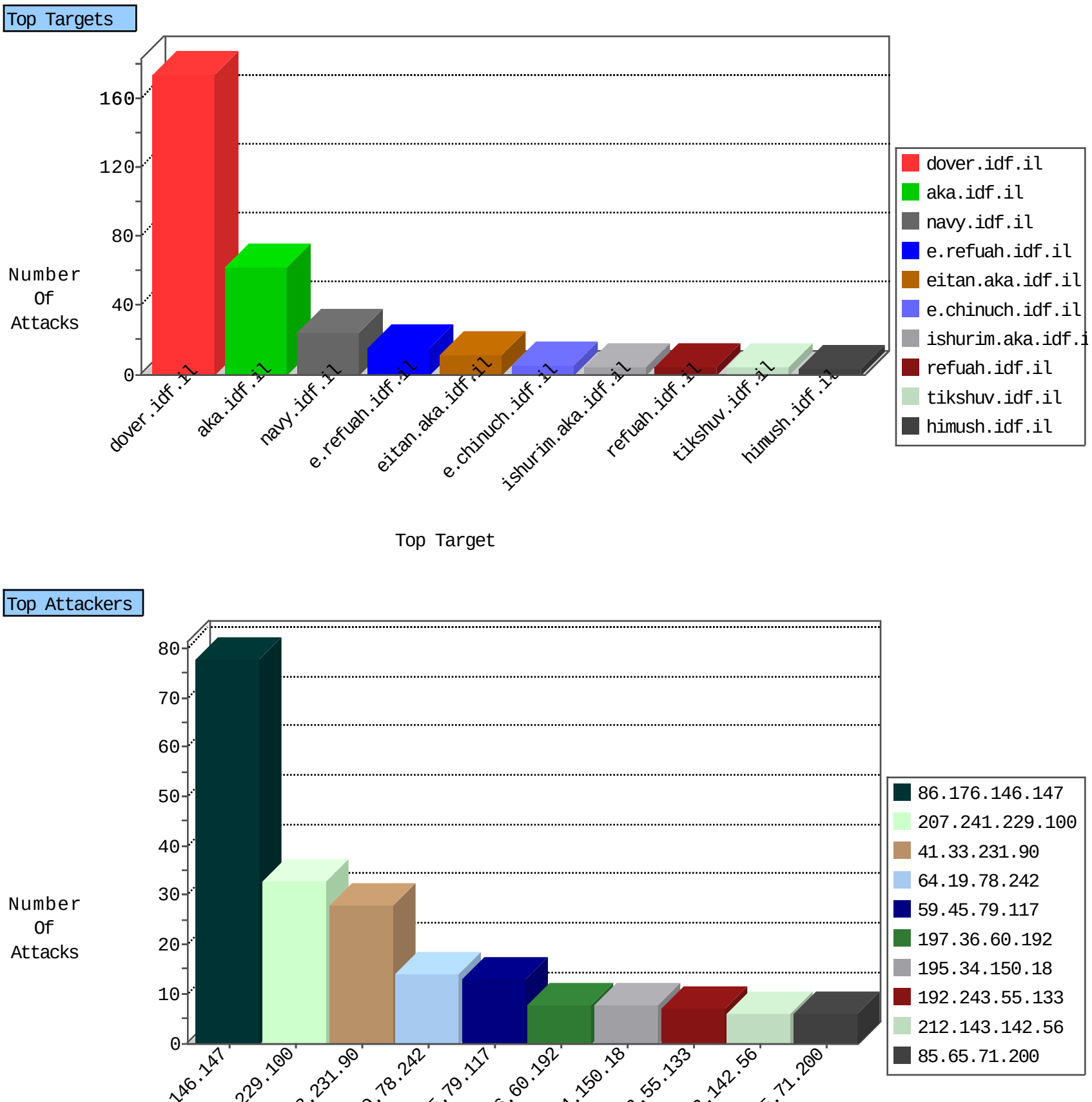
02-07-2016-04:04:07 to 02-07-2016-05:04:07

IDF Under Attack Daily Report



02-07-2016-04:04:07 to 02-07-2016-05:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.151.244.102	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

02-07-2016-04:04:07 to 02-07-2016-05:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-07-2016-04:04:07 to 02-07-2016-05:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
193.201.227.11	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Potential SSH Scan	3
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
189.203.240.181	147.237.0.15	Mexico	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.19	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.192.0.19	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.189.26.18	147.237.77.179	Austria	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
172.56.35.154	147.237.76.30	United States	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
59.45.79.117	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.21	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.21	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
201.172.146.99	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.20	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.20	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.11	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.20	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.192.0.19	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.192.0.19	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.117.208.243	147.237.76.196		e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
151.72.10.87	147.237.8.28	Italy	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.21	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.21	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.20	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.11	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.20	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1

02-07-2016-04:04:07 to 02-07-2016-05:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
86.176.146.147	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
207.241.229.100	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	33
64.19.78.242	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	14
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
197.36.60.192	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.190.2.188	Nigeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
65.55.210.141	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
70.162.97.240	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.78.137	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.162.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	3
85.65.71.200	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.78.144	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
172.56.35.154	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.65.133	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.65.71.200	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
74.6.254.127	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.86.102	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
162.223.46.68	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.12	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
198.20.69.74	United States	147.237.76.197	e.himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.19.78.243	United States	147.237.72.166	aka.idf.il	HTTP Format Sizes	'Cookies' header length exceeded maximum allowed length	monitor	1
184.105.139.83	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.186.168.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
216.218.206.112	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.168.152.6	United States	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.19.86.102	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
172.56.35.154	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.187.114.171	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.47	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
206.253.226.7	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.103	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.253.217.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP anomaly detected	Non-compliant TCP packets coming from multiple external sources were detected. This may result from potential network configuration problem.	drop	1
85.65.71.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

02-07-2016-04:04:07 to 02-07-2016-05:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
50.7.178.100	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.187.114.171	France	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
100.38.164.180	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.116.219.176	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.139.104	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
42.62.74.80	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
157.55.39.126	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

02-07-2016-04:04:07 to 02-07-2016-05:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	5
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	2
136.243.98.54	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	2
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	2
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	2
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	2
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	2
66.249.78.184	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter lang in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1638-he/refuah.aspx	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58604&docid=68885	Block	1
85.214.155.116	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21744-ar/idfgdover.aspx	Block	1
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1732	Block	1
37.142.190.206	Israel	147.237.0.34	tikshuv.idf.il	Suspicious Response Code	Block	1
207.46.13.34	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/size220x0/sip_storage	Block	1
74.82.47.3	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
37.142.190.206	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il./favicon.ico	Block	1
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18719-he/dover.aspx	Block	1
176.56.230.79	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/global.js	Block	1
64.19.78.243	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
181.215.1.105	Chile	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/>israel	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
66.249.64.133	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size338x0/sip_storage	Block	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20187-he/dover.aspx)	Block	1

02-07-2016-04:04:07 to 02-07-2016-05:04:07