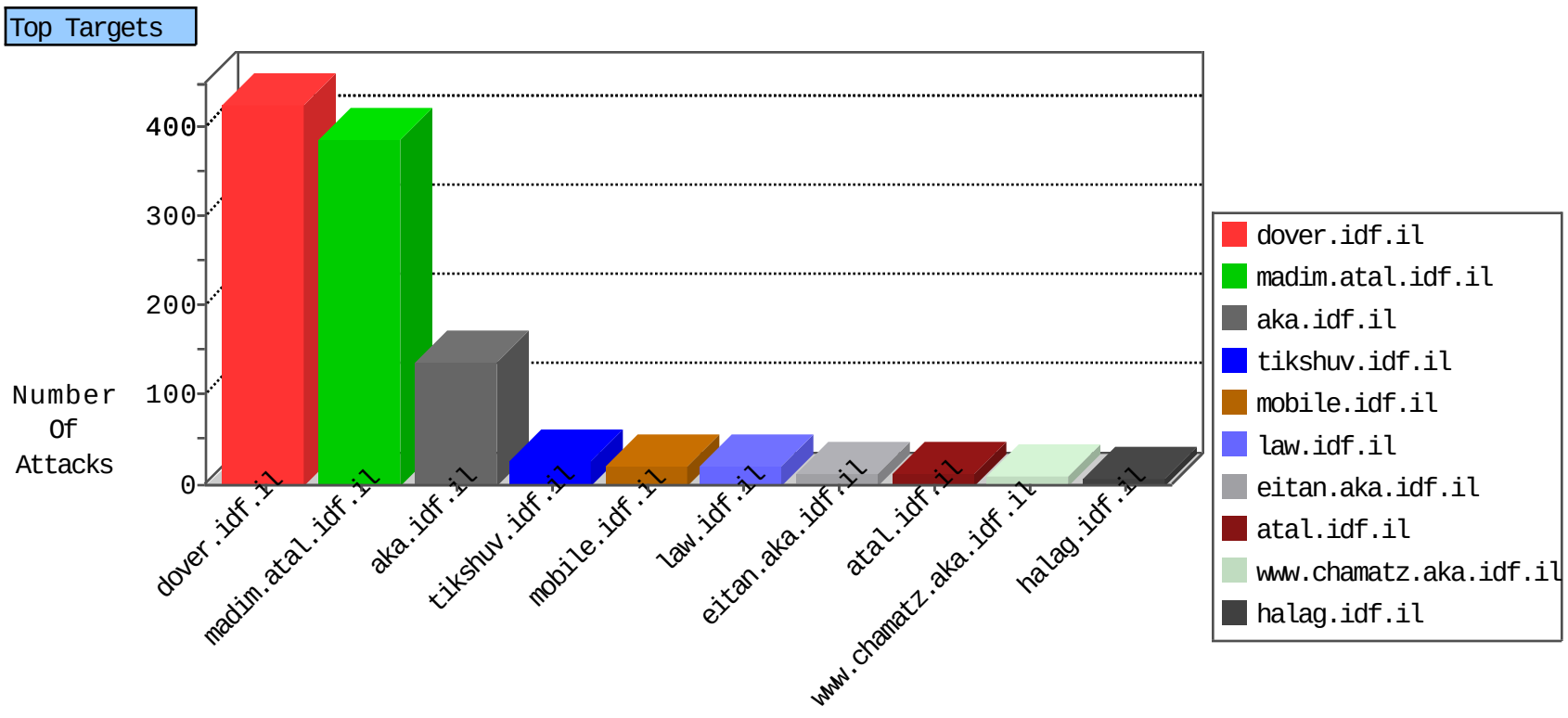
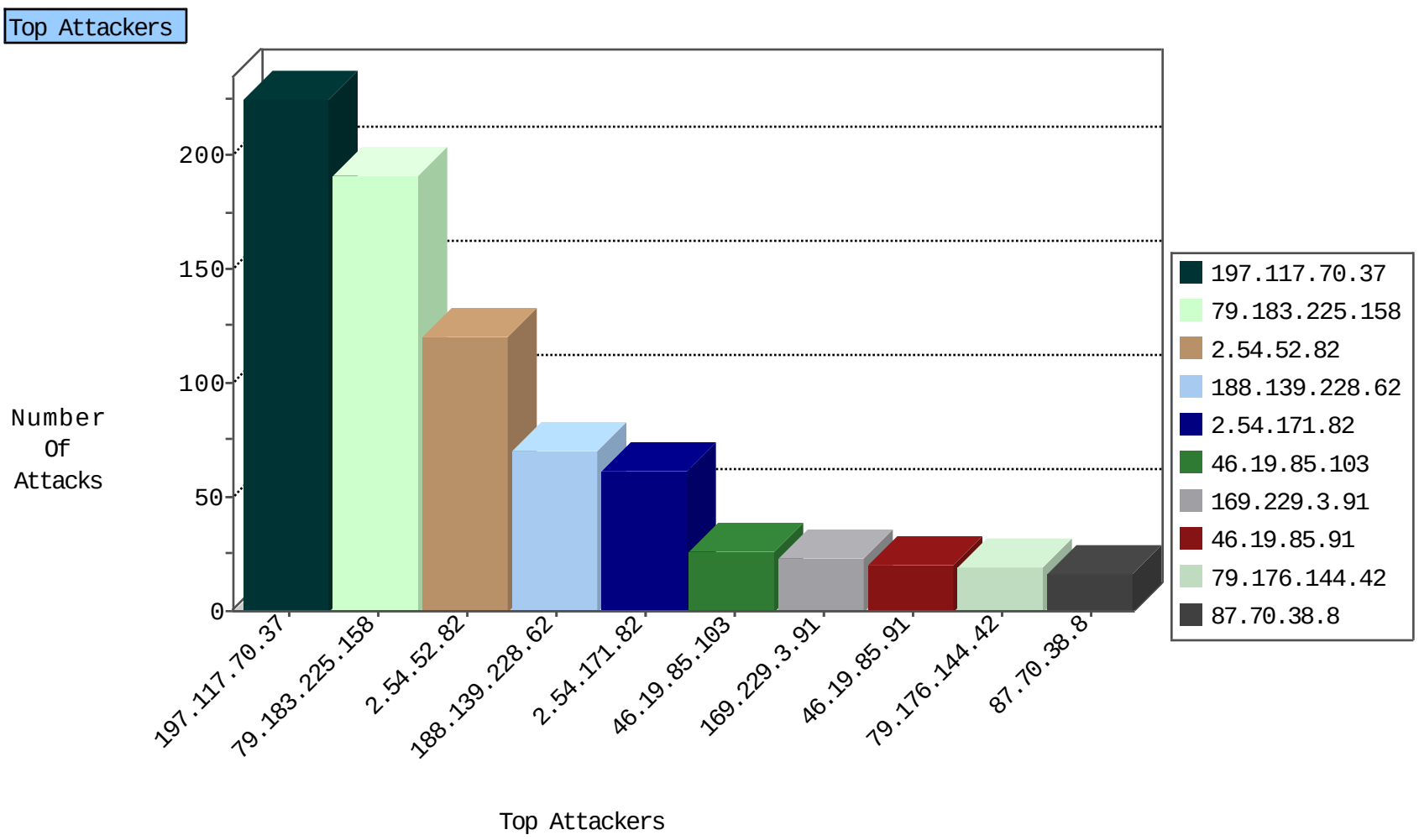
03-05-2016-15:04:08 to 03-05-2016-16:04:08

IDF Under Attack Daily Report





03-05-2016-15:04:08 to 03-05-2016-16:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.117.70.37	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	225
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
134.147.203.115	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	2
181.199.135.122	Peru	147.237.0.35	akaws.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
85.25.43.94	Germany	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
198.20.87.98	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
74.82.47.5	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

03-05-2016-15:04:08 to 03-05-2016-16:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.144.42	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
109.65.72.232	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
49.246.230.40	China	147.237.77.74	law.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2
109.64.41.47	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
10.0.0.9		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
188.165.15.97	France	147.237.77.234	halag.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-05-2016-15:04:08 to 03-05-2016-16:04:08

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
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	2
213.136.91.26	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
108.171.183.52	147.237.77.176	United States	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
210.14.157.131	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.8.28	Canada	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
210.14.157.131	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
210.14.157.131	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.76.38	Latvia	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.234	147.237.8.46	Switzerland	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
179.43.141.234	147.237.0.33	Switzerland	idf.il	ET SCAN NMAP -sS window 1024	1
159.122.220.108	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
223.4.174.30	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
120.142.24.238	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
213.136.91.26	147.237.72.166	Germany	aka.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.176	Canada	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
210.14.157.131	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
95.130.13.220	147.237.77.176	France	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
210.14.157.131	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
198.20.69.98	147.237.77.227	United States	e.hamaz.idf.il	ET DROP Dshield Block Listed Source	1
179.43.141.234	147.237.0.34	Switzerland	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
176.228.159.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
223.4.174.30	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1

03-05-2016-15:04:08 to 03-05-2016-16:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.139.228.62	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	35
188.139.228.62	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
87.71.36.165	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.65.15.44	Israel	147.237.77.243	mobile.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
2.54.140.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.38.8	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
109.253.223.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.251.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.144.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.103	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.46.13.111	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.42.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.195.96	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.103	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
31.168.197.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.207.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.237	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.195.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.104.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.145.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.180.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.38.8	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.170	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
149.78.25.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.183.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.198.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.38.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.8.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.243.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.68	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.218.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.56.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.223.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.207.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.21.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.115.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-05-2016-15:04:08 to 03-05-2016-16:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
77.127.163.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.153.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.138.79.137	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.54.175.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.227.198	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-05-2016-15:04:08 to 03-05-2016-16:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.225.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	188
2.54.52.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
2.54.171.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
131.253.25.237	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
65.55.210.255	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
37.26.149.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	4
109.253.209.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.209.164	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
2.52.63.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.64.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.65.217	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
115.239.212.198	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.30.25.46	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.109.241.204	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Distributed Abnormally Long Request	Block	1
82.102.221.227	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
66.249.66.23	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1396-he/atal.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.113.89	Block	1
84.228.195.232	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
46.19.86.139	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Distributed Malformed URL	Block	1
184.105.139.68	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
83.134.162.103	Belgium	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in URL	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/4/112424.pdf	Block	1
2.54.140.143	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
149.78.54.92	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/gen204	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	1
86.2.89.55	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
79.182.30.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Malformed URL from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Distributed Unknown HTTP Request Method	Block	1
110.34.178.35	Thailand	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.100.84.82		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
83.134.162.103	Belgium	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.66.67	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.66.67	Block	1
149.255.228.30	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
87.70.41.46	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Multiple Illegal Byte Code Character in Header Name from 169.229.3.91	Block	1

03-05-2016-15:04:08 to 03-05-2016-16:04:08