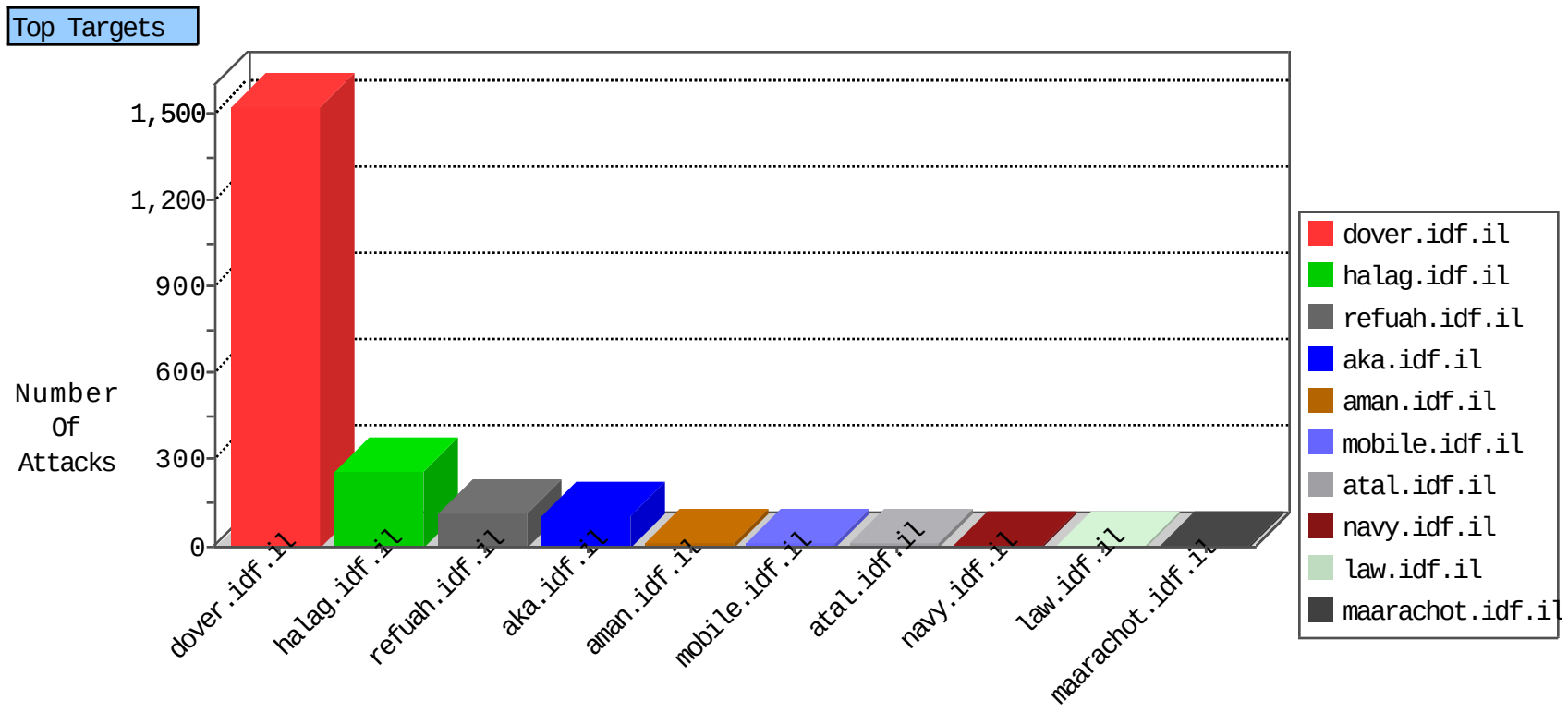
05-02-2015-16:03:00 to 05-02-2015-17:03:00

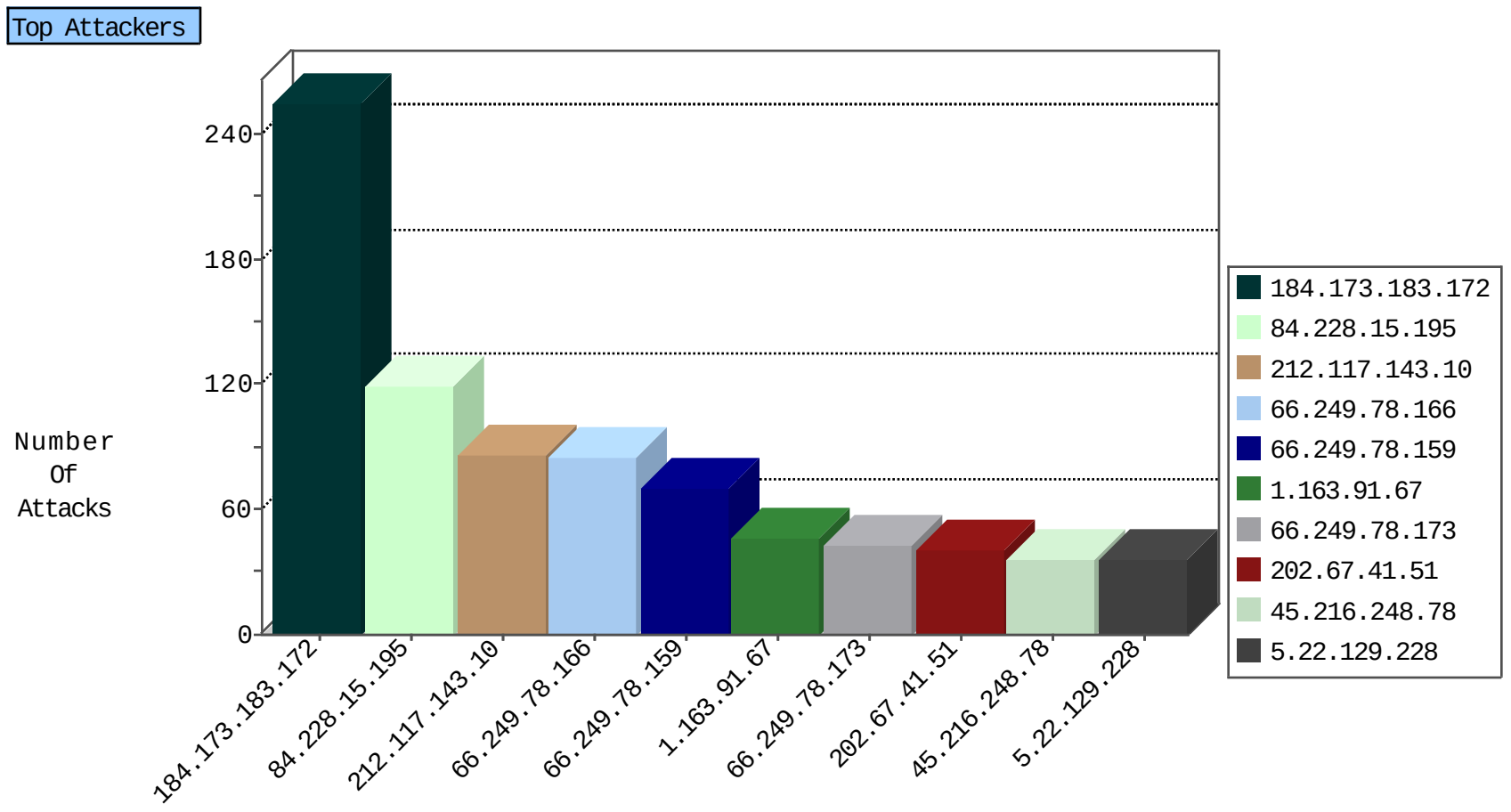
IDF Under Attack
05-02-2015-16:03:00

Top Targets



Top Target

Top Attackers



Top Attackers

05-02-2015-16:03:00 to 05-02-2015-17:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
79.177.170.211	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
140.242.64.131	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

05-02-2015-16:03:00 to 05-02-2015-17:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.234	halag.idf.il	DVRep_P-N_40-59	Permit	255
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
37.8.57.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
89.139.164.148	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.182.168.121	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
46.117.63.4	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.115.82.54	Anonymous Proxy	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
84.94.33.204	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
46.121.242.66	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
84.95.201.17	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
77.125.101.200	Israel	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
66.240.192.138	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
109.67.63.41	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
77.127.206.25	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1

05-02-2015-16:03:00 to 05-02-2015-17:03:00

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
187.101.132.36	Brazil	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	4
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
178.32.251.100	France	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
178.32.251.100	France	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
121.88.5.177	Korea, Republic of	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
198.100.100.50	United States	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1

05-02-2015-16:03:00 to 05-02-2015-17:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.228.15.195	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	103
212.117.143.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	86
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	62
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
1.163.91.67	Taiwan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
202.67.41.51	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
5.22.129.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
45.216.248.78		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
79.176.155.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
37.26.148.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
80.246.130.68	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
46.116.82.78	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
149.78.43.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
202.67.40.50	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
149.78.5.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
85.65.36.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
72.95.62.202	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
154.121.5.229		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
85.65.127.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
37.142.244.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.116.78.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
109.253.138.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
76.124.69.64	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
109.65.24.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
2.52.47.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
109.253.128.118	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
79.176.55.44	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
85.65.36.230	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
85.250.134.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
84.228.15.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
93.173.128.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
72.71.178.106	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
62.140.210.130	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
2.52.47.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.183.102.242	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.121.138.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	24
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	5
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
84.109.179.222	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.204	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.204	Block	3
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il//edim/yoman/enlarge.asp	Block	2
79.176.72.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/forms.aspx	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
5.29.37.140	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
136.243.36.97	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.69.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/skira/default.asp	Block	1
46.229.164.102	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
79.179.0.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
188.165.15.236	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1238-he/atal.aspx	Block	1
66.249.75.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1537-8763-he/atal.aspx	Block	1
66.249.67.42	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1056-en/hamaz.aspx	Block	1
85.64.117.244	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.176.30.217	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$txtOtherQuestion in www.aka.idf.il/main/giyus/faq.aspx	None	1
31.168.68.51	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q861 in www.aka.idf.il/main/giyus/login.aspx	None	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18063-he/dover.aspx	Block	1
149.88.91.70	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Illegal Parameter Encoding catId in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	1
79.182.154.201	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arafat/terrorism2/	Block	1
66.249.75.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/modules/forums/forum.aspx	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sachar/faq.aspx	Block	1
93.172.156.104	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.67.49	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71857-he/maarachot.aspx	Block	1
79.176.37.182	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
46.19.85.130	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0226-3.stm	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portal	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
77.127.159.120	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
66.249.75.117	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	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
109.253.128.118	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
46.120.174.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.159	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//	Block	1
84.228.15.195	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
77.127.206.25	Israel	147.237.76.86	navy.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 77.127.206.25	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18554-he/dover.aspx	Block	1