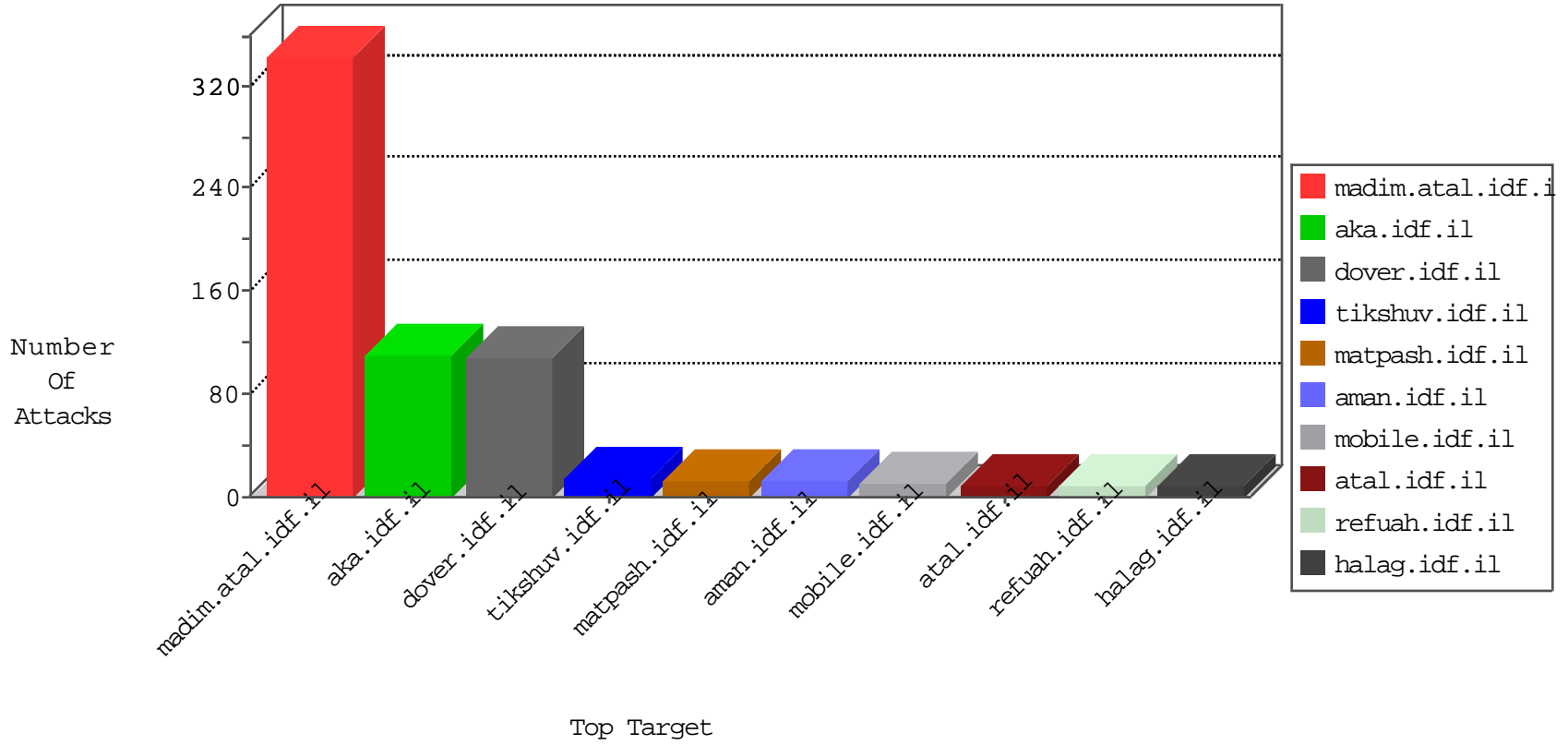


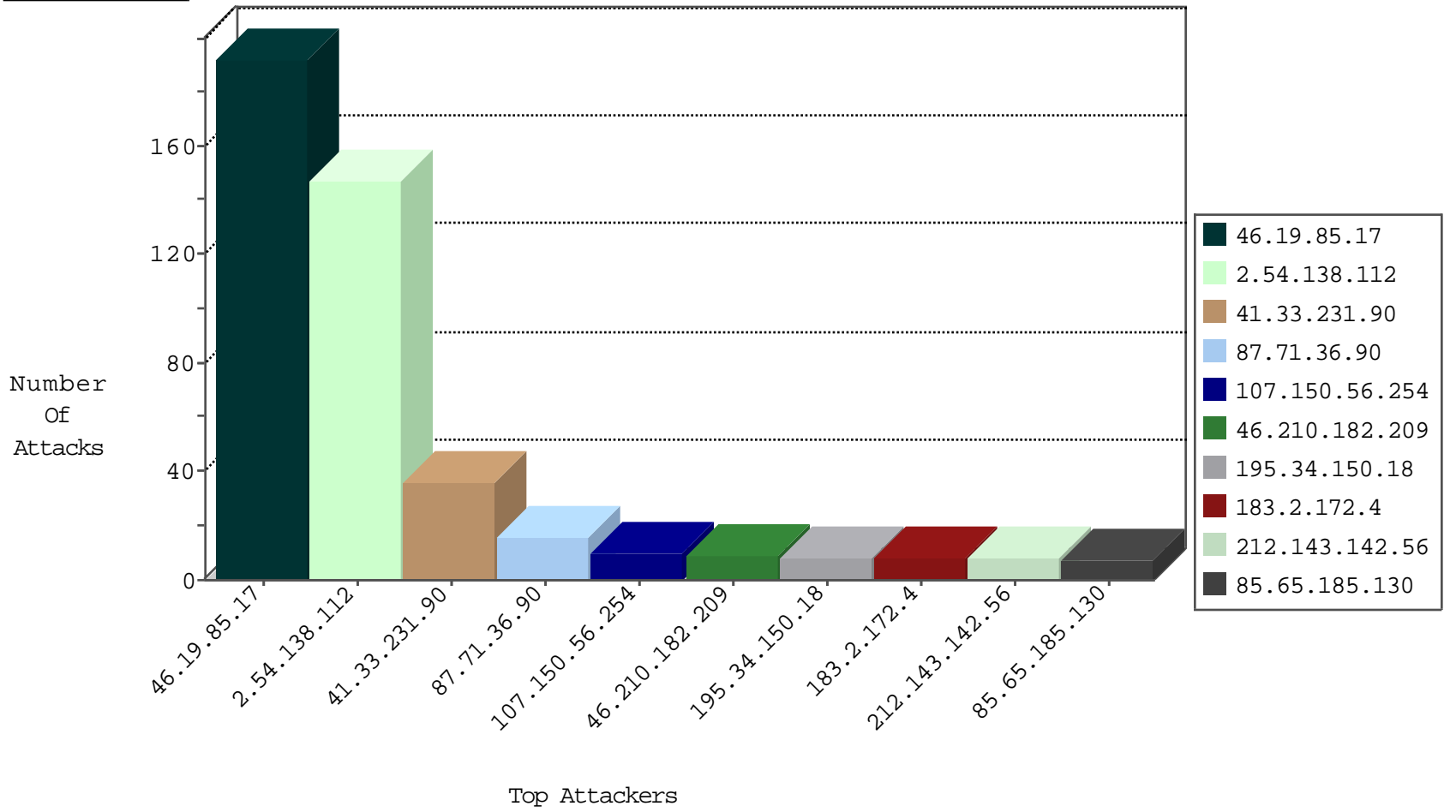
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.2.172.4	China	147.237.76.44	e.refuah.idf.il	I4 Source or Dest Port Zero	drop	2
183.2.172.4	China	147.237.76.86	navy.idf.il	I4 Source or Dest Port Zero	drop	2
183.2.172.4	China	147.237.0.34	tikshuv.idf.il	I4 Source or Dest Port Zero	drop	1
188.138.57.49	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.110	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
183.2.172.4	China	147.237.77.233	atal.idf.il	I4 Source or Dest Port Zero	drop	1
14.176.14.51	Vietnam	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.126	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.90	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
183.2.172.4	China	147.237.0.35	akaws.idf.il	I4 Source or Dest Port Zero	drop	1
188.138.57.49	Germany	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.110	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
183.2.172.4	China	147.237.77.243	mobile.idf.il	I4 Source or Dest Port Zero	drop	1
14.176.14.51	Vietnam	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.126	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.94	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.81	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.114	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.24.124.100	Turkey	147.237.76.199	e.nakchal.idf.il	I4 Source or Dest Port Zero	drop	1
184.105.139.110	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
14.176.14.51	Vietnam	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.122	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.86	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.176	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
37.26.149.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
107.150.56.254	United States	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	3
107.150.56.254	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
109.186.146.122	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
136.243.103.164	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.65.94	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
107.150.56.254	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
107.150.56.254	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.60	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.24	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.44	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.49	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.59	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	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
84.108.121.150	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
220.231.195.122	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
201.166.217.148	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.238.82.108	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.211.102.129	147.237.77.176	Russian Federation	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
201.166.217.148	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
176.13.11.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.148.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.146.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.210.182.209	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
87.71.36.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.171.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.148.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.36.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.180.199.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.30.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.167.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.233.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.3.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.207.53	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.149.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
87.71.36.90	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
5.22.134.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.54.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.36.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.139.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
188.120.154.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.53.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.140.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.36.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.181.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.210.182.209	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
85.65.185.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.3.147.8	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.29.207.53	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.142.64.104	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.3.147.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.142.64.104	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.65.185.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.176.149.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.210.182.209	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
94.230.86.229	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.65.185.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
193.90.12.88	Norway	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.138.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	147
46.19.85.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
46.19.85.17	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	85
109.253.203.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
112.215.63.12	Indonesia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.179.195.49	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.120.50.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
79.179.134.92	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
149.88.229.201	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
85.250.45.48	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
66.249.79.235	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
5.28.152.123	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct133 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.17	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
157.55.39.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.71.69.105	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.79.242	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
37.218.214.215	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
112.215.63.13	Indonesia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.203.112.188	Spain	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1927-en/cogat.aspx gaza semanales	Block	1
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.190	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/unselecatble.aspx	Block	1
93.106.221.99	Finland	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
72.52.75.27	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
40.77.167.92	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
112.215.63.19	Indonesia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.121.150	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
46.116.236.73	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
180.76.15.33	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layoutdev.css	Block	1
101.183.73.56	Australia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.16.45.96	Italy	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
113.76.90.196	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
84.108.121.150	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
2.54.163.203	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 112 cookies	Block	1