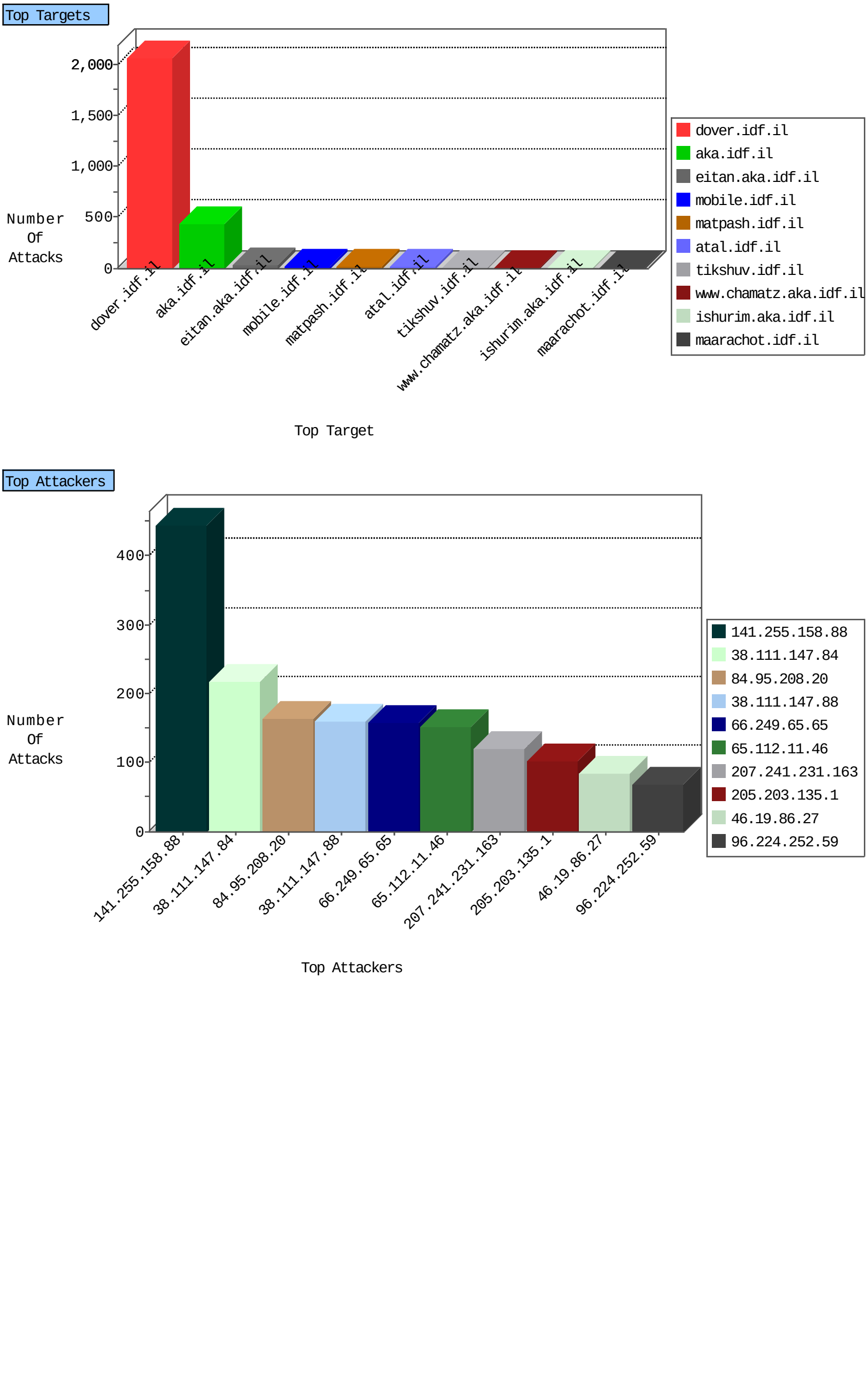
05-04-2016-02:04:07 to 05-04-2016-03:04:07

IDF Under Attack Daily Report



05-04-2016-02:04:07 to 05-04-2016-03:04:07

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	851
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	384
82.81.6.86	Israel	147.237.77.170	maarachot.idf.il	Invalid L4 Header Length	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
69.197.185.18	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
107.150.32.58	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
94.102.49.116	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
68.235.57.75	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1

05-04-2016-02:04:07 to 05-04-2016-03:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-04-2016-02:04:07 to 05-04-2016-03:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
141.255.158.88	147.237.77.216	Netherlands	dover.idf.il	Tehila - Perl LWP with fake user agent	151
141.255.158.88	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP login.htm access	12
141.255.158.88	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP admin.php access	10
141.255.158.88	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP adminlogin access	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
141.212.122.46	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential SSH Scan	1
218.6.125.237	147.237.0.19	China	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.73.224	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
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
173.193.130.54	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
115.47.12.162	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.77.74	United States	law.idf.il	ET DROP Dshield Block Listed Source	1

05-04-2016-02:04:07 to 05-04-2016-03:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
38.111.147.84	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	217
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	161
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	159
65.112.11.46	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	152
207.241.231.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	120
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
46.19.86.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
96.224.252.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
75.104.198.144	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
77.126.215.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
188.161.33.7	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
79.178.232.234	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.116.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.118.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
196.151.127.195	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.146.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.0.101.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
130.157.121.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.65.0.204	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
78.164.126.12	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
74.126.230.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.129.27.39	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.21.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
98.255.167.198	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.255.158.88	Netherlands	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.255.158.88	Block	97
141.255.158.88	Netherlands	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	93
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	72
141.255.158.88	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	71
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
149.202.239.135	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	6
131.253.25.159	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
173.192.138.226	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 173.192.138.226	Block	5
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
131.253.25.178	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
131.253.25.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
46.116.42.42	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
77.125.74.164	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
199.30.25.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.73.179	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
66.249.79.107	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1362-15365-he/dover.aspx	Block	1
54.210.18.124	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Distributed PHP Attempt	Block	1
66.249.73.224	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.79.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1379-11674-he/dover.aspx	Block	1
149.202.239.135	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
54.210.18.124	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
107.150.32.58	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.defences1.com/	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2690.jpg	Block	1
17.142.156.171	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	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
66.249.65.18	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2389.jpg	Block	1
31.168.67.217	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
69.197.185.18	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.defences1.com/	Block	1
173.192.138.226	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.73.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteyerua/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
141.255.158.88	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin/	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar/dover.aspx/	Block	1