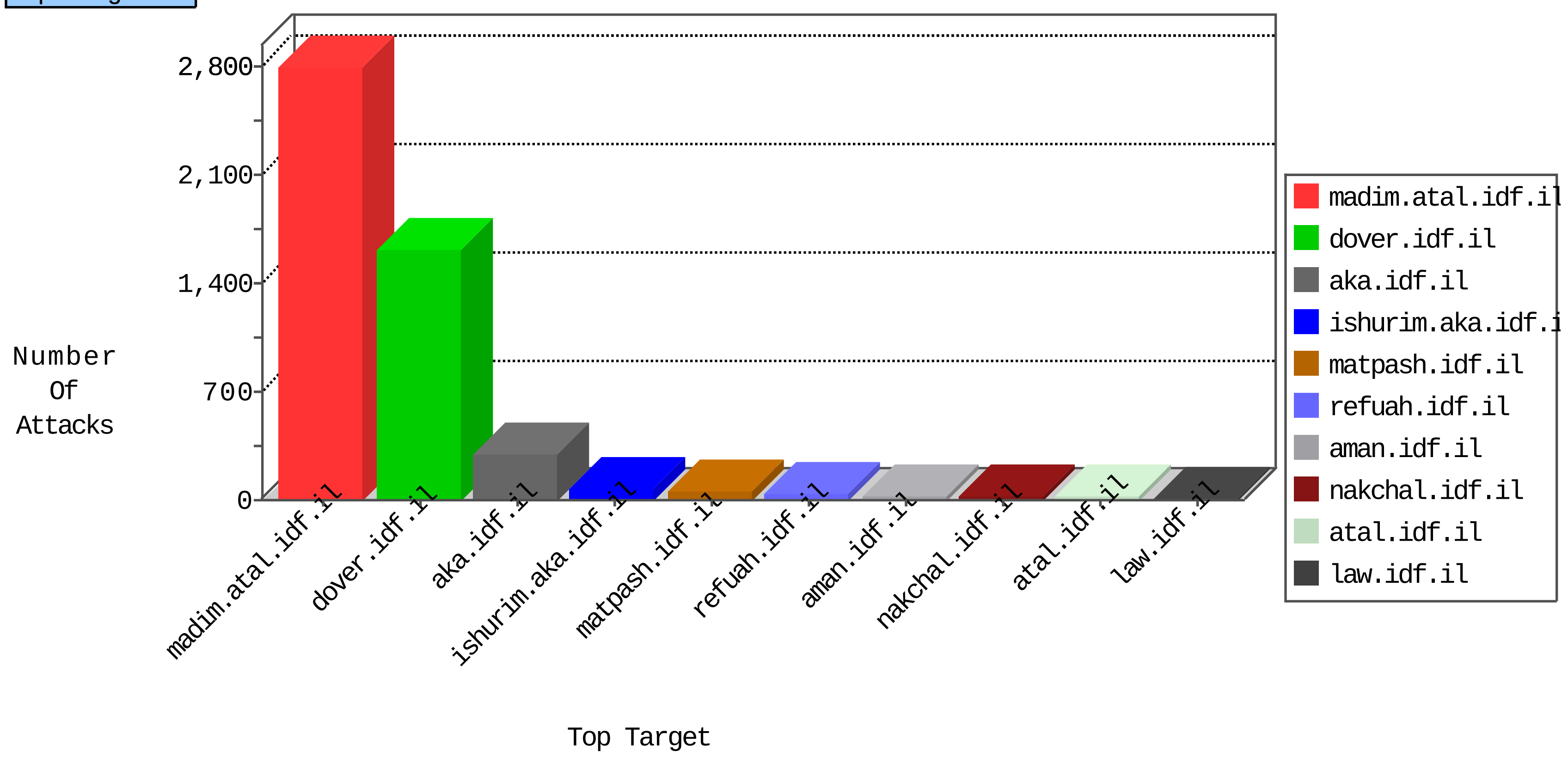
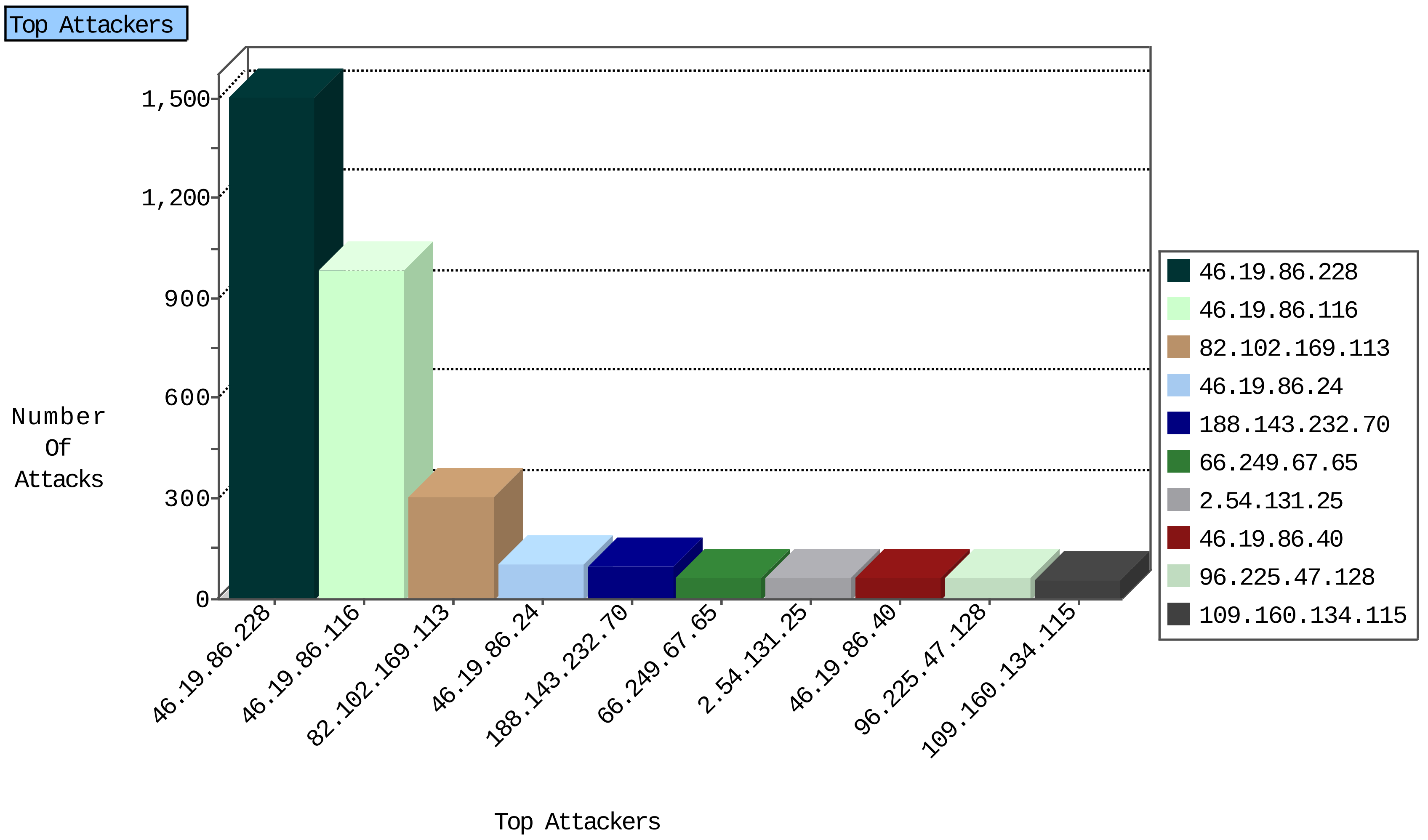
10-20-2015-07:04:09 to 10-20-2015-08:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-20-2015-07:04:09 to 10-20-2015-08:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.65	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3120
2.54.131.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	85
31.168.197.78	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
109.65.159.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.150.143.132	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.12.150.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.151.94	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
144.63.247.12	Sweden	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
138.134.192.10	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.142.107.167	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	2
174.236.0.195	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
41.215.151.246	Swaziland	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
41.215.151.246	Swaziland	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-20-2015-07:04:09 to 10-20-2015-08:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-20-2015-07:04:09 to 10-20-2015-08:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
185.58.201.28	147.237.76.30	Lebanon	himush.idf.il	ET SCAN NMAP -sA (2)	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
110.180.44.65	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.17	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
110.180.44.65	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
59.6.238.70	147.237.8.14	Korea, Republic of	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
110.180.44.65	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
110.180.44.65	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	147.237.77.234	Russian Federation	halag.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
110.180.44.65	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
182.48.151.231	147.237.76.30	New Zealand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
110.180.44.65	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
117.9.119.219	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
110.180.44.65	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
110.180.44.65	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
88.249.34.225	147.237.76.31	Turkey	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
110.180.44.65	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
59.6.238.70	147.237.8.46	Korea, Republic of	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
110.180.44.65	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
59.6.238.70	147.237.8.24	Korea, Republic of	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
223.115.56.142	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
110.180.44.65	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN NMAP -sS window 1024	1
110.180.44.65	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
110.180.44.65	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
119.10.8.133	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
110.180.44.65	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
110.180.44.65	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
104.171.122.161	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
110.180.44.65	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
110.180.44.65	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
59.6.238.70	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1

10-20-2015-07:04:09 to 10-20-2015-08:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
188.143.232.70	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
96.225.47.128	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
46.19.86.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
109.160.134.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
79.183.215.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
202.67.40.50	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
202.67.41.51	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.215.151.246	Swaziland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
100.100.54.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
188.244.211.128	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
37.142.125.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
46.19.86.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
80.178.201.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
144.63.247.12	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
199.30.25.247	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
104.131.234.217	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
77.127.191.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.146.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.142.166.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.8.5.250	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.54.131.25	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	11
2.54.38.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.235.136.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
24.185.95.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.168.197.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.210.186.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.54.38.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
46.19.86.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.93.234	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1508
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	988
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	299
46.19.85.196	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
80.179.19.40	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 80.179.19.40	Block	26
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	13
157.55.39.255	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283...en/dover.aspx	Block	13
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	13
54.235.136.3	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17416.jpg	Block	13
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	13
182.118.70.240	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scriptresource.axd%3fd	Block	13
79.179.121.176	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	13
62.219.165.164	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	13
212.179.21.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	13
100.11.14.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https:/twitter.com/	Block	13
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	13
46.19.86.126	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	13
66.249.65.31	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	13
109.67.57.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/resources/controls/captcha.ashx	Block	13
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	13
188.143.232.70	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	13
80.179.19.40	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/www.law.idf.il:×″×ž×—×¦×‘×•×ª	Block	13
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
41.215.151.246	Swaziland	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/en	Block	13
157.55.39.212	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	13
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	13
46.116.247.231	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/imagevideogallerylobby/imagevideogallerylobby.js	Block	13
80.246.139.197	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in aka.idf.il/main/giyus/login.aspx	None	13
188.143.232.70	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.70	Block	12
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/size220x0/12607.jpg	Block	12