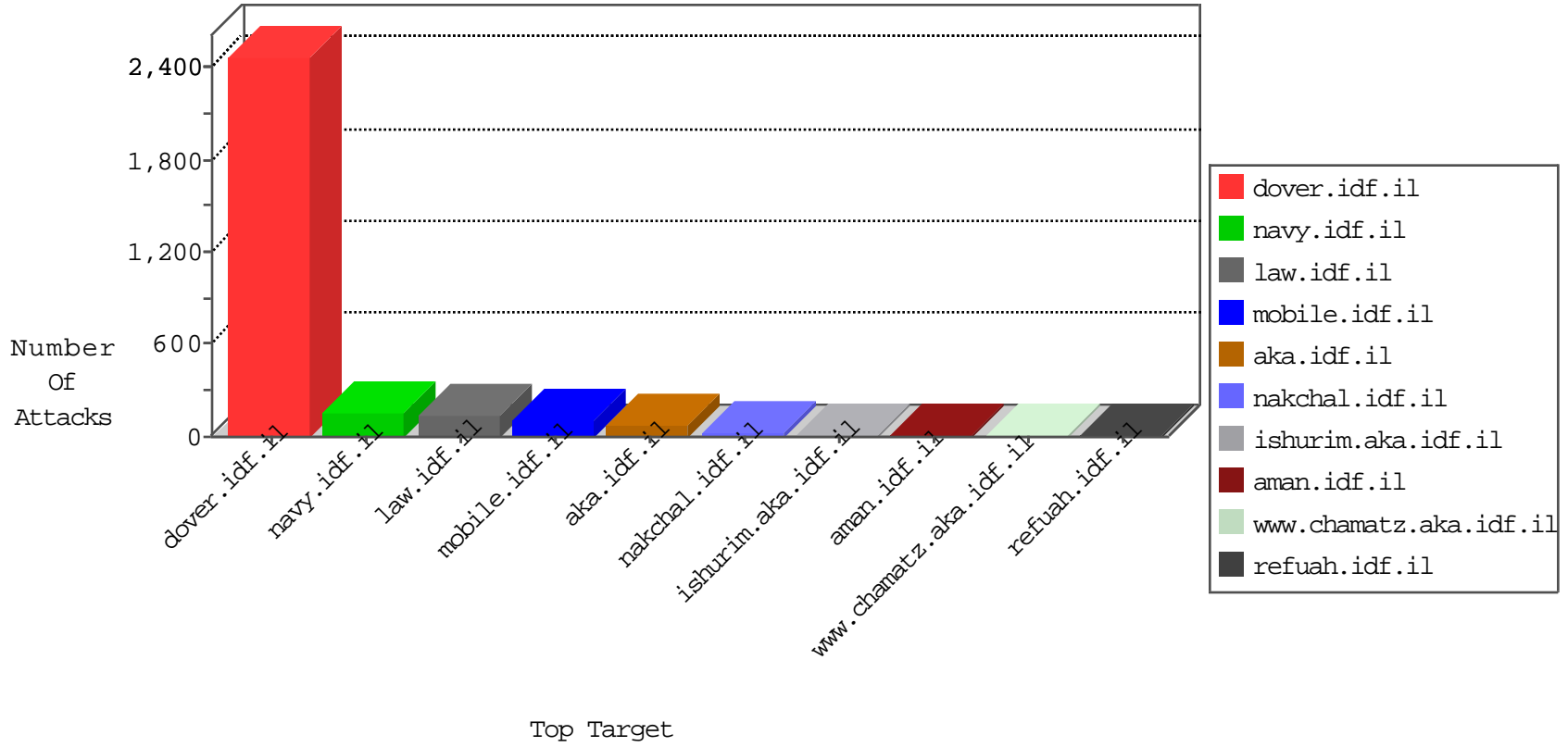
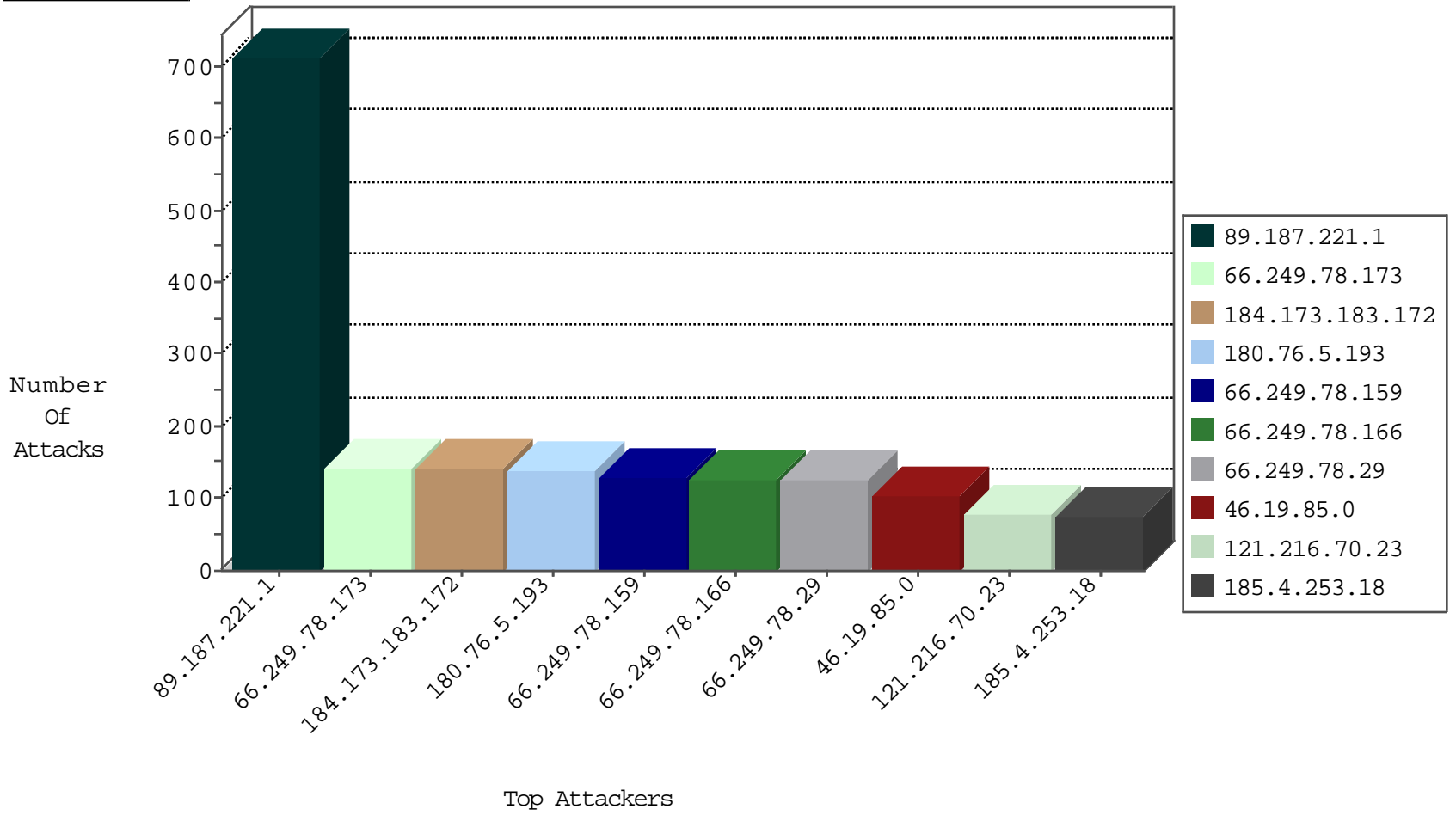




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
37.142.138.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	92
109.253.128.240	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	75
220.181.108.143	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	34
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
122.145.231.91	Japan	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
5.102.207.108	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
84.228.129.158	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
146.185.239.100	Russian Federation	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
192.3.206.130	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
112.117.62.158	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
192.3.206.130	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	142
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	140
199.168.141.77	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	8
222.127.18.123	Philippines	147.237.76.31	nakchal.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
84.109.74.157	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
199.168.141.77	United States	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
85.25.43.94	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	yochalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
89.139.172.245	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	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	126
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
134.191.232.70	Israel	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sA (2)	4
134.191.232.68	Israel	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sA (2)	4
85.65.91.238	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
94.102.60.140	Netherlands	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
178.32.251.100	France	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.238.134.92	Poland	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
74.87.109.44	United States	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
5.135.199.12	France	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.16.206	Russian Federation	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
89.187.221.1	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	713
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	132
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	122
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	118
46.19.85.0	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	105
121.216.70.23	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	79
185.4.253.18	Lebanon	147.237.77.216	dover.idf.il	TCP segment out of maximum allowed sequence. Packet dropped.	Streaming Engine: TCP Segment Limit Enforcement	drop	46
213.57.239.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
79.177.42.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
211.30.232.218	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
31.168.71.97	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
93.72.69.117	Ukraine	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
5.22.130.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
46.19.85.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
176.12.151.211	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
79.178.55.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
149.62.200.157	Bulgaria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
46.19.85.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
82.80.42.176	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
46.116.253.40	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
157.55.39.47	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.64.76	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
66.249.64.72	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
46.120.129.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
185.4.253.18	Lebanon	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	13
66.249.64.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
185.4.253.18	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.93.241	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	9
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
66.249.93.241	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	9
82.80.42.185	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
66.249.93.241	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
79.176.135.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
84.211.16.251	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
80.74.107.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
5.22.130.216	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.181.138.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.64.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
41.185.12.165	South Africa	147.237.76.86	navy.idf.il	SAM rule	drop	drop	6
87.69.1.249	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
157.55.39.61	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	Multiple Unauthorized URL Access from 157.55.39.61	Block	3
199.168.141.77	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.120.175.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.138	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.138	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
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
180.76.4.242	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
61.224.6.17	Taiwan	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method COOK in URL www.cogat.idf.il/1219-en/cogat.aspx	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unknown Parameter sOpenLinkIn in www.aka.idf.il/eitan/pratim/pirteychayal/	None	1
109.186.172.200	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$cpMain\$cpMain\$ct105 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.79.58	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
66.249.69.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/hinuch	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
213.251.182.103	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	1
84.94.77.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
184.105.247.195	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.78.87	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.136	Block	1
132.68.36.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/	Block	1
68.180.228.175	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19072-he/dover.aspx	Block	1
199.168.141.77	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ckeditor/ckfinder/core/connector.aspx/connector.aspx	Block	1
66.249.75.9	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/mobile/	Block	1
216.218.206.67	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
85.65.127.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	1
188.165.15.95	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9756-he/refuah.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20155-he/dover.aspx	Block	1
66.249.67.41	Israel	147.237.77.170	naarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
136.243.36.97	Germany	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.78	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.78	Block	1
66.249.78.38	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unknown Parameter 55bffe68 in www.aka.idf.il/main/home/default.aspx	None	1
46.229.164.111	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
109.65.145.74	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149-he/dover...x xæx?	Block	1
188.165.15.195	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.195	Block	1
66.249.67.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/28-he/patzar.aspx	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.23.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13450-en/dover.aspx forcerecrawl: 0	Block	1
66.249.78.73	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
46.229.164.113	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//giyus/kadatz	Block	1
109.186.4.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1