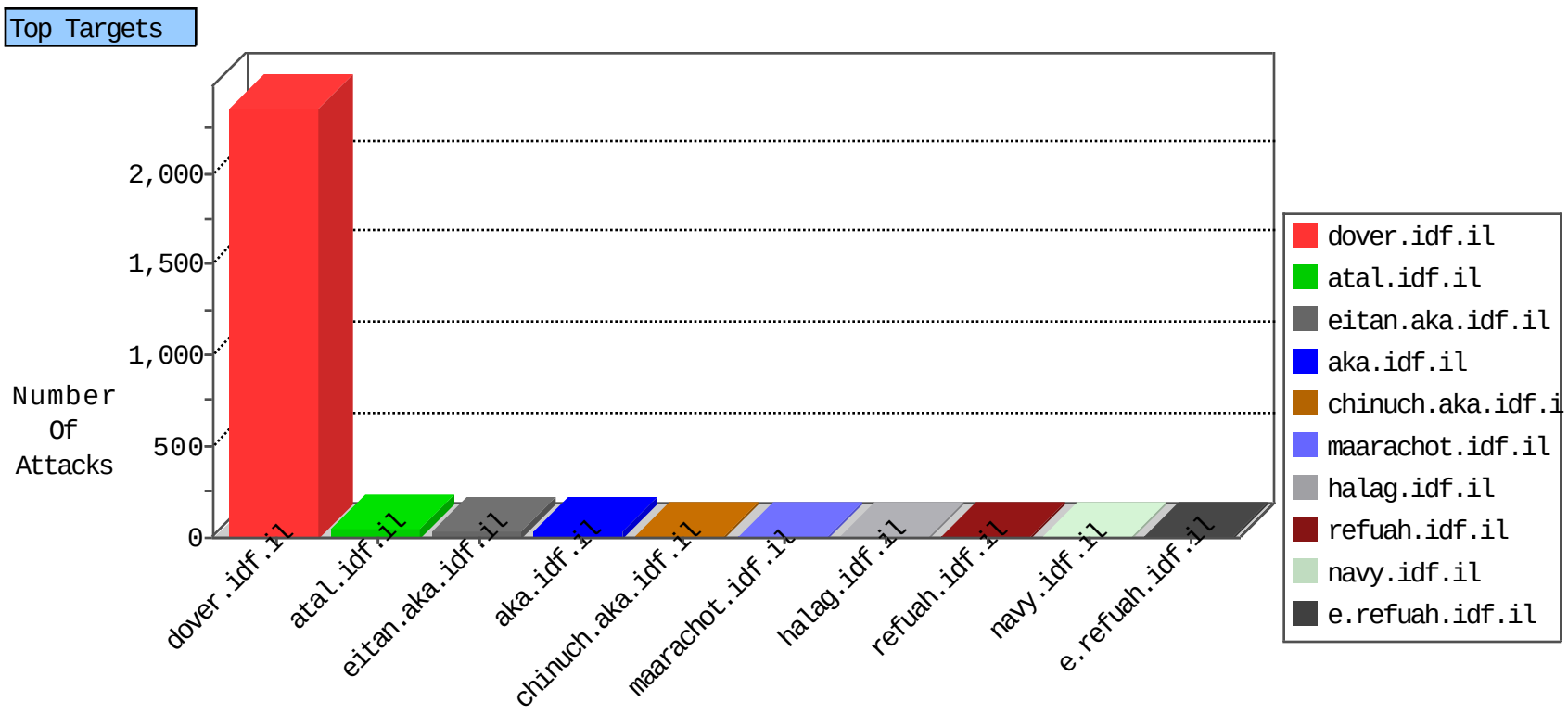
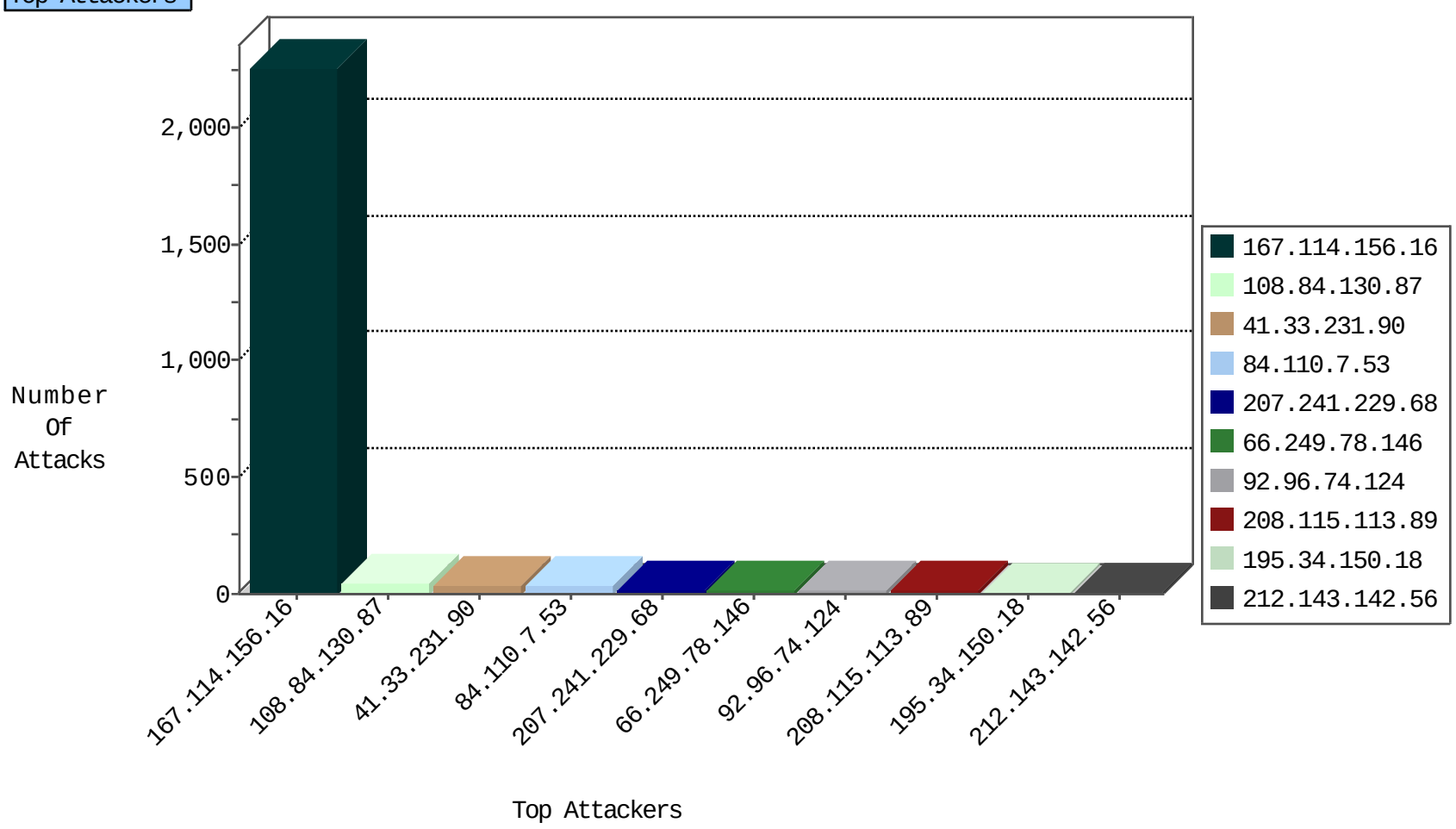
12-19-2015-05:04:06 to 12-19-2015-06:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-19-2015-05:04:06 to 12-19-2015-06:04:06

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	3154
66.249.69.171	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	192

12-19-2015-05:04:06 to 12-19-2015-06:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.198.242	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-19-2015-05:04:06 to 12-19-2015-06:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.31	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
172.98.200.238	147.237.76.198		e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
166.63.122.229	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
125.65.97.66	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -f -sS	1
221.10.66.60	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
61.244.49.137	147.237.8.46	Hong Kong	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
202.98.157.52	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
199.191.56.187	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
172.98.200.238	147.237.76.198		e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
166.63.122.229	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
125.65.97.66	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
96.81.223.109	147.237.76.34	United States	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
221.10.66.60	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -f -sS	1
14.53.229.87	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
202.98.157.52	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -f -sS	1
199.191.56.187	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.76.198		e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1

12-19-2015-05:04:06 to 12-19-2015-06:04:06

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	36
84.110.7.53	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
207.241.229.68	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
108.84.130.87	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
108.84.130.87	United States	147.237.77.233	atal.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	13
108.84.130.87	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	13
108.84.130.87	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
92.96.74.124	United Arab Emirates	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	5
199.30.24.209	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	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
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
66.249.81.209	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.11	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.69.171	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.98	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
92.96.74.124	United Arab Emirates	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
207.46.13.36	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.169	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
92.96.74.124	United Arab Emirates	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
184.105.139.96	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
183.61.1.178	China	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
118.26.248.2	China	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.72	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
101.254.199.22	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
183.61.153.210	China	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.249.66.28	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
139.196.104.39	China	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
221.10.66.60	China	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
92.96.74.124	United Arab Emirates	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
184.105.139.103	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.26	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
183.61.1.178	China	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
125.65.97.66	China	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.76	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
101.254.199.22	China	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
202.98.157.52	China	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
183.134.31.50	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.220	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.34	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
183.61.153.210	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
139.196.104.39	China	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.92	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
101.254.204.82	China	147.237.0.34	tikshuv.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
157.55.39.194	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	4
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	4
207.46.13.169	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	3
46.19.86.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
109.65.130.47	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
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	2
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.equalheights.js	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;list in www.aka.idf.il/chinuch/klali/default.asp	None	1
199.47.81.11	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15196-en/dover	Block	1
97.93.100.34	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 97.93.100.34	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;catid in www.aka.idf.il/rights/asp/info.asp	None	1
108.84.130.87	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 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/1133-22461-he/dover.aspx.	Block	1
97.93.100.34	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/japanese/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;list in www.aka.idf.il/patzar/klali/default.asp	None	1
54.175.251.198	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
216.218.206.68	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
66.249.73.217	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/tmuna/default.asp	Block	1
207.46.13.169	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/ui.datepicker.js	Block	1
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
71.71.234.99	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.73.228	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8613-he/navy.aspx.aspx	Block	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
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-ui.js	Block	1
220.166.62.101	China	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
172.98.67.17		147.237.77.74	law.idf.il	Parameter Type Violation pos in www.law.idf.il/163-6712-he/patzar.aspx	Block	1
84.110.37.147	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
40.77.167.105	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	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
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