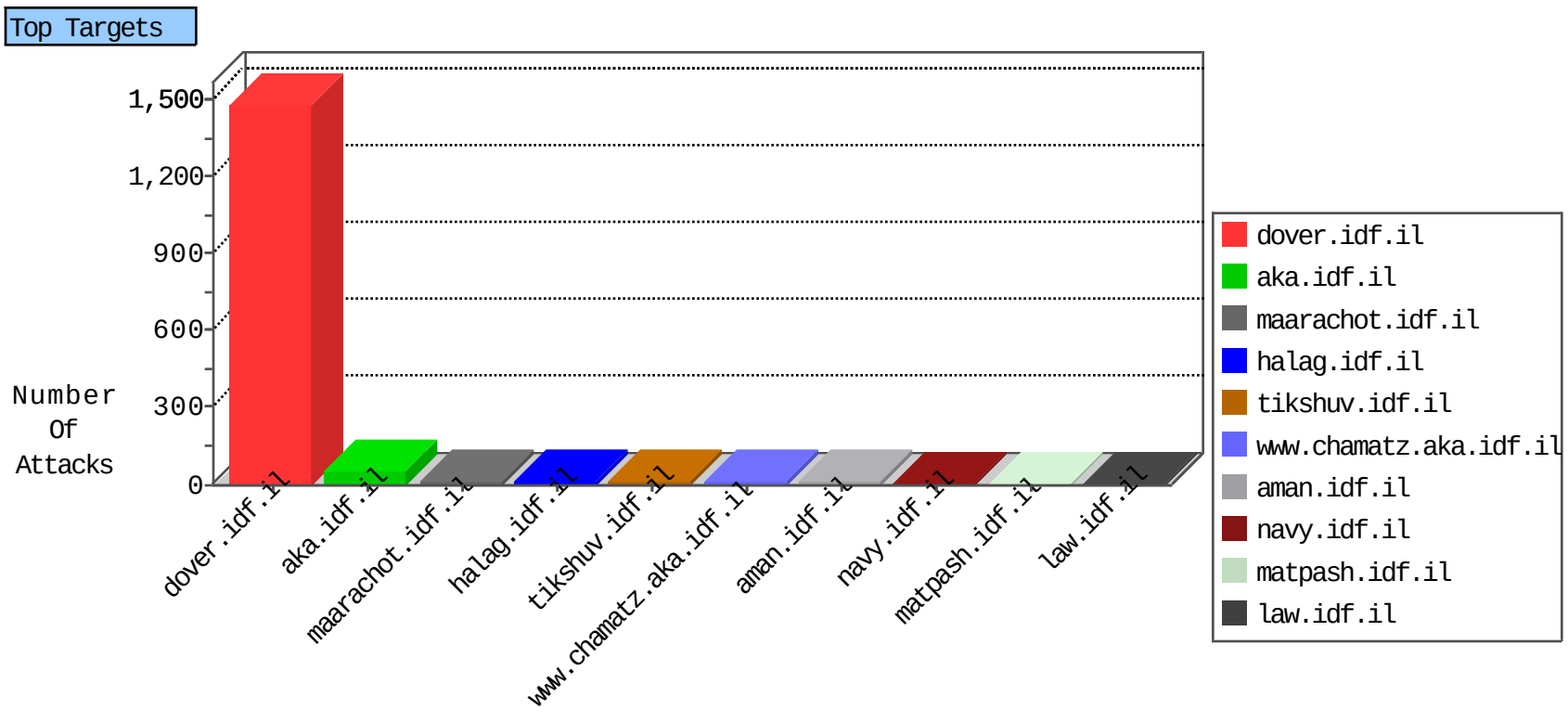
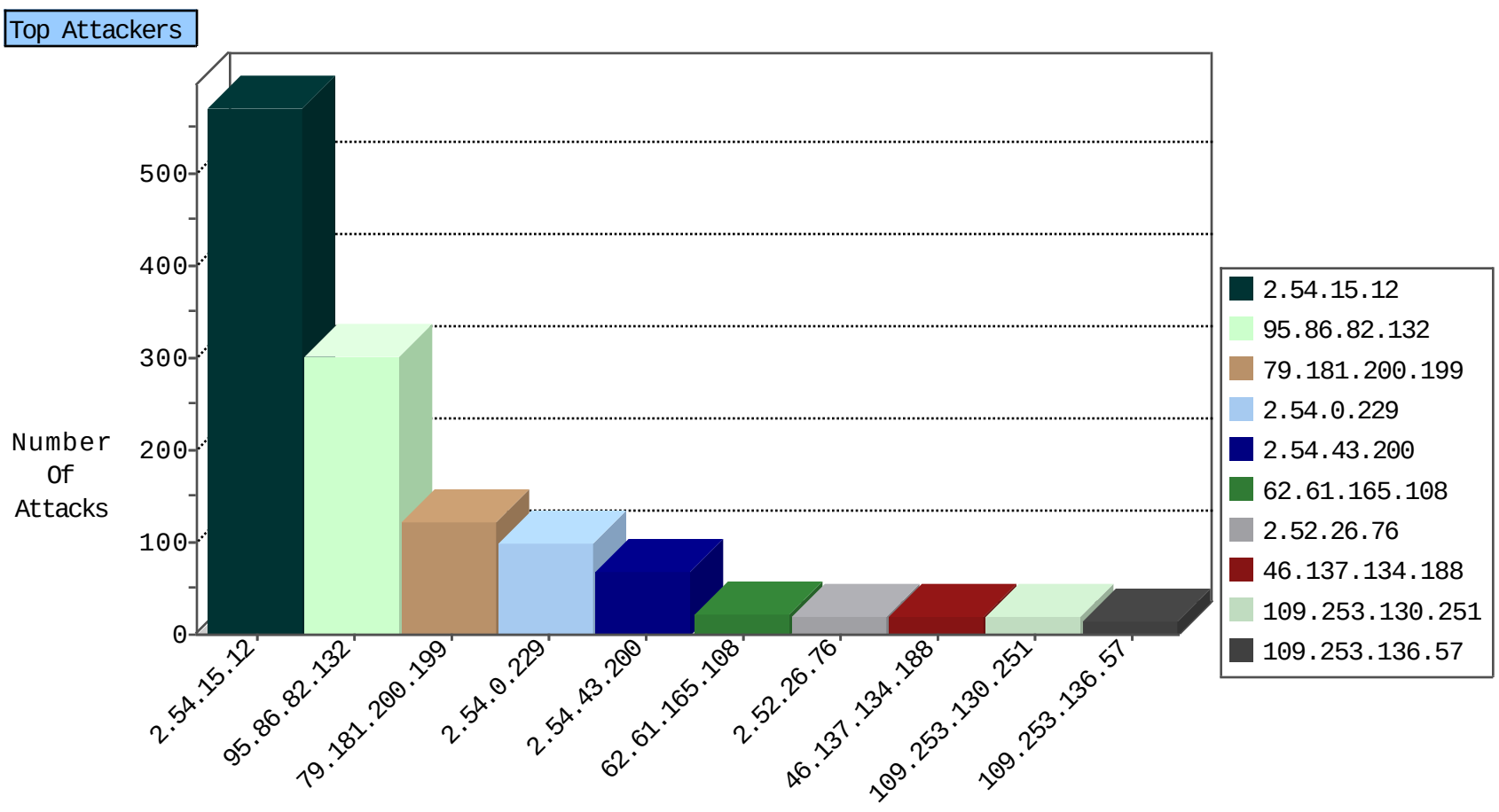
04-24-2015-17:03:03 to 04-24-2015-18:03:03

IDF Under Attack
04-24-2015-17:03:03

Top Targets



Top Attackers



04-24-2015-17:03:03 to 04-24-2015-18:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
46.19.85.204	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	531
109.66.201.146	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
220.181.108.160	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	1

04-24-2015-17:03:03 to 04-24-2015-18:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
84.109.9.69	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	2
84.109.165.72	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
79.179.146.81	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.36	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
150.210.231.30	United States	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
179.43.148.66	Switzerland	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1

04-24-2015-17:03:03 to 04-24-2015-18:03:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
109.67.177.217	Israel	147.237.0.34	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
46.120.84.189	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.41.72.13	France	147.237.77.176	matpash.idf.il	GPL SCAN nmap TCP	2
109.67.168.146	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.73.219	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.78.147	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.16.232.231	India	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.67	China	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
194.78.216.163	Belgium	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.67	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
109.67.177.217	Israel	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
61.240.144.67	China	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.132.118	Russian Federation	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.72.217	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.16.232.231	India	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.67	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
194.78.216.163	Belgium	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.67	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5800-5820	1
91.224.132.118	Russian Federation	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.132.118	Russian Federation	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

04-24-2015-17:03:03 to 04-24-2015-18:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.15.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	572
95.86.82.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	302
79.181.200.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	122
2.54.0.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	100
2.54.43.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	67
62.61.165.108	Oman	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
2.52.26.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
109.253.130.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
109.253.136.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
46.116.211.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
176.12.151.124	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.67.96	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
46.19.85.214	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
74.65.20.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
87.69.17.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
109.253.146.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
84.109.9.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.93.164	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.46.11.218	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.79.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
2.54.21.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
81.32.104.10	Spain	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
79.176.224.219	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
77.126.234.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.179.46.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
85.130.241.93	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
84.228.243.239	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.86.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.253.57.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
5.29.125.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
77.127.203.110	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
213.41.72.26	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
149.88.104.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
80.246.130.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.67.177.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
31.210.186.211	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.176.114.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.64.112.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.228.46.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.90.233.147	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
93.173.142.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.64.218.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
164.138.127.129	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.142.2.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.66.6.39	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.228.189.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.113.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
77.126.174.31	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.121.105.176	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	2
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	2
87.68.79.9	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
190.201.166.199	Venezuela	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1
46.120.55.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.149.184	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
95.86.118.207	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
79.182.207.40	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
212.66.34.134	Ukraine	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
171.96.183.156	Thailand	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1
66.249.78.148	Israel	147.237.76.30	himush.idf.il	Unknown Parameter lang in www.chimush.atal.idf.il/994-he/himush.aspx	None	1
5.29.164.40	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
109.67.162.50	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.138.192.72	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
77.126.200.143	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
194.44.127.201	Ukraine	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method COOK in URL www.cogat.idf.il/894-en/matpash.aspx	Block	1
149.88.77.229	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.57.51.209	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.183.140.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.58.14.75		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/.php.id=12	Block	1
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/french/facts.stm	Block	1
31.134.105.26	Ukraine	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
109.186.38.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
89.139.15.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
79.177.3.161	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
204.12.204.154	United States	147.237.72.166	aka.idf.il	SQL injection on parameter docId in www.aka.idf.il/chinuch/klali/default.asp	Block	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/giyus.asp	Block	1
66.249.65.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
109.65.168.178	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/popups/markivsachar.aspx	None	1
213.57.239.248	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.100.107	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
188.165.15.94	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.21	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
109.186.184.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.172.186.242	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
79.178.53.90	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
207.46.13.116	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/fund/×³Ö³Æ'Ö²Â¯Ö³â€šÖ²Â¿Ö³â€šÖ²Â½×³Ö³Æ'Ö²Â¯Ö³â€šÖ²Â¿Ö³â€šÖ²Â½×³Â§×³Ö³Æ'Ö²Â¯Ö³â€šÖ²Â¿Ö³â€šÖ²Â½×³Ö³Æ'Ö²Â¯Ö³â€šÖ²Â¿Ö³â€šÖ²Â½	Block	1
157.55.39.12	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/894-he/refuah.aspx	Block	1
66.249.65.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
109.67.39.130	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
87.68.60.78	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
190.42.152.243	Peru	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
46.120.24.190	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
149.78.112.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
95.86.98.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
79.182.115.27	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.135	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1244-he/atal.aspx	Block	1