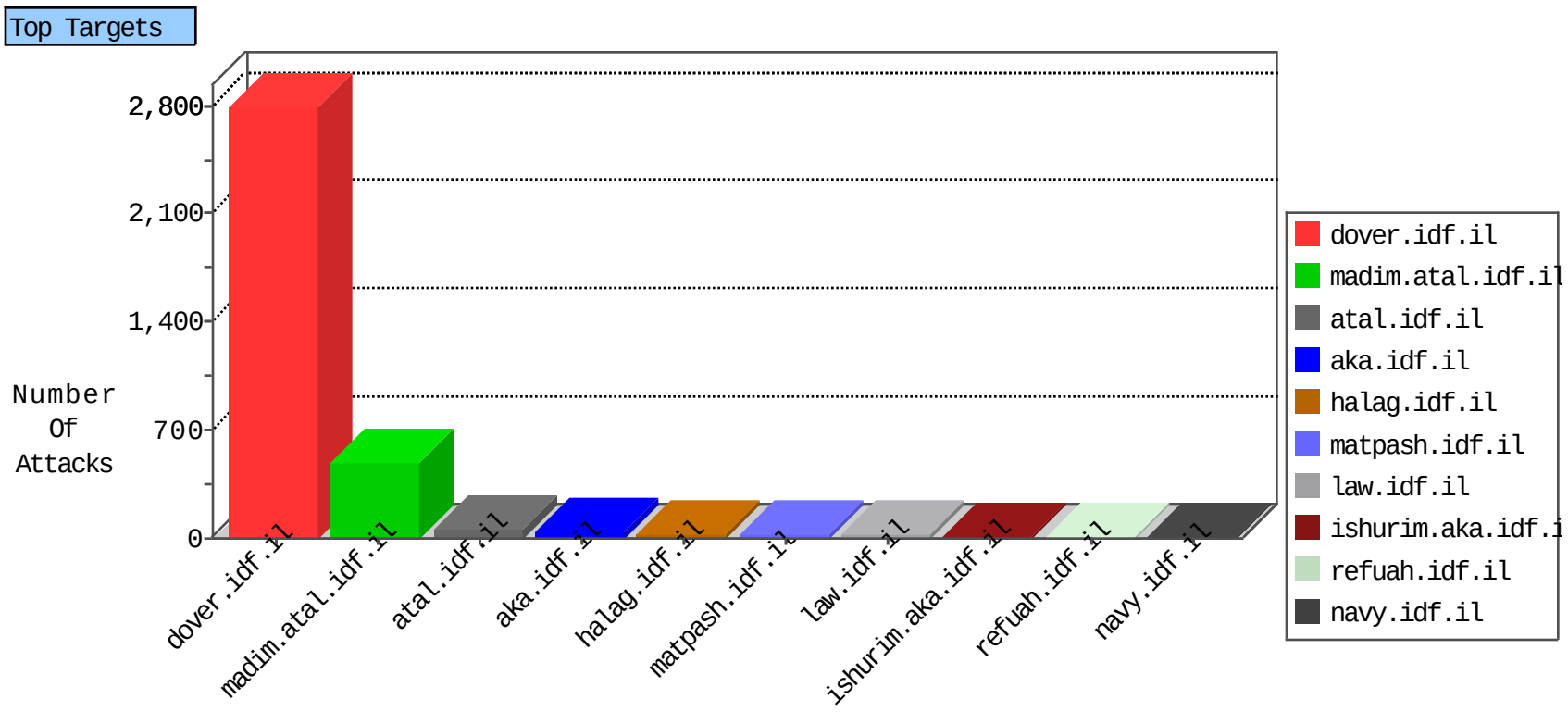
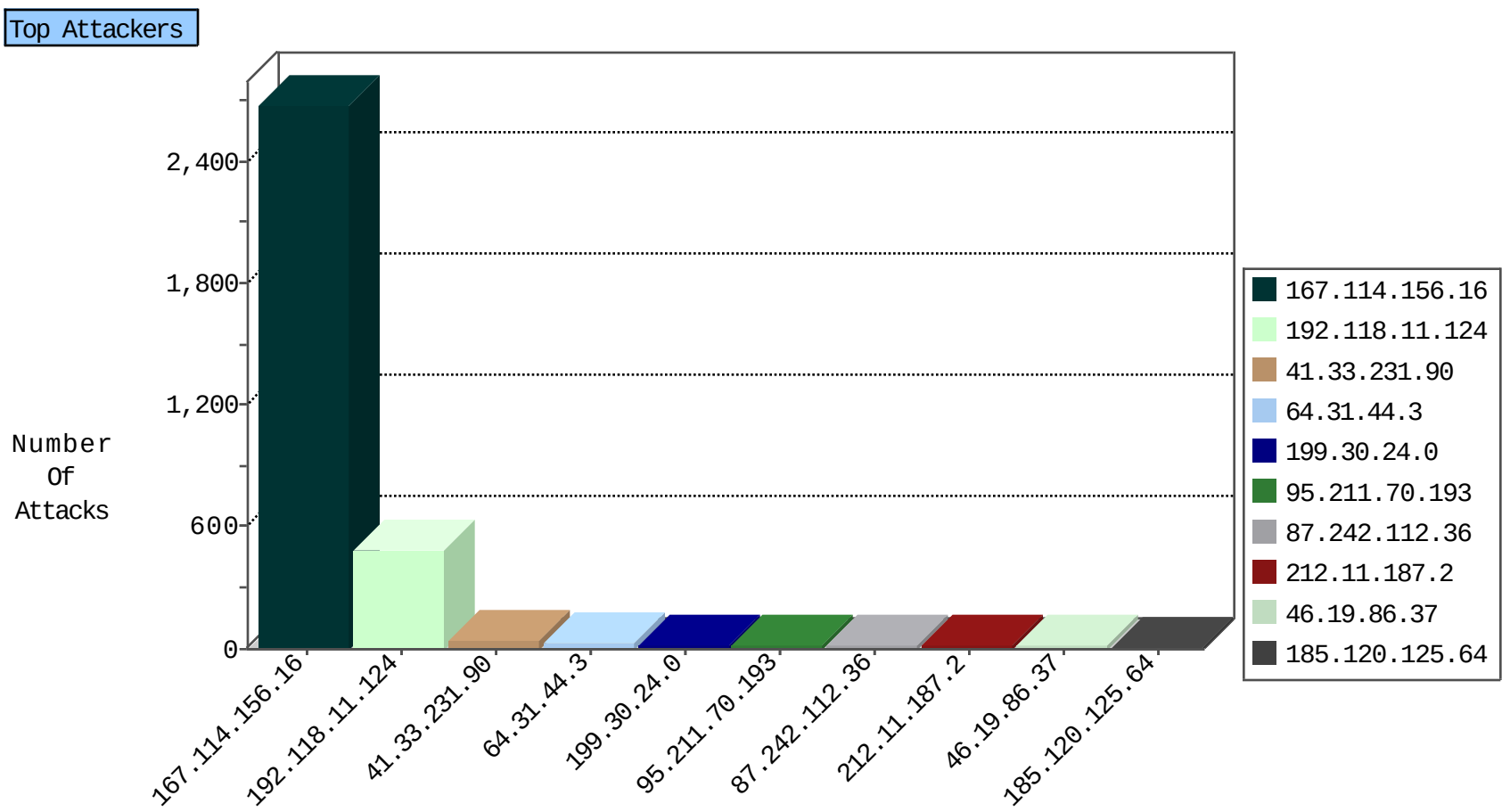
12-03-2015-05:04:01 to 12-03-2015-06:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-03-2015-05:04:01 to 12-03-2015-06:04:01

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	3572
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
85.25.43.94	Germany	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

12-03-2015-05:04:01 to 12-03-2015-06:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
64.31.44.3	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
95.211.70.193	Netherlands	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
87.242.112.36	Russian Federation	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8

12-03-2015-05:04:01 to 12-03-2015-06:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
64.31.44.3	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	18
95.211.70.193	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	10
87.242.112.36	147.237.77.233	Russian Federation	atal.idf.il	SQL Injection - Select From	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
209.126.116.147	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	2
178.169.143.78	147.237.72.156	Bulgaria	aman.idf.il	ET SCAN NMAP -sS window 2048	1
119.186.49.134	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.113	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
61.239.72.154	147.237.0.19	Hong Kong	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
200.35.150.97	147.237.76.39	Panama	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
5.148.157.229	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
200.35.150.97	147.237.76.31	Panama	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
200.35.150.97	147.237.72.156	Panama	aman.idf.il	ET SCAN Potential SSH Scan	1
178.169.143.78	147.237.72.156	Bulgaria	aman.idf.il	ET SCAN NMAP -sS window 4096	1
178.169.143.78	147.237.72.156	Bulgaria	aman.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.113	147.237.77.227	Ukraine	e.hamaz.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
200.35.150.97	147.237.76.42	Panama	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
40.115.58.160	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
200.35.150.97	147.237.76.31	Panama	nakchal.idf.il	ET SCAN Potential SSH Scan	1
200.35.150.97	147.237.72.167	Panama	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1

12-03-2015-05:04:01 to 12-03-2015-06:04:01

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
199.30.24.0	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
185.120.125.64		147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
46.19.86.19	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
212.11.187.2	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
2.54.152.195	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.46	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.182.48.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
212.11.187.2	Saudi Arabia	147.237.77.176	matpash.idf.il	drop		drop	4
37.26.148.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.26.148.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.11.187.2	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
197.37.49.160	Egypt	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	2
124.106.88.130	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.196	United States	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
124.106.88.130	Philippines	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
62.210.209.237	France	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
46.19.86.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
124.106.88.130	Philippines	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.115	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
47.20.73.216	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.224	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
157.55.39.196	United States	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.114	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.194	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
68.58.141.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.75	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.19	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.121.206	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.74	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
61.135.190.197	China	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.247.239	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.196	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
68.58.141.10	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.108	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.207	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.88	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.11.124	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 192.118.11.124	Block	281
192.118.11.124	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	104
192.118.11.124	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 192.118.11.124	Block	97
2.54.13.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
157.55.39.17	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
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	2
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	2
157.55.39.18	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.103	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.69	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
61.135.190.69	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
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
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/06092010masaiyot.aspx	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
157.55.39.115	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
73.200.13.209	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
66.249.66.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/smalim/showbig.aspx	Block	1
141.85.0.121	Romania	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.67.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
173.245.81.55	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
87.250.241.67	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
141.85.0.121	Romania	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
66.249.75.209	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/enlarge.asp	Block	1
46.163.68.109	Germany	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/shared/usercontrols/headerupper/	Block	1
207.46.13.110	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
178.63.96.242	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 178.63.96.242	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
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
192.118.11.124	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.75.217	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/yohalan/forums/asp/showforum.asp	Block	1
54.153.32.246	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
207.46.13.110	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/auto/misc/cc/js.php	Block	1
178.63.96.242	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/	Block	1