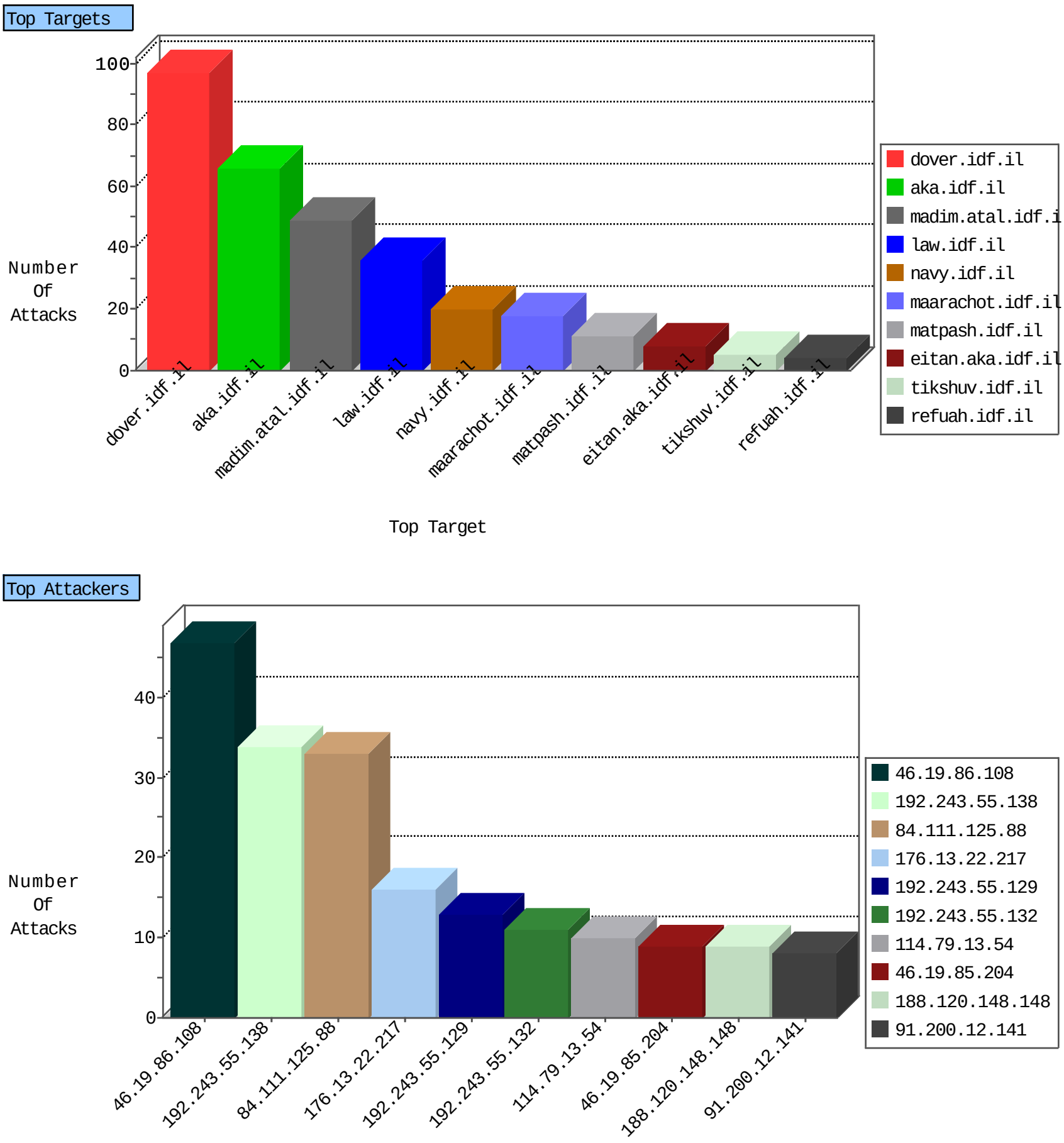
03-09-2016-06:04:02 to 03-09-2016-07:04:02

IDF Under Attack Daily Report



03-09-2016-06:04:02 to 03-09-2016-07:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.125.88	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	33
114.79.13.54	Indonesia	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
184.105.139.124	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.108	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.232	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.84	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
65.196.5.13	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.116	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
104.156.246.165	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
23.228.107.104	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.88	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.50	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.124	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
23.228.107.104	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.92	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1

03-09-2016-06:04:02 to 03-09-2016-07:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.4.148	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
46.116.110.197	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.4.148	Germany	147.237.77.170	maarachot.idf.il	C1000074: HTTP: majestic bot	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
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-09-2016-06:04:02 to 03-09-2016-07:04:02

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	2
104.215.89.20	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 2048	1
104.215.89.20	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -f -sS	1
94.20.191.70	147.237.72.156	Azerbaijan	aman.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.77.216	China	dover.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
40.76.95.41	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
198.180.198.185	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
104.215.89.20	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
94.20.191.70	147.237.72.156	Azerbaijan	aman.idf.il	ET SCAN NMAP -sS window 2048	1
93.189.26.18	147.237.77.19	Austria	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
40.76.95.41	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
218.246.0.97	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
198.180.198.185	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

03-09-2016-06:04:02 to 03-09-2016-07:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.22.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
188.120.148.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.4.102	Israel	147.237.72.166	aka.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
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
192.243.55.138	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
5.28.185.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
83.149.34.216	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.194	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.138	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.149.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.22.68	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	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.138	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence		monitor	2
91.200.12.143	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	2
46.19.86.99	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
91.200.12.141	Ukraine	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
207.46.13.127	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.54.3.99	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
77.237.138.202	Czech Republic	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
91.200.12.141	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.129	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
65.55.210.180	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.129	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.138	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
108.19.86.184	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
82.166.93.85	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
65.55.218.40	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.200	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.219	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

03-09-2016-06:04:02 to 03-09-2016-07:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	47
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
67.85.177.37	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	2
211.76.254.2	Taiwan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	2
198.252.106.75	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp/wp-admin/	Block	1
176.13.22.217	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ca in www.aka.idf.il/main/rabanut/general.aspx	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 52.; in URL _pk_ses.20.8afc=*	Block	1
185.112.248.32		147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
109.253.212.77	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
205.186.180.16	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wordpress/wp-admin/	Block	1
176.13.22.217	Israel	147.237.72.166	aka.idf.il	Unknown Parameter cat in www.aka.idf.il/main/rabanut/general.aspx	None	1
46.19.86.99	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
190.60.88.70	Chile	147.237.76.86	navy.idf.il	Cookie Tampering on cookie __atrfs: Expected ab/	None	1
141.212.122.209	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/shared/usercontrols/navmenu/undefined	Block	1
5.28.180.24	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx	Block	1
207.46.13.70	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
176.13.22.217	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catI in www.aka.idf.il/main/rabanut/general.aspx	None	1
107.15.209.219	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/englisch	Block	1
157.55.39.150	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
185.28.20.201	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/test/wp-admin/	Block	1
107.15.209.219	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 107.15.209.219	Block	1
46.19.86.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube	Block	1
176.13.22.217	Israel	147.237.72.166	aka.idf.il	Unknown Parameter c in www.aka.idf.il/main/rabanut/general.aspx	None	1
67.85.177.37	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_ses.20.8afc=*	Block	1
219.94.128.197	Japan	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/blog/wp-admin/	Block	1
185.82.200.91		147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
108.29.111.117	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
64.71.32.23	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp-admin/	Block	1

03-09-2016-06:04:02 to 03-09-2016-07:04:02