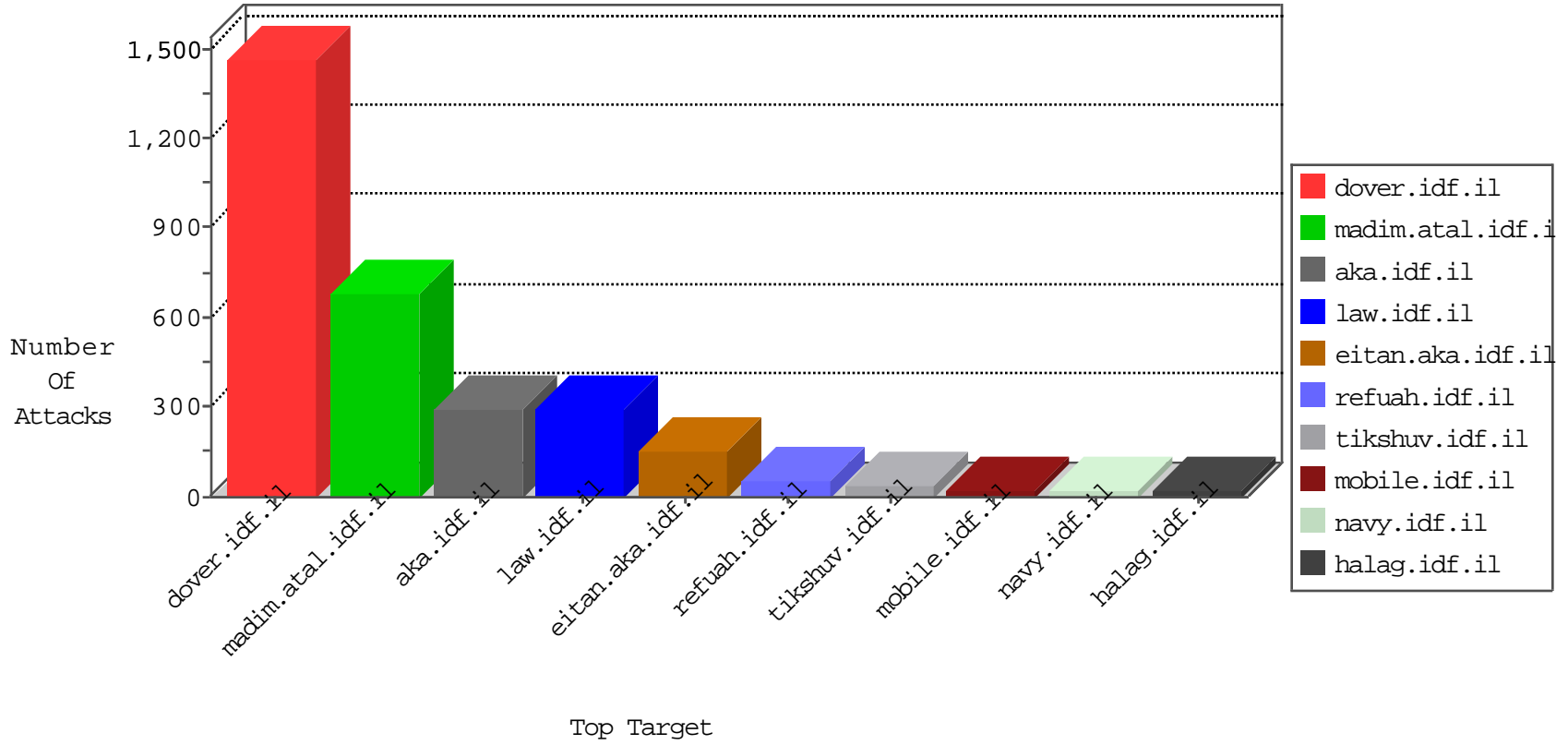


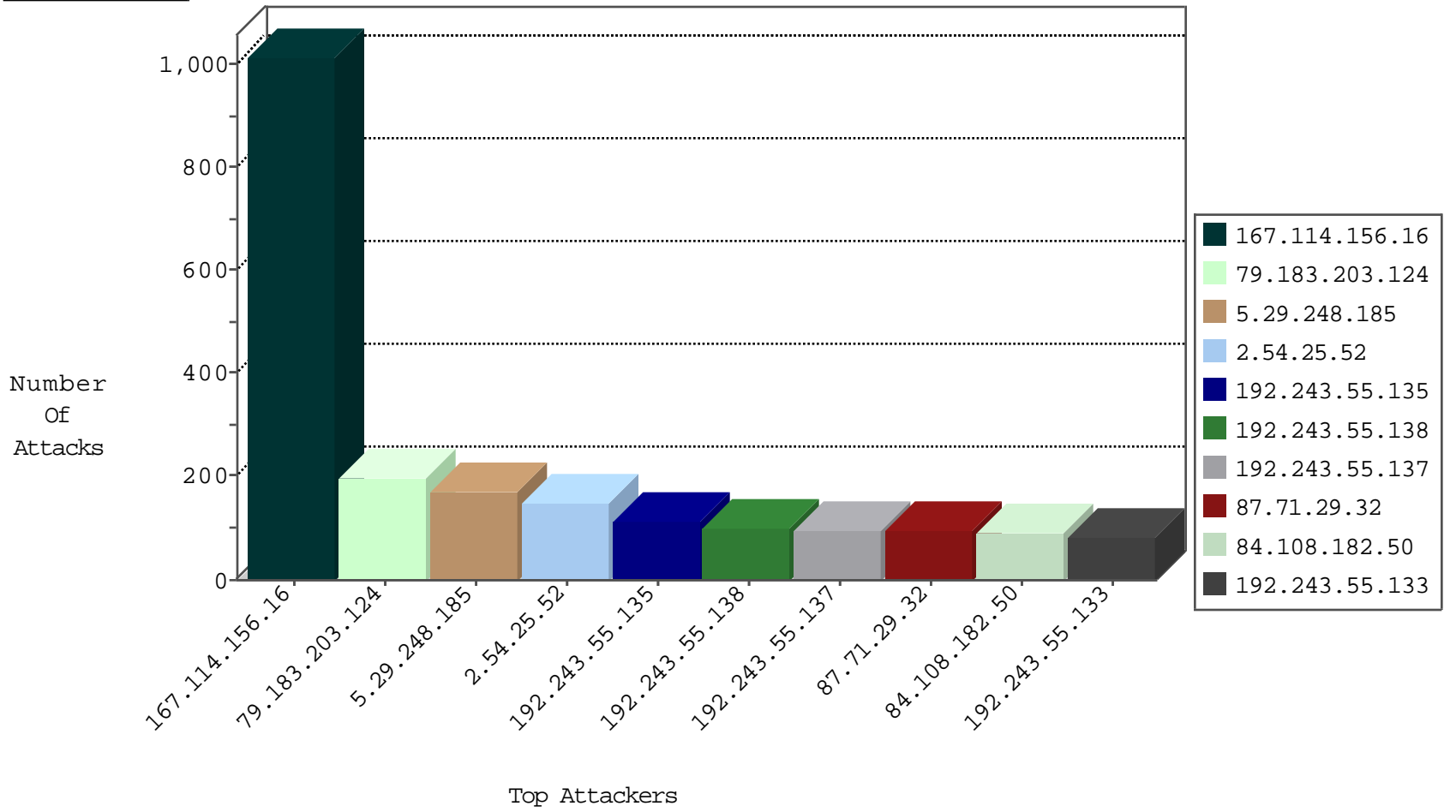
IDF Under Attack Daily Report



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	3986
146.185.239.100	Russian Federation	147.237.76.86	navy.idf.il	block-sp-traf1	forward	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	2
58.97.74.88	Thailand	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.206	Netherlands	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
120.26.199.234	China	147.237.0.34	tikshuv.idf.il	I4 Source or Dest Port Zero	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.112.25	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
109.67.113.176	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
207.232.46.209	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.54.143.211	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.79.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
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

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
173.224.117.146	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
1.52.59.143	147.237.76.31	Vietnam	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
173.224.117.146	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
173.224.117.146	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
173.224.117.146	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
147.175.16.71	147.237.76.197	Slovakia	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
135.0.34.34	147.237.0.19	Canada	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.76.39	Austria	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.126.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.224.117.146	147.237.77.234	United States	halag.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.253	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
173.224.117.146	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
1.52.59.143	147.237.76.31	Vietnam	nakchal.idf.il	ET SCAN NMAP -f -sS	1
173.224.117.146	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
173.224.117.146	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
173.224.117.146	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
147.175.16.71	147.237.76.197	Slovakia	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.77.19	Austria	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.8.27	Austria	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
173.224.117.146	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential SSH Scan	1
80.246.133.14	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.25.52	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	150
149.50.0.191	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
185.120.126.12		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.121.156.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
109.67.119.172	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
192.243.55.135	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
87.68.251.126	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
192.243.55.135	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.134	Dominica	147.237.77.74	law.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	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.133	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
5.29.248.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.138	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
93.173.32.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.136	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.131	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	drop	First packet isn't SYN	drop	8
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	8
192.243.55.129	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.203.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	196
5.29.248.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	157
87.71.29.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	95
84.108.182.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
46.19.85.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
176.13.19.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
79.180.71.39	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.180.71.39	Block	22
91.200.12.7	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	12
91.200.12.7	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.200.12.7	Block	11
79.183.229.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
5.29.248.185	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.180.71.39	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	2
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19142-en/dover	Block	1
45.55.141.217		147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
91.200.12.7	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
66.249.64.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/8/109008.pdf	Block	1
85.64.52.157	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/spanish/	Block	1
66.249.74.106	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.74.106	Block	1
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/327-he/patzar.aspx?pagenum=2	Block	1
45.55.145.69		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
104.131.167.195	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
31.154.163.39	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/mmmmmmmmm=1d9c348emmmmmmmmm_1d9c348e	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation pageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
109.67.119.172	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.253	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.26.146.255	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
185.32.179.49	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
70.39.184.154	Satellite Provider	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/112786.pdf	Block	1
5.29.248.185	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ***** *****, Observed ***** *****	None	1
149.50.0.191	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
84.108.44.15	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 84.108.44.15	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/twitter.com/idfonline	Block	1
37.142.68.49	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
66.249.64.53	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/107527.pdf	Block	1
157.55.39.65	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.74.104	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.74.104	Block	1