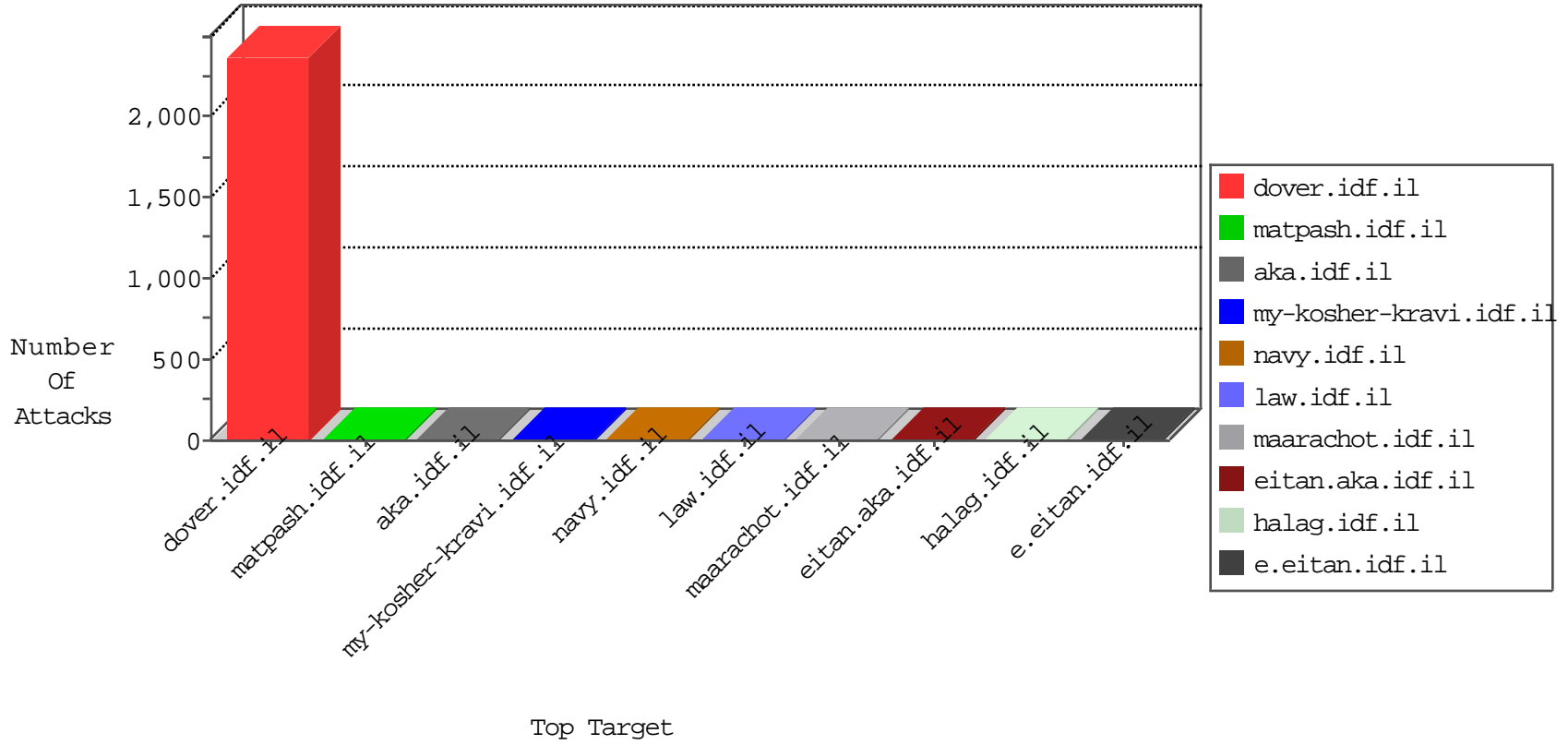


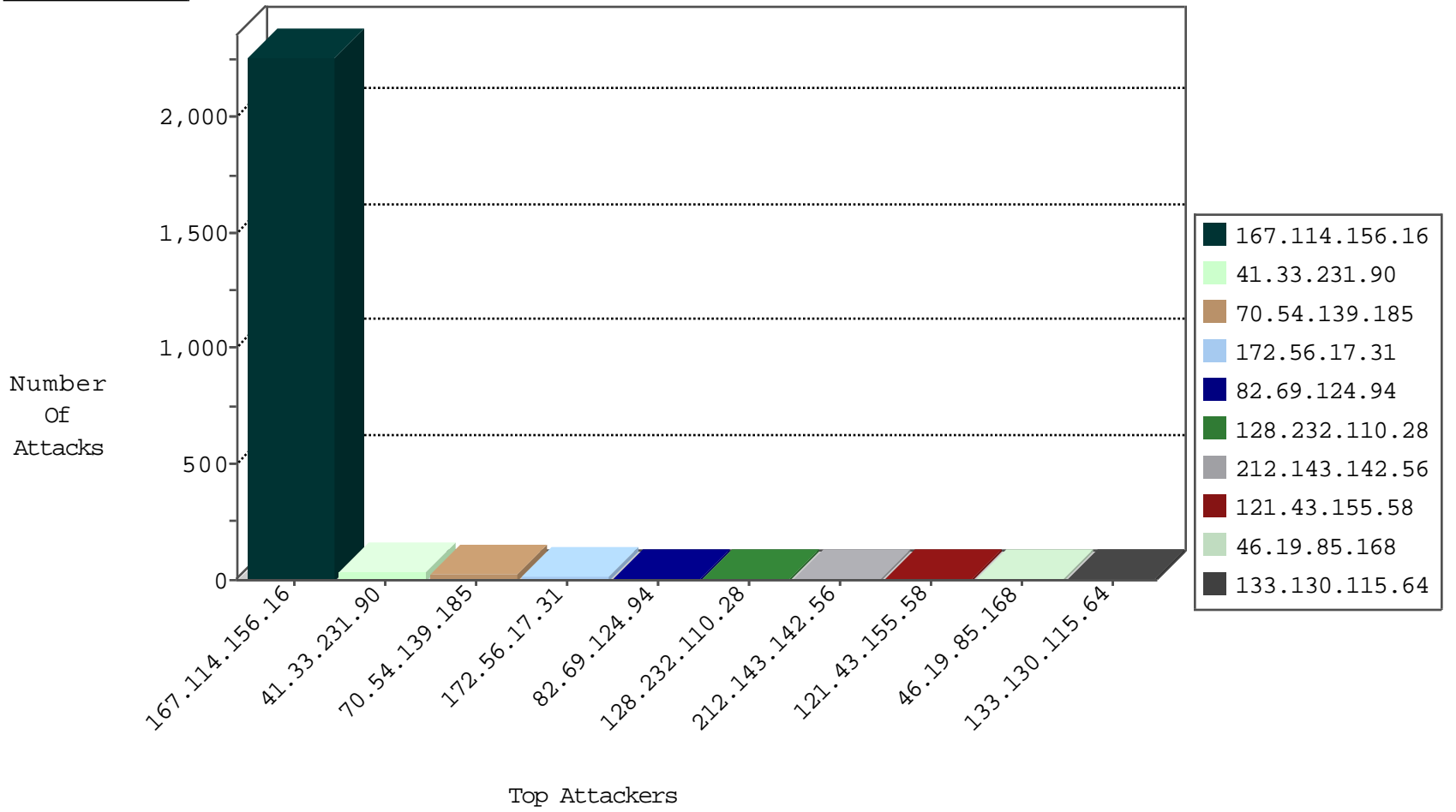
IDF Under Attack Daily Report



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	3422
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	91

12-08-2015-03:04:07 to 12-08-2015-04:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	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
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
121.43.155.58	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
91.143.102.180	147.237.76.44	Austria	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
201.232.25.160	147.237.0.33	Colombia	idf.il	ET SCAN NMAP -sS window 3072	1
91.143.102.180	147.237.76.44	Austria	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
201.232.25.160	147.237.0.33	Colombia	idf.il	ET SCAN NMAP -f -sS	1
82.166.184.187	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
66.249.66.45	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
173.14.248.34	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
121.43.155.58	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
121.43.155.58	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
121.43.155.58	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.143.102.180	147.237.76.44	Austria	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
201.232.25.160	147.237.0.33	Colombia	idf.il	ET SCAN NMAP -sS window 2048	1
88.249.106.23	147.237.76.34	Turkey	yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.178	147.237.76.34	United States	yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
173.14.248.34	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
173.14.248.34	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
121.43.155.58	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
121.43.155.58	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	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
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
70.54.139.185	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
172.56.17.31	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
82.69.124.94	United Kingdom	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
199.30.24.76	United States	147.237.76.200	eitan.aka.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
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
70.54.139.185	Canada	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.168	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.137.202	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
128.232.110.28	United Kingdom	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
213.57.132.99	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
82.69.124.94	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	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
128.232.110.28	United Kingdom	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
128.232.110.28	United Kingdom	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
104.156.240.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.168	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.145	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
133.130.115.64	Japan	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
141.212.122.139	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
131.253.24.142	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
115.250.235.35	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
206.45.197.74	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.146	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
133.130.115.64	Japan	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
89.138.229.162	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.155.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.140	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
131.253.24.151	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
123.125.71.14	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
206.45.197.74	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.154	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
137.116.71.170	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.100	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.142	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
133.130.115.64	Japan	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
123.125.71.80	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
206.45.197.74	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.155	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.132	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.215	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.143	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
133.130.115.64	Japan	147.237.76.147	chimuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	2
46.117.181.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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
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
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
8.37.71.71	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/869-he/patzar.aspx&usg=alkjrhj_bjv9vzcrghuhsnyu cx9s41snaq	Block	1
178.154.243.116	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
141.212.122.129	United States	147.237.72.167	ishurim.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
66.249.66.45	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.166.186.230	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1283-en/dover.aspx	Block	1
157.55.39.255	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/896-he/cogat.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
8.37.71.95	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/869-2028-he/patzar.aspx&usg=alkjrhjugjamv9q2iio wud0or4c2ttuclw	Block	1
178.255.215.87	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.129	United States	147.237.77.170	maarachot.idf.il	Multiple Malformed URL from 141.212.122.129	Block	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/coordinationgaza/rasheiaza	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1379-he/dover.aspx	Block	1
46.166.190.160	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
176.199.146.185	Germany	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/templates/navmenu/navmenu.css.aspx	Block	1
5.255.253.114	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	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
37.140.141.34	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
184.105.247.195	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
141.212.122.129	United States	147.237.77.176	matpash.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/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
52.33.184.164	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
178.154.243.93	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
8.37.70.135	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/205-he/patzar.aspx&usg=alkjrhjtc4vdvzce7xqidctrg nkfiistra	Block	1
130.193.50.21	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/video http://www.youtube.com/v/tv4zoxi3kn	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/size220x0/13032.jpg	Block	1
157.55.39.17	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/widget/clickstream/_rvi	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.65.118	Block	1
178.154.243.111	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
8.37.70.143	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/590-he/patzar.aspx&usg=alkjrhijw3brxeatvihj6i9 6zdctcdka	Block	1
130.193.50.36	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.166.186.208	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1153-he/dover.aspx	Block	1
157.55.39.119	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1