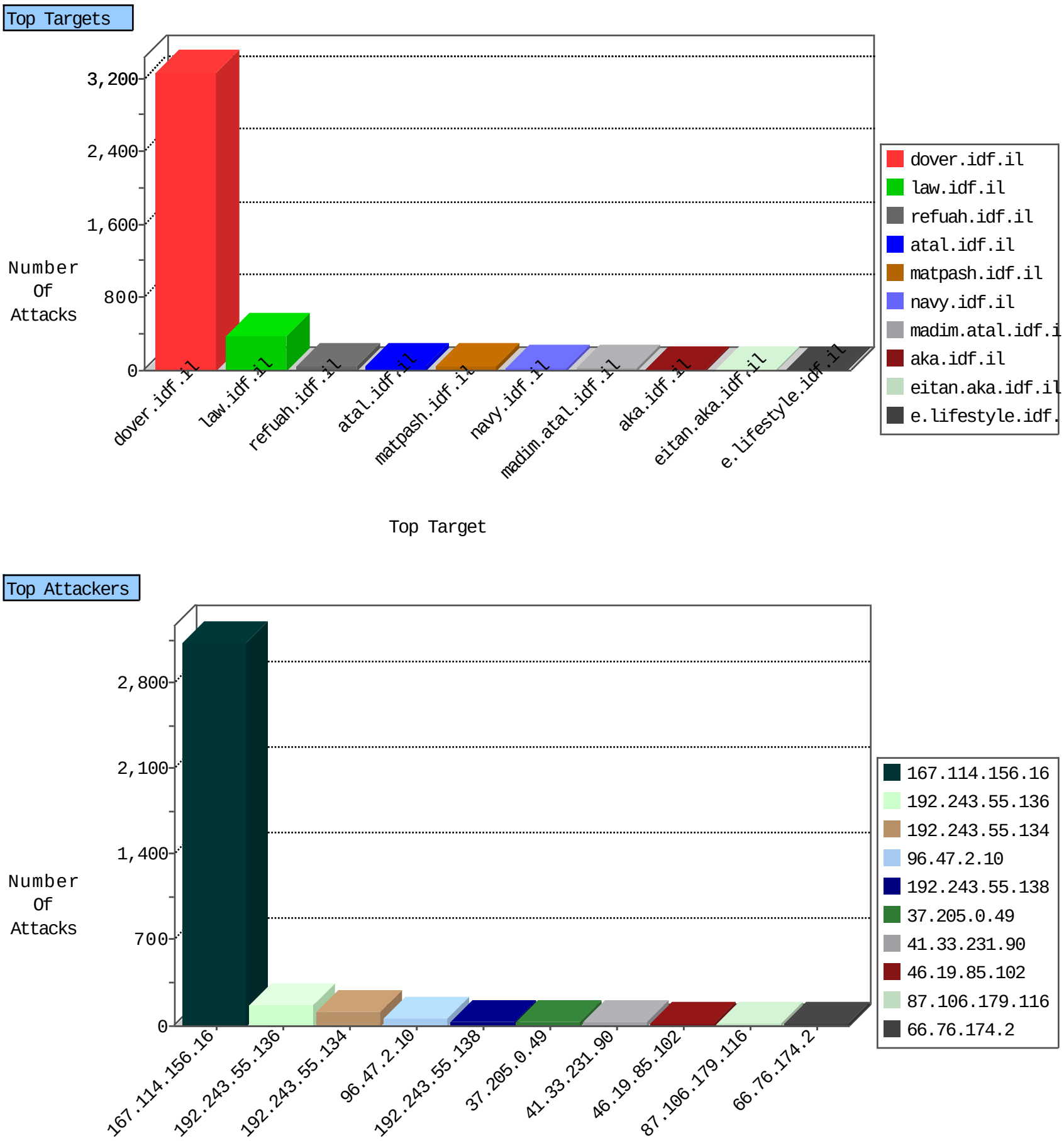
04-13-2016-04:04:05 to 04-13-2016-05:04:05

IDF Under Attack Daily Report



04-13-2016-04:04:05 to 04-13-2016-05:04:05

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	3123
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
179.43.144.31	Switzerland	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
74.82.47.50	United States	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.31	Switzerland	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.31	Switzerland	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
185.35.62.218	Switzerland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.31	Switzerland	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.31	Switzerland	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.79	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.31	Switzerland	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.31	Switzerland	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

04-13-2016-04:04:05 to 04-13-2016-05:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.106.179.116	Germany	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
37.205.0.49	Turkey	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
96.47.2.10	United States	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
96.47.2.10	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
96.47.2.10	United States	147.237.77.176	matpash.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
37.205.0.49	Turkey	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.246.49.97	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
96.47.2.10	United States	147.237.77.176	matpash.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.247.63.11	Netherlands	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
96.47.2.10	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.76.174.2	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
184.168.193.34	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
23.91.70.119	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
66.135.63.82	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
209.15.196.171	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
61.135.189.98	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.168	France	147.237.0.34	tikshuv.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
92.176.142.53	France	147.237.77.176	matpash.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
151.80.31.180	France	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-13-2016-04:04:05 to 04-13-2016-05:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.205.0.49	147.237.76.42	Turkey	refuah.idf.il	SQL Injection - Select From	22
96.47.2.10	147.237.77.176	United States	matpash.idf.il	SQL Injection - Select From	18
96.47.2.10	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	14
213.247.63.11	147.237.77.233	Netherlands	atal.idf.il	SQL Injection - Select From	12
66.76.174.2	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	12
87.106.179.116	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	10
23.91.70.119	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
209.15.196.171	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	6
184.168.193.34	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
213.246.49.97	147.237.77.74	France	law.idf.il	SQL Injection - Select From	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
13.92.246.145	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
113.240.250.154	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
108.190.157.157	147.237.76.30	United States	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.82.78.38	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.246.145	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1

04-13-2016-04:04:05 to 04-13-2016-05:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	40
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	39
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	33
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	29
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	13
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	12
94.73.150.148	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.120.145.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.138	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
62.83.141.109	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.182.155.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
61.135.189.98	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	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
128.232.110.29	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.29	United Kingdom	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
128.232.110.29	United Kingdom	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
157.55.39.42	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
212.179.90.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.29	United Kingdom	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
128.232.110.29	United Kingdom	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
79.177.98.223	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.29	United Kingdom	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
200.74.240.180	Panama	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.249.79.31	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
8.37.227.81	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
106.184.3.122	Japan	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
159.226.95.66	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.84	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.196	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.249.66.247	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
124.135.164.209	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
95.185.2.209	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
68.180.229.226	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
40.77.167.92	United States	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

04-13-2016-04:04:05 to 04-13-2016-05:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	19
138.163.240.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
88.21.93.158	Spain	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
66.249.66.186	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
88.21.93.158	Spain	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
68.191.206.71	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	2
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
197.231.221.211	Liberia	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
157.55.39.32	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
204.236.235.245	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.66.186	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
157.55.39.64	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
212.47.233.68	France	147.237.0.15	kosher-kravi.idf.i	Distributed Unauthorized URL Access on 147.237.0.15/	Block	1
98.200.7.41	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.index,xml	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
181.28.219.232	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter tab in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
46.19.85.33	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/1141-he-orchot.aspx	Block	1
138.163.240.41	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
192.243.55.134	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1

04-13-2016-04:04:05 to 04-13-2016-05:04:05