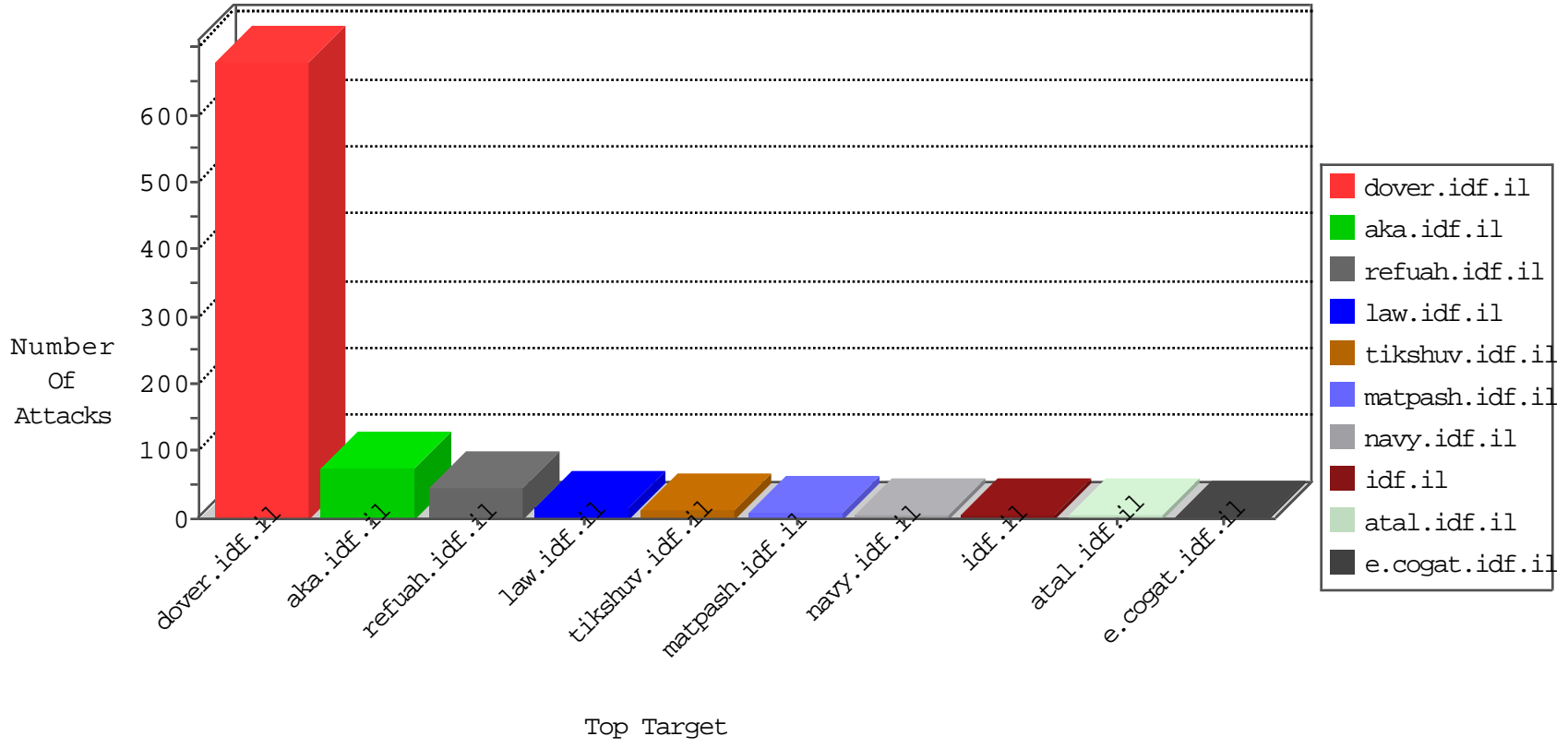
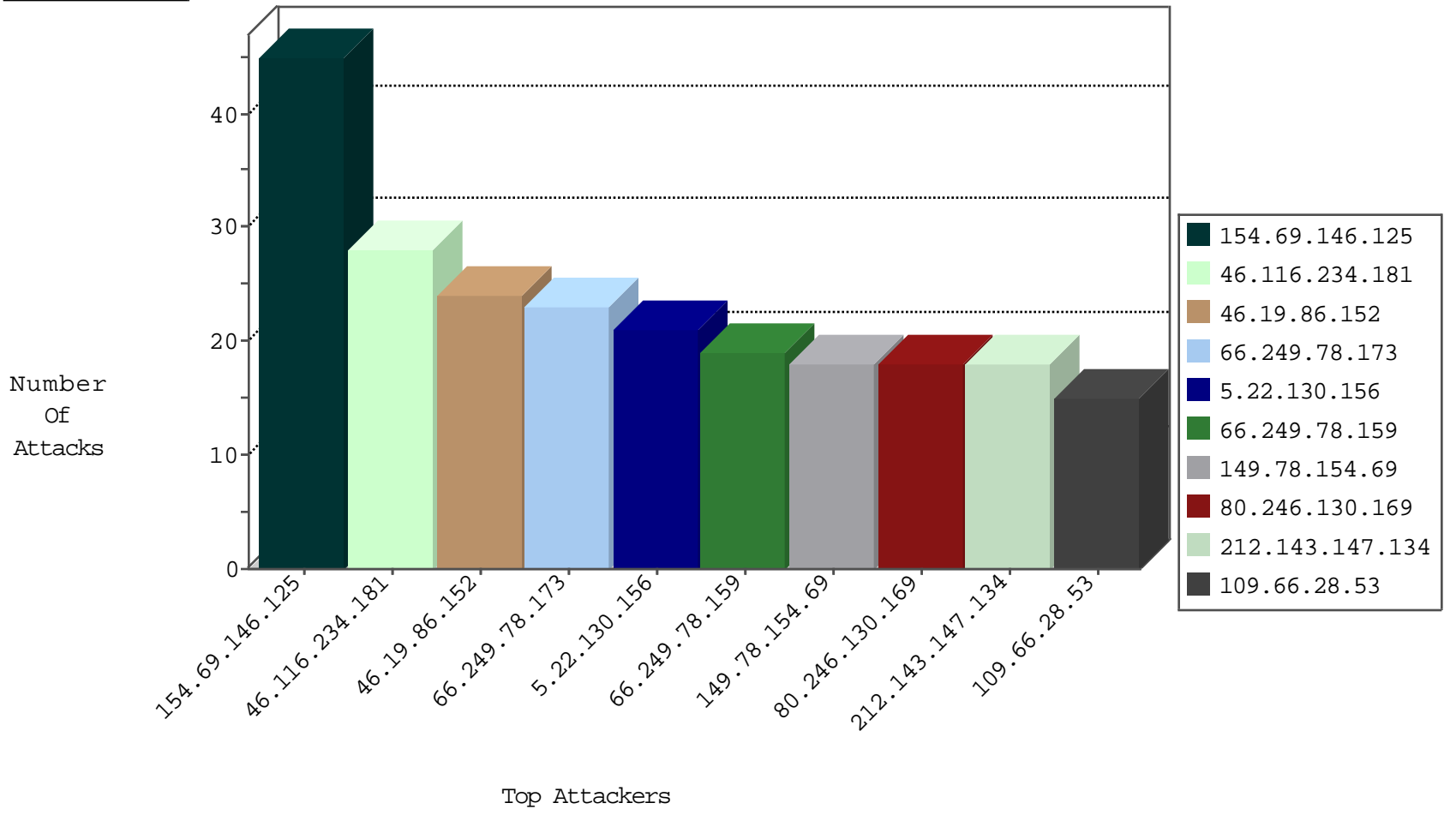




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4704
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2555
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	608
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	87
212.143.147.134	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
46.19.86.152	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
109.66.28.53	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
212.143.147.134	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
37.26.147.229	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
109.67.159.231	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
46.19.86.26	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
195.37.190.86	Germany	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
2.54.22.55	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
85.64.136.134	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.86.26	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
195.37.190.86	Germany	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
2.54.22.55	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.116.234.181	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
92.97.207.238	United Arab Emirates	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
131.72.136.11		147.237.77.243	mobile.idf.il	EgovRep_B-N_70-99	Block	1
79.253.3.212	Germany	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	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
2.52.1.112	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
206.82.22.116	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.198	e.ychalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
109.66.140.70	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	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	7610: IP Reputation	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	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
109.66.146.94	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	7610: IP Reputation	Block	1
66.240.192.138	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
87.68.213.104	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	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.177	ncore.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	3
79.177.56.54	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
185.75.56.44		147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.145.87	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
85.64.136.134	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.221.156	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
82.103.128.88	Denmark	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
67.159.16.3	United States	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.3	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
109.253.135.52	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.223.231	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
82.103.128.88	Denmark	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	1
46.117.205.160	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.6.132.45	China	147.237.77.178	e.matpash.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
154.69.146.125	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
5.22.130.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
80.246.130.169	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
46.116.234.181	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	18
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
50.201.125.63	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
46.19.86.152	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	9
46.19.86.152	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
212.76.127.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
212.179.21.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
54.224.21.23	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
5.28.178.110	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
86.144.3.22	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.176.105.80	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
80.246.130.98	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.67.37.36	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
84.228.221.156	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
46.117.205.160	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
84.228.221.156	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
85.64.76.69	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
109.65.48.200	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	6
2.239.24.189	Italy	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.116.74.193	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.93.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
149.78.177.78	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
37.26.147.148	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
2.52.33.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
84.108.188.117	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
95.86.121.112	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	5
93.94.40.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
24.104.66.174	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
109.65.48.200	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	5
82.102.240.4	Palestinian Territory, Occupied	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
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
2.52.137.9	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	4
154.69.146.125	South Africa	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
109.64.109.98	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
46.116.234.181	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
92.231.230.220	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.76.127.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.66	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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.186.180.206	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
80.246.130.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.178.231.73	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.176.37.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.75.117	Block	2
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.177.51.172	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmi	Block	1
157.55.39.158	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
46.116.234.181	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/kkkkkkk=44a4b8f5kkkkkkk_44a4b8f5	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16054-en/dover.asp	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluilml/	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.137.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
93.84.52.85	Belarus	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1283-17607-en/dover.aspx	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18590-he/dover.aspx	Block	1
157.55.39.192	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.192	Block	1
112.64.235.91	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.116.234.181	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
81.218.48.37	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
180.76.4.204	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
68.180.228.167	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.79.249.71	Russian Federation	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/14-en/patzar.aspx	Block	1
95.86.75.112	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
79.179.9.78	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
212.179.144.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.78.125	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/565-he/patzar.aspx	Block	1
157.55.39.222	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/unselecatble.aspx	Block	1
149.88.76.8	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
62.90.143.57	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.54.254	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
188.138.17.205	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
77.125.126.64	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
37.142.153.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giys	Block	1
109.65.48.200	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
79.180.204.117	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 79.180.204.117	Block	1
213.151.53.90	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
157.55.39.248	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/general/	Block	1
66.249.78.133	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
150.70.173.45	Japan	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
62.90.143.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giys	Block	1
84.228.184.237	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
198.154.184.254	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-10015-en	Block	1