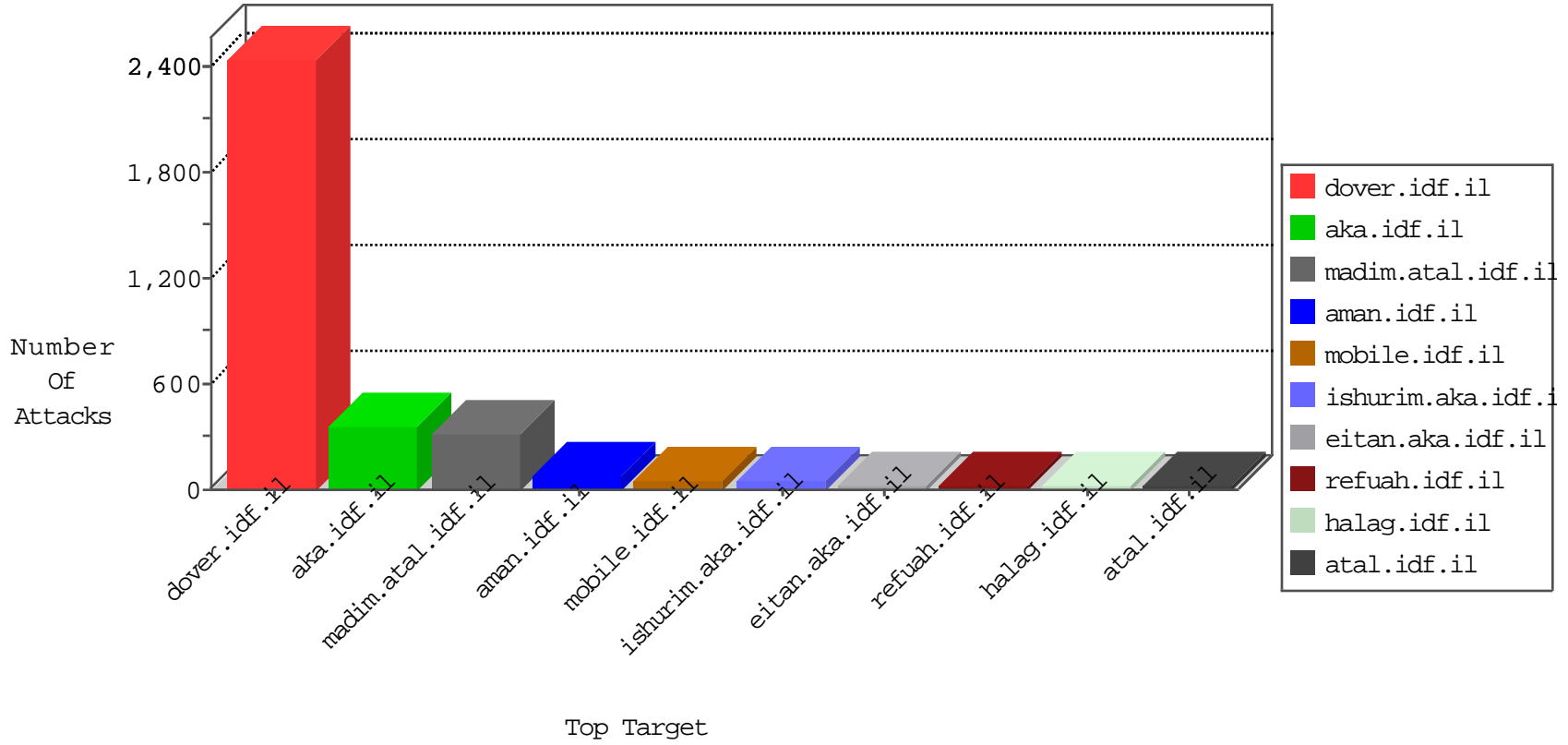


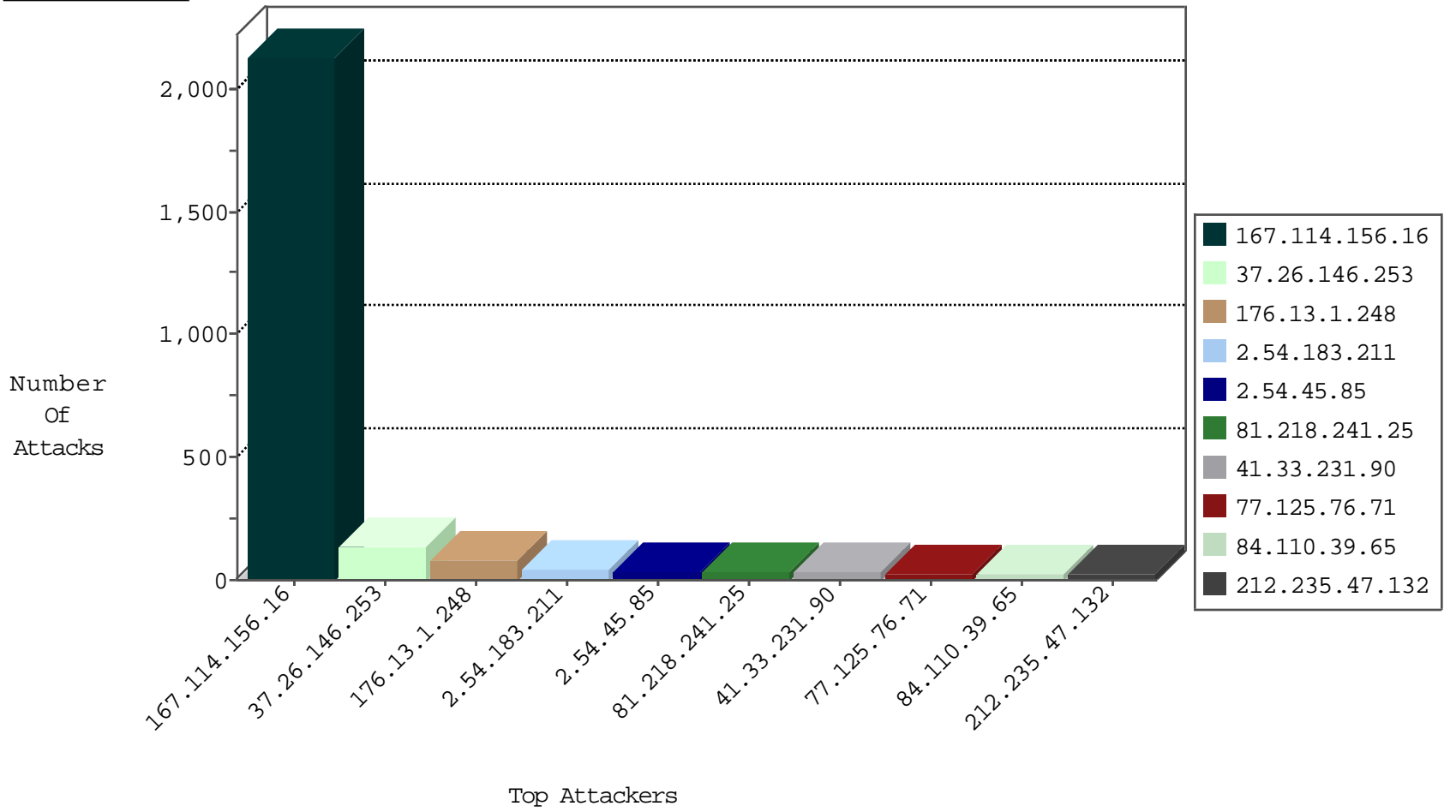
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3119
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	151
109.65.161.151	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
109.65.161.151	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	3
79.177.239.228	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
114.207.112.188	Korea, Republic of	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
81.218.101.250	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
94.102.51.30	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
86.106.18.76	Romania	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

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
66.249.78.2	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
79.177.207.46	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	1
219.153.15.122	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
2.54.183.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
182.75.6.126	147.237.77.226	India	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
178.20.72.19	147.237.76.44	Italy	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
140.242.217.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.201.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.241.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.160.240.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.46.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.107	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
182.75.6.126	147.237.0.17	India	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
119.42.86.144	147.237.76.34	Thailand	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
87.68.245.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.11.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
77.125.76.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
84.110.39.65	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
213.57.90.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.183.211	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
2.54.183.211	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.86.184	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
212.235.47.132	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
2.52.181.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.183.211	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
82.81.32.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.133.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.47.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.132	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
62.0.207.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	7
207.232.37.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.86.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.148.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.28.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.172.143.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.168.179.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
93.172.191.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.172	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.155.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
93.172.143.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.190.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.144.108	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.120.167.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
81.218.50.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.148.172	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	alert	5
185.7.120.101	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.148.172	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	5
212.235.47.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.117.137.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.158.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.120.148.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.186.44.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.158.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
176.13.14.17	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
176.13.1.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
2.54.45.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
37.26.146.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
84.109.154.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.13.11.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.54.137.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.13.5.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.85.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.1.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
109.253.133.218	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Parameter Type Violation on m.my-kosher-kravi.idf.il/templates/login.aspx parameter returnUrl	Block	4
46.19.85.114	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.85.114	Block	4
109.65.42.92	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.65.42.92	Block	3
37.26.148.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.25.102.63	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 212.25.102.63 (Unknown SSL Session)	None	3
2.54.47.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.8.147	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
91.200.12.139	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.114	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
2.52.32.19	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.120.167.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.149.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.182.217.137	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
46.19.85.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.50.127.119	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
8.37.71.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/&usg=alkjrh31qub0ic-yxqjluivptitn_gua	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/englisch	Block	1
212.199.57.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1361-10651-he/dover.aspx	Block	1
176.13.22.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
91.200.12.139	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 91.200.12.139	Block	1
176.12.151.204	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	1
84.108.174.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.18.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
5.22.134.51	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.54.15.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.230.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.166.190.175	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.111	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
157.55.39.253	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/giyus/qanda/default.asp	None	1
81.218.74.164	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
37.26.146.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.42.92	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/62532.pdfg2=whvq9jgvov3igm-oflegda	Block	1