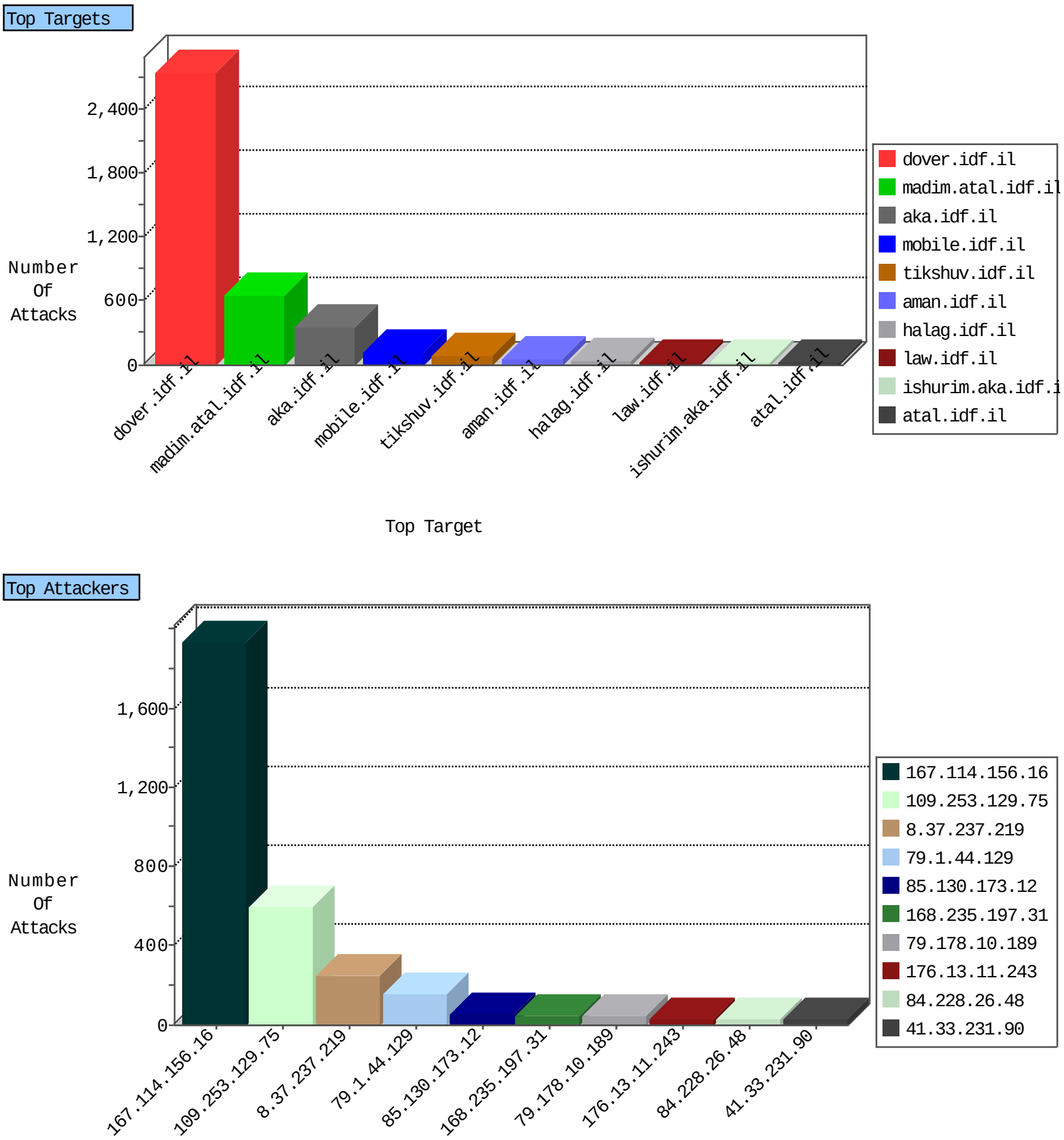
01-07-2016-18:04:09 to 01-07-2016-19:04:09

IDF Under Attack Daily Report



01-07-2016-18:04:09 to 01-07-2016-19:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3516
8.37.237.219	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	64
8.37.237.219	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	37
188.242.107.124	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
66.249.66.28	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
37.26.146.237	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
8.37.237.219	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
168.235.197.31	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

01-07-2016-18:04:09 to 01-07-2016-19:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-07-2016-18:04:09 to 01-07-2016-19:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
58.253.96.122	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -f -sS	1
222.186.21.92	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
40.77.167.16	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.241.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.120.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.161.194.97	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.131.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.101.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.100.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
69.248.129.181	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
222.186.21.92	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.86.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.21.92	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.26.147.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.83.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.13.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.86.109.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.111.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.115.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.153	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1

01-07-2016-18:04:09 to 01-07-2016-19:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.1.44.129	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	154
8.37.237.219	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	110
168.235.197.31	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	48
8.37.237.219	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	40
84.228.26.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
107.167.103.225	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
176.13.10.30	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
80.246.133.211	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
85.130.173.12	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.85.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
85.130.173.12	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.13	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
62.0.200.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
84.228.78.60	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
149.88.5.20	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
84.228.5.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.160.144.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.160.144.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
85.130.173.12	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
198.204.249.34	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
8.37.237.219	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.90	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.130.173.12	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
209.56.132.253	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
94.230.86.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.170.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.24.164	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
167.58.28.235	Uruguay	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.3.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.158.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.88.148.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
167.58.28.235	Uruguay	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
167.58.28.235	Uruguay	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.20.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.164.221	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.196	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.190.5	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
31.13.112.120	Ireland	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.129.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	373
109.253.129.75	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	118
109.253.129.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	102
79.178.10.189	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.178.10.189	Block	44
8.37.237.219	United States	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	33
176.13.11.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
85.130.129.175	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
176.13.10.30	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.20.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.145.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.139.52.25	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.253.147.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.68.51.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.193.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.66	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
2.52.1.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.88.52.63	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.88.52.63	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.19.85.43	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
84.228.104.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.8.204.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.164.221	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
198.71.228.21	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
109.253.132.177	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.176.178.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.162.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1882	Block	1
157.55.39.75	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.42.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.216.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.230.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
79.180.19.112	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	1
46.19.85.240	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
109.160.167.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
41.96.63.21	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
93.173.232.205	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
2.54.52.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.130.173.12	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.230.230.230	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
149.88.51.21	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
80.246.136.103	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1