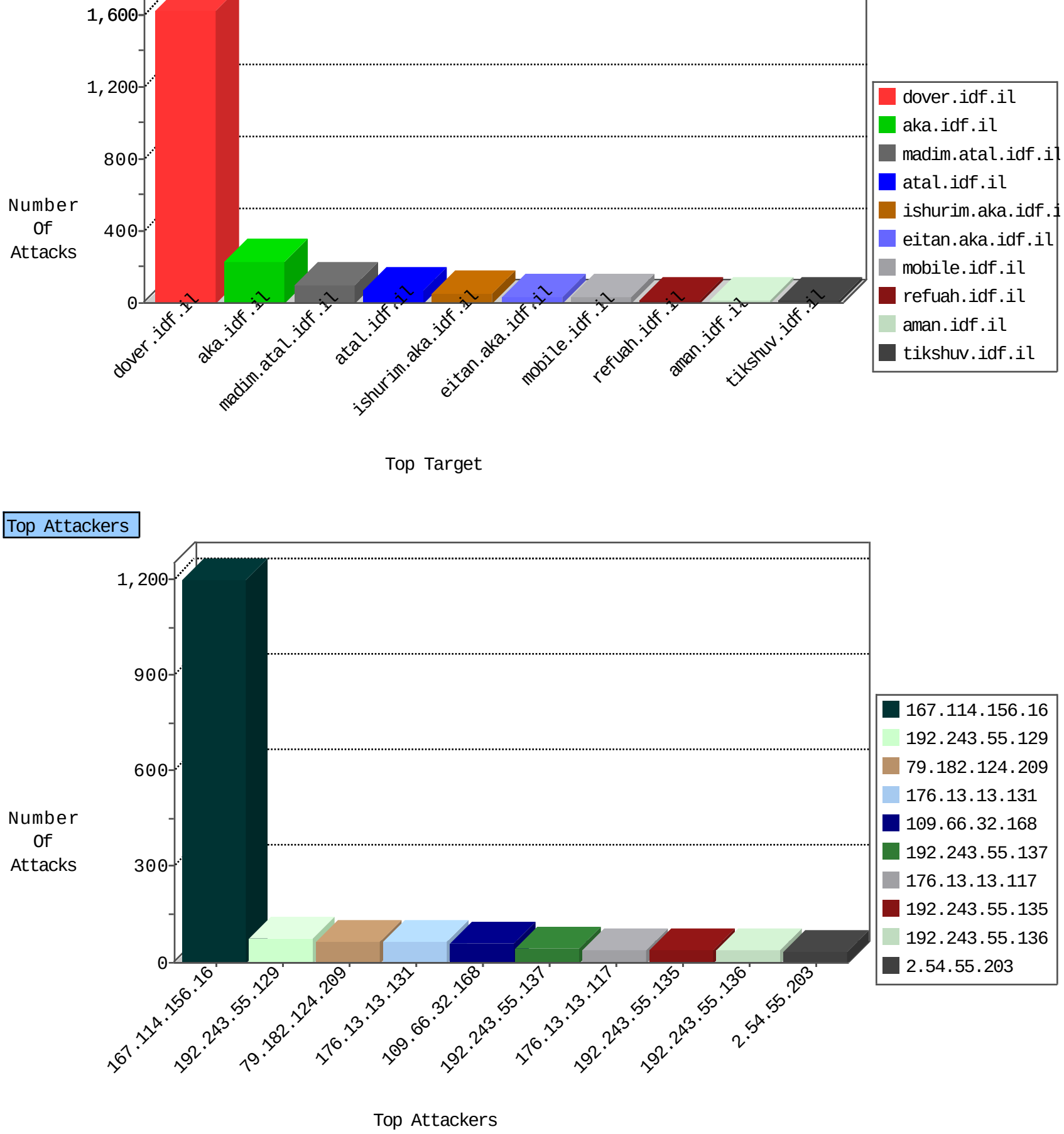
03-12-2016-13:04:05 to 03-12-2016-14:04:05

IDF Under Attack Daily Report



03-12-2016-13:04:05 to 03-12-2016-14:04:05

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	DOS-Tool-SwitchbladG	dest-reset	3603
82.145.220.147	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
134.147.203.115	Germany	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
80.82.64.220	Netherlands	147.237.72.156	aman.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
177.80.105.92	Brazil	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.33	Switzerland	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.33	Switzerland	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
188.138.17.205	France	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
145.14.1.3	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.33	Switzerland	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
179.43.144.33	Switzerland	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1

03-12-2016-13:04:05 to 03-12-2016-14:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.127.55	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
159.203.4.142	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1

03-12-2016-13:04:05 to 03-12-2016-14:04:05

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
93.113.125.12	147.237.72.167	Romania	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
40.74.124.12	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
218.246.0.97	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
203.197.205.118	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.77.216	Sweden	dover.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.12	147.237.77.226	Romania	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.222.126.18	147.237.72.156	Taiwan	aman.idf.il	ET SCAN NMAP -sS window 1024	1
203.197.205.118	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
193.105.134.220	147.237.0.35	Sweden	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.12	147.237.77.227	Romania	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

03-12-2016-13:04:05 to 03-12-2016-14:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.13.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
79.182.124.209	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	58
176.13.13.117	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
172.56.40.120	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	29
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	24
2.54.18.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
141.0.15.232	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
79.180.68.191	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
84.228.24.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
188.32.227.41	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
2.54.55.203	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
89.178.134.31	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.42.167.236	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
79.182.124.209	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
79.177.99.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.64.123.234	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.65.94.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.55.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.31.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.132.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.55.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.54.55.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
129.45.120.65		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.55.203	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.179.102.94	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.55.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.68.58.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

03-12-2016-13:04:05 to 03-12-2016-14:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.32.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
176.13.14.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.191.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.179.102.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.250.204.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.230.93.33	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
188.161.64.169	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.148.238	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Malformed URL a"˛[[ט#6]]	Block	1
140.115.111.116	Taiwan	147.237.72.166	aka.idf.il	Unknown Parameter request in www.aka.idf.il/brothers/kishur/default.asp	None	1
87.71.9.228	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
197.32.157.14	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	Malformed URL +ף)ד•<‘’sp¯œŽ˜$ž˙6[[#4ם]]9˛ף4fv1]]4#[[רק	Block	1
66.249.64.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/106627.pdf	Block	1
2.54.160.107	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Header Name	Block	1
94.230.93.36	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.181.54.68	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.120.25.125	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Unknown HTTP Request Method ‡ók[[#19]]x[[#12]]”ìç×&[[#14]][[#15]][[#28]][[#30]]n[[#22]] in URL a"˛[[ט#6]]	Block	1
140.115.111.116	Taiwan	147.237.72.166	aka.idf.il	Unknown Parameter request in www.aka.idf.il/faq.asp	None	1
197.32.157.14	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
87.71.9.228	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	Unknown HTTP Request Method /JS[[#2]]Ðµ¬ý”¦[[#4]]^†E~ÕûÉ)[[#20]]›ùØ in URL +ף)ד•<‘’spר þ4r[[#4]]1vfף9˛ם]]#4[[$ž˙6¯œž	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20027-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Method ‡ók[[#19]]x[[#12]]”ìç×&[[#14]][[#15]][[#28]][[#30]]n[[#22]]	Block	1
94.230.93.100	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.182.124.209	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	Abnormally Long Request method	Block	1
61.244.30.166	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
140.115.111.116	Taiwan	147.237.72.166	aka.idf.il	Unknown Parameter service in www.aka.idf.il/brothers/skira/default.asp	None	1
197.135.127.172	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
94.230.93.1	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in URL a"˛[[ט#6]]	Block	1
194.135.154.201	Azerbaijan	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	Illegal Byte Code Character in Method /JS[[#2]]Ðµ¬ý”¦[[#4]]^†E~ÕûÉ)[[#20]]›ùØ	Block	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/112406.pdf	Block	1
141.212.122.160	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
94.230.93.20	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
184.105.247.196	United States	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19/	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3049.jpg	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal HTTP Version Ô@>–,?ã\Ó,	Block	1
140.115.111.116	Taiwan	147.237.72.166	aka.idf.il	Unknown Parameter request in www.aka.idf.il/brothers/contact/	None	1
194.135.154.201	Azerbaijan	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-12-2016-13:04:05 to 03-12-2016-14:04:05