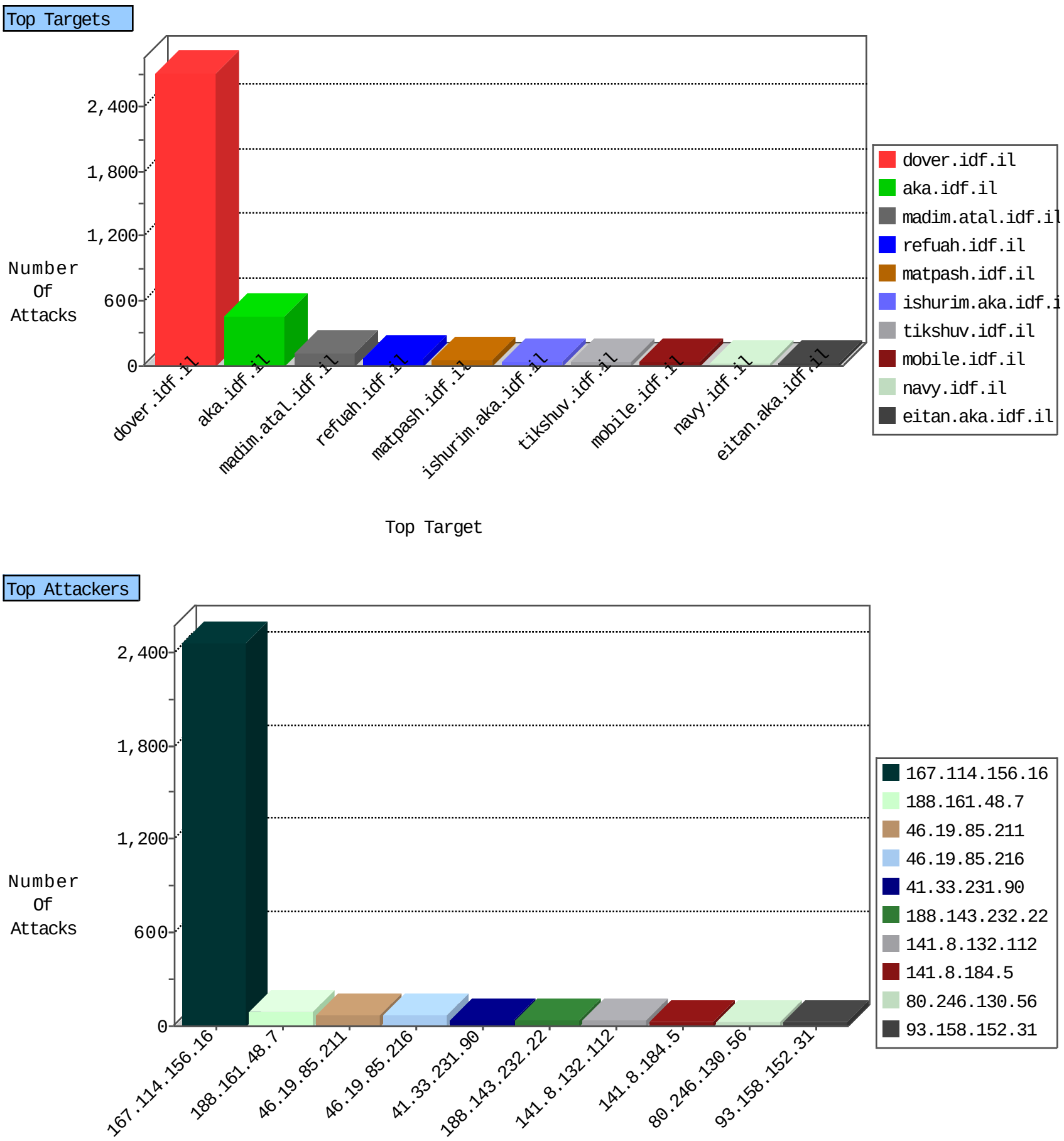
01-24-2016-08:04:00 to 01-24-2016-09:04:00

IDF Under Attack Daily Report



01-24-2016-08:04:00 to 01-24-2016-09:04:00

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	3070
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
204.42.253.2	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
159.104.163.17	United Kingdom	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
89.248.174.4	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
159.104.163.18	United Kingdom	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
168.235.197.44	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1
89.248.174.4	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
159.104.163.19	United Kingdom	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
159.104.163.20	United Kingdom	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1

01-24-2016-08:04:00 to 01-24-2016-09:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.20.9.132	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1

01-24-2016-08:04:00 to 01-24-2016-09:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
163.172.13.173	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.63.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.161.40.120	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
109.67.158.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.186.12	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
39.191.155.176	147.237.76.198	China	e.yohalan.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

01-24-2016-08:04:00 to 01-24-2016-09:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
141.8.184.5	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
188.161.48.7	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
93.158.152.31	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
80.246.130.56	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
188.161.48.7	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	24
168.235.197.44	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
141.8.184.25	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.181.212.46	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
188.143.232.22	Russian Federation	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
2.52.33.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.19.85.122	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
188.143.232.22	Russian Federation	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.22	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
157.55.39.169	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.179.10.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
188.161.48.7	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
188.161.48.7	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
188.161.48.7	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
188.161.48.7	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
207.46.13.104	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.81.212	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
176.13.4.95	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
81.218.178.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
207.46.13.7	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.253.192.88	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.161	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.65.105.196	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.135.102.176	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.2.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.69.189.146	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.69.189.146	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.22	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.143.232.22	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.178.138.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.178.138.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

01-24-2016-08:04:00 to 01-24-2016-09:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.22	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
109.253.192.88	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.179.191.202	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
81.218.118.126	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 81.218.118.126	Block	17
46.19.85.211	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.211	Block	13
46.19.85.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
89.248.110.167	Spain	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.248.110.167	Block	10
176.13.1.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
185.32.179.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.54.189.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
176.13.23.95	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	3
46.19.85.48	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
109.253.200.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.145.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.21.158	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.21.158	Block	3
2.54.22.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.12.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.19.86.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.21.158	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1564	Block	2
80.178.98.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.102	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/searchresults/searchresults.aspx	Block	1
176.13.1.166	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1272-he/atal.aspx	Block	1
109.253.158.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
94.199.151.22	United Kingdom	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.69.33	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/110731.pdf	Block	1
212.179.129.6	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.178.57.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17275-he/×—×™×œ ×″ ×?×•×•×™¨ ×ª×§×£ ×©×œ×•×© ×žx˜×¨×•×ª ×˜×¨×•× ×‘ ×¨×¦×•×¢″ ×‘×ª×•×›× ×″×§×˜×•×ª.aspx	Block	1
66.249.78.51	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/107830.pdf	Block	1
2.52.2.7	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
89.248.110.167	Spain	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/application/configs/application.ini	Block	1
49.151.28.85	Philippines	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
193.34.56.101	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
80.179.109.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.154.183	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
109.253.192.88	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.69.49	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
212.227.106.175	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
94.242.228.108	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.95.226.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.100.100	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
5.29.104.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.81.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/107131.pdf	Block	1
2.52.60.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.129.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1