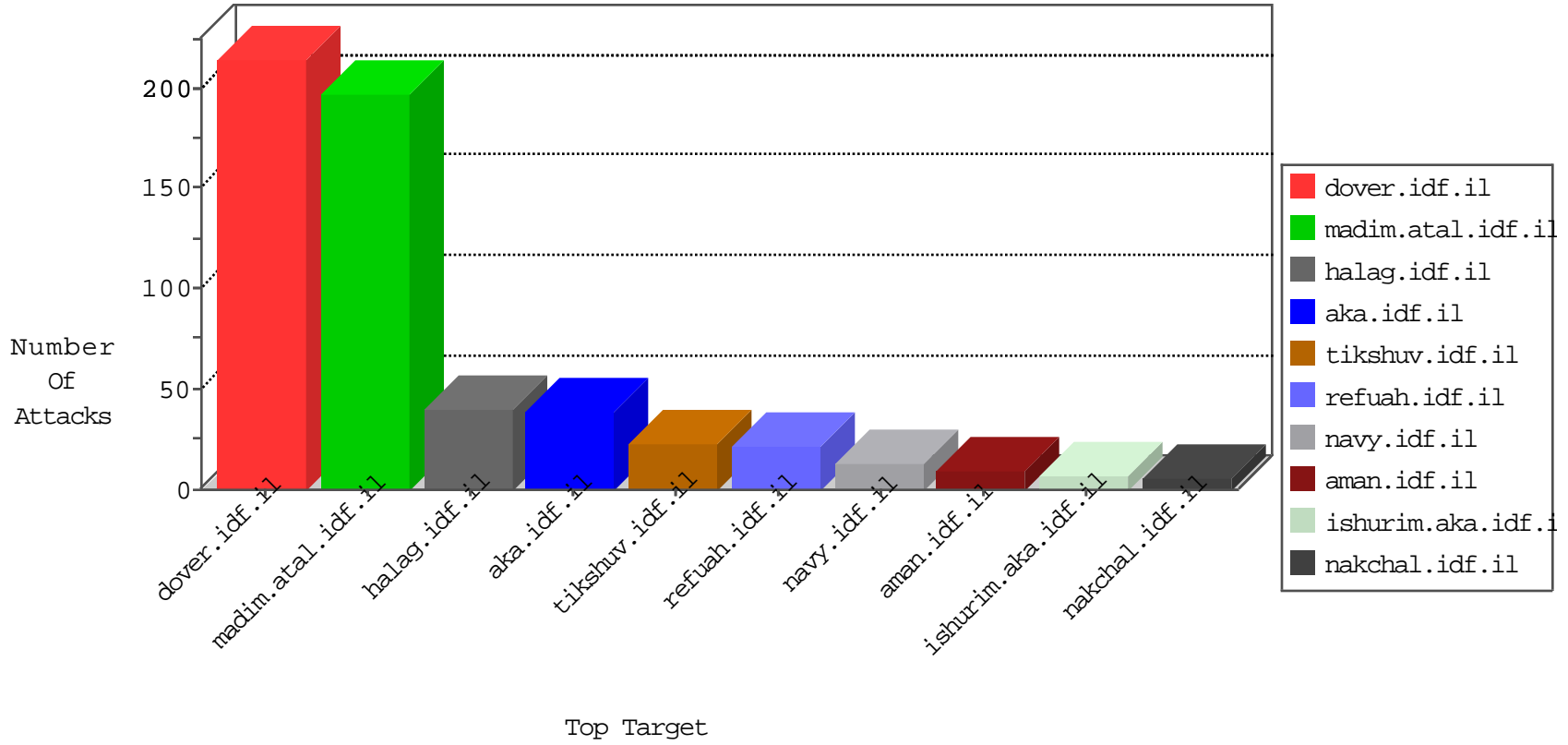
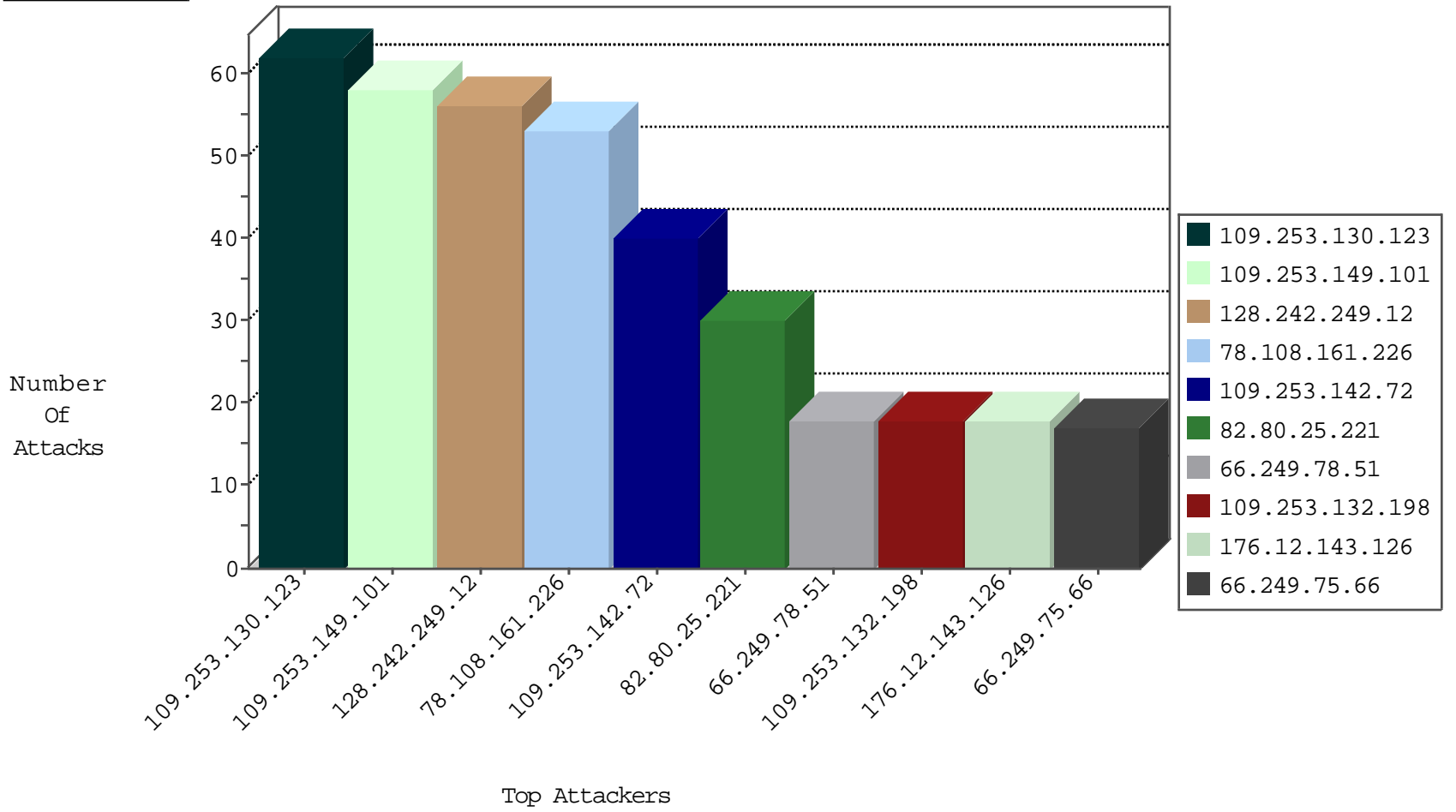


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
46.19.86.24	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
116.234.45.218	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	2
198.48.92.104	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	56
212.29.202.206	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
2.52.25.187	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.165.200	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	2
77.127.127.78	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
188.161.14.41	Palestinian Territory, Occupied	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	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
217.115.10.131	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
217.115.10.131	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.34	tikshuv.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	6
66.249.84.139	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.14	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
183.136.216.7	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
169.54.237.52	Switzerland	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
101.226.2.99	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
85.250.146.221	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.189.145	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.7	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.138.1	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.0.19	madim.atal.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
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	30
176.12.143.126	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.75.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
66.249.75.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
176.12.141.18	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
78.108.161.226	Lebanon	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	12
78.108.161.226	Lebanon	147.237.77.234	halag.idf.il	First packet isn't SYN	drop	drop	12
77.127.127.78	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	8
78.108.161.226	Lebanon	147.237.76.86	navy.idf.il	First packet isn't SYN	drop	drop	8
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.75.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
192.12.88.242	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.136.24	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
93.172.13.254	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	5
78.108.161.226	Lebanon	147.237.76.42	refuah.idf.il	First packet isn't SYN	drop	drop	5
46.120.242.134	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
66.249.64.92	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
109.253.130.26	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
78.108.161.226	Lebanon	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	3
78.108.161.226	Lebanon	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	3
109.253.132.106	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	2
80.246.138.212	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
199.30.25.232	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
80.246.138.212	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
98.143.148.107	United States	147.237.76.198	e.yohalan.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
46.19.85.136	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
46.19.86.24	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
213.204.127.33	Lebanon	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
46.120.242.134	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
46.19.85.136	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
80.246.138.212	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
2.54.180.233	Israel	147.237.72.167	ishurim.aka.idf.il		Bad TCP sequence	monitor	2
46.19.86.104	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
216.218.206.80	United States	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
61.160.247.153	China	147.237.76.200	eitan.aka.idf.il		drop	drop	1
2.54.180.233	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.19.86.151	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.123	United States	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
2.54.180.233	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
213.204.127.33	Lebanon	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.175	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
184.105.247.203	United States	147.237.0.35	akaws.idf.il		drop	drop	1
108.160.148.98	United States	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.130.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	62
109.253.149.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	58
109.253.142.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
109.253.132.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
109.253.138.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
109.253.157.139	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.157.139	Block	7
109.253.145.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
66.249.75.74	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.74	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
66.249.75.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.66	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
164.138.121.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	2
109.160.240.245	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
176.12.148.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.89.118.108	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1010-1.stm	Block	1
85.64.149.76	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTARGUMENT in aka.idf.il/main/sachar/	None	1
66.249.69.36	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/netunim.stm.	Block	1
109.253.130.26	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
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
109.253.142.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.55.19	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
208.113.198.126	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/old/wp-admin/	Block	1
61.135.190.69	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
86.47.80.147	Ireland	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/modiin/default.aspx	Block	1
66.249.75.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
46.19.86.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.127.78	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
216.218.147.196	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ie-welcome.stm	Block	1
66.249.69.2	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
108.160.148.98	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/"	Block	1
66.249.75.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//894-he	Block	1
176.12.140.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.89.118.108	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
84.111.185.46	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.69.32	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-8434-he/dover.aspx	Block	1