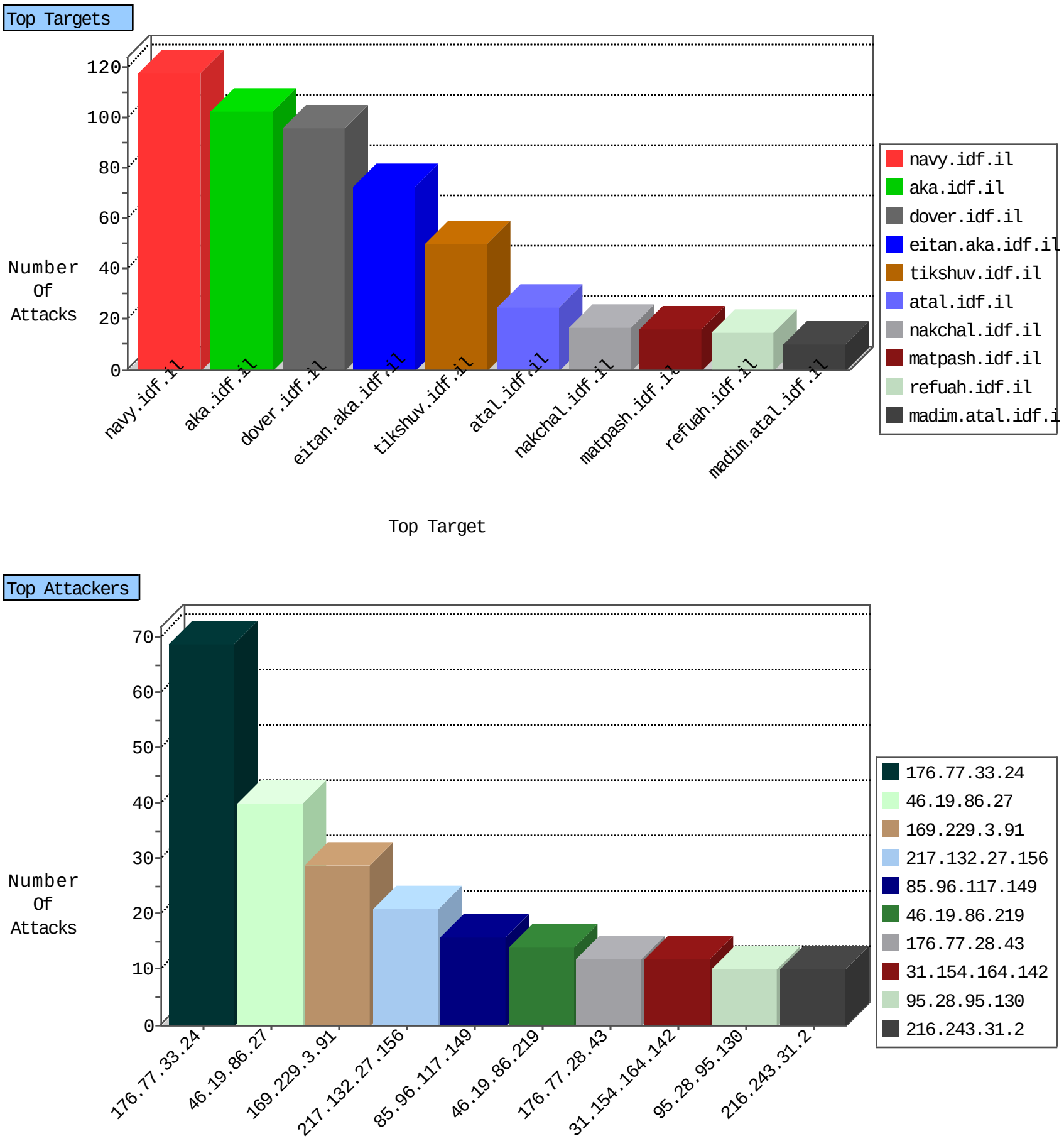
03-05-2016-13:04:03 to 03-05-2016-14:04:03

IDF Under Attack Daily Report



03-05-2016-13:04:03 to 03-05-2016-14:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.241.250	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	7
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
176.77.33.24	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
176.77.33.24	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.130.5.224		147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1

03-05-2016-13:04:03 to 03-05-2016-14:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.75.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
91.121.101.78	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
46.121.214.54	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.57.0.201	Ukraine	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Block	1
119.74.148.71	Singapore	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
85.96.117.149	Turkey	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1

03-05-2016-13:04:03 to 03-05-2016-14:04:03

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
85.96.117.149	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP admin.php access	1
218.246.0.97	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
159.122.220.108	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.185	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
159.122.220.108	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

03-05-2016-13:04:03 to 03-05-2016-14:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.77.33.24	Russian Federation	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	62
46.19.86.27	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
217.132.27.156	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
31.154.164.142	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.77.28.43	Russian Federation	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	11
95.28.95.130	Russian Federation	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	10
87.71.26.43	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
5.164.126.92	Russian Federation	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	9
85.65.234.243	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.219	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.219	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.136.49	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.219.190	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.26.146.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.33.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.107.241	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.111.136.140	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.46.38.96	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
119.136.94.214	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
176.13.6.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.230.220.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.238.116.94	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.65.129.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.86	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.46.38.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
217.132.236.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.65.248.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.161.3.178	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
2.52.34.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.152.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.95.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.187.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.90.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.175.126	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.253.214.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.126.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.86	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.46.38.96	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
87.71.23.123	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
188.120.154.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

03-05-2016-13:04:03 to 03-05-2016-14:04:03

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.121.60.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.3.147.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.210.186.84	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

03-05-2016-13:04:03 to 03-05-2016-14:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.96.117.149	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 85.96.117.149	Block	5
85.96.117.149	Turkey	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
66.249.66.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	4
2.54.53.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
134.249.81.88	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	3
46.118.155.216	Ukraine	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
207.46.13.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
79.177.36.193	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.135.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.96.117.149	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 85.96.117.149	Block	3
110.38.219.97	Pakistan	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.52.16.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.72.219	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.25.105.88	Italy	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
87.70.56.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Abnormally Long Request from 169.229.3.91	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/general.aspx	Block	1
46.120.72.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
157.55.39.58	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
37.57.0.201	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/user/	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
87.71.26.43	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
79.180.205.123	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in URL	Block	1
66.249.69.81	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1405-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
46.117.107.241	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
176.77.28.43	Russian Federation	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 176.77.28.43	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Abnormally Long Request method	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
157.55.39.208	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1927-en/cogat.aspx gaza semanales	Block	1
38.111.147.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1
79.181.115.176	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	NULL Character in URL	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Malformed URL	Block	1
66.249.69.89	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
119.136.94.214	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
46.118.155.216	Ukraine	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
185.89.217.227		147.237.77.74	law.idf.il	URL is Above Root Directory www.law.idf.il/../images/1.he/navigation/navigation_arrow.gif	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Header Name	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1
54.244.49.197	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1403-he/atal.aspx	Block	1
162.243.188.75	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
91.108.88.154	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/main.asp	Block	1
46.19.85.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
79.181.173.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-05-2016-13:04:03 to 03-05-2016-14:04:03