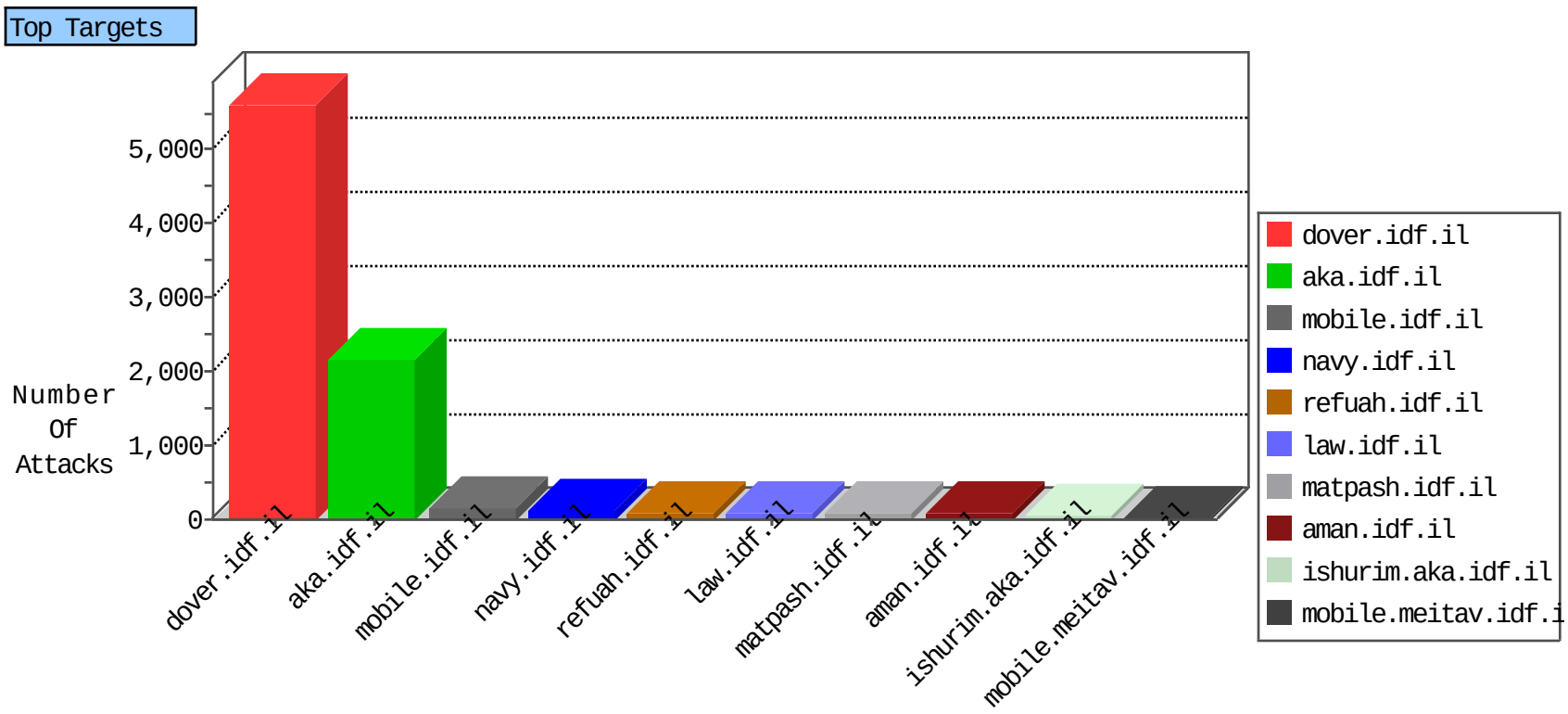
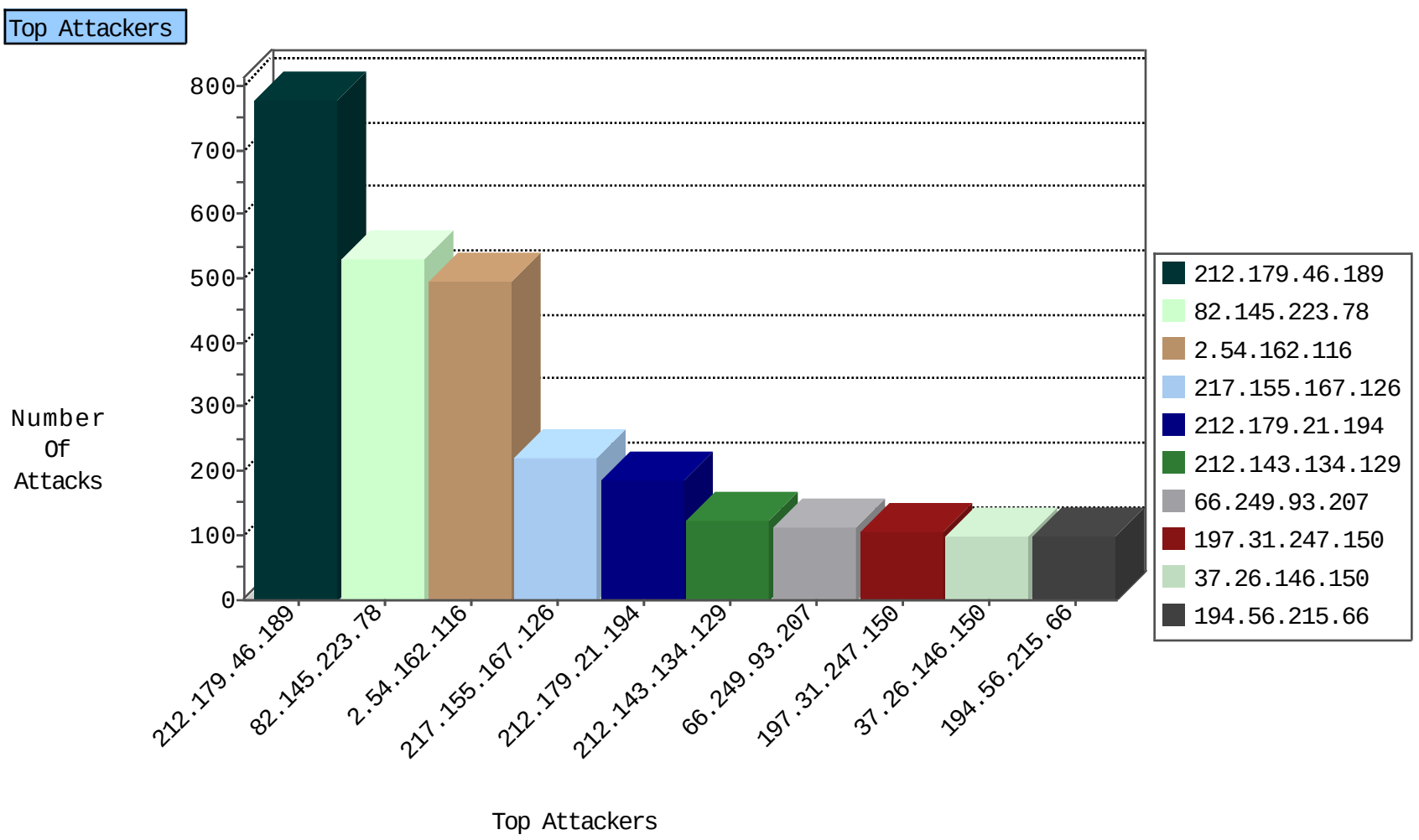
10-20-2015-13:04:01 to 10-20-2015-14:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-20-2015-13:04:01 to 10-20-2015-14:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	128
66.249.67.202	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	100
95.86.101.95	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	58
79.178.181.183	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
2.54.132.239	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
212.143.134.129	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
109.226.17.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.19.85.145	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	7
109.108.238.252	Ukraine	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
213.244.121.4	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.64.98.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
5.22.129.158	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
2.52.7.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.10.19	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.40	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
213.151.35.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
132.64.30.253	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.12.149.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.139.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
80.246.140.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.52.6.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
95.35.82.61	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.13.17.228	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
80.246.140.207	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.26.147.176	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
222.186.56.42	China	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
93.174.93.181	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
176.13.11.232	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
93.174.93.181	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.181	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
194.56.215.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.108.214.168	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
93.174.93.181	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

10-20-2015-13:04:01 to 10-20-2015-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-20-2015-13:04:01 to 10-20-2015-14:04:01

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	5
91.195.163.17	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.189.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.236	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.145.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
204.13.204.139	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
5.39.222.253	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
192.115.248.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.1.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
117.21.176.93	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
87.69.234.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.201.201	147.237.8.45	Israel	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.67.73	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.54.148.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
190.96.6.130	147.237.0.34	Chile	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.48.243	147.237.77.176	Singapore	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

10-20-2015-13:04:01 to 10-20-2015-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.145.223.78	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	530
2.54.162.116	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	492
217.155.167.126	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	222
212.179.21.194	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	185
212.143.134.129	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	122
197.31.247.150	Tunisia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	105
37.26.146.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	101
194.56.215.66	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	97
66.249.93.203	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	83
66.249.93.199	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	75
212.150.218.70	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	73
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	71
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	68
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	66
85.64.241.151	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	64
66.249.93.207	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	61
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
37.142.101.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	57
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	55
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	54
82.166.229.224	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
212.199.51.125	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
46.19.86.0	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
169.253.194.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
176.13.0.31	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
79.178.182.192	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
213.244.123.218	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
168.63.200.167	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
2.54.175.202	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
79.178.181.183	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
85.154.100.55	Oman	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
93.172.184.58	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
151.80.31.115	Italy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
2.54.43.24	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
164.138.112.184	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
79.180.163.191	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
5.22.129.176	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
147.236.238.40	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
148.177.129.212	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
82.166.25.245	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
37.142.207.142	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
212.199.195.219	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
213.6.64.67	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
46.19.85.225	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
66.249.67.53	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.46.189	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	780
75.126.122.176	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	78
37.26.149.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	52
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	52
82.80.216.12	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	39
213.151.55.247	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	39
176.67.56.245	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	39
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
79.176.215.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	26
66.249.93.207	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/info.asp	Block	26
84.228.80.11	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.80.11	Block	26
176.12.145.88	Israel	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/657-en/patzar.aspx	Block	26
46.19.85.169	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	26
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	26
46.19.85.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	26
109.66.131.126	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
95.86.125.180	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/default.aspx/	Block	26
37.26.148.147	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in mobile.meitav.idf.il/1494-he/meitav.aspx	Block	13
84.110.39.87	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	13
66.249.79.202	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	13
157.55.39.199	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	13
46.19.85.165	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	13
109.64.17.193	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	13
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
2.52.160.146	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	13
201.208.162.248	Venezuela	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
147.236.34.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/default.asp	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
213.8.122.115	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	13
66.249.79.209	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	13
109.64.39.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	13
2.52.190.216	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
212.68.153.241	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	13
149.78.251.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/https:/aka.idf.il/	Block	13
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
84.228.80.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sahar	Block	13
79.182.140.19	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$rptEmailSubjectsListT2 in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	13
66.249.93.199	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/rights/info.asp	Block	13
109.66.81.120	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
46.19.86.248	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	13
82.166.229.224	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	13
2.54.150.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
74.82.47.2	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	13
149.78.251.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
87.69.81.241	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/https:/aka.idf.il/	Block	13
217.194.199.74	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;utm_campaign in www.aka.idf.il/main/home/default.aspx	None	13
66.249.93.207	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.93.207	Block	13
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/kkkkkkk=567d5ab1kkkkkkk_567d5ab1	Block	13