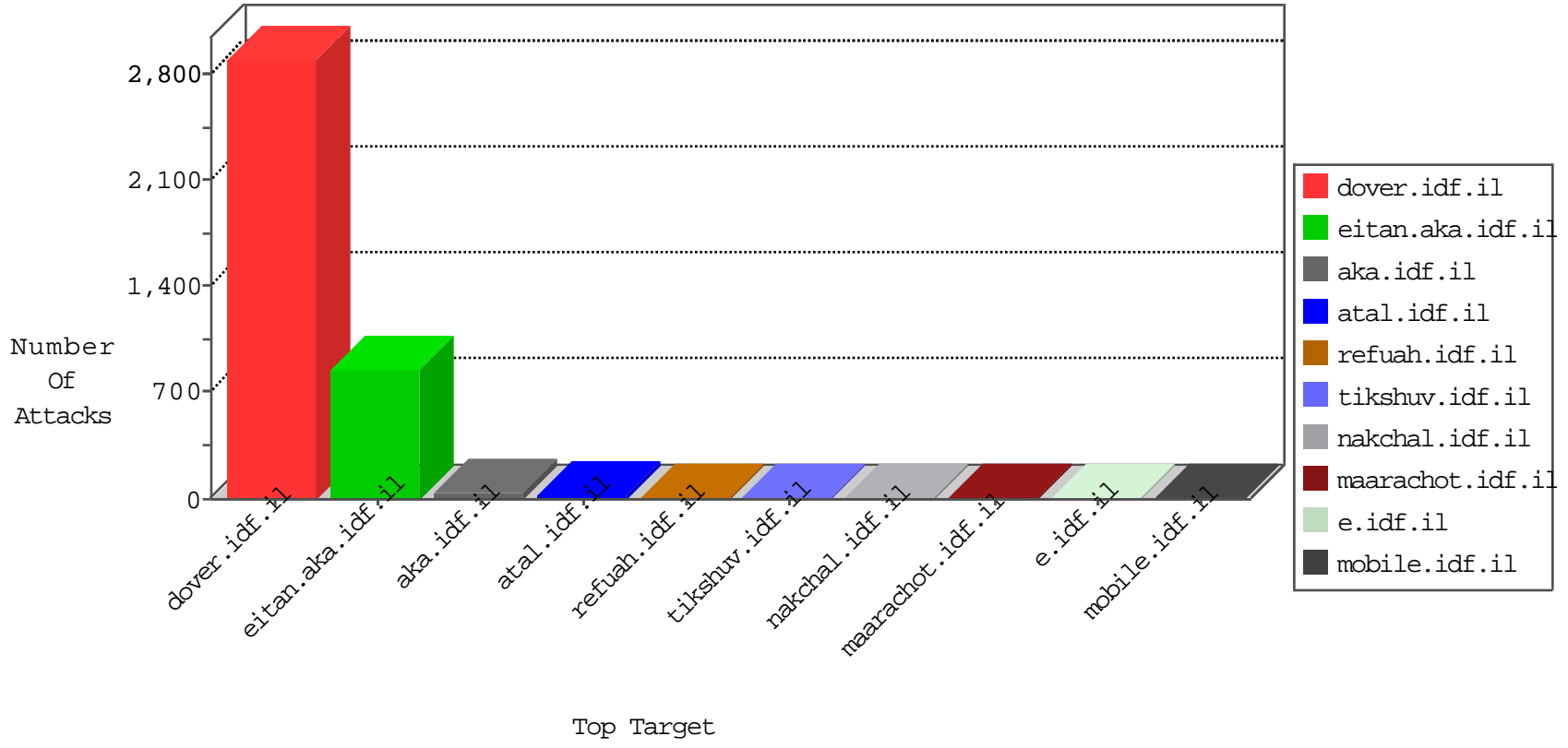


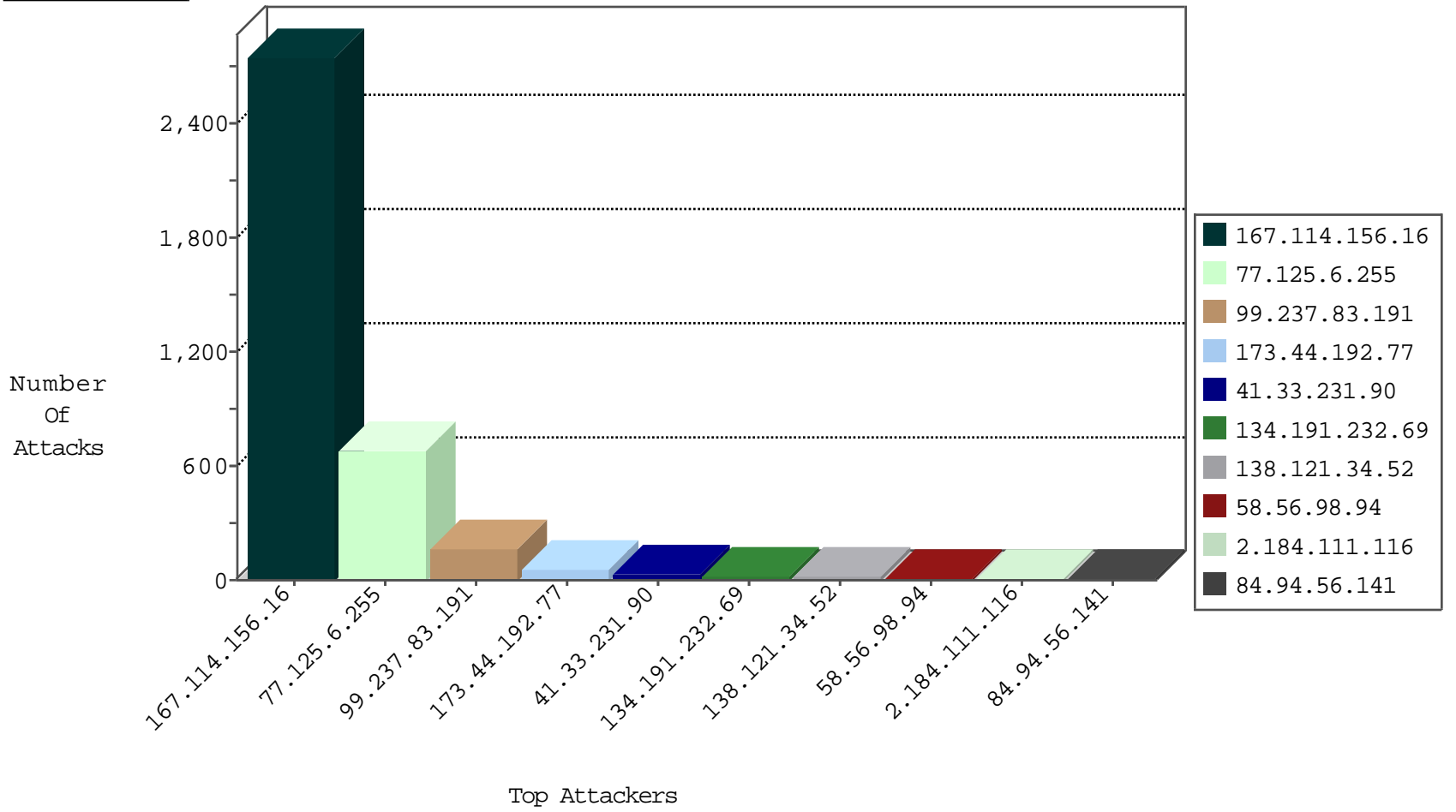
IDF Under Attack Daily Report



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	3543
134.191.232.69	Israel	147.237.77.233	atal.idf.il	JIM_Purple_Con_Limit_Http	drop	100
134.191.232.69	Israel	147.237.77.233	atal.idf.il	JIM_Purple_Con_Limit_Tcp	drop	50
71.6.167.142	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
192.3.170.124	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
198.20.70.114	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.132	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.44.192.77	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
173.44.192.77	United States	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	12
198.204.243.114	United States	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
198.20.69.74	United States	147.237.8.46	e.chinuch.idf.il	13840: TLS: OpenSSL Heartbeat Packet	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	4
138.121.34.52	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	2
113.240.250.155	147.237.77.216	China	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
138.121.34.52	147.237.77.170		maarachot.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.0.35	Germany	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.67.232	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
138.121.34.52	147.237.77.61		e.cogat.idf.il	ET SCAN Potential SSH Scan	1
62.212.73.196	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
138.121.34.52	147.237.76.198		e.yochalan.idf.il	ET SCAN Potential SSH Scan	1
58.56.98.94	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
138.121.34.52	147.237.76.44		e.refuah.idf.il	ET SCAN Potential SSH Scan	1
58.56.98.94	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
138.121.34.52	147.237.76.31		nakchal.idf.il	ET SCAN Potential SSH Scan	1
58.56.98.94	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
125.39.160.92	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.56.98.94	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
138.121.34.52	147.237.77.234		halag.idf.il	ET SCAN Potential SSH Scan	1
121.97.143.246	147.237.76.30	Philippines	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.56.98.94	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
138.121.34.52	147.237.77.212		e.dover.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.155	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
138.121.34.52	147.237.77.179		e.mazi.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.76.176	Germany	test.noore.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.177	Netherlands	noore.idf.il	ET SCAN NMAP -sS window 1024	1
138.121.34.52	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1
62.212.73.196	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
138.121.34.52	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
62.212.73.196	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
138.121.34.52	147.237.76.148		ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
58.56.98.94	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
138.121.34.52	147.237.76.34		yochalan.idf.il	ET SCAN Potential SSH Scan	1
58.56.98.94	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
58.56.98.94	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
122.3.67.94	147.237.76.30	Philippines	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.56.98.94	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
138.121.34.52	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
138.121.34.52	147.237.77.205		prisha.idf.il	ET SCAN Potential SSH Scan	1
58.56.98.94	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.201	Canada	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.125.6.255	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	591
99.237.83.191	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
99.237.83.191	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.56.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.184.111.116	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.17.19.157	Belarus	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.120.130.9	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.67.224.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
64.233.172.160	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	3
94.230.86.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.64.193	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.203.175	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.30.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.176.117.23	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.184.111.116	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.22.129.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
199.30.24.80	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.54.31.145	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
157.55.2.131	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.8.204.39	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.178.60.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.154.227.118	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
61.219.69.178	Taiwan	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.88	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.107	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.181	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
99.237.83.191	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.51	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.235	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.72	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
113.240.250.155	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.31.145	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.20.69.74	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.88	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.182	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
103.242.216.226	Bangladesh	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.252	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.73	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
134.191.232.69	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.125.6.255	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	92
99.237.83.191	Canada	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 99.237.83.191	Block	80
37.26.149.173	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
109.65.30.124	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
82.166.242.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.120.230.39	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
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
79.182.224.130	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/1397-en/dover.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
141.212.121.176	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-12715-he/dover.aspx	Block	1
99.237.83.191	Canada	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
5.28.147.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.118.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
185.3.146.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.232	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.120.230.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.120.230.39	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
81.144.138.34	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info.asp	Block	1
157.55.39.255	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20140-he/idfgdover.aspx	Block	1
5.102.217.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.118.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
197.37.37.121	Egypt	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 197.37.37.121	Block	1
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.181.48.210	Belgium	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
173.44.192.77	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ckeditor/ckfinder/core/connector/asp/connector.asp	Block	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	1
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	1
5.255.253.151	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.99.94	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9738-he/refuah.aspx	Block	1
197.37.37.121	Egypt	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
113.240.250.155	China	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 113.240.250.155 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
84.94.56.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
184.105.139.67	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.66.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	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
79.179.99.94	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
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	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
113.240.250.155	China	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.111.159.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1