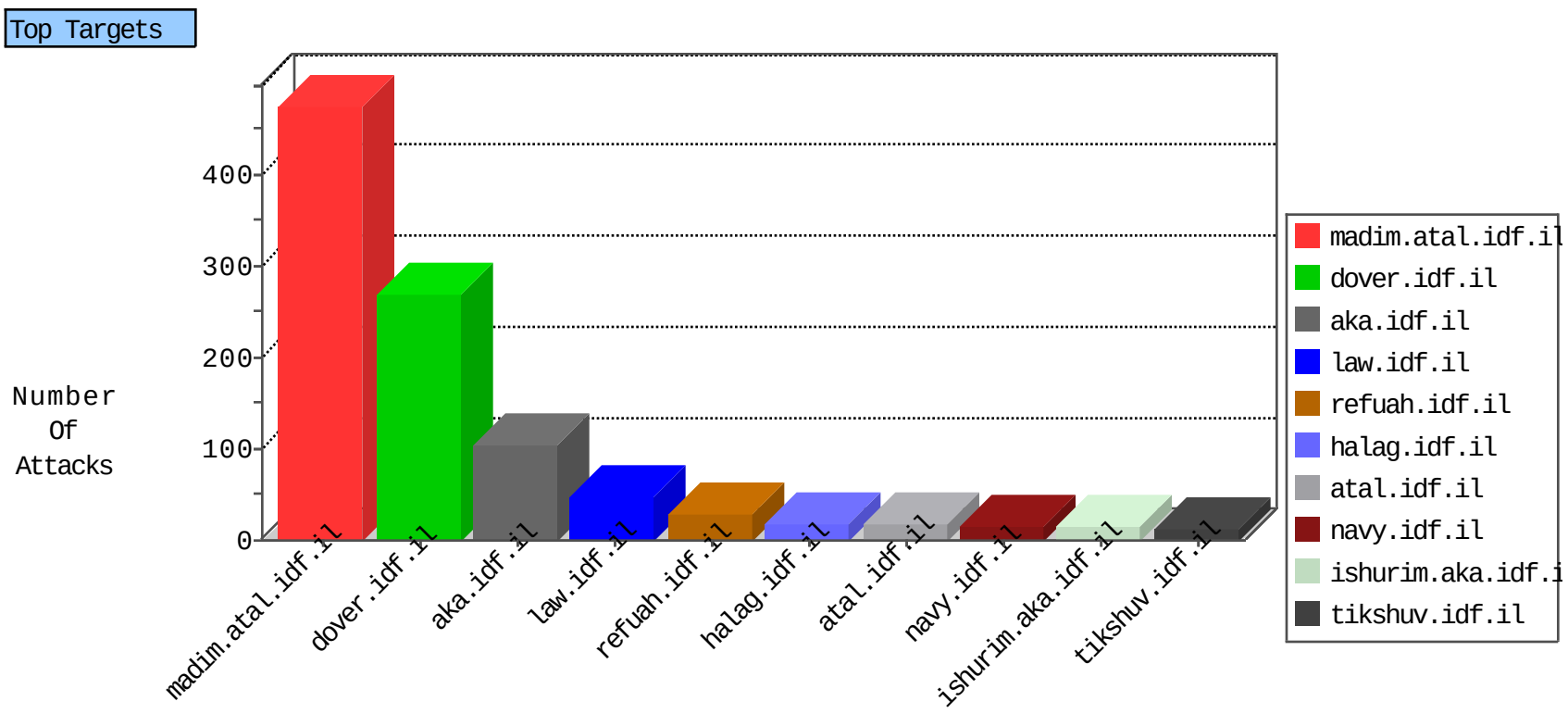
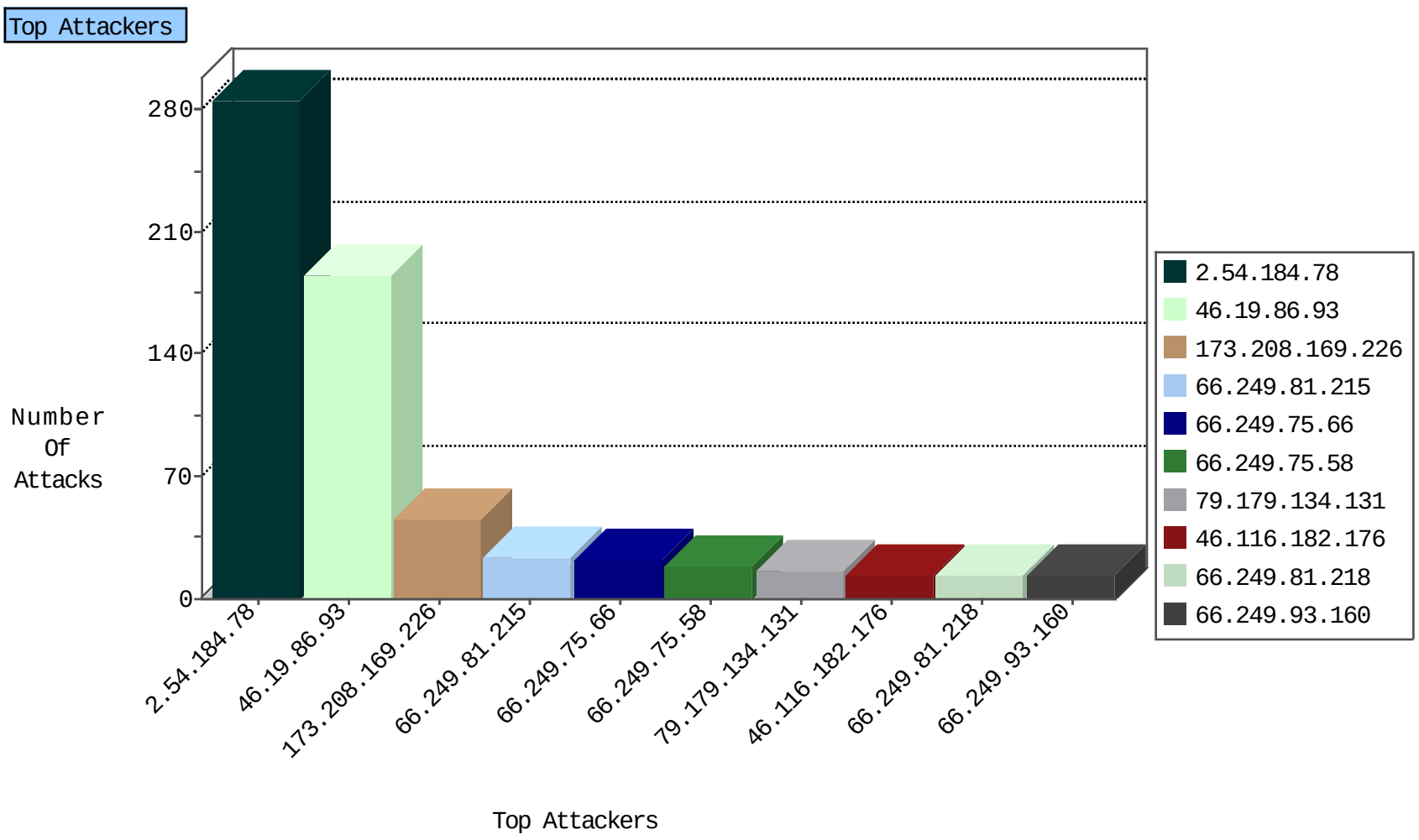
04-01-2015-20:03:03 to 04-01-2015-21:03:03

IDF Under Attack
04-01-2015-20:03:03

Top Targets



Top Attackers



04-01-2015-20:03:03 to 04-01-2015-21:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
77.125.145.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
199.180.114.192	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
202.103.220.101	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.53	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

04-01-2015-20:03:03 to 04-01-2015-21:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.116.182.176	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
149.78.215.133	United States	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.19.85.71	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
194.98.203.34	France	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.160.149.223	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
151.177.106.92	Sweden	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	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	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
176.58.66.97	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
93.172.192.72	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	7610: IP Reputation	Block	1
46.19.86.93	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
77.125.215.218	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	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
79.179.134.131	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1

04-01-2015-20:03:03 to 04-01-2015-21:03:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
84.110.209.9	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.14.231	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.123	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
91.121.10.32	France	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	1
66.249.69.122	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.240.144.67	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
200.146.119.102	Brazil	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.170	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
117.79.156.130	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
117.79.156.130	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
222.236.44.115	Korea, Republic of	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
200.146.119.102	Brazil	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.170	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
169.54.237.52	Switzerland	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.170	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
117.79.156.130	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1

04-01-2015-20:03:03 to 04-01-2015-21:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
173.208.169.226	United States	147.237.77.74	law.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	22
66.249.75.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
66.249.75.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.93.160	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
109.253.158.26	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.133.80	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.139.207	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.75.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
31.210.186.132	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
79.179.134.131	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	10
46.19.85.33	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
46.116.182.176	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.93.164	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.158.196	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
2.54.184.78	Israel	147.237.0.19	madim.atal.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
85.65.100.81	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
84.108.22.44	Israel	147.237.76.31	nakchal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	5
46.19.85.205	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
46.19.85.244	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
79.179.134.131	Israel	147.237.77.234	halag.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	4
188.120.148.245	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
46.19.85.205	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
31.168.208.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
93.86.203.38		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
188.120.148.147	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
46.19.85.155	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.85.155	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
46.19.85.223	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
31.210.186.174	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
37.46.39.78	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.117.80.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.52.154.204	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
46.19.85.38	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
109.253.143.109	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
185.32.177.24	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
109.253.133.38	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
54.241.198.78	United States	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	2
2.52.154.204	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
185.32.177.24	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
46.19.85.33	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
66.249.64.96	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
84.108.22.44	Israel	147.237.77.74	law.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
176.12.138.29	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.184.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	280
46.19.86.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	184
173.208.169.226	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 173.208.169.226	Block	21
188.120.148.245	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.184.195.166	Block	4
209.15.21.94	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//english/&quot	Block	3
37.59.29.19	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
109.65.68.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
66.249.75.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.66	Block	2
109.67.130.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.244	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
81.218.226.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
54.197.65.97	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
37.16.72.139	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.16.72.139	Block	2
77.127.54.175	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
83.130.101.107	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.111.225.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/updateuserdetails.aspx	Block	1
54.241.198.78	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/&quot	Block	1
212.199.239.56	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
79.181.189.185	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
2.54.152.36	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.138.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.226.200	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
66.249.75.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
91.121.10.32	France	147.237.72.166	aka.idf.il	Multiple signatures from 91.121.10.32	Block	1
46.120.129.92	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
203.133.171.92	Korea, Republic of	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
84.108.22.44	Israel	147.237.76.31	nakchal.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
79.178.97.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/default.aspxgiyus	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
173.208.169.226	United States	147.237.77.74	law.idf.il	Admin Blocking	Block	1
84.228.103.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter isTaz in aka.idf.il/main/sachar/	None	1
58.22.77.143	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/2/4082.pdf/trackback/	Block	1
217.132.99.222	Israel	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to www.e.lc4.gov.il/trytrh.php	Block	1
46.19.85.63	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
188.225.171.154	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
79.182.190.39	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
109.253.145.212	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.237.138.51	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
94.230.92.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
84.108.69.216	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
46.121.247.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
207.46.13.79	United States	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
79.178.174.136	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
37.16.72.139	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
77.125.95.164	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/statistics/gens.stm	Block	1
84.229.185.183	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.219.133.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.0.80.128	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//english/&quot	Block	1