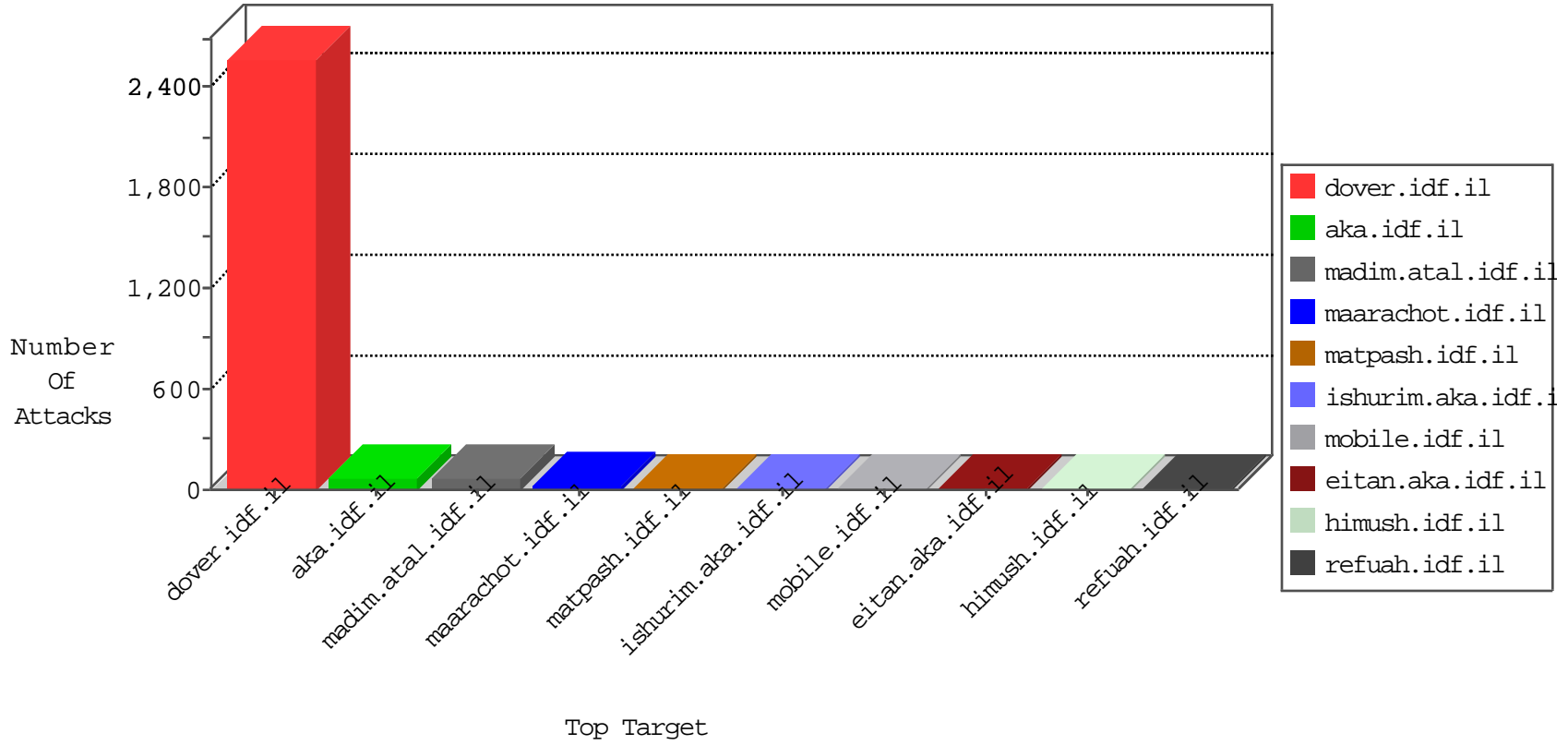


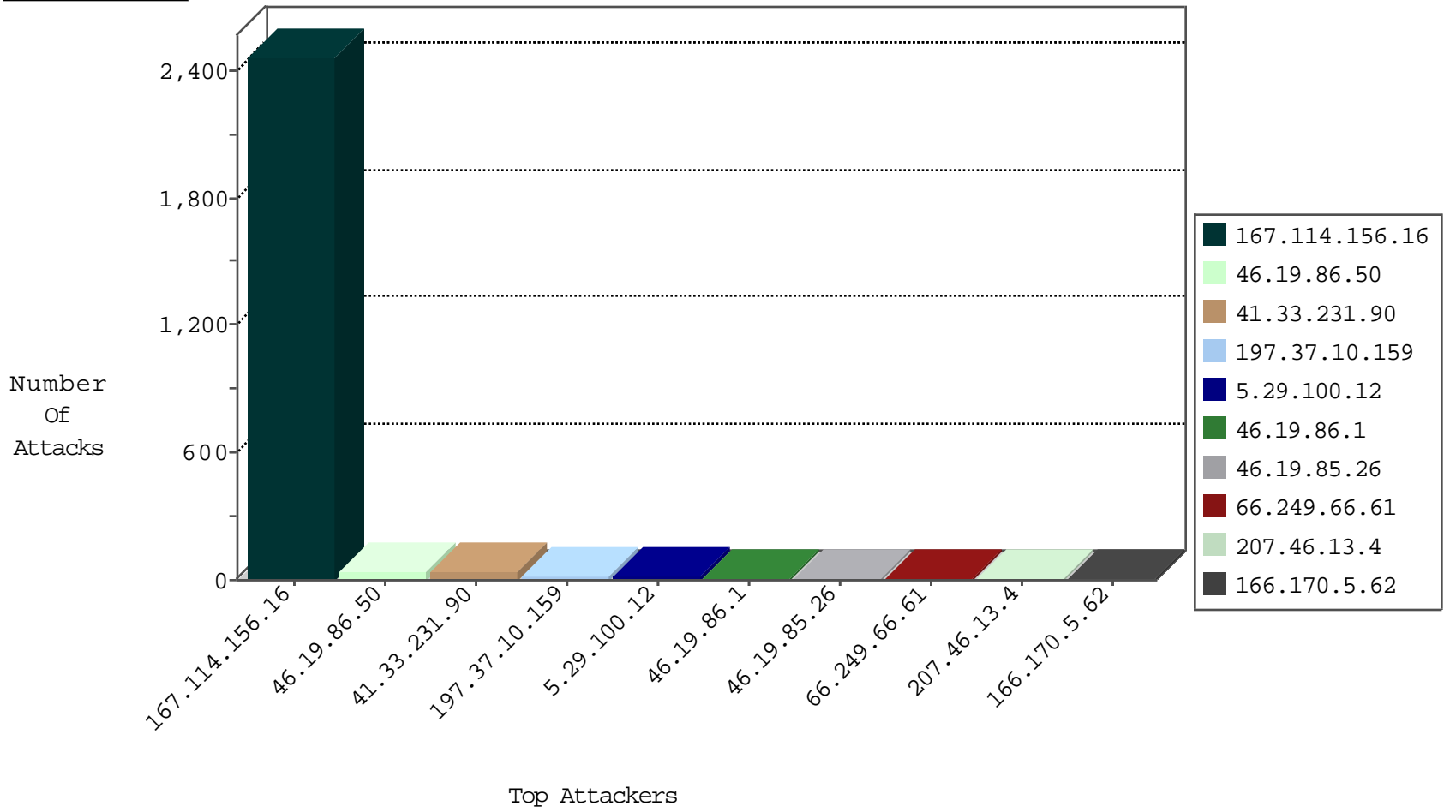
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3338
66.249.66.111	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	488
74.143.58.3	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.210	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
103.224.22.13	Hong Kong	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
93.174.93.151	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.210	Netherlands	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.121.169.194	France	147.237.76.86	navy.idf.il	C1000106: HTTP: majestic bot	Block	1
151.80.31.129	Italy	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.154.188.224	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
171.232.56.152	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN Potential SSH Scan	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
61.240.144.66	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
51.254.46.129	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.174.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.46	147.237.77.235		sviva.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.148	Netherlands	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.174.70.237	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 4096	1
51.254.46.129	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	1
24.121.225.29	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.46	147.237.77.227		e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
151.25.203.142	147.237.76.31	Italy	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.174.70.237	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.4	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
166.170.5.62	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.130	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	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.18.56	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.12.84	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.1	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.29.100.12	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		monitor	4
79.182.127.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.255.253.120	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.250.155.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.250.155.109	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
77.126.24.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
5.29.100.12	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.29.100.12	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.111.137.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.175.183.170	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.29.100.12	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
212.235.98.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.26	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.29.100.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
109.66.141.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
207.46.13.158	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.29.100.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.64.125.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.97.106.162	China	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.52.151.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.36	China	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.95	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.117.126.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.88.141.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.149.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
109.64.221.89	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.227	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.161	China	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
216.218.206.123	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.125.239.232	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
213.175.183.170	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
197.37.10.159	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	10
197.37.10.159	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	10
46.19.85.26	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	6
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
77.127.64.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.28.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8921-he/refuah.aspx	Block	1
213.25.22.226	Poland	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
167.114.242.197	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
85.65.71.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
207.46.13.4	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.4	Block	1
157.55.39.46	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
213.25.22.226	Poland	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 213.25.22.226	None	1
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/idf_in_pictures/2002/april/	Block	1
5.22.131.121	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1065-he/kkkkkkkk=9267336dkkkkkkkk_9267336d	Block	1
93.87.106.135		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/19-25.09.10.aspx	Block	1
207.46.13.103	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/h	Block	1
157.55.39.76	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/image_captcha/72212181/1448699690	Block	1
79.180.69.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
213.25.22.226	Poland	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	1
188.116.33.163	Poland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
93.87.106.135		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.67.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.86.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.196	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
82.166.237.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17154-he/dover.aspx	Block	1
216.218.206.67	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
41.108.17.220	Algeria	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
93.157.99.148	Poland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71538-he/maarachot.aspx	Block	1
167.114.242.197	Canada	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
84.111.137.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.36.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
41.108.17.220	Algeria	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
149.88.141.40	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1