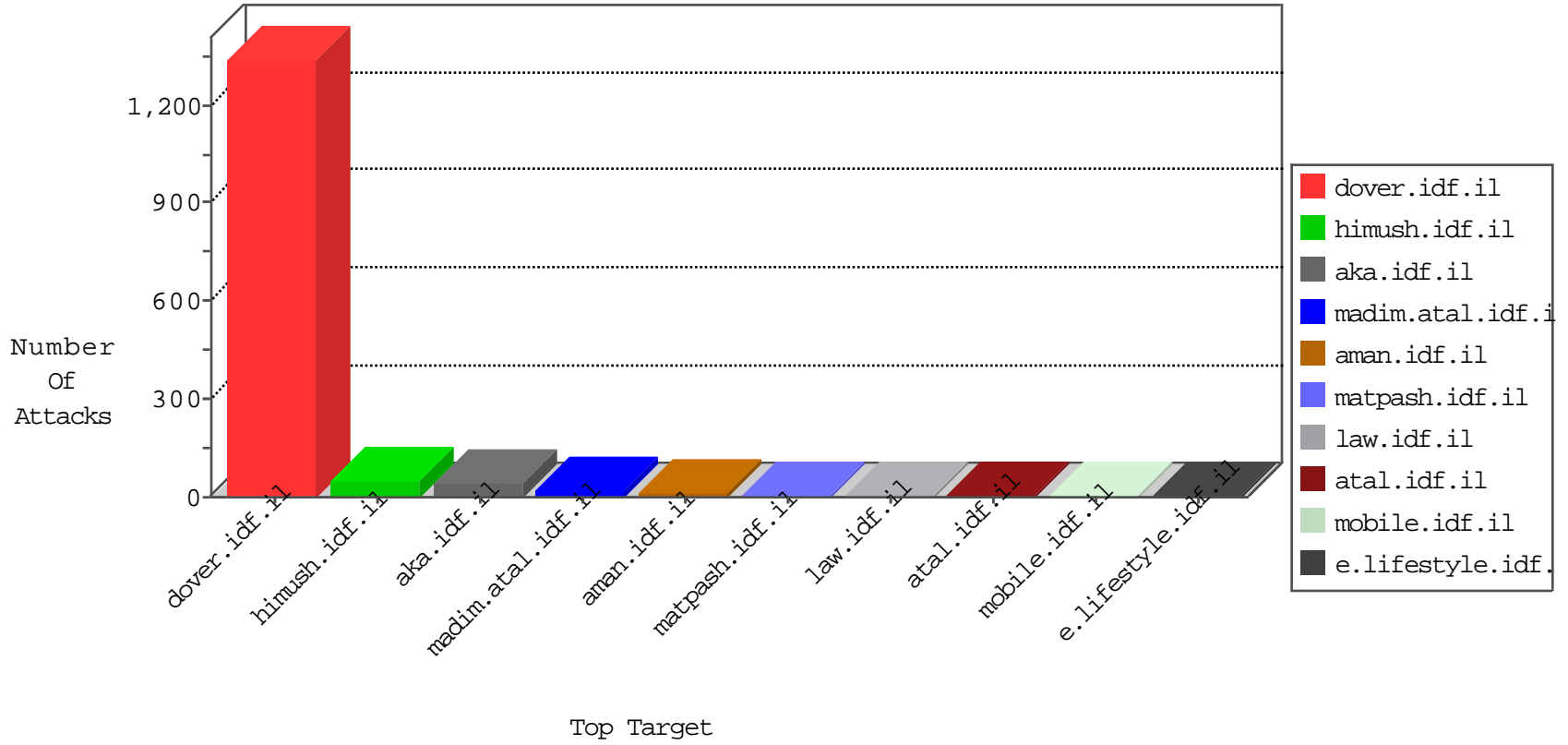


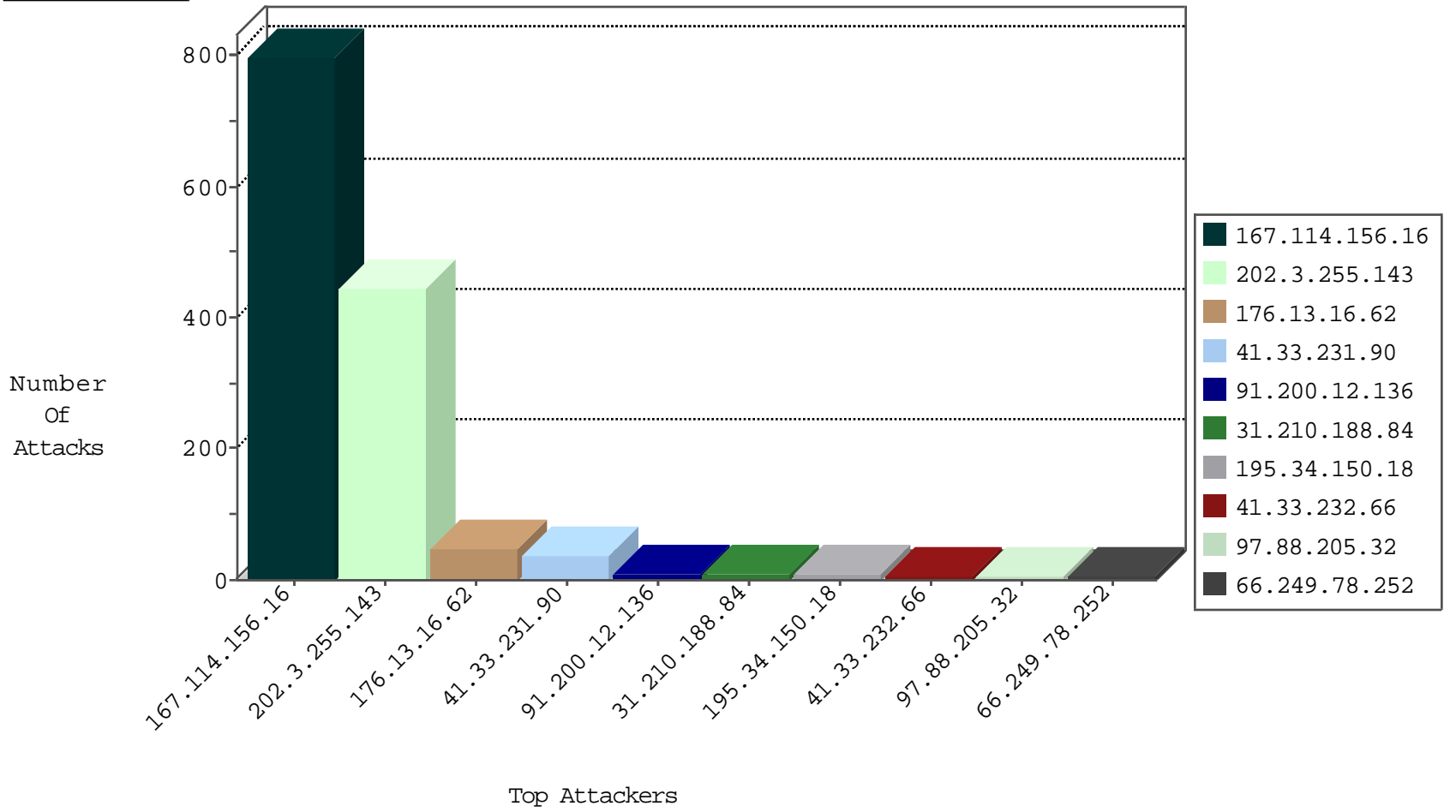
# IDF Under Attack Daily Report



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	3001
42.200.37.18	Hong Kong	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
208.67.1.66	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
74.91.28.62	United States	147.237.0.19	madim.atal.idf.il	block-sp-trafl	forward	1
107.150.55.210	United States	147.237.77.233	atal.idf.il	block-sp-trafl	drop	1
89.248.168.218	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
162.248.100.195	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
89.248.168.218	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
95.83.240.92	Ireland	147.237.8.24	e.lifestyle.idf.il	L4 Source or Dest Port Zero	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
180.254.202.45	Indonesia	147.237.77.216	dover.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	3
209.173.241.141	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
66.76.174.2	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
159.203.4.142	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	409
176.13.16.62	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.76.174.2	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
66.249.69.93	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
172.98.200.238	147.237.72.167		ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.77.212	Turkey	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
105.159.62.229	147.237.76.202	Morocco	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
105.159.62.229	147.237.76.202	Morocco	e.halag.idf.il	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
91.198.127.157	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.58.106.95	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.238	147.237.72.167		ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
112.16.76.209	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.77.212	Turkey	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
105.159.62.229	147.237.76.202	Morocco	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
104.236.76.210	147.237.0.16		my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
98.119.105.221	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
176.13.16.62	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
176.13.16.62	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
31.210.188.84	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
91.200.12.136	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	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
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.52	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.50	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.143.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.249.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
74.63.228.226	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
97.88.205.32	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
5.28.155.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.177	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.146.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
128.232.110.28	United Kingdom	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
37.48.101.193	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
157.55.39.12	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
169.0.177.135		147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
84.228.212.218	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
31.210.188.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.159.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
109.253.159.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.3.144.84	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.109.206.19	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
195.62.53.168	Russian Federation	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.16	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.120.125.51		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.0	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.102.253.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
107.150.55.211	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.109.206.19	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.91	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.23	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
188.44.55.20	Russian Federation	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.64.7.179	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
70.210.74.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.123	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
94.230.86.135	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.35	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
173.161.52.213	United States	147.237.77.233	atal.idf.il	Header Rejection	header rejection pattern found in request	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.193.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	3
185.120.126.78		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
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
109.253.203.111	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Byte Code Character in Parameter Value from 109.253.203.111	Block	2
2.54.166.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.238	Block	2
185.13.193.36	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
37.142.64.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.130.133.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
190.92.20.126	Honduras	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/spanish	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
40.77.167.96	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
162.247.72.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
74.91.28.62	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to www.x8s2.com/	Block	1
66.249.66.45	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/540-he/patzar.aspx	Block	1
190.92.20.73	Honduras	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/spanish	Block	1
91.109.247.173	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
192.187.99.154	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	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
173.161.52.213	United States	147.237.77.233	atal.idf.il	E-mail collector robots 14	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.125.158.135	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
190.92.20.88	Honduras	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.67	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/111351.pdf	Block	1
128.52.128.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
97.88.205.32	United States	147.237.72.156	aman.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
194.177.26.192	Ukraine	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
66.249.78.154	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
173.161.52.213	United States	147.237.77.233	atal.idf.il	eMail Hoarding	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.110.192.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.83.40.239	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
190.92.20.113	Honduras	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.126	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/109020.pdf	Block	1
128.232.110.29	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
97.88.205.32	United States	147.237.72.156	aman.idf.il	Multiple signatures from 97.88.205.32	Block	1
194.177.26.192	Ukraine	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
74.63.228.226	United States	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
85.64.195.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
190.92.20.123	Honduras	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
157.55.39.143	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
104.236.76.210		147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
74.63.228.226	United States	147.237.72.166	aka.idf.il	Multiple signatures from 74.63.228.226	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
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/unitfs.asp	Block	1