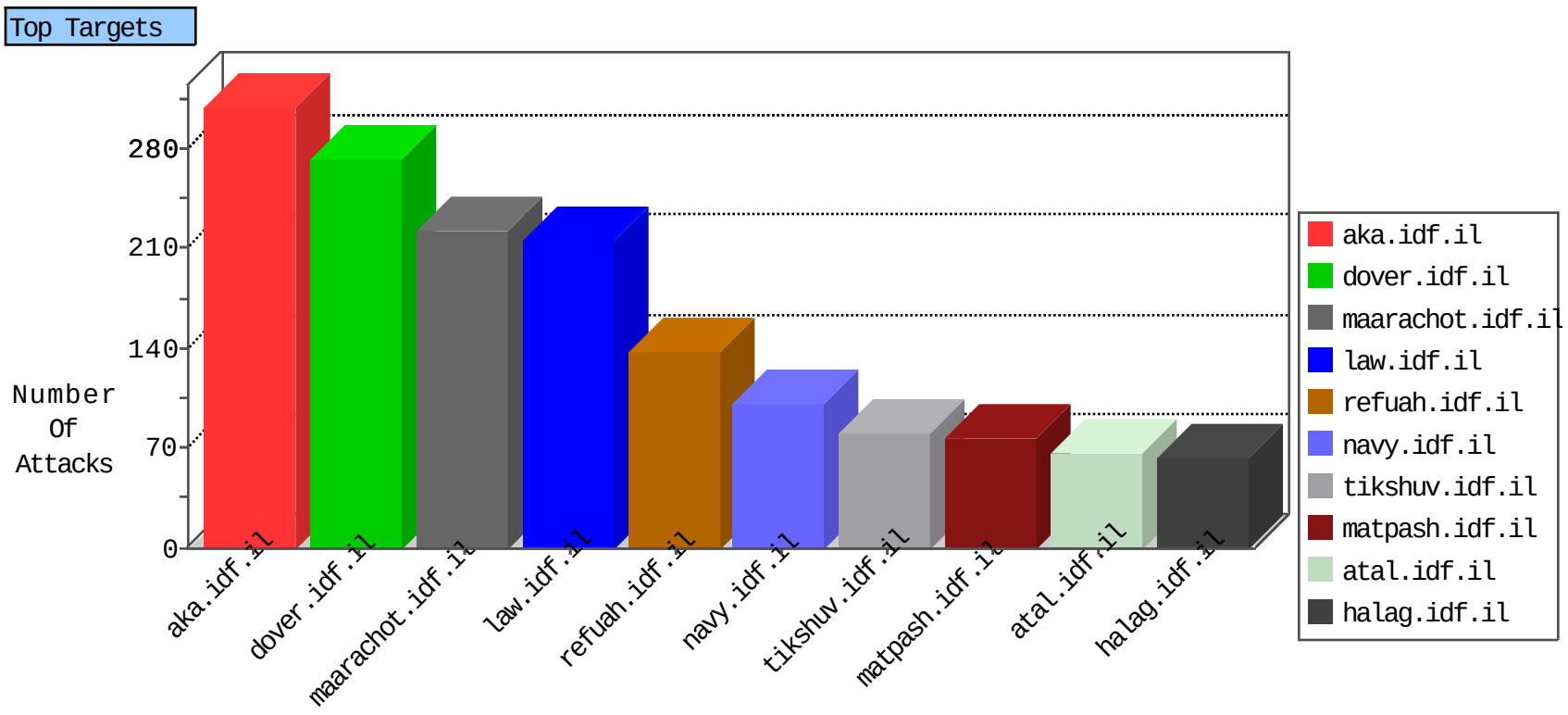
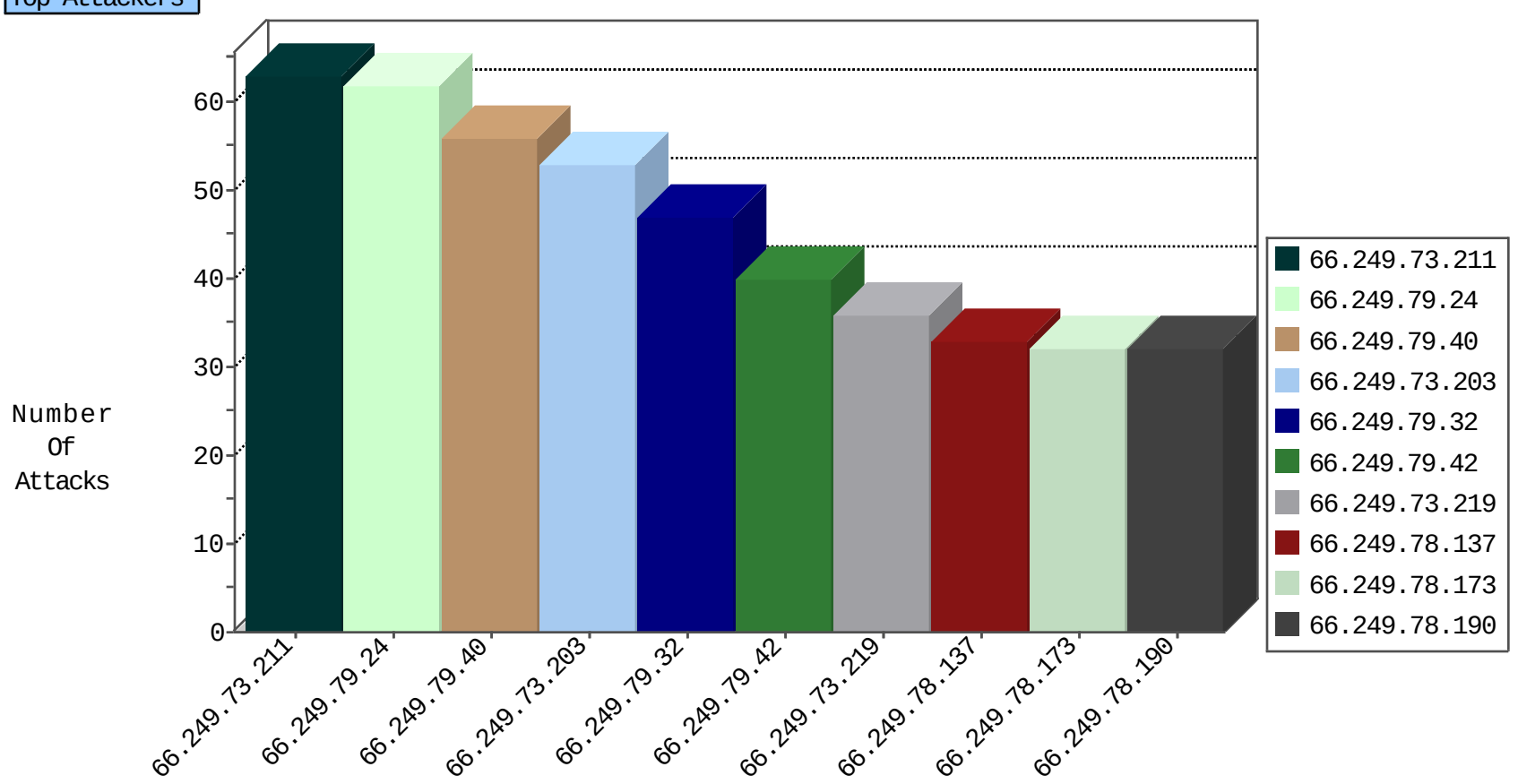
04-05-2015-19:03:02 to 04-05-2015-20:03:02

IDF Under Attack
04-05-2015-19:03:02

Top Targets



Top Attackers



04-05-2015-19:03:02 to 04-05-2015-20:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.73.211	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	63
66.249.79.24	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	62
66.249.79.40	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	54
66.249.73.203	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	53
66.249.79.32	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	47
66.249.73.219	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	36
66.249.78.137	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	33
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	32
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	32
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	31
66.249.73.195	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	30
66.249.65.199	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	30
66.249.73.187	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	28
66.249.79.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	28
66.249.73.129	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	27
66.249.67.73	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	25
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	24
66.249.65.195	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	24
66.249.67.81	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	24
66.249.67.89	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	24
66.249.78.144	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	23
66.249.79.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	21
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	21
66.249.73.241	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	21
66.249.93.208	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	19
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	19
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	18
66.249.79.13	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	17
66.249.67.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	17
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	17
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	16
66.249.75.104	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	16
66.249.79.5	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
66.249.78.130	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	16
66.249.93.158	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	15
66.249.67.29	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	15
66.249.79.50	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	15
66.249.79.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	14
66.249.75.112	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	14
66.249.79.157	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.61	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	12
66.249.67.31	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	12
66.249.73.230	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	12
66.249.79.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	12
66.249.93.204	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	11
66.249.65.191	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	11
66.249.78.54	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	10
66.249.67.37	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.93.200	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	10
66.249.67.39	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	9

04-05-2015-19:03:02 to 04-05-2015-20:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.95.83.134	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1

04-05-2015-19:03:02 to 04-05-2015-20:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
5.28.158.189	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
101.226.2.99	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
81.200.91.2	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
81.200.91.2	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
213.136.84.245	Germany	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
208.39.68.33	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.51	Germany	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
171.111.158.207	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
149.78.154.69	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
119.97.231.102	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
81.200.91.2	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
218.77.79.43	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
208.39.68.33	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
171.111.158.207	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
171.111.158.207	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
119.97.231.102	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1

04-05-2015-19:03:02 to 04-05-2015-20:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
199.30.25.80	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
50.117.41.63	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	10
109.67.186.102	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	9
65.55.210.107	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.141.53	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
173.252.114.113	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
109.253.156.145	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
5.102.254.125	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
79.183.7.60	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	5
46.19.86.14	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
37.46.39.71	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
80.246.139.94	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
66.119.41.34	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
188.120.148.159	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
69.171.228.123	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	3
69.171.228.118	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	3
145.255.180.81	Kazakstan	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
69.171.228.119	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	3
87.76.254.11	Ukraine	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
46.19.85.34	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
31.210.186.132	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
69.171.228.116	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	3
46.19.86.234	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
37.19.209.244	Ukraine	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
105.210.180.197	South Africa	147.237.77.216	dover.idf.il	SAM rule	drop	drop	2
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.117.185.214	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
193.43.245.250	Israel	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	2
207.241.229.147	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
69.171.228.120	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
46.117.185.214	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
109.253.129.128	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
69.171.228.122	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
46.197.239.64	Turkey	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
94.230.86.128	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
212.199.76.176	Israel	147.237.76.86	navy.idf.il	First packet isn't SYN	drop	drop	2
84.111.114.3	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
128.232.110.29	United Kingdom	147.237.8.50	e.tikshuv.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
85.64.249.151	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
141.212.122.57	United States	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
109.253.138.95	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.116.237.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
87.69.203.136	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
213.136.84.245	Germany	147.237.0.35	akaws.idf.il		drop	drop	1
84.111.114.3	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.138.17.205	France	147.237.76.198	e.yohalan.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
5.22.129.231	Israel	147.237.77.74	law.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
79.177.174.213	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
128.232.110.29	United Kingdom	147.237.76.34	yohalan.idf.il		drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.57.142.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
212.235.74.160	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
37.26.147.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.178.62.57	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
213.251.182.10	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
185.32.176.88	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.181.16.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	3
109.64.177.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
62.90.243.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
109.67.54.175	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.142.233.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.64.217.118	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
84.228.113.21	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
146.185.56.162	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
114.112.90.54	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
77.126.21.89	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.55.189	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/profs.asp	Block	1
203.133.169.157	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/dayan.stm	Block	1
85.64.76.231	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.175.88	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.136.80	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.136.159	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.76.254.11	Ukraine	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.34	Israel	147.237.72.166	aka.idf.il	Malformed URL _pk_ref.101.3ebc=["","",1422446132,"https://www.google.co.il/"]	Block	1
213.233.90.79	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
84.110.8.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
5.29.151.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/kkkkkkk=40ee37adkkkkkkk_40ee37ad	Block	1
114.112.90.54	China	147.237.77.235	sviva.idf.il	Unauthorized HTTP Method	Block	1
46.120.7.136	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//https:/aka.idf.il/	Block	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
80.246.139.94	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.90.243.37	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.253.146.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.171.79.16	Ukraine	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
46.19.85.34	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method 588.2.1422446147.1412085588.; in URL	Block	1
84.111.38.64	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
5.29.219.229	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
141.212.121.160	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
109.86.128.127	Ukraine	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1
46.120.7.136	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
38.119.62.105	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.104	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
85.250.195.204	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
84.50.241.236	Estonia	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
176.12.146.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
114.112.90.54	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
94.231.76.138	Ukraine	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/320-en/patzar.aspx	Block	1