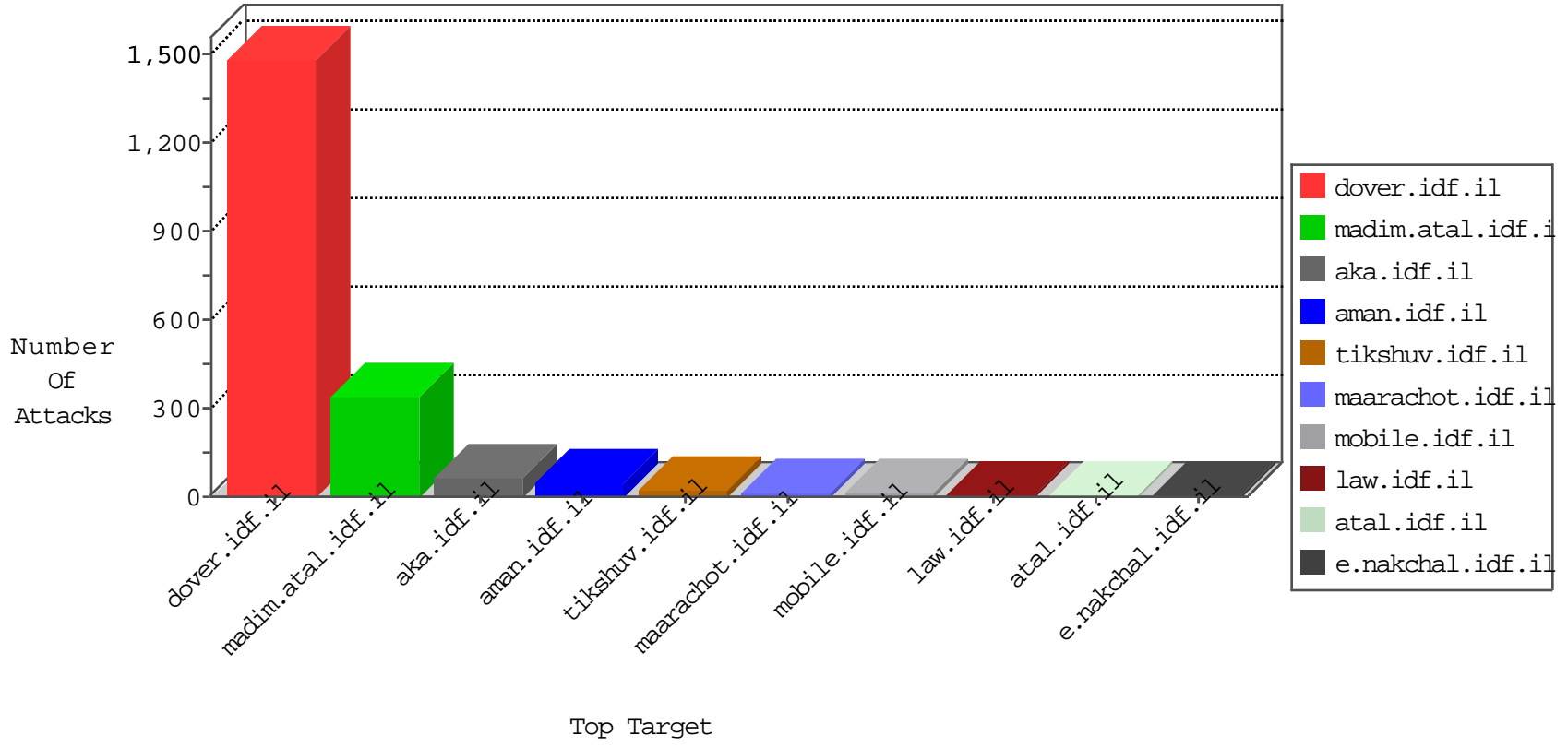
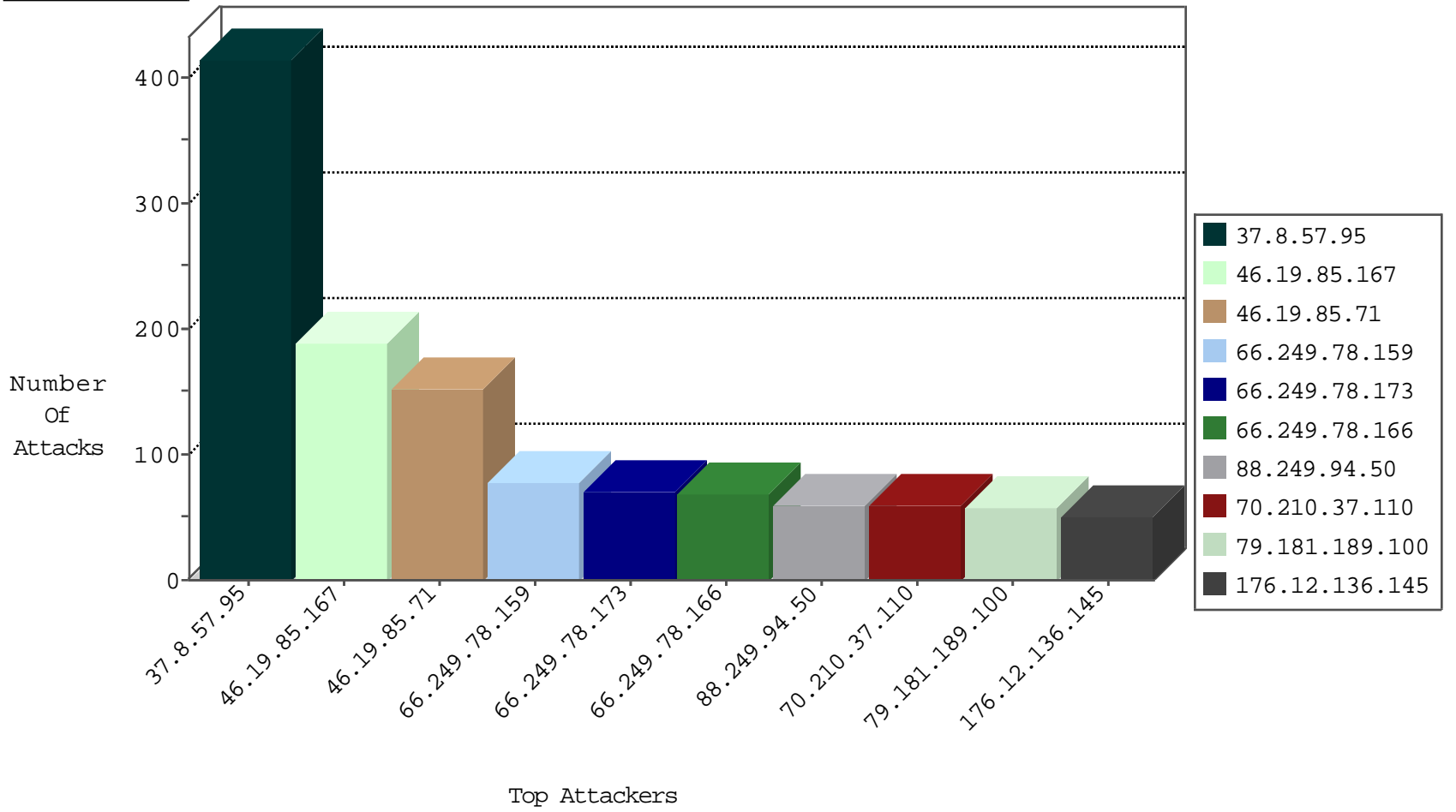




Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	web Site	Signature	Device Action	Count
79.176.20.208	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	611
46.19.85.15	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
109.65.29.230	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
2.54.168.237	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
71.6.167.142	United States	147.237.76.198	e.ychalan.idf.il	Block_Udp_All_Nets	drop	1
212.29.252.81	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
37.26.148.131	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.8.57.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	10
93.172.40.1	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	2
37.8.57.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	C023: HTTP: administrator in URI	Permit	2
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
54.79.66.122	United States	147.237.0.34	tikshuv.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
89.139.180.23	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
37.8.57.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	C003: HTTP: phpMyAdmin access	Block	1
84.108.232.78	Israel	147.237.72.166	aka.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
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
37.8.57.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP login.htm access	34
37.8.57.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP adminlogin access	30
37.8.57.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	22
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.79.22	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
109.253.130.56	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.163	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
82.165.11.63	Germany	147.237.76.201	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.163	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
82.165.11.63	Germany	147.237.76.176	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.163	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
82.165.11.63	Germany	147.237.76.44	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.163	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
82.165.11.63	Germany	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.26.148.208	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
187.11.121.110	Brazil	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
5.135.199.12	France	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
182.23.39.210	Indonesia	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
106.39.95.194	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
82.165.11.63	Germany	147.237.76.202	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.163	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
82.165.11.63	Germany	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.163	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
82.165.11.63	Germany	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
213.210.205.2	Saudi Arabia	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.163	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
82.165.11.63	Germany	147.237.0.200	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.163	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.90	United States	147.237.77.216	dover.idf.il	ET DROP Dshield Block Listed Source	1
82.165.11.63	Germany	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
190.77.126.107	Venezuela	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
182.23.39.210	Indonesia	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.65	China	147.237.76.177	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.171.167	Netherlands	147.237.76.202	e.halag.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
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	74
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	68
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	68
88.249.94.50	Turkey	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	60
79.181.189.100	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
70.210.37.110	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
176.12.136.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
46.19.85.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
162.243.210.161	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
162.243.61.230	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
46.19.85.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
69.175.127.10	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
62.219.154.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.19.86.225	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	13
93.172.62.137	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
82.145.220.26	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
62.219.154.129	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.138	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
62.219.154.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
93.172.129.178	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
112.198.83.83	Philippines	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
31.154.25.42	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	7
89.138.221.187	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
195.34.150.18	Austria	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	6
66.249.64.72	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
173.56.75.63	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.64.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
208.69.40.107	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
80.179.78.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
5.102.254.136	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
109.65.58.219	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
84.108.30.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.64.76	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.116.78.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.247.36.101	Netherlands	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
77.126.211.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.167	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.167	Block	188
37.8.57.95	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.8.57.95	Block	180
46.19.85.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	153
37.8.57.95	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 37.8.57.95	Block	71
37.8.57.95	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	PHP Attempt	Block	64
157.55.39.138	United States	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	4
109.67.58.35	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
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.182.200.127	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.75.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1421-he/atal.aspx	Block	1
46.19.85.167	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
207.46.13.19	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5480-he/patzar.aspx	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.218.134.195	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authenticationservice.aspx/getuserdatails	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
66.249.75.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1293-he/atal.aspx	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.204	Block	1
109.186.54.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authenticationservice.aspx/getuserdatails	Block	1
77.127.244.212	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigation.asp	Block	1
66.249.78.133	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
66.249.69.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
85.64.168.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.79.66	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
178.137.166.68	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
115.25.81.70	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
46.229.164.114	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
2.54.175.213	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1
79.182.125.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/main/giyus/general.aspx	Block	1
66.249.69.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1638-he/refuah.aspx	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.136	Block	1
109.64.50.187	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international-training	Block	1
188.165.15.195	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/idf_in_pictures/2000/september/5.stm	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
149.78.149.184	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
46.229.164.114	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube	Block	1
37.8.46.107	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	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
109.66.4.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
68.180.229.27	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
207.46.13.19	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.102	Block	1