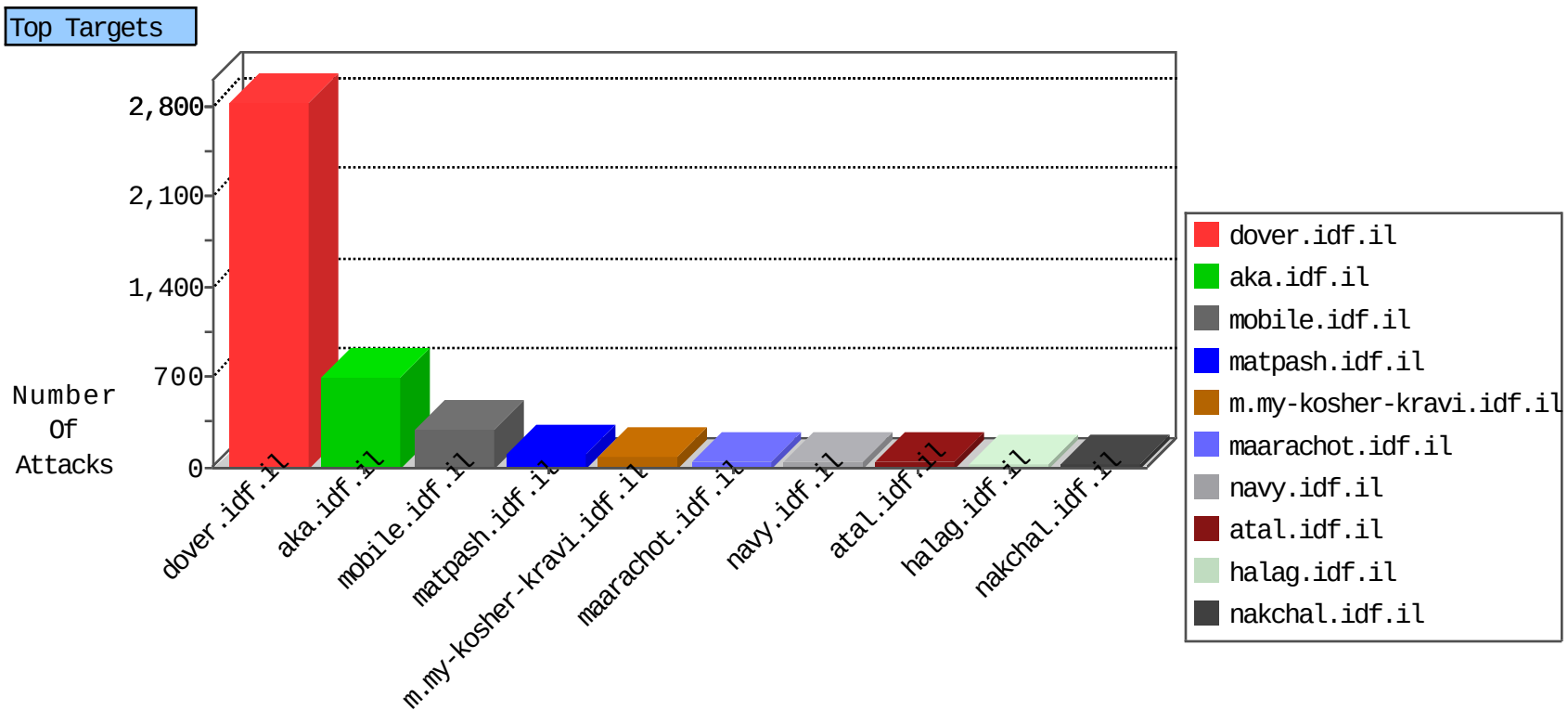
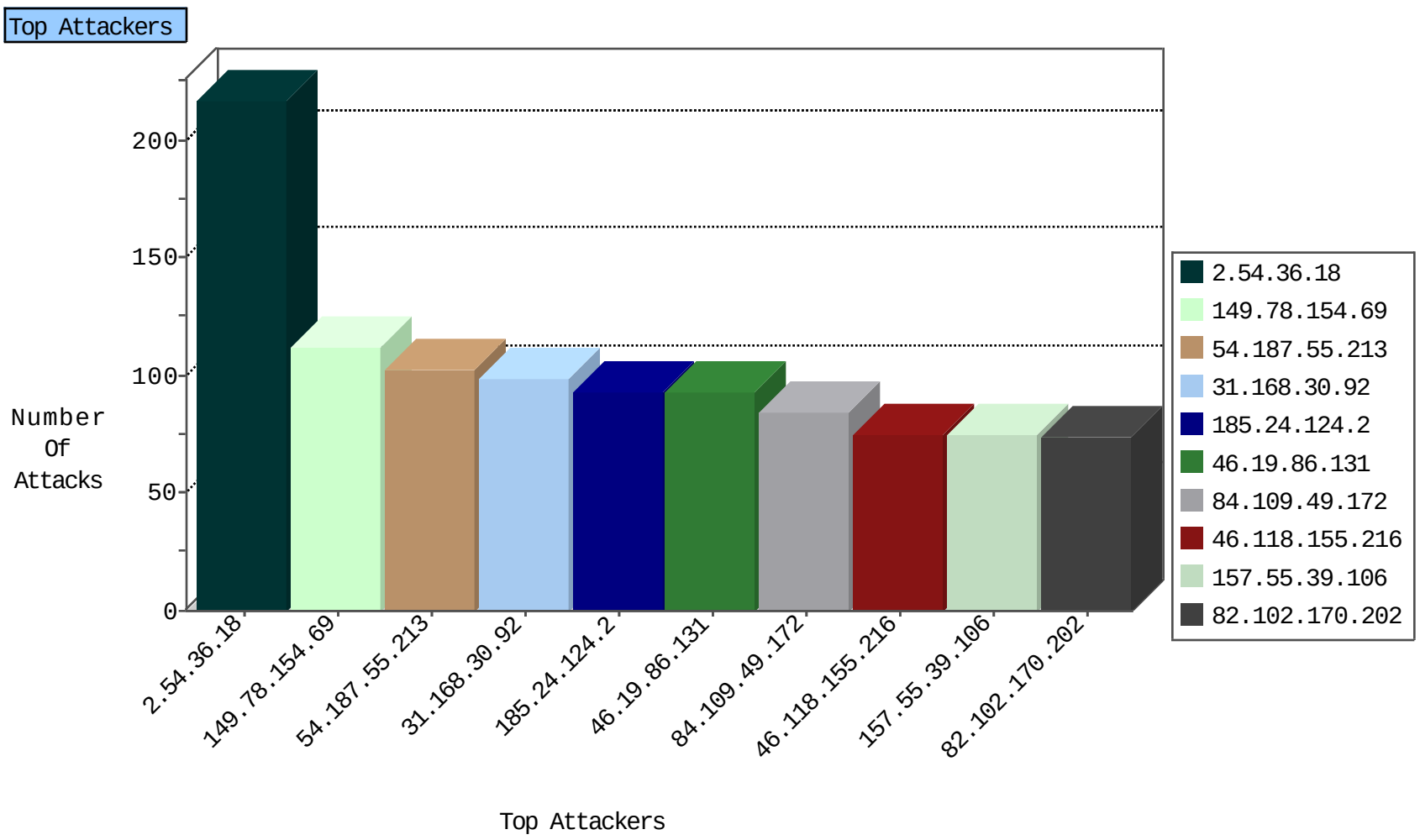
10-30-2015-19:04:05 to 10-30-2015-20:04:05

IDF Under Attack Daily Report





10-30-2015-19:04:05 to 10-30-2015-20:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.235.6	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2586
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1102
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	291
66.249.69.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	179
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	111
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	109
176.12.136.38	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
37.26.148.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
68.196.87.94	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
109.65.120.222	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
93.172.167.213	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.54.128.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.177.42.203	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6
66.249.69.92	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
2.54.10.25	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
89.139.176.55	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.181.109.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
194.75.182.226	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
82.166.22.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.52.60.117	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.179.1.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
96.53.124.158	Canada	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.52.23.20	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
77.127.109.138	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
178.152.206.119	Qatar	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
176.13.0.30	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
87.69.48.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
82.102.170.202	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.136.38	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.151.203	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
83.244.99.205	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
46.19.86.131	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
176.13.0.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.52.23.20	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.13.0.184	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.191.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
146.185.239.100	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1

10-30-2015-19:04:05 to 10-30-2015-20:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.50.115	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3

10-30-2015-19:04:05 to 10-30-2015-20:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.131	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	54
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.27	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
79.181.176.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
69.64.32.110	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.253.96.122	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 3072	1
23.24.18.118	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.21.196	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.8.66.110	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.196	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
184.106.185.15	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
69.64.32.110	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.151.54.209	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.196	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.8.66.110	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.196	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.8.66.110	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.196	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
189.18.192.147	147.237.8.27	Brazil	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-30-2015-19:04:05 to 10-30-2015-20:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.36.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	217
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	111
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
185.24.124.2	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
82.102.170.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
197.116.74.194	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
68.99.117.228	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
84.109.49.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
200.115.154.235	Panama	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
178.152.206.119	Qatar	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
109.186.4.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
212.227.118.21	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
79.181.214.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
46.19.85.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
46.19.86.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
46.19.86.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
84.111.38.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
185.120.126.51		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
84.109.49.172	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
166.216.157.126	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
50.162.178.25	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
176.13.12.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.54.10.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.54.128.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
12.237.119.20	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
2.54.50.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
100.100.9.29		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
68.196.87.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
5.169.128.37	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
79.179.1.108	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
96.53.124.158	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
85.250.177.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
208.102.192.207	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
188.92.11.23	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
107.77.165.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.117.83.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
176.12.147.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.30.92	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 31.168.30.92	Block	60
79.179.1.108	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	45
5.28.143.229	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	45
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	45
87.69.63.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/ge...px	Block	30
2.54.157.189	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	30
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	30
31.168.30.92	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1872	Block	30
176.13.15.35	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	30
149.88.96.100	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	30
46.19.85.172	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	30
2.54.25.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
178.255.215.87	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	15
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/brothers/home	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	15
157.55.39.106	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/patzar/klali/default.asp	None	15
46.121.106.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	15
203.142.50.58	Malaysia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	15
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	15
176.13.15.35	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
105.157.82.234	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1154-ar/dover.aspx/ip	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/900-he/chinuch.aspx	Block	15
84.110.111.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	15
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
157.55.39.106	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/gallery/	None	15
66.249.64.75	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	15
88.198.16.122	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 88.198.16.122	Block	15
79.179.129.13	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	15
207.46.13.36	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.78.66	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	15
109.64.13.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	15
84.228.134.8	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	15
2.54.188.110	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	15
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/size220x0/17344.jpg	Block	15
79.176.16.136	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation searchText in www.atal.idf.il/1559-he/atal.aspx	Block	15
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71806-he/maarachot.aspx	Block	15
157.55.39.106	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/brothers/faq/default.asp	None	15
66.249.65.251	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	15
88.198.16.122	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/	Block	15
79.183.168.216	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	15
37.140.141.17	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8/4538.pdf	Block	15
212.76.96.122	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	15
176.13.18.139	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	15
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	15