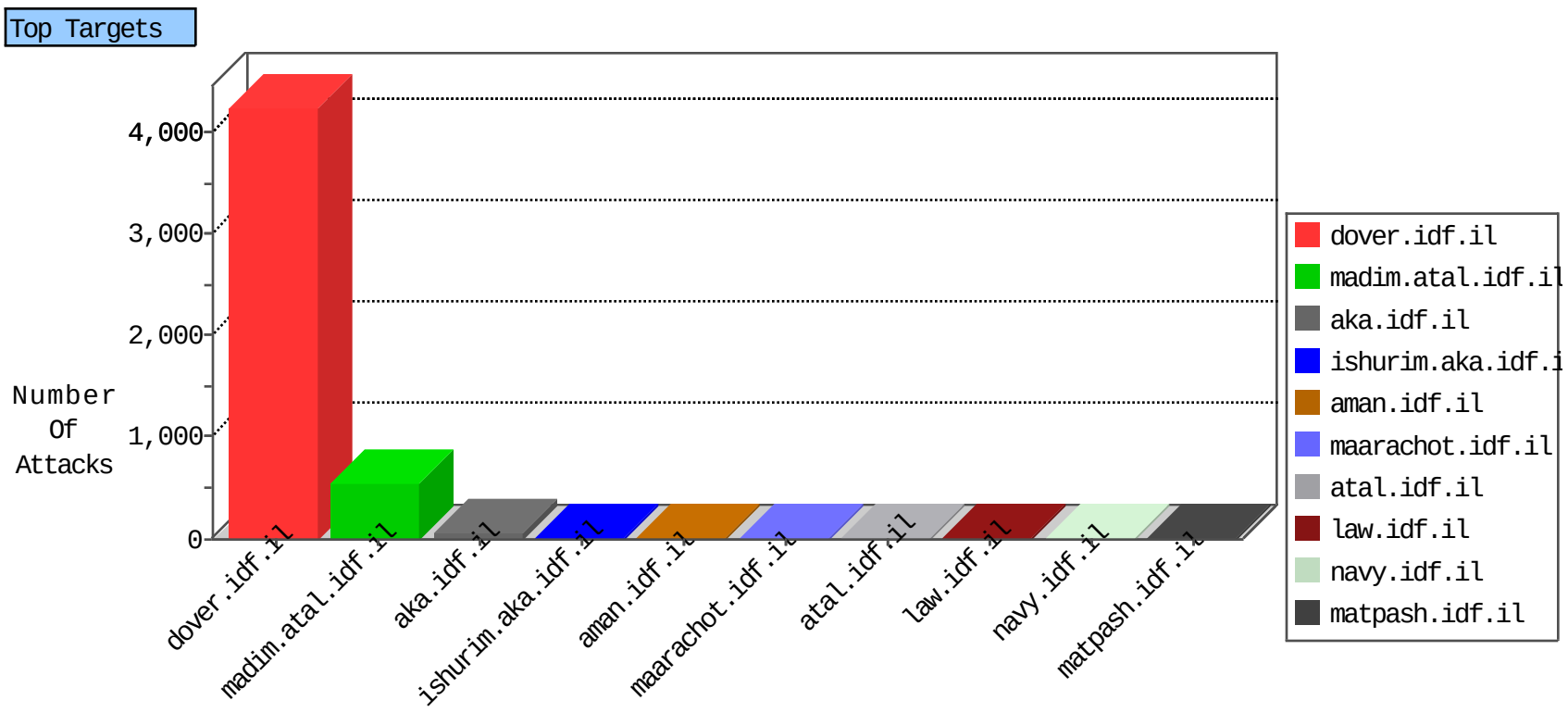
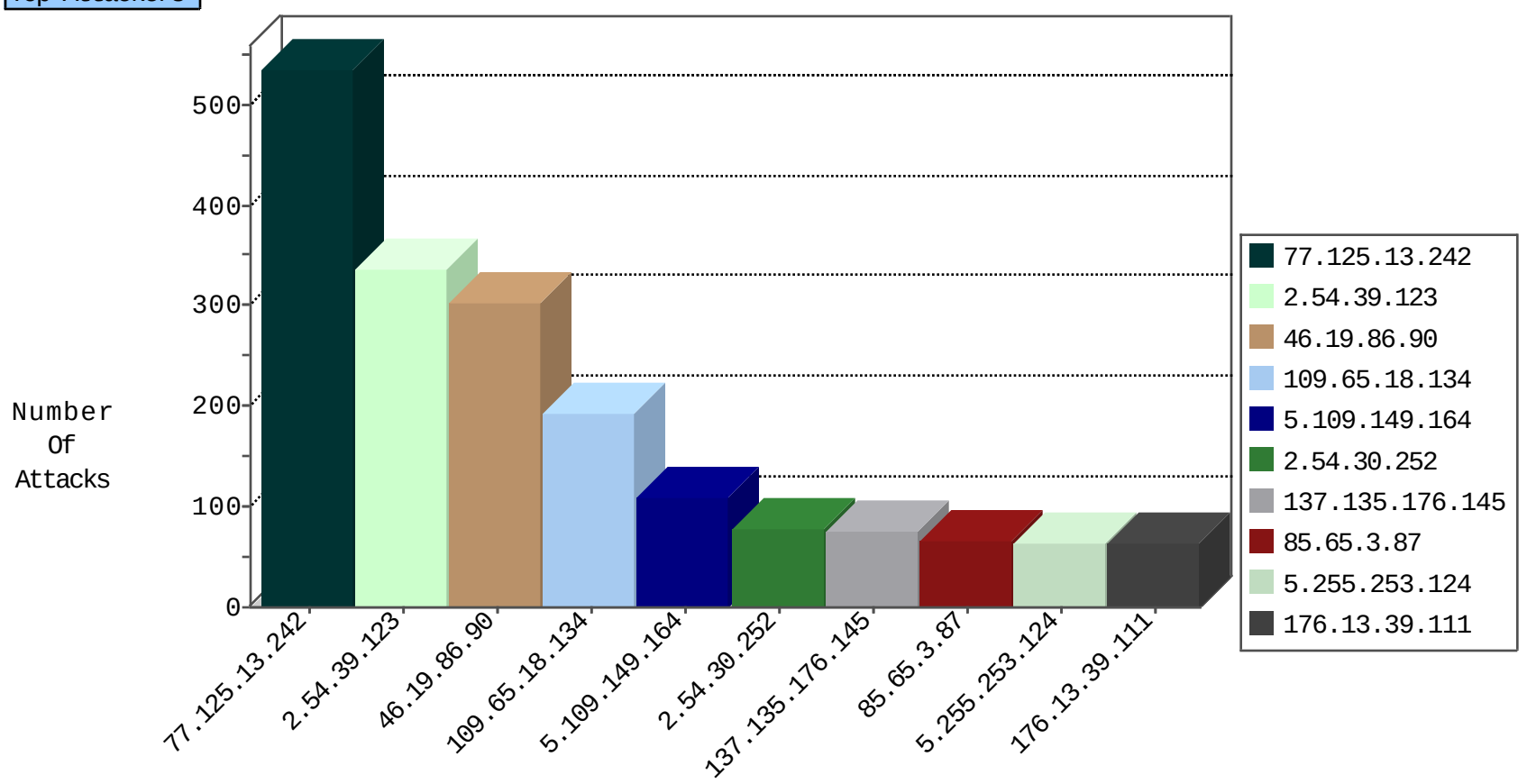
04-18-2015-12:03:08 to 04-18-2015-13:03:08

IDF Under Attack
04-18-2015-12:03:08

Top Targets



Top Attackers



04-18-2015-12:03:08 to 04-18-2015-13:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	810
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	541
5.29.163.91	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
31.210.187.193	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	46
137.135.176.145	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	27
212.129.61.222	France	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
203.142.62.80	Malaysia	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
212.71.237.205	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.129.61.222	France	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

04-18-2015-12:03:08 to 04-18-2015-13:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.176.30.122	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.250.139.7	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	2
46.19.85.54	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.197	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
84.109.69.125	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.65.131.185	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-18-2015-12:03:08 to 04-18-2015-13:03:08

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	16
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.72	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
168.235.154.235		147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
113.21.226.56	New Zealand	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
176.12.139.10	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
168.235.154.235		147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.144.56	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

04-18-2015-12:03:08 to 04-18-2015-13:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.39.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	337
46.19.86.90	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	304
109.65.18.134	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	193
5.109.149.164	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	108
2.54.30.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	77
137.135.176.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	74
85.65.3.87	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	65
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
212.71.237.205	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	60
176.13.39.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
109.186.32.182	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
46.121.214.59	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
109.66.69.153	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
46.120.137.164	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
46.19.85.197	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
85.250.132.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
66.249.93.164	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
82.102.141.248	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
176.12.140.254	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
79.178.155.6	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
2.54.136.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
176.12.138.246	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
82.102.170.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
136.243.36.88	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
188.120.148.205	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
109.253.144.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
2.54.135.218	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
79.181.29.10	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
82.80.25.221	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
109.253.158.30	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
84.228.158.65	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
109.67.130.187	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
109.67.16.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
62.219.123.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
85.250.139.7	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
2.52.167.227	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
204.237.22.235	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
109.253.136.124	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
82.205.66.168	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
77.127.134.53	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
37.218.210.48	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
207.46.13.35	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
46.19.85.54	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
109.253.137.134	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.125.13.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	536
79.178.133.232	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	5
136.243.36.88	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 136.243.36.88	Block	5
79.180.169.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
87.68.76.249	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
190.107.177.252	Chile	147.237.76.42	refuah.idf.il	PHP Attempt	Block	2
64.50.185.11	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	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
109.66.38.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
79.176.148.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 202.112.50.77	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
66.249.64.20	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/scriptresource.axd	Block	1
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.63	Block	1
109.66.185.144	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/templates/journalview/journalview.aspx	Block	1
64.50.185.11	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Unknown HTTP Request Method quit in URL	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0123-2.stm	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.213	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.64.22	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/giyus/faq.aspx	None	1
93.172.143.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
5.28.135.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.125.94.196	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.78.94	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133	Block	1
180.76.5.65	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/shared/clientscripts/jquery/' + url + '	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Unknown Parameter do in www.aka.idf.il/chinuch/klali/default.asp	None	1
93.172.166.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
41.223.215.114	Gambia	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
77.237.138.51	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18775-he/dover.aspx	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Malformed URL	Block	1
136.243.36.88	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1589- en/dover.aspx	Block	1
66.249.64.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
79.183.109.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iis)+dos+and+possible+remote+code+execution.+patch+now/19583	Block	1
66.249.64.16	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on 147.237.76.86//scriptresource.axd	Block	1
66.249.81.222	Israel	147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/../favicon.ico	Block	1
188.165.15.206	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/news/×¢×œ ×?×£ ×©×?×™ × ×• × ×—×©×' ×¡×˜×•×"× ×˜ ×¢×œ ×¤×™ ×§×•×'×¥ ×"×•×¨×?×• ×ª ×"×§×¨×™×?×" ×œ×©×ž"×¤, ×¨×©×?×™ ×œ×"×'×™×© ×'×§×©×" ×ž×"×•×¨ ×•×œ×ª"×?.	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=2&catid=22703&docid=22716	Block	1
109.65.71.84	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1