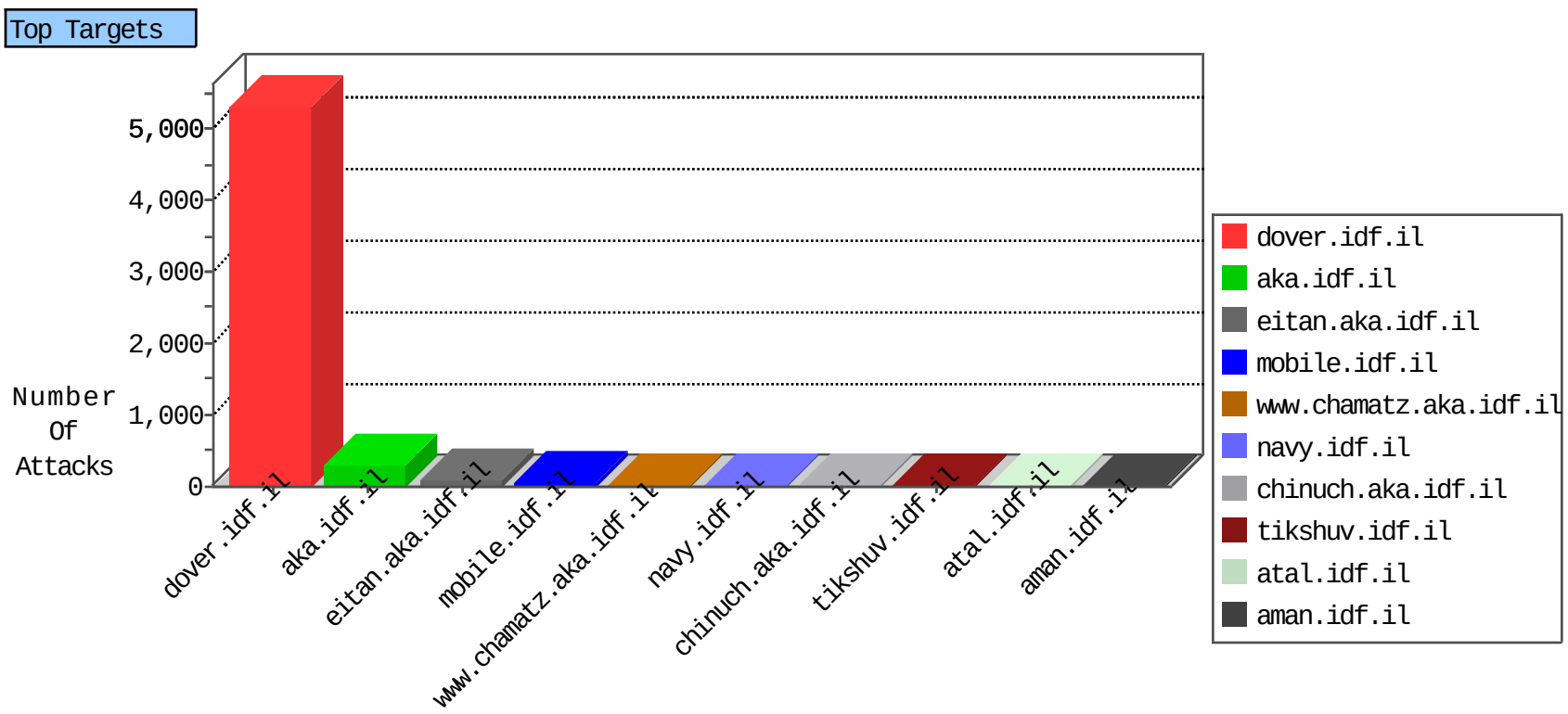
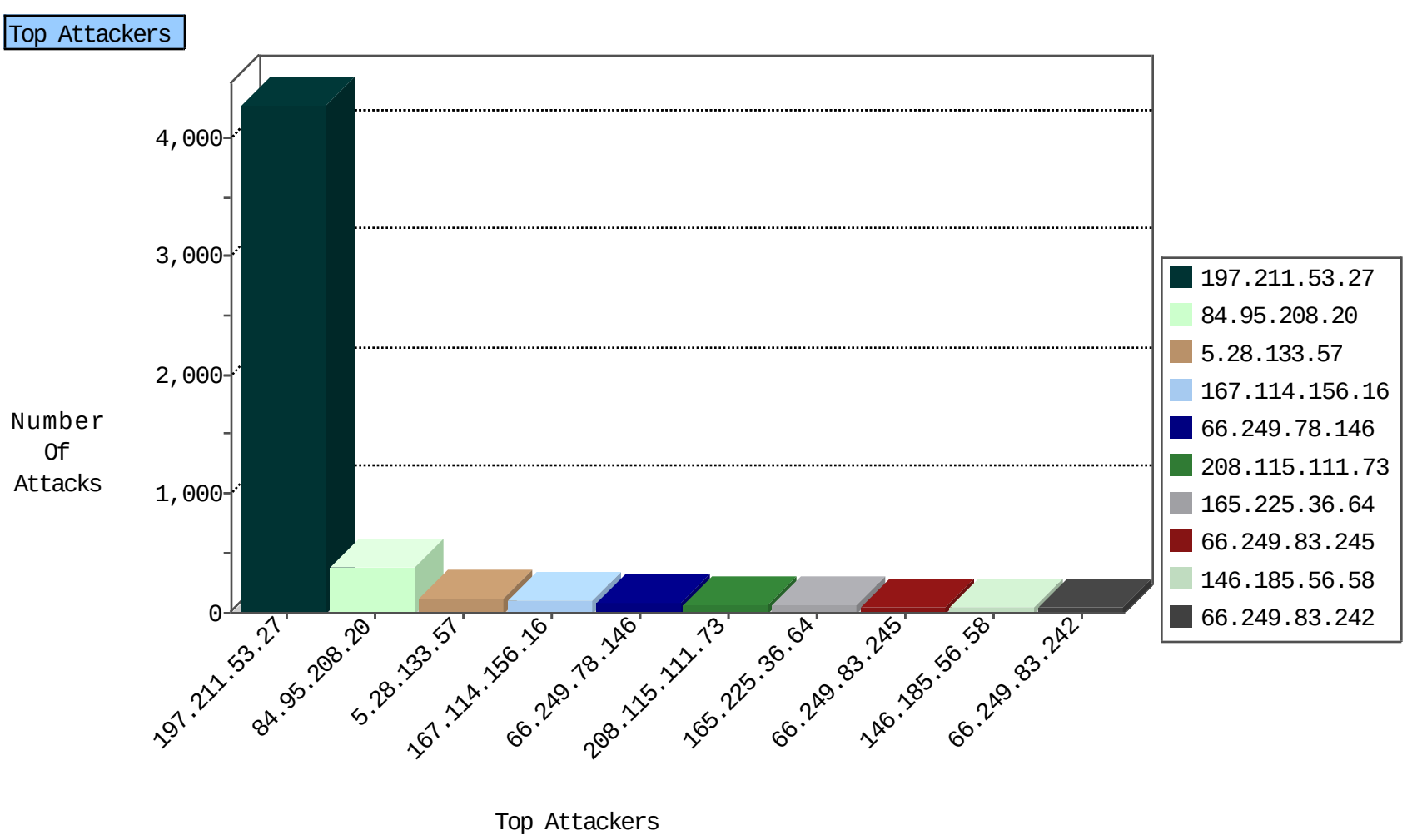
04-28-2016-02:04:01 to 04-28-2016-03:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-28-2016-02:04:01 to 04-28-2016-03:04:01

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	TCP handshake violation, first packet not syn	drop	49453
208.115.111.73	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7912
52.29.223.39	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3278
45.35.64.142	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3157
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	55
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	11
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
197.211.53.27	Nigeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
212.25.121.195	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
208.115.125.226	United States	147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1
208.115.125.226	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

04-28-2016-02:04:01 to 04-28-2016-03:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.190.69.10	Germany	147.237.76.147	chinuch.aka.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

04-28-2016-02:04:01 to 04-28-2016-03:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
146.185.56.58	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	33
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
13.92.245.177	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
161.202.120.146	147.237.8.50	Japan	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
106.184.2.29	147.237.72.217	Japan	e.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
80.82.79.104	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.141.210.203	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
161.202.120.146	147.237.76.30	Japan	himush.idf.il	ET SCAN NMAP -sS window 1024	1
161.202.120.146	147.237.0.16	Japan	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
107.170.8.228	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential SSH Scan	1
80.82.79.104	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1

04-28-2016-02:04:01 to 04-28-2016-03:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.211.53.27	Nigeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4286
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
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
165.225.36.64	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
66.249.83.245	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.249.83.242	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
66.249.83.248	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
5.28.133.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
5.28.133.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	28
5.28.133.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
5.28.133.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
105.106.79.188	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
134.191.220.75	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
207.46.13.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.69.62	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
200.31.14.243	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.69.54	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
5.28.133.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
203.133.169.210	Korea, Republic of	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
157.55.39.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.253.221.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.190	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	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
37.46.41.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.221.43.177	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.250	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
185.3.147.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
162.234.45.241	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop		drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	119
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	72
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	22
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	12
146.185.56.58	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 146.185.56.58	Block	11
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	10
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
149.202.239.135	France	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter PageNum	Block	6
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	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
149.202.239.134	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	4
146.185.56.58	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 146.185.56.58	Block	3
84.95.208.20	Israel	147.237.77.233	atal.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	147.237.0.34	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
134.191.220.74	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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
46.19.85.190	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.2	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.250	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.204	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.204	Block	2
109.253.221.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
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
134.191.220.72	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3491.jpg	Block	1
45.72.208.176	Canada	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
149.202.239.135	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
198.58.103.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
146.185.56.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
157.55.39.133	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/templates/general/general.aspx	Block	1
134.191.220.75	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
134.191.220.76	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.50	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	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
37.46.41.57	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18058-en/dover.aspx <a href=	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1