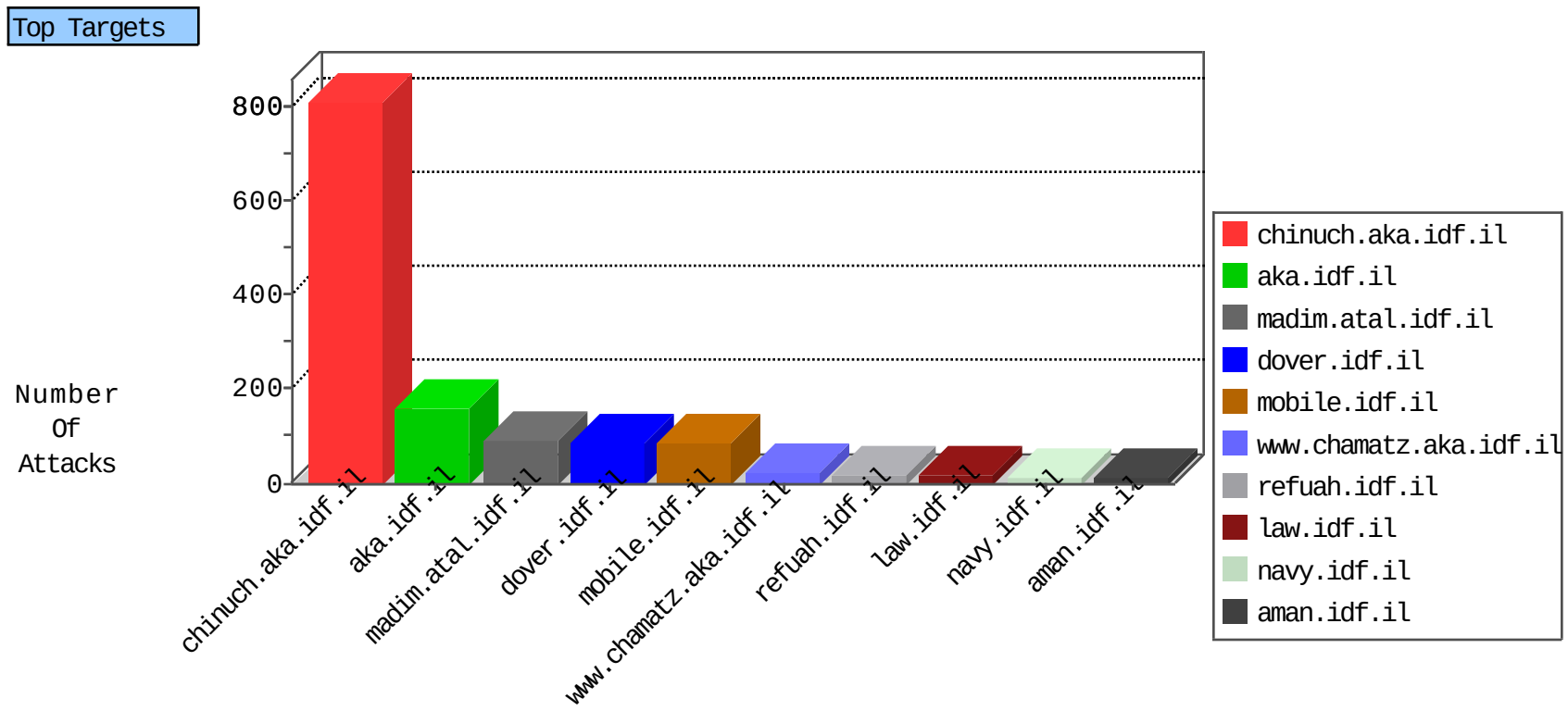
09-27-2016-00:04:14 to 09-27-2016-01:04:14

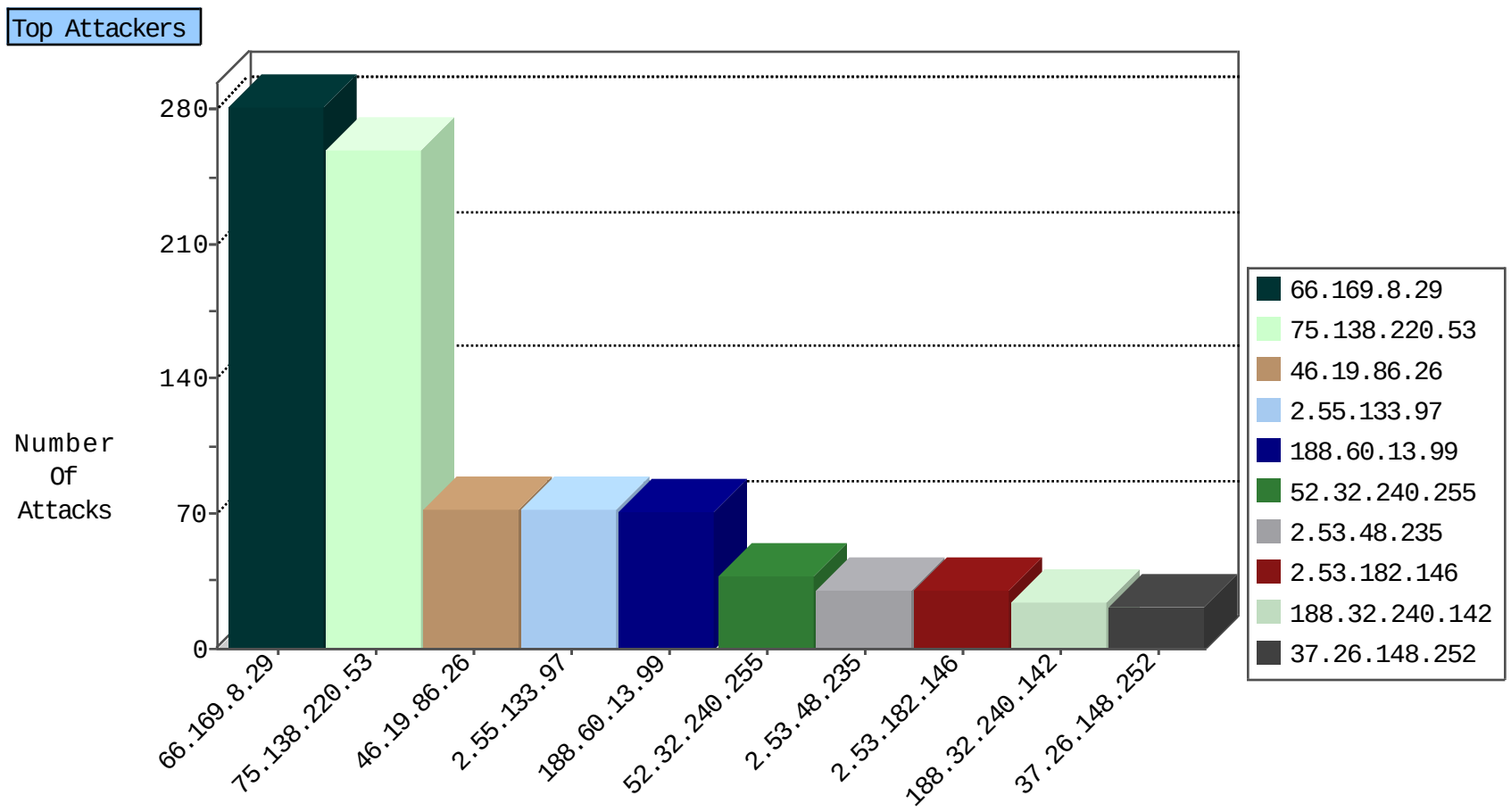
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-27-2016-00:04:14 to 09-27-2016-01:04:14

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.248.63	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15
42.112.10.85	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.66	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
45.32.204.130	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
42.112.10.74	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.89	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.69	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
120.132.50.135	China	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
42.112.10.75	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
45.32.199.242	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
42.112.10.70	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.81	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
45.32.204.130	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
42.112.10.73	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1

09-27-2016-00:04:14 to 09-27-2016-01:04:14

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	11
51.254.215.140	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
51.254.215.140	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-27-2016-00:04:14 to 09-27-2016-01:04:14

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
217.114.14.106	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.169.150	147.237.0.19	United Kingdom	madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
139.162.187.89	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.187.89	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
77.126.8.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.47.62.157	147.237.77.176	Saudi Arabia	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
161.106.88.6	147.237.77.19	France	law-forum.idf.il	ET SCAN Potential SSH Scan	1
139.162.187.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
78.129.171.173	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1

09-27-2016-00:04:14 to 09-27-2016-01:04:14

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.169.8.29	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	282
75.138.220.53	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	260
52.32.240.255	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	33
2.53.48.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.182.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.55.133.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	28
2.55.133.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	28
188.32.240.142	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	24
188.60.13.99	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
188.60.13.99	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	17
2.55.133.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
188.60.13.99	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
188.60.13.99	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	15
46.147.210.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
62.128.48.50	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
46.121.226.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
188.60.13.99	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.117.133.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.48.204	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
80.246.136.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
24.185.84.162	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
24.185.84.162	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
24.185.84.163	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
70.24.84.137	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
104.121.70.198	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
73.99.102.129	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
172.72.87.70	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
101.183.150.244	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.178.35.234	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
197.117.56.168	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
77.138.59.205	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
73.99.102.129	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
46.121.226.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
24.185.84.163	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
2.55.19.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
24.185.84.163	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
46.121.226.167	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.132	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
70.24.84.137	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
24.46.197.140	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
2.55.19.107	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.121.226.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.132	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
73.99.102.129	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
172.72.87.70	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4

09-27-2016-00:04:14 to 09-27-2016-01:04:14

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
37.26.148.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.85.79	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	5
85.64.12.36	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
85.64.12.36	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	3
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.228	Block	3
80.246.136.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.141.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.122.148	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunsummary.aspx	Block	2
213.57.70.8	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.66.239	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.239	Block	2
46.121.226.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
157.55.39.28	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8921-he/refuah.aspx	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
40.143.136.38	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/index.php	Block	1
85.64.12.36	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 85.64.12.36	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1
46.19.85.199	Israel	147.237.77.234	halag.idf.il	Unknown HTTP Request Method e=6dd9b75173255de2.1474926977.1.1474926977.1474926977.; in URL _pk_ses.284.4cde=*	Block	1
213.8.204.4	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
5.226.86.2	Poland	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.174.61.152	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	1
66.249.64.106	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_text.asp	Block	1
213.8.204.4	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
31.168.68.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.148	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	1
46.19.85.199	Israel	147.237.77.234	halag.idf.il	Abnormally Long Request method	Block	1
46.19.86.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.237.138.202	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized Method HEAD for /	Block	1
46.19.85.199	Israel	147.237.77.234	halag.idf.il	Illegal HTTP Version	Block	1
91.64.76.185	Germany	147.237.77.74	law.idf.il	Parameter Type Violation Master$ContentPlaceHolder1$FAQListViewTemplate1$InternalSearch1$txtFreeTextSearch in www.law.idf.il/327-he/patzar.aspx	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
37.26.148.252	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.239	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/israeliinkalkilia04012011.aspx	Block	1
46.19.85.199	Israel	147.237.77.234	halag.idf.il	Malformed URL _pk_ses.284.4cde=*	Block	1

09-27-2016-00:04:14 to 09-27-2016-01:04:14