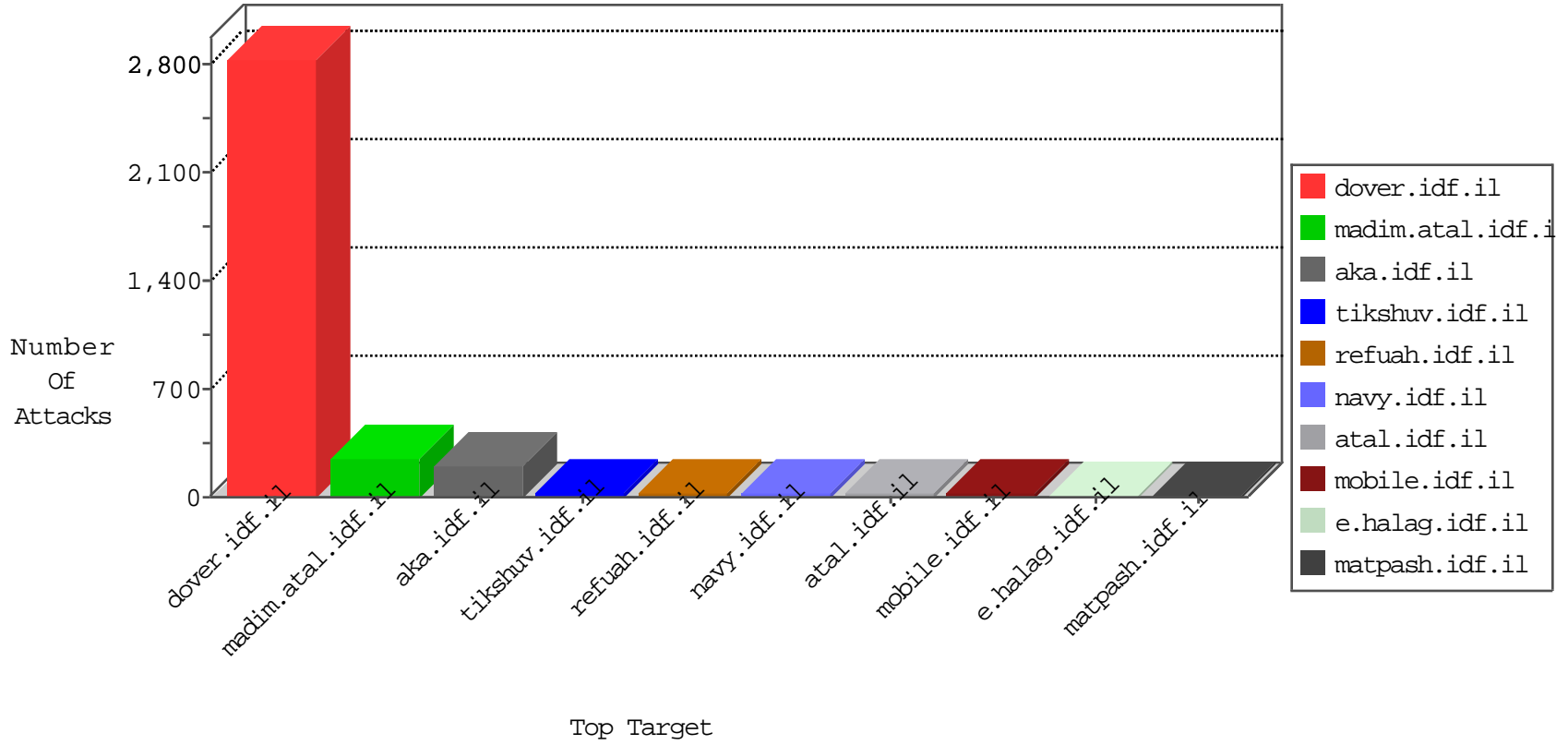


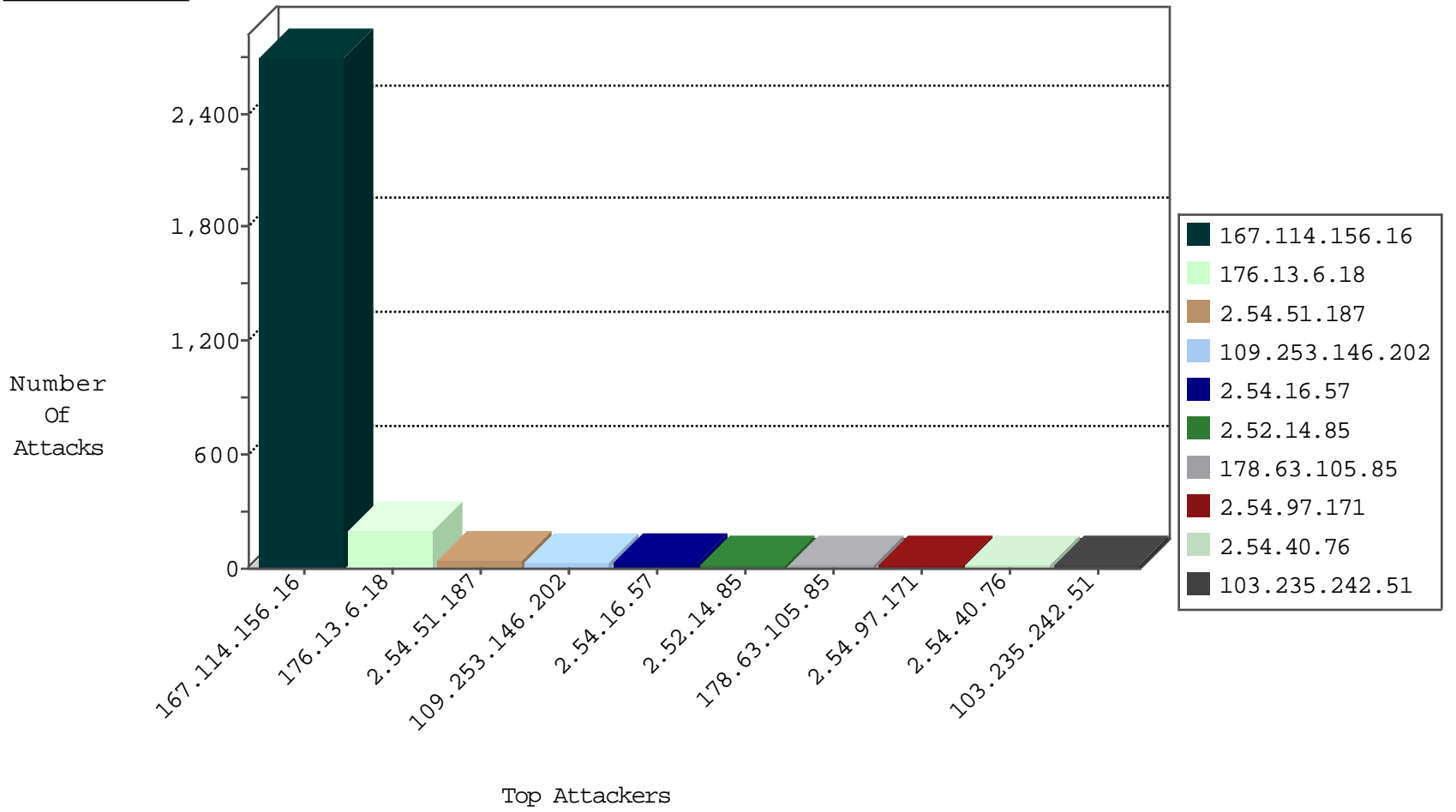
IDF Under Attack Daily Report



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	3438
31.168.218.41	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
103.235.242.51	China	147.237.0.33	idf.il	L4 Source or Dest Port Zero	drop	3
81.218.56.245	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
103.235.242.51	China	147.237.8.45	e.eitan.idf.il	L4 Source or Dest Port Zero	drop	3
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
103.235.242.51	China	147.237.8.50	e.tikshuv.idf.il	L4 Source or Dest Port Zero	drop	2
103.235.242.51	China	147.237.0.19	madim.atal.idf.il	L4 Source or Dest Port Zero	drop	2
103.235.242.51	China	147.237.77.235	sviva.idf.il	L4 Source or Dest Port Zero	drop	2
103.235.242.51	China	147.237.77.227	e.hamaz.idf.il	L4 Source or Dest Port Zero	drop	2
184.105.139.106	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
103.235.242.51	China	147.237.77.234	halag.idf.il	L4 Source or Dest Port Zero	drop	1
103.235.242.51	China	147.237.77.212	e.dover.idf.il	L4 Source or Dest Port Zero	drop	1
103.235.242.51	China	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.40.76	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
80.246.133.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
82.81.101.177	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
82.81.101.178	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.64.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	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	2
217.21.4.68	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
93.189.26.18	147.237.72.217	Austria	e.idf.il	ET SCAN NMAP -sS window 1024	1
37.46.38.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
42.112.16.126	147.237.76.42	Vietnam	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	78
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
2.54.51.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	16
79.176.172.83	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
2.54.97.171	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	12
2.54.16.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.54.97.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.102.9.3	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
37.26.148.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.14.85	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.4.85	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.147.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.16.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.	drop	SAM rule	drop	6
2.54.16.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.114.2.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.16.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.108.79.212	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
2.54.51.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.51.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.52.14.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.14.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.54.51.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.51.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.14.85	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
66.249.93.252	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
2.52.14.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.148.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
62.0.206.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.	drop	SAM rule	drop	4
66.249.93.252	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
87.70.89.129	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.182.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.2.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.201.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.122.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.4.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.0.73.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.30.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.185.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.184.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.22.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.16.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.238.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.185	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.6.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	195
109.253.146.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.19.86.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	5
118.193.137.94	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 118.193.137.94	Block	3
46.19.86.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.130.133	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.210.205.184	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.246.130.139	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.199.108.138	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	2
46.117.110.21	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
173.254.236.52	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	2
101.222.162.0	India	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
46.19.86.46	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.108.4.69	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.83.155	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.121.66.197	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
17.142.156.171	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1
80.246.130.133	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
157.55.39.70	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/giyus/ganda/default.asp	None	1
2.54.6.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/giyus.aspx	Block	1
87.69.158.111	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.83.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.22.193	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/topcap.gif	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
173.254.236.52	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 173.254.236.52	Block	1
2.54.18.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam	Block	1
87.69.158.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
79.176.172.83	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1274-he/atal.aspx	Block	1
60.249.218.109	Taiwan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
118.193.137.94	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.26.146.255	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.194.206.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/3468.gif	Block	1
2.54.49.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
190.148.39.136	Guatemala	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.85.7	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakchal.idf.il/1072-he/nakchal.aspx	Block	1
66.249.75.24	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.75.24	Block	1
46.117.160.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy.	Block	1
173.254.236.52	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/wp-login.php	Block	1
2.54.170.165	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1