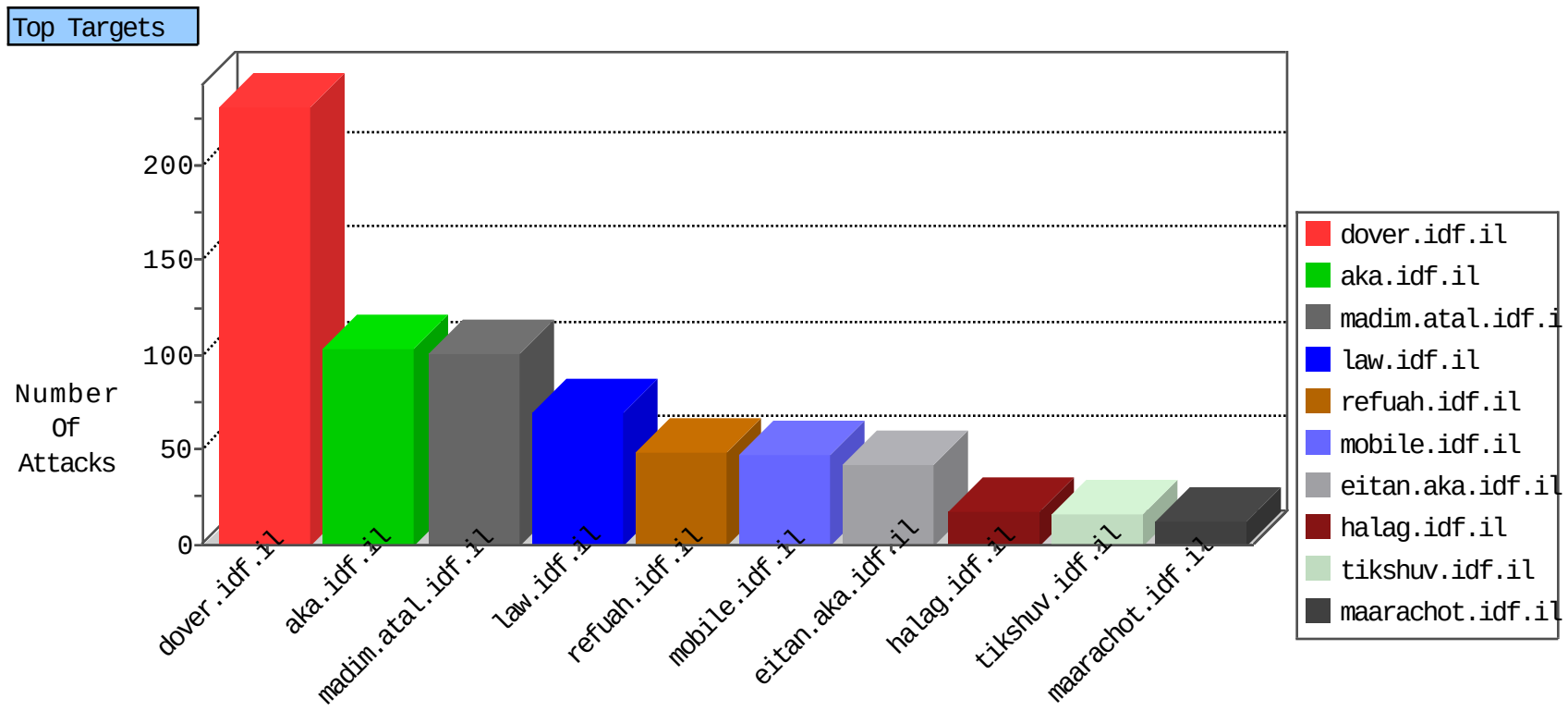
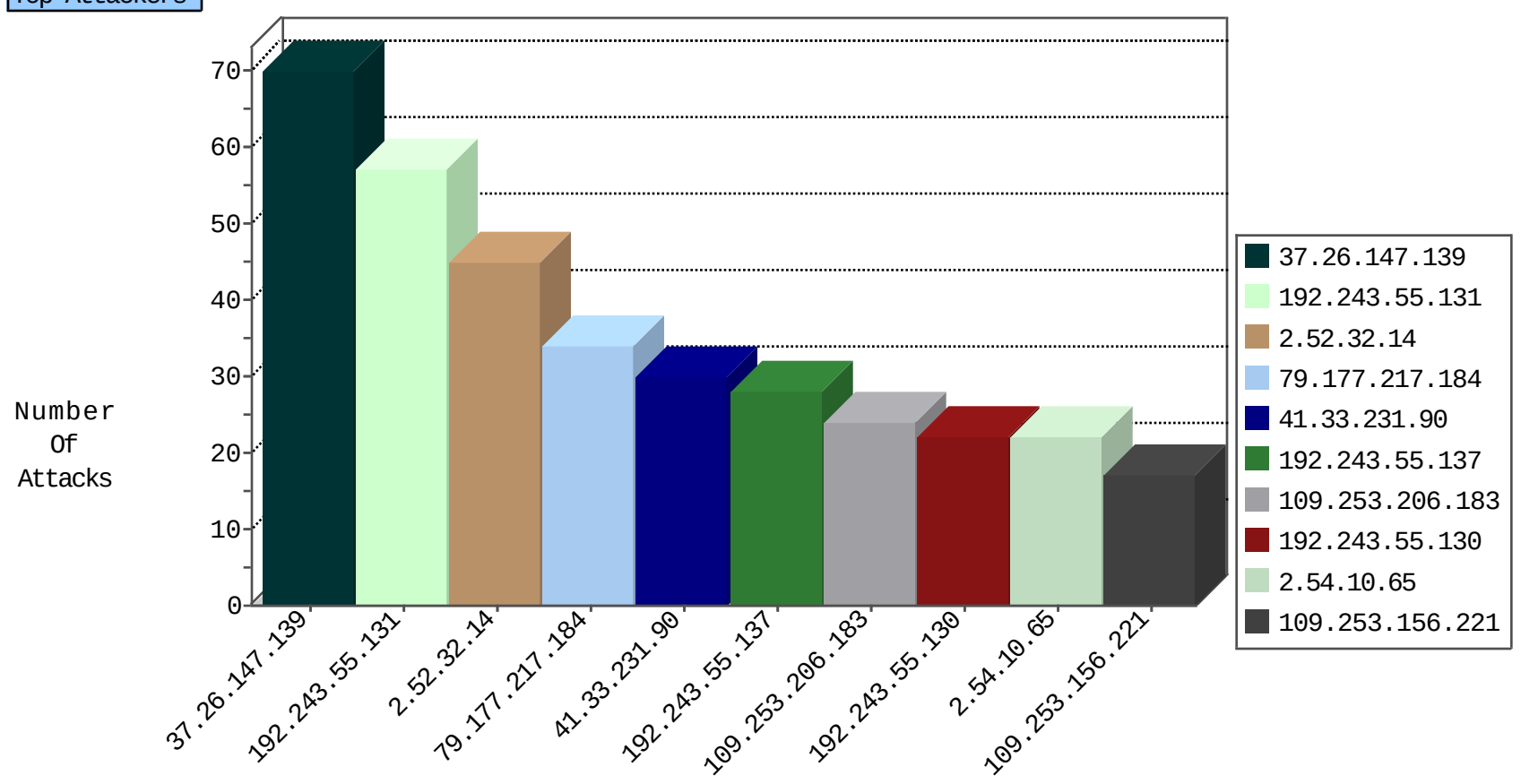
03-04-2016-08:04:06 to 03-04-2016-09:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-04-2016-08:04:06 to 03-04-2016-09:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
82.145.222.16	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
204.42.253.2	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
188.253.52.29	Iran, Islamic Republic of	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1
82.222.223.221	Turkey	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1
193.222.63.122	Romania	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
181.211.160.195	Ecuador	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1

03-04-2016-08:04:06 to 03-04-2016-09:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.154.214	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
85.250.86.43	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
89.137.220.110	Romania	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	2
69.30.198.178	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
173.234.153.122	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
195.154.187.115	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
80.246.133.146	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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
79.179.130.103	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-04-2016-08:04:06 to 03-04-2016-09:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.99.32.3	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sA (2)	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
218.246.0.97	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.0.33	Cote D'Ivoire	idf.il	ET SCAN NMAP -sS window 3072	1
104.232.98.38	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 1024	1
223.149.84.99	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
209.126.116.147	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.0.33	Cote D'Ivoire	idf.il	ET SCAN NMAP -sS window 4096	1
104.232.98.38	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 4096	1
27.4.125.28	147.237.76.39	India	mobile.meitav.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

03-04-2016-08:04:06 to 03-04-2016-09:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.32.14	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
79.177.217.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.253.156.221	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
185.130.5.193		147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
79.181.36.239	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.179.155.129	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
93.173.164.2	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
149.78.26.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.12.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.210.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.19.13	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.58	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.253.134.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.179.149	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.194.206.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.131	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
2.54.33.250	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.151	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
216.145.11.94	United States	147.237.77.176	matpash.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
2.54.135.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.181.58.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.172.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.12.160.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.206.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.6.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.99.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-04-2016-08:04:06 to 03-04-2016-09:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
109.253.206.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
2.54.10.65	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.10.65	Block	19
79.177.222.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.10.65	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
85.65.43.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.119.122.177	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	3
109.253.142.253	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.253.142.253	Block	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
46.19.86.81	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
95.86.101.117	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 95.86.101.117	Block	2
83.177.230.79	Latvia	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
83.177.230.79	Latvia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
87.68.248.116	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
207.46.13.136	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
37.26.148.154	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.253.134.197	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.228.12.55	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.182	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/6/1066.pdf	Block	1
151.236.162.125	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
46.19.85.67	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 46.19.85.67	Block	1
93.91.194.25	Iraq	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.179.149	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.64.101	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
217.172.29.53	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
37.26.148.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/news/news.in.aspx	Block	1
181.209.167.129	Guatemala	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.67	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/109621.pdf	Block	1
2.54.19.13	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
79.179.216.27	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/resource/userfollowresource/create/	Block	1
217.172.29.53	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
40.77.167.94	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
85.130.211.93	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
77.125.6.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/idkunpratimishiyim.aspx	Block	1
185.89.101.37		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
66.249.66.64	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/110475.pdf	Block	1
129.215.203.127	United Kingdom	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
45.55.67.78		147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 45.55.67.78	Block	1
87.68.248.116	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.68.248.116	Block	1
79.177.217.184	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
185.112.232.94		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
37.26.147.139	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.101.117	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/1440-he/atal.aspx&sa=u&ved=0ahukewif47_juqblahujrrokhbcycyiqfggimaa&usg=afqjcnewy2ykdtpnx1bua-b4wxbopwiblg	Block	1
66.249.66.69	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/081210gaza141.aspx	Block	1
138.36.0.3		147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/index.php	Block	1
45.55.67.78		147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1

03-04-2016-08:04:06 to 03-04-2016-09:04:06