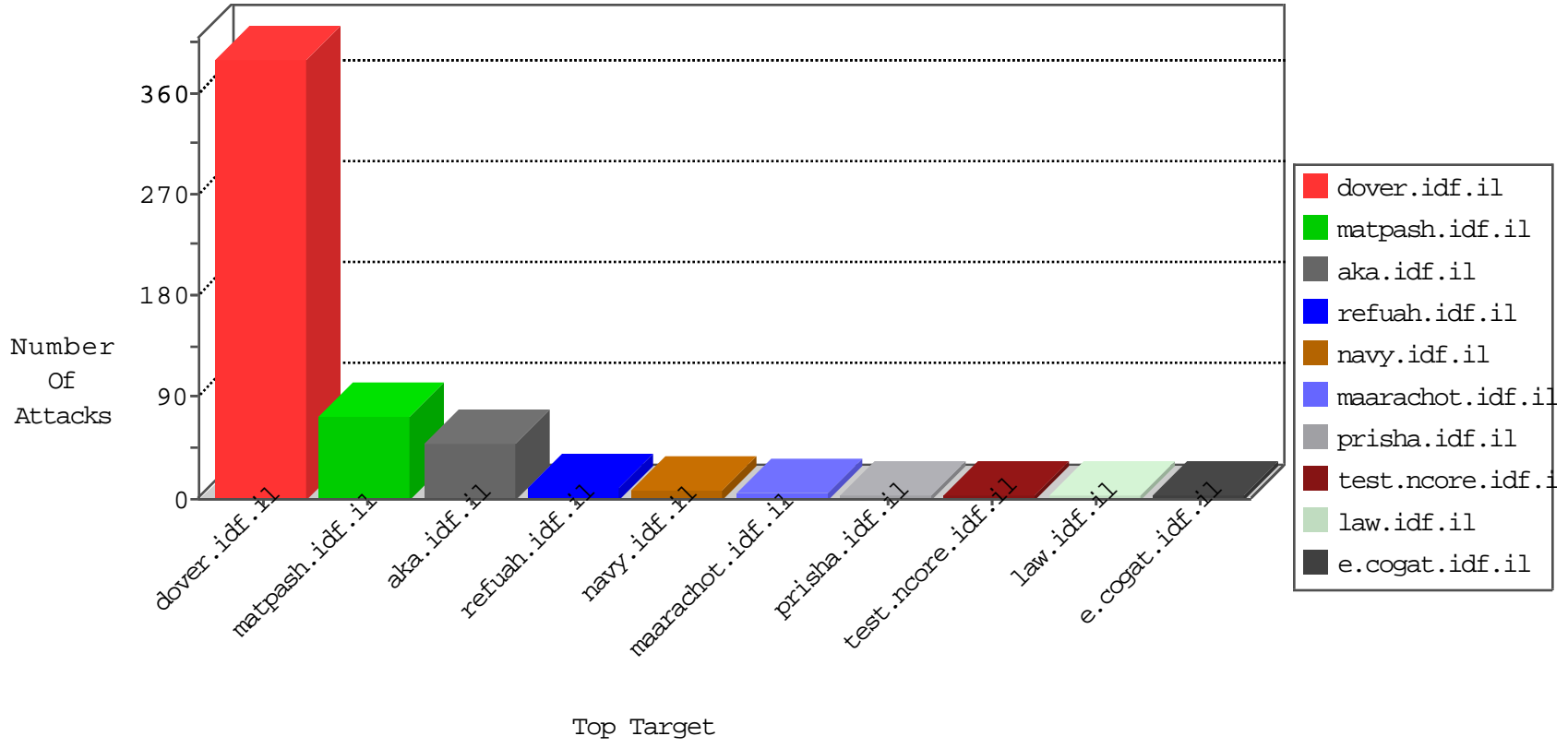
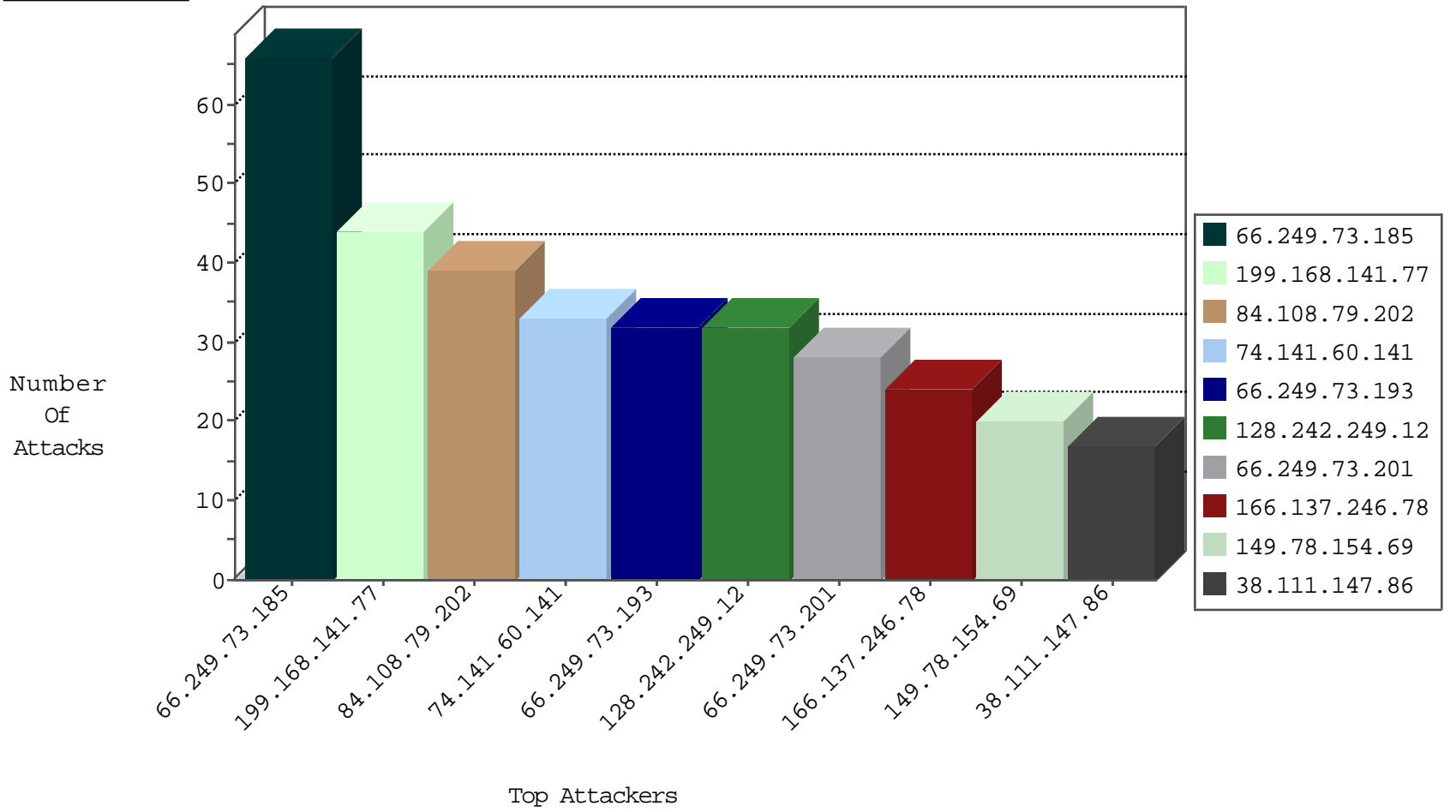




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.168	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	115
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	44
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
146.185.239.100	Russian Federation	147.237.0.34	tikshuv.idf.il	block-sp-trafl	drop	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
199.168.141.77	United States	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	35
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	32
199.168.141.77	United States	147.237.77.176	matpash.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
188.138.9.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
220.181.125.15	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.138.9.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
191.183.243.161	Brazil	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1

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	4
66.249.78.14	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.162	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
117.135.163.104	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -f -sS	1
104.128.144.130		147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
210.61.150.154	Taiwan	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
210.61.150.154	Taiwan	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
210.61.150.154	Taiwan	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
185.45.192.252	Seychelles	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.163.104	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
104.128.144.130		147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 3072	1
72.251.234.218	United States	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
210.61.150.154	Taiwan	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
210.61.150.154	Taiwan	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
1.192.129.232	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 4096	1
210.61.150.154	Taiwan	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
117.135.163.104	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
84.108.79.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
74.141.60.141	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	27
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
166.137.246.78	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
38.111.147.86	United States	147.237.72.166	aka.idf.il		drop	drop	17
41.196.79.106	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
173.252.88.182	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
74.141.60.141	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
67.84.76.182	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
93.173.177.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
173.252.88.184	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
173.252.88.180	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.139	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
194.90.66.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
173.252.88.186	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
199.168.141.77	United States	147.237.77.176	matpash.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	4
185.26.182.28	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
173.252.88.183	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
24.146.195.120	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
104.211.2.128		147.237.72.166	aka.idf.il	SAM rule	drop	drop	2
71.110.205.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.142.2.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.192	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.6	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
173.252.88.187	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
107.197.105.70	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.65.223	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
125.209.235.174	Korea, Republic of	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
80.246.130.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
213.57.109.176	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
173.252.88.185	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.52.50.237	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1
173.252.88.181	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.120.5.103	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
85.64.228.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
213.151.32.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.243	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
104.211.2.128		147.237.77.216	dover.idf.il	SAM rule	drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
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	6
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.32	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
199.168.141.77	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
67.84.76.182	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 67.84.76.182	Block	1
188.93.144.48	Netherlands	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
66.249.64.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
157.55.39.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/print_bottom.asp	Block	1
85.25.136.37	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/media/navy	Block	1
199.168.141.77	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/ckeditor/ckfinder/core/connector/asp/connector.asp	Block	1
46.116.207.106	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/main.asp	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
67.84.76.182	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/pazan/oded.stm	Block	1
188.165.15.14	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-welcome.stm	Block	1
66.249.67.92	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-6421-he/patzar.aspx	Block	1
157.55.39.123	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/pages/reports.aspx	Block	1
95.86.113.48	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.73.205	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listfaq/1942	Block	1
217.69.133.243	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
180.76.4.16	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
52.1.129.74	United States	147.237.77.170	maarachot.idf.il	URL is Above Root Directory maarachot.idf.il/..	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sachar/forms/downloadform.asp	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0125-1.stm	Block	1
188.165.15.176	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9824-he/refuah.aspx	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.236.19.214		147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	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
217.146.69.7	Estonia	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
180.76.4.168	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
65.55.210.96	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
199.168.141.77	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 199.168.141.77	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15466-he/dover.aspxxžxoxsx"	Block	1
109.66.173.17	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1258-he/refuah.aspx	Block	1
185.32.178.4	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.199	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
84.111.233.26	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	1
2.54.182.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sachar/forms/downloadform.asp	Block	1
125.209.235.174	Korea, Republic of	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1