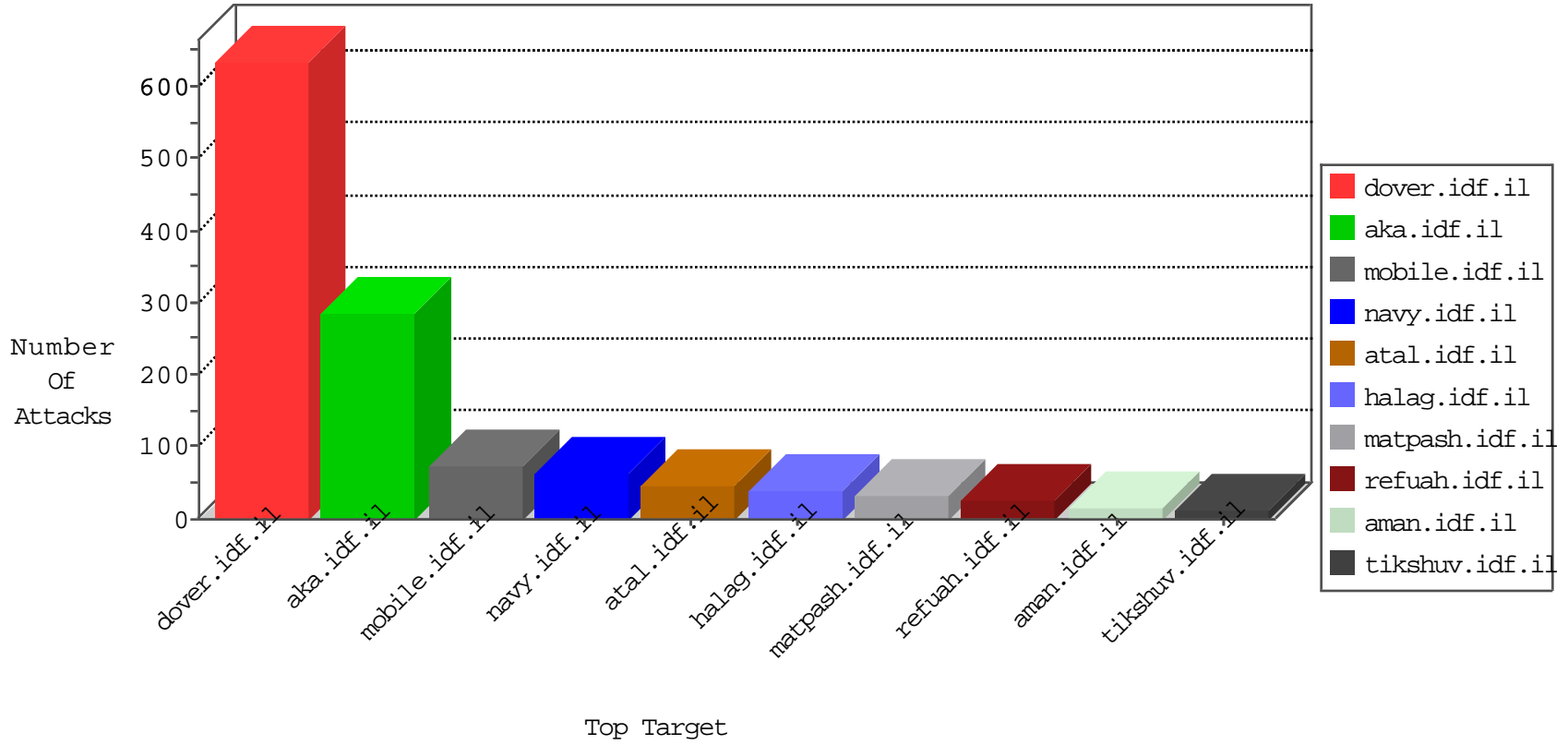


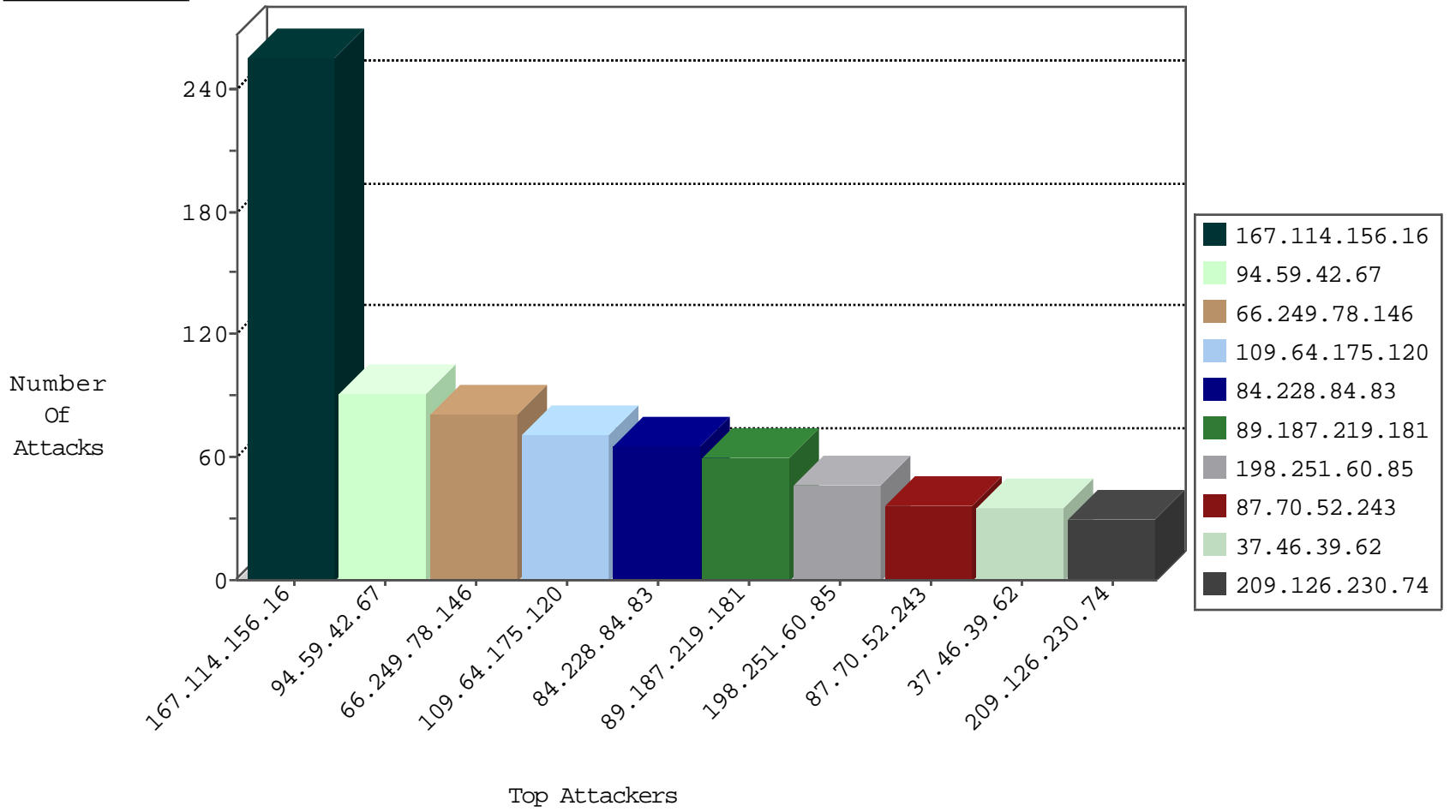
IDF Under Attack Daily Report



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	HTTP-POST-Segmented-DoS	dest-reset	9371
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1324
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
104.153.173.100	United States	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	2

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
209.15.196.171	Canada	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
93.90.147.81	Sweden	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
93.190.69.10	Germany	147.237.76.147	chinuch.aka.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
93.190.69.10	Germany	147.237.72.166	aka.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.90.147.81	147.237.72.166	Sweden	aka.idf.il	SQL Injection - Select From	6
209.15.196.171	147.237.72.166	Canada	aka.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
189.68.88.189	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Potential SSH Scan	2
189.68.88.189	147.237.0.15	Brazil	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
60.249.179.44	147.237.76.176	Taiwan	test.ncoore.idf.il	ET SCAN NMAP -sS window 4096	1
192.127.94.7	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
189.68.88.189	147.237.0.33	Brazil	idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.140.23	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
86.57.1.140	147.237.0.34	Iran, Islamic Republic of	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
60.249.179.44	147.237.76.176	Taiwan	test.ncoore.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.74	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
189.218.18.202	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
189.68.88.189	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
89.187.219.181	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
94.59.42.67	United Arab Emirates	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
198.251.60.85	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
84.228.84.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
109.64.175.120	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
109.64.175.120	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
46.19.85.166	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
37.46.39.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
84.228.84.83	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	23
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
176.13.2.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
149.78.72.170	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
45.55.59.6	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
24.115.108.7	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
94.59.42.67	United Arab Emirates	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	9
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
197.157.19.34	Uganda	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
94.59.42.67	United Arab Emirates	147.237.76.198	e.yochalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.220.5	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.59.42.67	United Arab Emirates	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
66.249.93.247	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.1.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.39.180.210	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
82.205.45.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.146.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.168.161.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
121.42.0.63	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.146.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.146.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.146.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
85.130.231.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.78.216.54	Netherlands	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
79.183.98.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.106.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
209.126.230.74	United States	147.237.77.170	maarachot.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.46.39.62	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.66.184	Block	2
46.19.85.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
149.78.72.170	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.64.175.120	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
80.246.136.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
209.126.230.74	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
46.120.113.66	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$c in www.aka.idf.il/main/sachar/	None	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
89.139.50.66	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
176.13.1.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.26.146.244	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
109.64.214.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.94.114.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
209.126.230.74	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
46.120.113.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
93.173.39.45	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
176.13.16.246	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
109.65.215.216	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.228.233.247	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-he/cogat.aspx	Block	1
209.212.22.130	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.175	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/login/newsservice.aspx/js	Block	1
149.50.31.55	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
94.59.42.67	United Arab Emirates	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.78.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/login/authentication-service.aspx/js	Block	1
192.206.203.100	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
109.67.228.230	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.228.233.247	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
2.53.43.161	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
94.59.42.67	United Arab Emirates	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/get_status.cgi	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
209.126.230.74	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
46.19.85.91	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$ucFaqControl\$txtSearch in www.nakchal.idf.il/1072-he/nakchal.aspx	Block	1
109.99.71.63	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
87.71.66.159	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
2.53.158.174	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.27	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/klali.aspx	Block	1