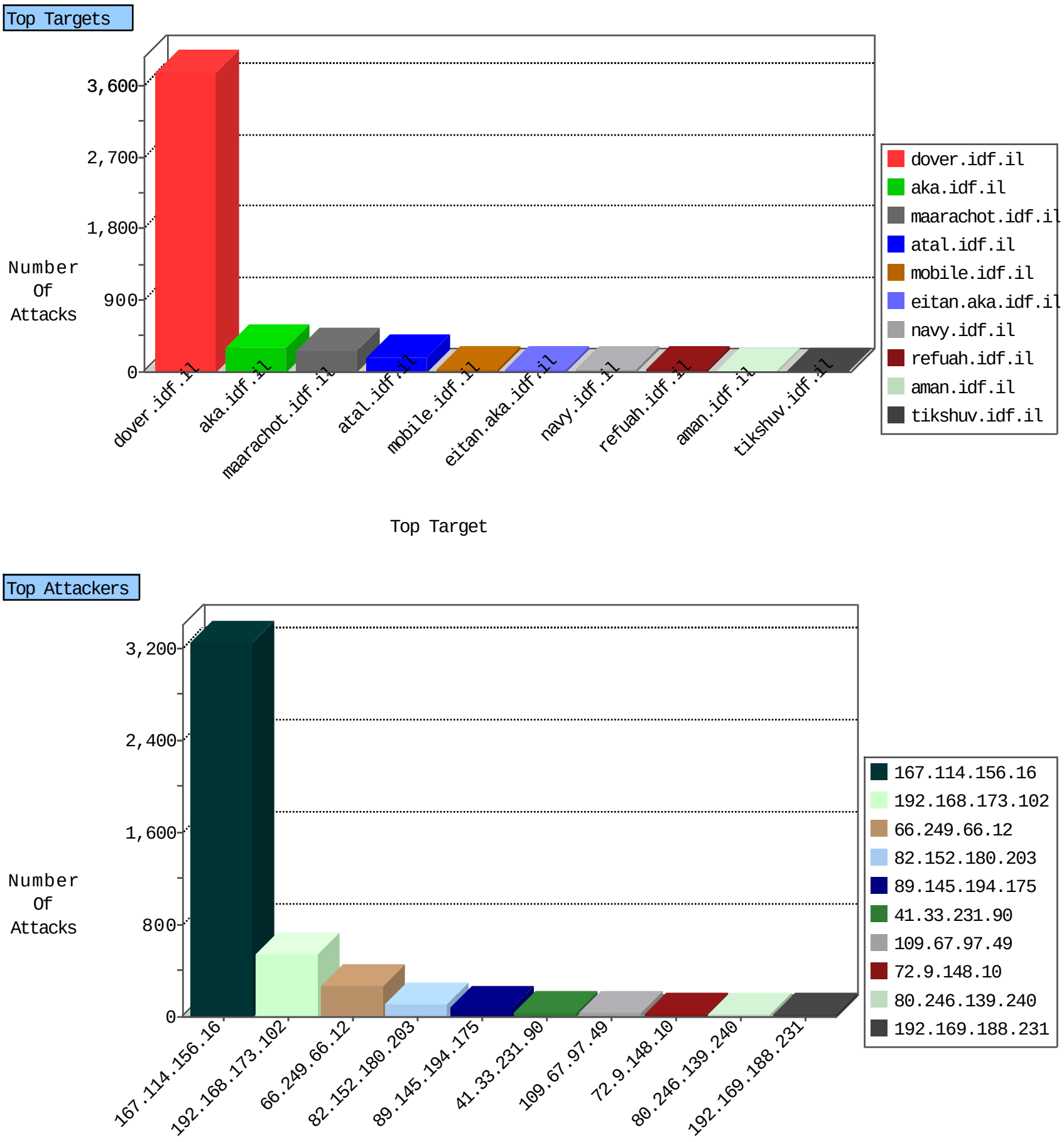
04-08-2016-11:04:01 to 04-08-2016-12:04:01

IDF Under Attack Daily Report



04-08-2016-11:04:01 to 04-08-2016-12:04:01

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	Block_Ip_Web_In	drop	3261
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
46.242.121.156	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
82.145.221.116	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3
204.42.253.2	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	2
185.3.147.126	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.242.121.156	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	2
66.249.69.93	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
91.15.194.153	Germany	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

04-08-2016-11:04:01 to 04-08-2016-12:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.115.4	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
208.83.7.157	United States	147.237.77.216	dover.idf.il	12634: HTTP: JS LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	6
46.117.20.148	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
31.129.248.85	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
195.154.187.115	France	147.237.72.167	ishurim.aka.idf.i	C1000074: HTTP: majestic bot	Block	2
195.154.187.115	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
31.129.248.85	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1

04-08-2016-11:04:01 to 04-08-2016-12:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	272
87.118.118.207	147.237.77.216	Germany	dover.idf.il	Tehila - Perl LWP with fake user agent	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
192.169.188.231	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
124.105.255.211	147.237.76.30	Philippines	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
192.169.188.231	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
101.200.82.129	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
192.169.188.231	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.79.104	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
192.169.188.231	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.169.188.231	147.237.76.86	United States	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
23.102.168.255	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
192.169.188.231	147.237.72.166	United States	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.169.188.231	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.169.188.231	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.85.221.63	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
190.145.17.209	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
192.169.188.231	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.192.0.226	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
192.169.188.231	147.237.77.212	United States	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.169.188.231	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.79.104	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
192.169.188.231	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
23.102.168.255	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
192.169.188.231	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.169.188.231	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.100.26.228	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
192.169.188.231	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

04-08-2016-11:04:01 to 04-08-2016-12:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	350
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	190
82.152.180.203	United Kingdom	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	56
82.152.180.203	United Kingdom	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	46
89.145.194.175	United Kingdom	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
89.145.194.175	United Kingdom	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
109.67.97.49	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
176.13.6.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.102.254.218	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.178.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.154.128.9	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.115.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.242.121.156	Russian Federation	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
185.3.147.150	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.242.121.156	Russian Federation	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
109.186.19.120	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.101.163.114	Germany	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
82.152.180.203	United Kingdom	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
91.216.51.36	Poland	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
198.101.202.28	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
91.216.51.36	Poland	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.139.240	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.106.52.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.57.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.139.240	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.128.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.181.6.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.51.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.139.240	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
87.70.58.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.139.240	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.64.135.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.19.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.152.180.203	United Kingdom	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
80.246.139.240	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.178.108.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.67.255	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.48.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.135.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
84.108.37.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
80.246.139.240	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.159.253	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 212.179.159.253	Block	13
79.177.206.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
217.132.97.200	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 217.132.97.200	Block	5
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.216	Block	3
46.19.86.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.14.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.159.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.179.159.253	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1806.jpg	Block	2
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/15710.jpg	Block	1
23.81.235.21	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/shared/usercontrols/headerupper/	Block	1
141.212.122.209	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
82.152.180.203	United Kingdom	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
216.218.206.66	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Method	Block	1
40.77.167.54	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
91.108.88.175	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1881	Block	1
202.79.209.94	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.19.86.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
23.106.166.130	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
149.88.166.49	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	1
84.200.45.89	Germany	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.78.13	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/style/1.he/popup.css	Block	1
41.45.126.121	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
91.108.88.214	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
2.54.138.100	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1882	Block	1
46.120.12.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.115	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
23.106.166.175	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
157.55.39.200	United States	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/robots.txt	Block	1
84.200.45.159	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1638-he/refuah.aspx	Block	1
66.249.78.20	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
217.132.97.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
185.80.220.181	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.85.113	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.65.114.13	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
23.80.147.64	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	1
74.82.47.4	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
54.153.33.233	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
23.106.211.129	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
157.55.39.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/armored/barak.stm<p>	Block	1
89.145.194.175	United Kingdom	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
217.132.97.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.80.220.181	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/components/com_hdflvplayer/hdflvplayer/-download.php	Block	1
46.19.86.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
23.80.148.202	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
23.106.244.47	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/shared/usercontrols/headerupper/	Block	1