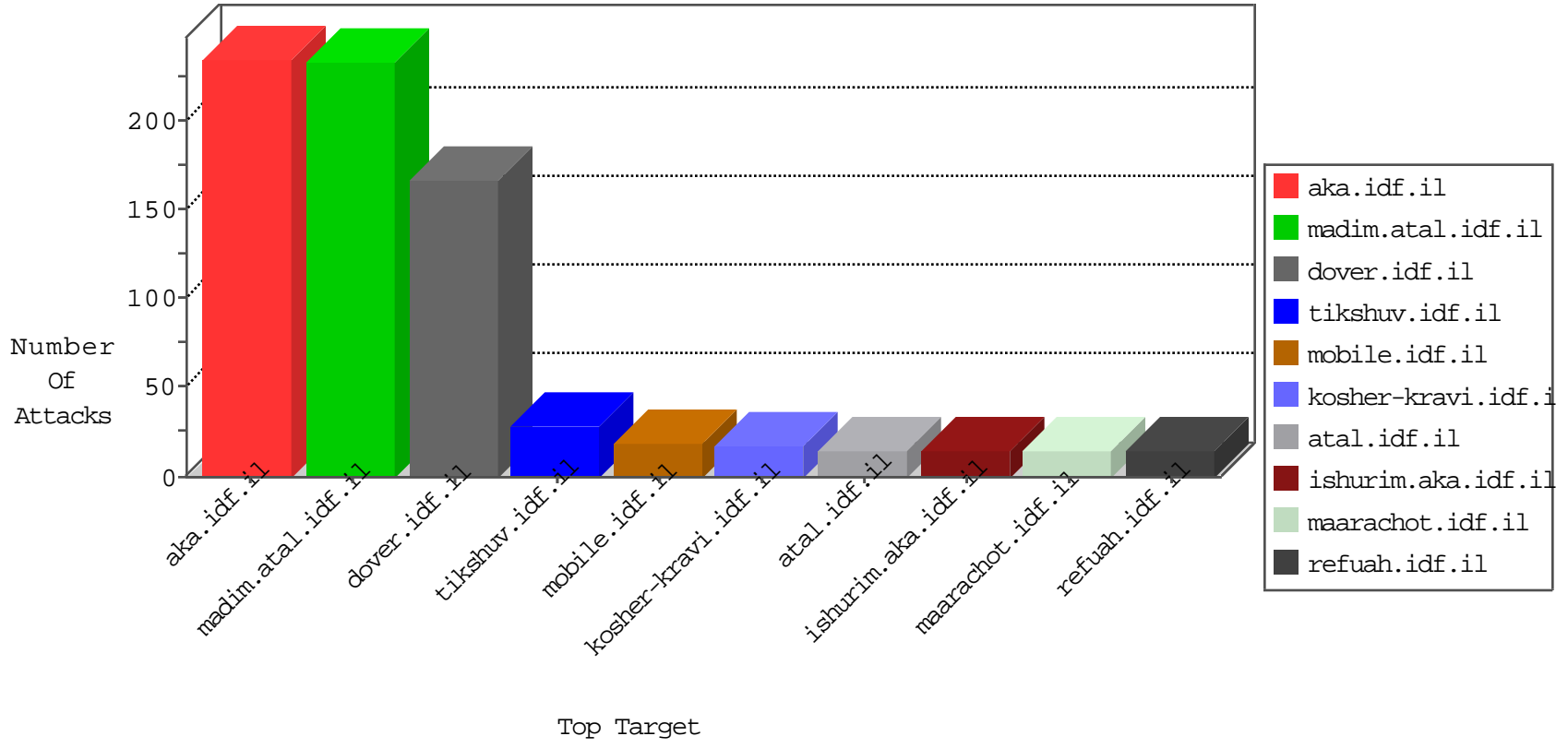


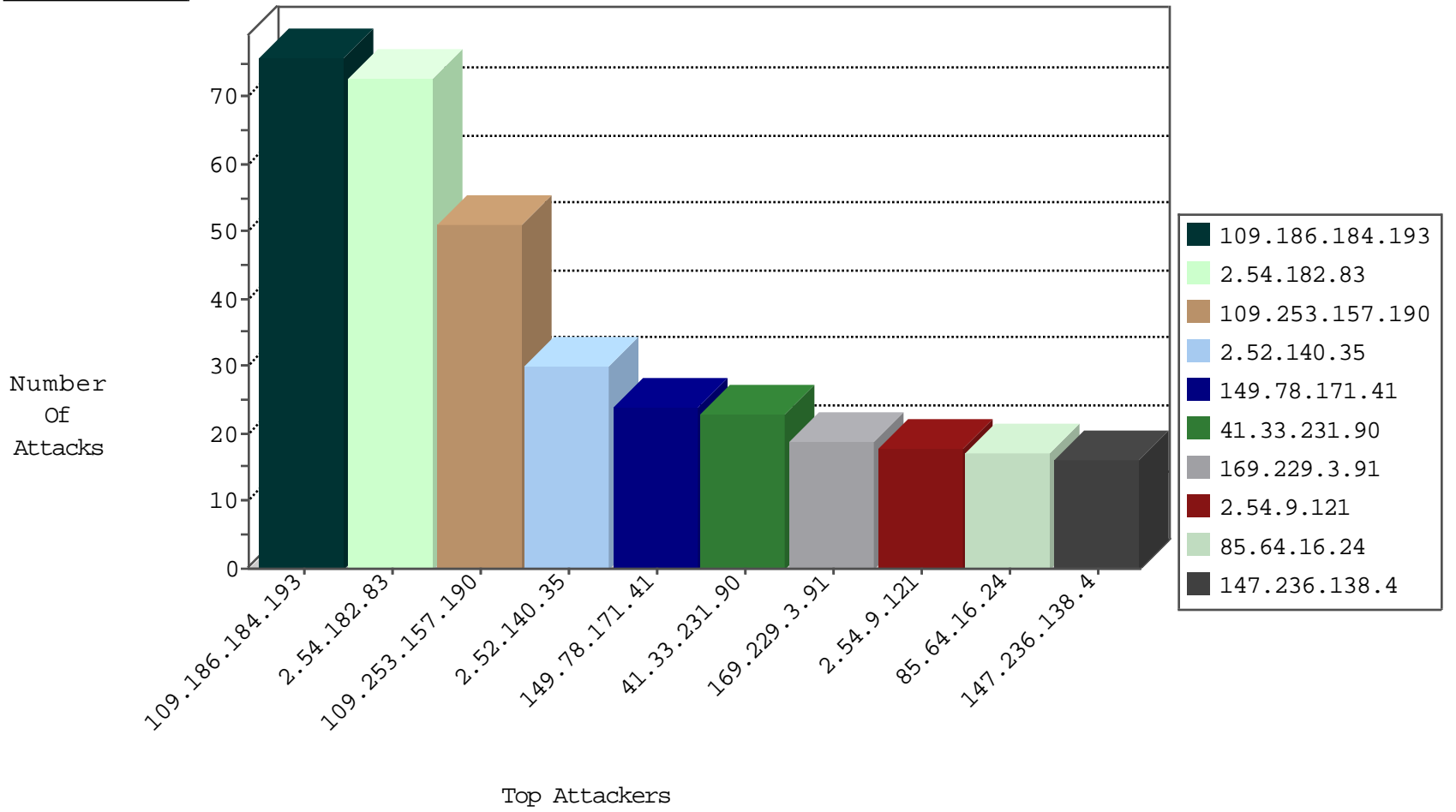
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.219.172	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
213.57.88.74	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
219.138.216.130	China	147.237.77.178	e.matpash.idf.il	Invalid TCP Flags	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
115.239.228.10	China	147.237.76.198	e.yohanan.idf.il	JIM_Purple_Con_Limit_Http	drop	1
115.239.228.10	China	147.237.76.201	e.atal.idf.il	JIM_Purple_Con_Limit_Http	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.8.46	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
136.243.5.215	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
51.254.131.242	United Kingdom	147.237.77.216	dover.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	147.237.77.176	matpash.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

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.205.155.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.105.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.174.14.195	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.236	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.32.84.108	147.237.76.177		ncore.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.236.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.177.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.253.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.16.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
69.64.46.86	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.105.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.32.84.108	147.237.76.176		test.ncore.idf.il	ET SCAN Potential SSH Scan	1
37.26.146.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.140.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
109.253.216.158	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
149.78.171.41	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
37.26.146.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
81.218.11.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.236.138.4	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.123	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
197.134.255.147	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.198.33	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.140.109	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.121.89.247	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
176.13.0.211	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.80	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
188.120.148.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
31.154.25.42	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
2.54.9.121	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.9.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
189.219.197.194	Mexico	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
2.54.9.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
147.236.138.4	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
2.54.9.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
82.80.198.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.253.134.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.181.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.0.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
147.236.138.4	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.180.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.196.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.187.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.30.201	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	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
212.179.45.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.77.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.221.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.216.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.181.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.186.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-23-2016-14:04:00 to 02-23-2016-15:04:00

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.209.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.67.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.186.184.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
2.54.182.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
109.253.157.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
149.78.171.41	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 149.78.171.41	Block	14
85.64.16.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.16.24	Block	11
131.253.25.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
212.143.133.107	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
85.64.16.24	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
82.81.45.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
31.168.205.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.253.133.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.118.155.216	Ukraine	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
2.54.63.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.152.103	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
109.160.178.203	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.160.178.203	Block	3
2.54.5.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.178.98.149	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.178.98.151	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.160.178.203	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
192.115.130.253	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/112907.pdf	Block	2
88.246.29.30	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
2.54.204.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
87.68.248.116	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
37.26.146.187	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.13.4.189	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Header Name [[#1]]ü•°[[#31]]s[[#25]]€S~	Block	1
49.148.170.189	Philippines	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
5.255.253.75	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Method e•+î•°aF[[#14]]lñóšo[[#8]]lè+AL[[#17]]kD°-o:výklö	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
46.118.155.216	Ukraine	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
212.179.133.50	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
109.253.216.158	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
176.13.8.60	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.175.193	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	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Method %a{[[#30]][[#23]],ã	Block	1
149.88.108.130	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
62.219.47.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
46.19.86.243	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in URL	Block	1
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1