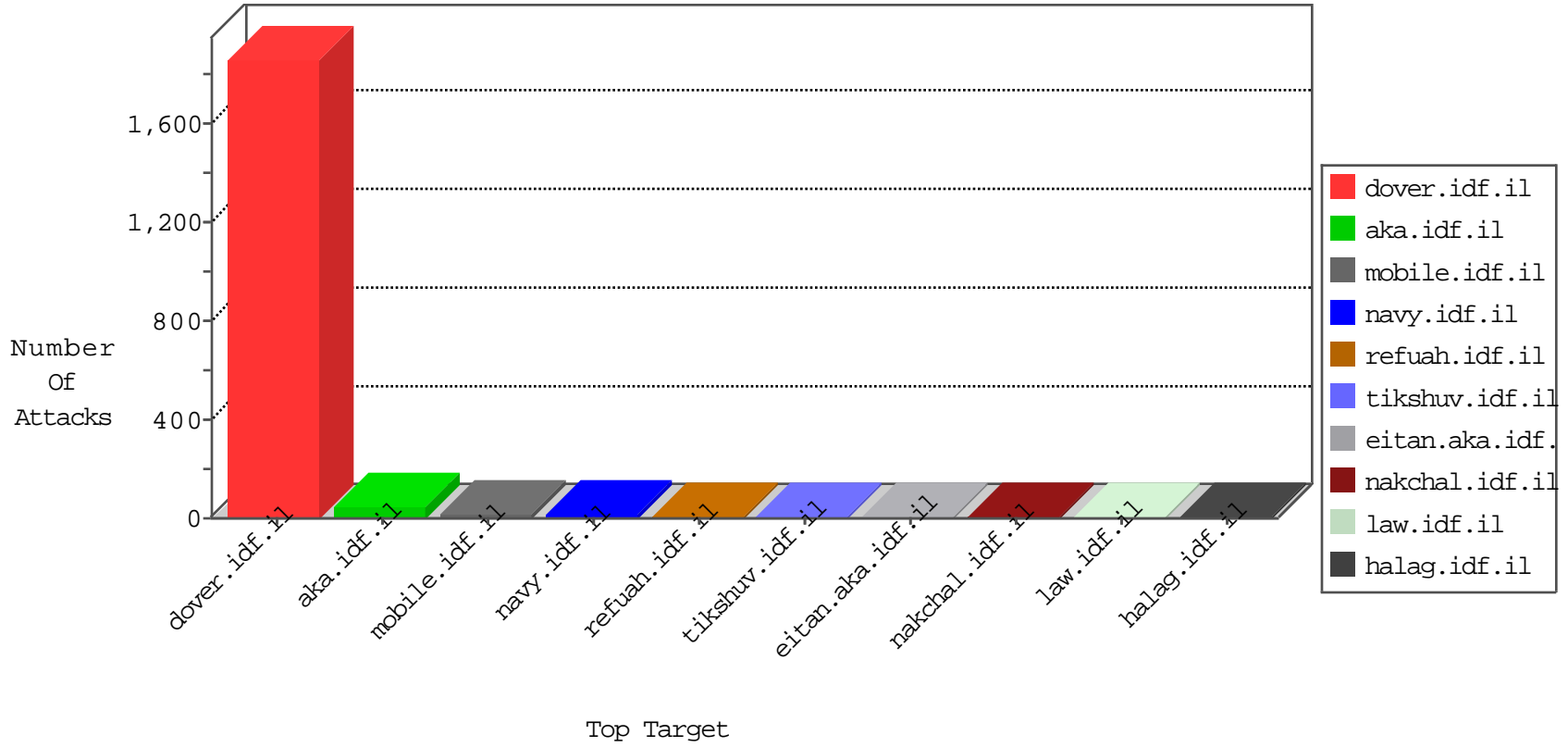


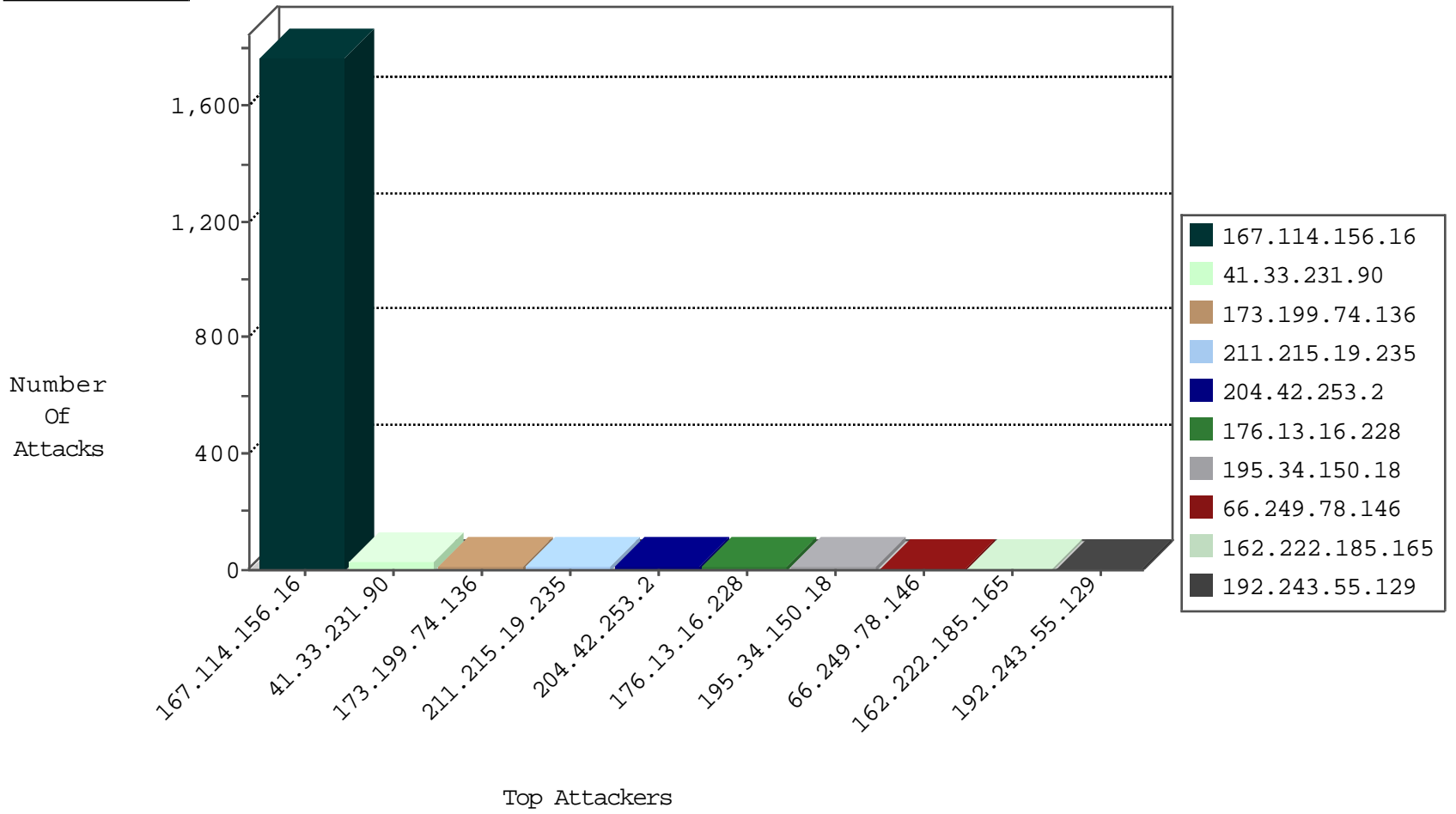
IDF Under Attack Daily Report



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	3026
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	555
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
162.222.185.165	United States	147.237.76.199	e.nakchal.idf.il	JIM_Purple_Con_Limit_Tcp	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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	4
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
115.182.17.13	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
211.215.19.235	147.237.77.234	Korea, Republic of	halag.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.215.19.235	147.237.77.226	Korea, Republic of	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
173.199.74.136	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
211.215.19.235	147.237.77.179	Korea, Republic of	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
37.210.54.24	147.237.77.74	Qatar	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.199.74.136	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.215.19.235	147.237.77.176	Korea, Republic of	matpash.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.215.19.235	147.237.77.74	Korea, Republic of	law.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.215.19.235	147.237.77.19	Korea, Republic of	law-forum.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
177.236.4.75	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.222.185.165	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
211.215.19.235	147.237.77.243	Korea, Republic of	mobile.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
115.182.17.13	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
211.215.19.235	147.237.77.233	Korea, Republic of	atal.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.76.198	United Kingdom	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.215.19.235	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.215.19.235	147.237.77.178	Korea, Republic of	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.215.19.235	147.237.77.121	Korea, Republic of	e.navy.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
211.215.19.235	147.237.77.61	Korea, Republic of	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
190.252.174.186	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.222.185.165	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	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
176.13.16.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.24.194	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
168.235.197.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
65.55.210.100	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
180.183.44.128	Thailand	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.67.33.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.186.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.200.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.129	Dominica	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
45.55.53.138		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
109.253.132.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
74.82.47.20	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.243.55.129	Dominica	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
176.228.20.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
104.200.154.84	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.89	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.133.169.220	Korea, Republic of	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.59	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.17.130	Germany	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
149.202.240.85	Germany	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.106	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
173.254.216.69	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.90	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.49	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
192.243.55.129	Dominica	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.76.15.137	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.202.240.85	Germany	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.199	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
141.212.122.107	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.44.224.176	Spain	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
192.243.55.129	Dominica	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
180.180.122.22	Thailand	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
149.202.240.85	Germany	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.69	United States	147.237.0.35	akaws.idf.il	drop		drop	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.20	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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
31.210.188.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
207.46.13.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
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	2
66.249.69.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1726	Block	1
192.243.55.136	Dominica	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/shared/usercontrols/headerupper	Block	1
181.29.223.92	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
207.46.13.157	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19116-en/dover.aspxhaz	Block	1
66.249.78.199	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.asp	Block	1
46.19.86.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	1
109.66.191.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.112	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58570&docid=65113	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/haredim/general.aspx	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.aspx	Block	1
5.102.253.8	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.108.38.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69681.pdf	Block	1
62.210.77.51	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=62160&docid=76640	Block	1
109.201.154.164	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9004-he/refuah.aspx	Block	1
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	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	1
23.239.10.144	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
94.242.250.117	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3048.jpg	Block	1
213.8.204.33	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
192.243.55.135	Dominica	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/110539.pdf,	Block	1
157.55.39.2	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
74.82.47.3	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/klali/default.asp?catid=43334&docid=46161	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3426.jpg	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
192.243.55.135	Dominica	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector	Block	1
157.55.39.5	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/general/	Block	1
74.82.47.4	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/print_text.asp	Block	1
40.77.167.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58339&docid=68495	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2418.jpg	Block	1