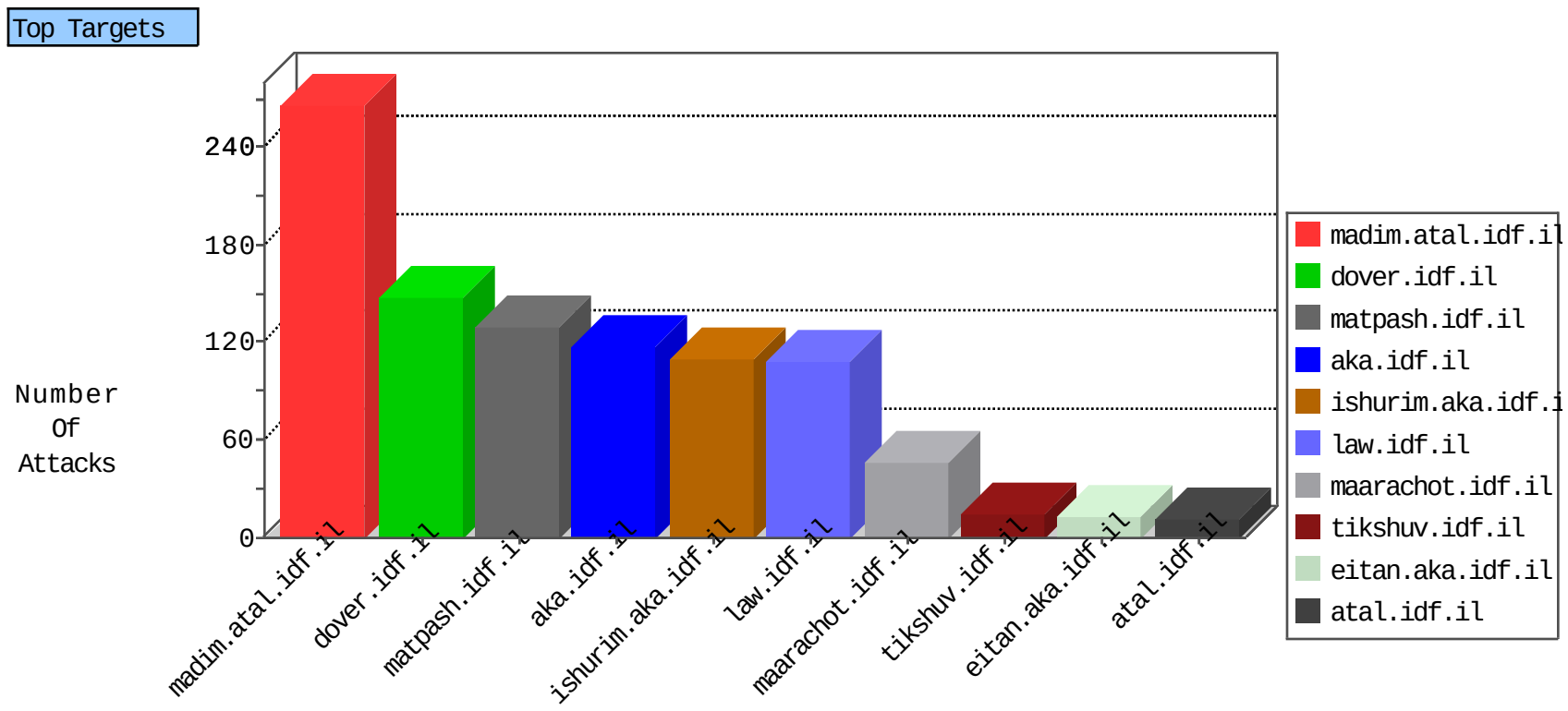
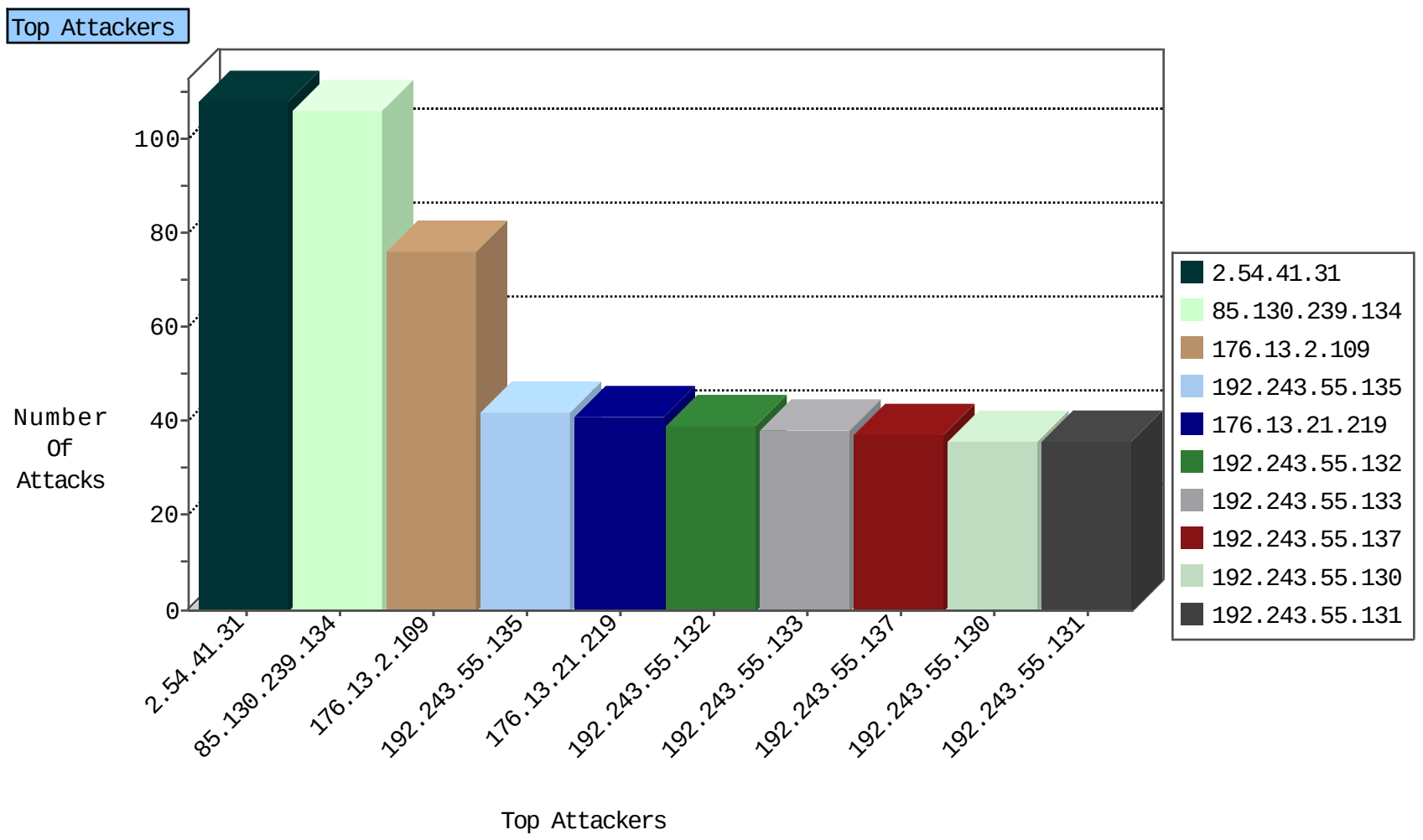
03-09-2016-07:04:05 to 03-09-2016-08:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-09-2016-07:04:05 to 03-09-2016-08:04:05

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
87.69.165.171	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
184.105.139.88	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
198.167.129.9	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.67	United States	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	1
23.228.107.104	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.100	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.67	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
23.228.107.104	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.116	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
23.228.107.104	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.120	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
107.6.113.220	Singapore	147.237.72.167	ishurim.aka.idf.il	L4 Source or Dest Port Zero	drop	1

03-09-2016-07:04:05 to 03-09-2016-08:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	6
212.29.223.233	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.117.233.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
176.13.3.67	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.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
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-09-2016-07:04:05 to 03-09-2016-08:04:05

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
185.130.5.113	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.76.39	Canada	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
37.1.209.203	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.113	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.234	147.237.77.61	Switzerland	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
37.1.209.203	147.237.77.121	United States	e.navy.idf.il	ET SCAN Potential SSH Scan	1
37.1.209.203	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1

03-09-2016-07:04:05 to 03-09-2016-08:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.130.239.134	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
37.26.149.149	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.52.133.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
147.236.33.36	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.239.134	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
5.22.129.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.21.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
69.31.51.31	Anonymous Proxy	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	9
85.130.239.134	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
172.172.18.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.130.239.134	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	7
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.130	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
79.179.228.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.137	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.130	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	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
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.133	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
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.204.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.138	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.65.121.248	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	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
176.13.3.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-09-2016-07:04:05 to 03-09-2016-08:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.41.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
176.13.2.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
176.13.21.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
37.26.149.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
109.253.159.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.183.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.76.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.65.121.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.149.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
103.193.116.59		147.237.77.216	dover.idf.il	PHP Attempt	Block	1
65.75.160.133	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/old/wp-admin/	Block	1
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.99.7.92	Albania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
185.82.200.91		147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.17/	Block	1
103.193.116.59		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
199.212.86.48		147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.99.7.92	Albania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
185.82.200.91		147.237.76.39	mobile.meitav.idf.il	Distributed Unauthorized URL Access on 147.237.76.39/	Block	1
109.65.61.107	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
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
207.46.13.100	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	1
109.65.61.107	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.65.61.107	Block	1
66.249.66.179	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/1095-he/patzar.aspx	Block	1
216.218.206.67	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
180.40.168.85	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	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
62.210.254.52	France	147.237.72.166	aka.idf.il	Malformed URL p://www.aka.idf.il/main/sachar/resources/images/icons/favicon.png	Block	1
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcdhphdmltxdewmtguzg9j&infocenteritem=true	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
184.105.247.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1

03-09-2016-07:04:05 to 03-09-2016-08:04:05