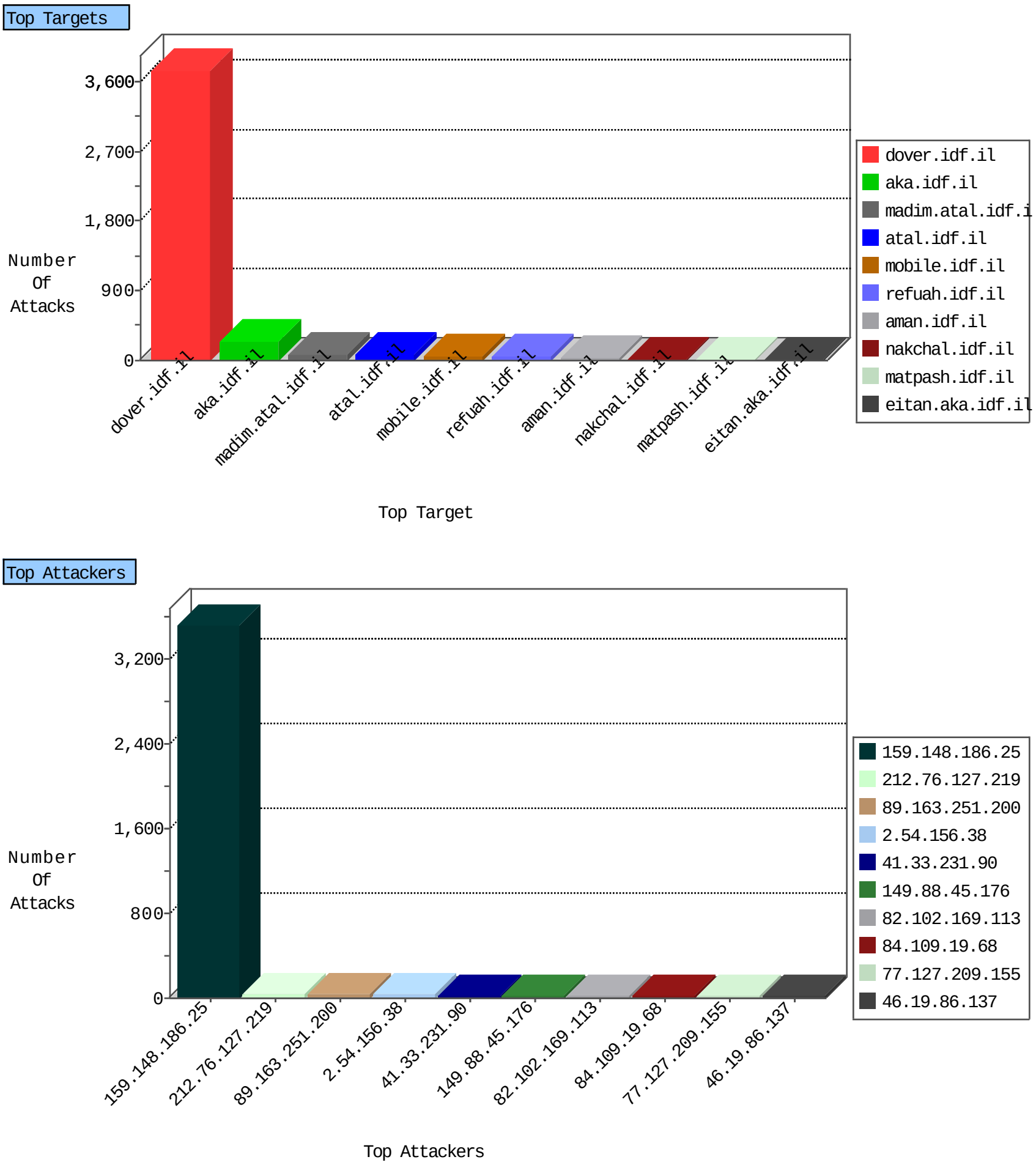
02-17-2016-20:04:02 to 02-17-2016-21:04:02

IDF Under Attack Daily Report



02-17-2016-20:04:02 to 02-17-2016-21:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5227
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	3667
66.249.93.103	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	9
37.8.35.56	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.179.148.4	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
64.110.129.208		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

02-17-2016-20:04:02 to 02-17-2016-21:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-17-2016-20:04:02 to 02-17-2016-21:04:02

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	4
79.178.5.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.88.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.56.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.87.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.64.169.106	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
176.13.10.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.193.224	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
88.249.106.23	147.237.8.24	Turkey	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
68.180.229.239	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.254.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.149.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.50.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.240	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.139.209	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

02-17-2016-20:04:02 to 02-17-2016-21:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2192
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	316
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
149.88.45.176	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.108.244.47	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
93.173.147.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.201.171.208	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
81.218.173.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.109.119.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
80.74.119.186	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
109.253.139.209	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.205	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.178.168.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.30.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.203	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.102.169.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
199.195.108.113	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.102.169.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
89.163.251.200	Germany	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	5
109.253.139.209	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
81.218.173.63	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
188.120.148.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
213.151.48.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.195.108.113	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.66.104.52	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
89.163.251.200	Germany	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
2.54.35.83	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.42.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.144.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.163.251.200	Germany	147.237.77.74	law.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
5.39.93.143	France	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.85.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.181.5.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
78.119.178.126	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.184.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.117	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.166.219.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.54.120	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	3
185.27.106.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.38.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-17-2016-20:04:02 to 02-17-2016-21:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.156.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
84.109.19.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
82.166.22.37	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.166.22.37	Block	10
164.138.122.72	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 164.138.122.72	Block	7
46.19.85.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.85.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.153.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
168.235.205.98	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
84.111.2.81	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
84.108.51.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.222.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.55.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.137	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
87.69.102.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.173.36.91	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
217.194.194.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
93.173.36.91	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
212.179.132.202	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/113272.pdf/	Block	1
86.165.130.56	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
173.66.40.163	United States	147.237.76.86	navy.idf.il	Unknown HTTP Request Method Â,[[#0]][[#0]][[#0]][[#22]]Â¡ in URL	Block	1
81.7.137.98	Denmark	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
66.76.174.2	United States	147.237.72.166	aka.idf.il	Multiple signatures from 66.76.174.2	Block	1
109.64.147.249	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$14 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
40.77.167.29	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
197.38.197.170	Egypt	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
89.163.251.200	Germany	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /phpmyadmin/scripts/setup.php	Block	1
84.108.244.47	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method POST for www.eitan.aka.idf.il/1105-he/contactus.aspx	None	1
173.66.40.163	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method Â,[[#0]][[#0]][[#0]][[#22]]Â¡	Block	1
79.177.11.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$117 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
141.0.15.29	Europe	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/schar	Block	1
95.86.106.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewi_4n2ktv_kahwesbqkheewdl4qfggimaa&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	1
213.57.103.184	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
86.165.130.56	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
164.138.122.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/&sa=u&ved=0ahukewji0tq3t__kahwjhjokhvnwbokqfgghmaa&sig2=qadcomnssqjahxwucpigfa&usg=afqjcneeywysowwcocycbntx0qxav9lbkw	Block	1
81.7.137.98	Denmark	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
66.249.64.70	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.67.17.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$67 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
207.46.13.32	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
89.163.251.200	Germany	147.237.77.74	law.idf.il	Unauthorized URL Access to /phpmyadmin/scripts/setup.php	Block	1
173.66.40.163	United States	147.237.76.86	navy.idf.il	Malformed URL	Block	1
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	1
79.177.208.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$55 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
104.128.144.131	Canada	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
46.19.86.143	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
213.57.145.103	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
197.36.250.183	Egypt	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.64.139	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.253.145.195	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1

02-17-2016-20:04:02 to 02-17-2016-21:04:02