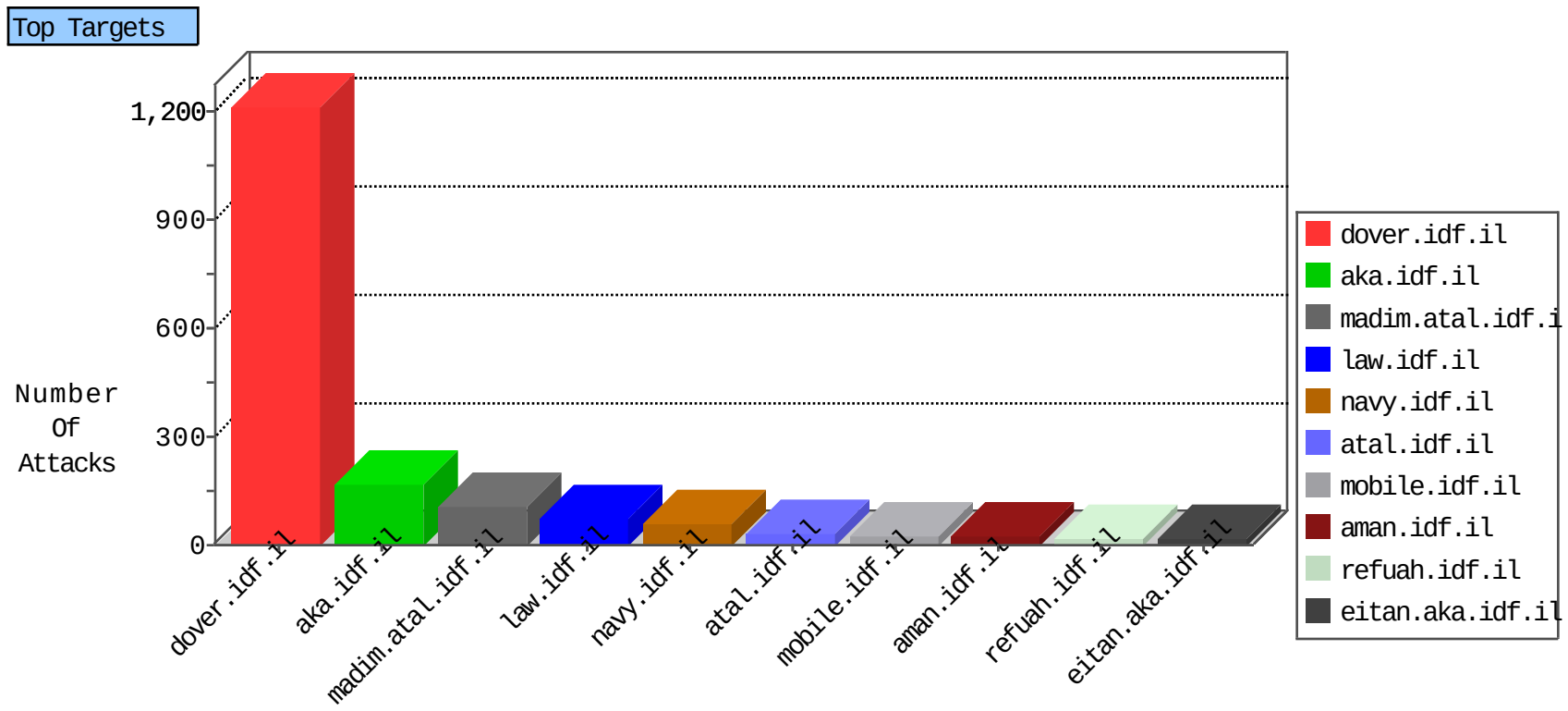
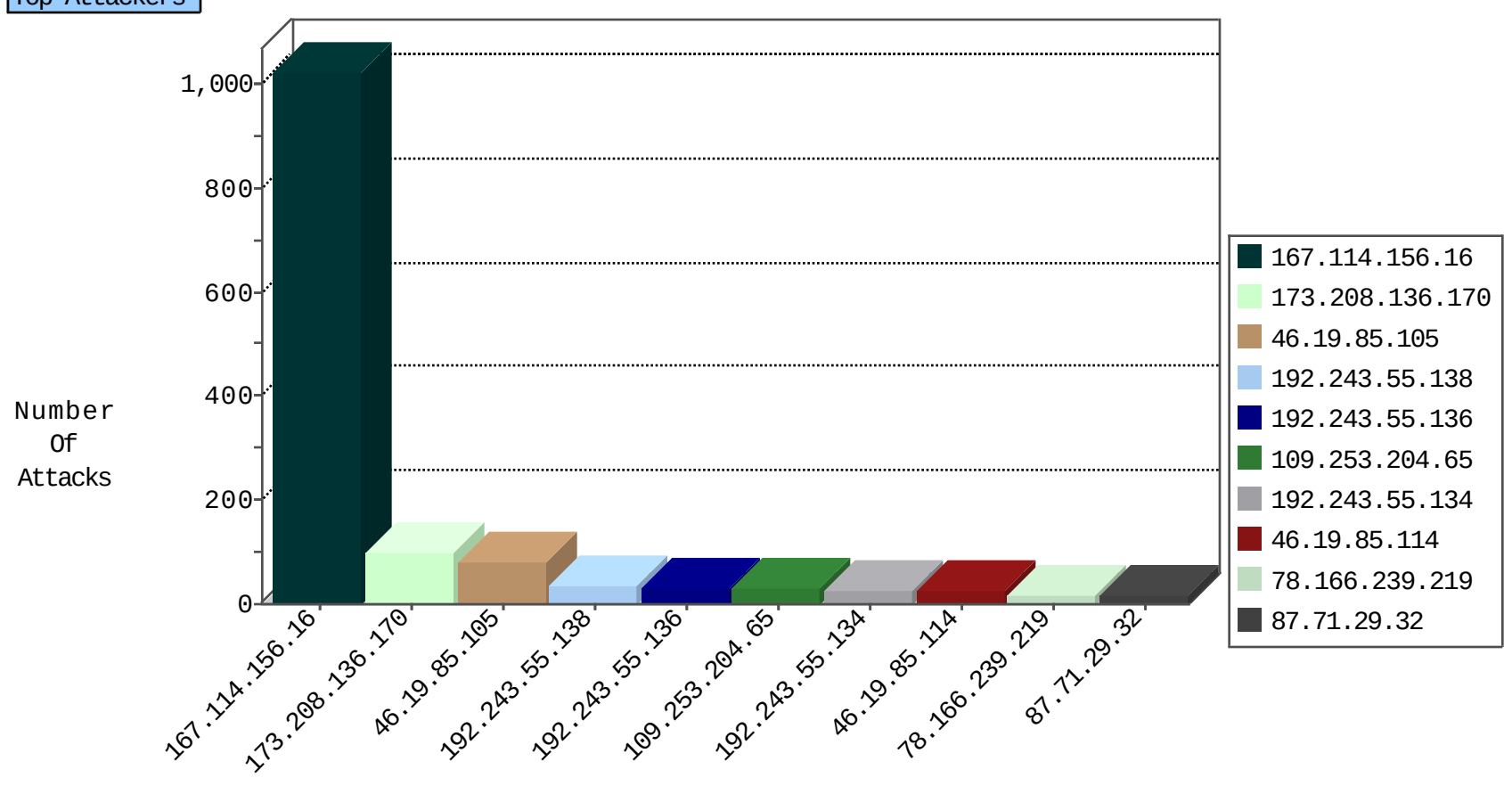
03-11-2016-12:04:06 to 03-11-2016-13:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-11-2016-12:04:06 to 03-11-2016-13:04:06

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	4000
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	2
173.208.176.162	United States	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
173.208.176.162	United States	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.73	United States	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1
218.57.11.7	China	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

03-11-2016-12:04:06 to 03-11-2016-13:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.79.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
78.166.239.219	Turkey	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.169	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-11-2016-12:04:06 to 03-11-2016-13:04:06

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
109.253.204.65	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
104.128.144.131	147.237.76.200	Canada	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
93.189.26.18	147.237.76.197	Austria	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
78.166.239.219	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP admin.php access	1
218.57.11.7	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
23.96.109.87	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
177.239.92.32	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.224.117.146	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.72.217	India	e.idf.il	ET SCAN NMAP -sS window 4096	1
93.189.26.18	147.237.77.61	Austria	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.76.86	Austria	navy.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
23.96.109.87	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
198.20.69.74	147.237.77.179	United States	e.mazi.idf.il	ET DROP Dshield Block Listed Source	1
178.63.11.208	147.237.0.17	Germany	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
173.224.117.146	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
173.224.117.146	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.72.217	India	e.idf.il	ET SCAN NMAP -sS window 3072	1

03-11-2016-12:04:06 to 03-11-2016-13:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.204.65	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.253.204.65	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.53.11.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
95.86.121.42	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.146.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.179.203.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.16.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.198.122	Israel	147.237.72.166	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	6
46.19.85.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
90.185.59.44	Denmark	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
5.22.130.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.136.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
141.0.14.213	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.138	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
89.138.189.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.117.89.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.134	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.182.162.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.54.59.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.39	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.193.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.15.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.102	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
185.3.146.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.138	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.106.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-11-2016-12:04:06 to 03-11-2016-13:04:06

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.181.2.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
173.208.136.170	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	Block	40
173.208.136.170	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	Block	40
46.19.85.114	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.85.114	Block	17
87.71.29.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
173.208.136.170	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	8
173.208.136.170	United States	147.237.76.86	navy.idf.il	Multiple Admin Blocking from 173.208.136.170	Block	7
46.19.85.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
78.166.239.219	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 78.166.239.219	Block	5
78.166.239.219	Turkey	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
109.253.204.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.85.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
78.166.239.219	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 78.166.239.219	Block	3
109.253.133.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.9.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	2
46.19.85.148	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/defau	Block	2
40.77.167.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
173.208.136.170	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/acg-nwl/assetmanager/assetmanager.asp	Block	1
46.19.85.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/v	Block	1
104.236.31.103		147.237.72.156	aman.idf.il	Unauthorized Method HEAD for 147.237.72.156/	Block	1
104.131.62.174	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
45.55.143.179		147.237.76.86	navy.idf.il	Unauthorized Method HEAD for 147.237.76.86/	Block	1
79.183.26.14	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.74.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/109406.pdf	Block	1
104.236.14.55		147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
37.26.148.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
104.131.166.147	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
45.55.143.248		147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
2.53.31.247	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	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
83.130.108.116	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	1
173.208.136.170	United States	147.237.76.86	navy.idf.il	Admin Blocking	Block	1
66.249.74.106	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/110526.pdf	Block	1
104.236.17.218		147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
37.26.148.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.138.89.241	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main.sachar/defult.aspx	Block	1
104.131.173.213	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
45.55.143.248		147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
2.54.29.60	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
217.69.133.247	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter sidescroll in aka.idf.il/giyus/leshakot/	None	1
84.108.44.15	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.74.108	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/112335.pdf	Block	1
46.19.85.105	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
104.236.28.93		147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
93.172.248.108	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
78.166.239.219	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
173.208.136.170	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/acg-nwl/assetmanager/assetmanager.asp	Block	1
115.239.212.203	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1