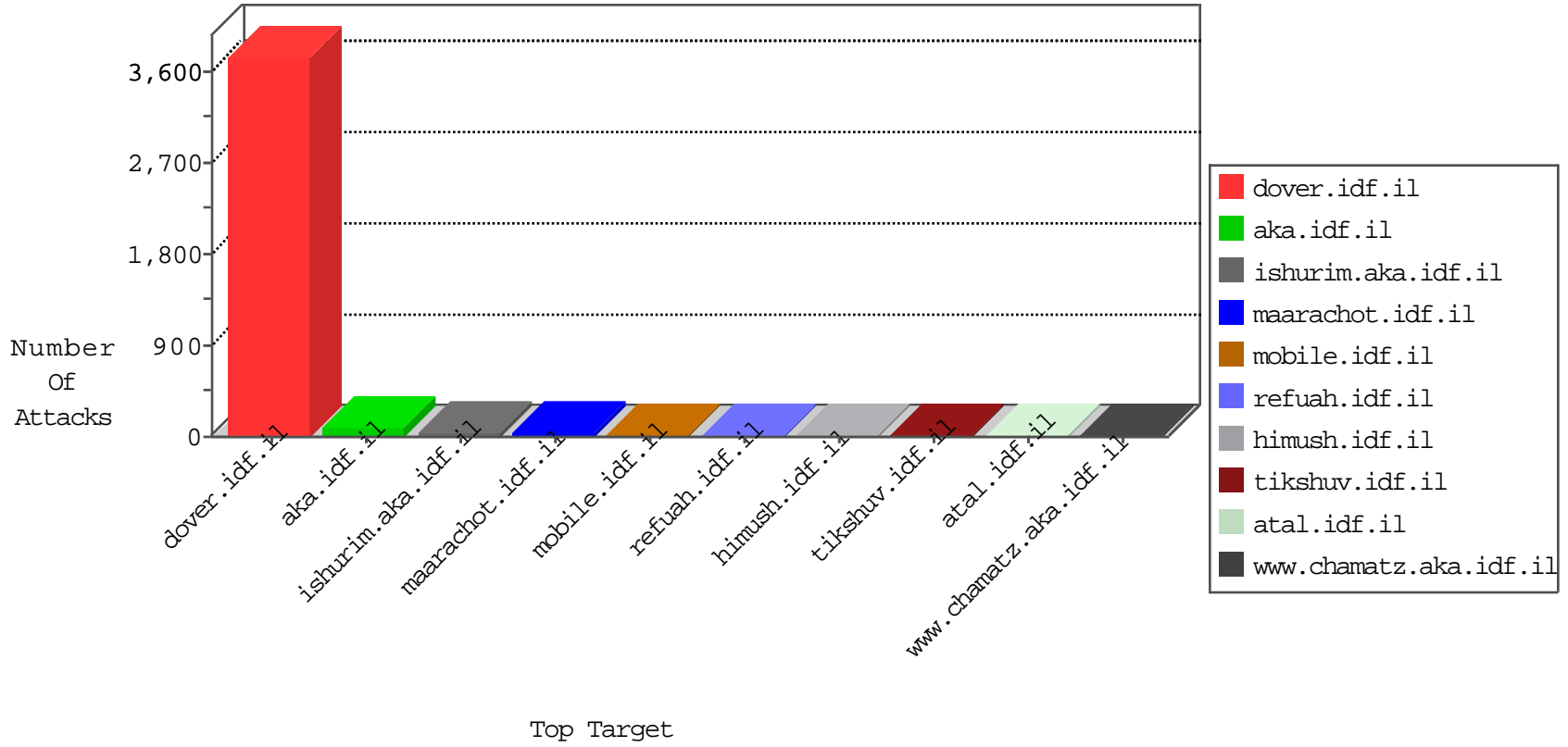
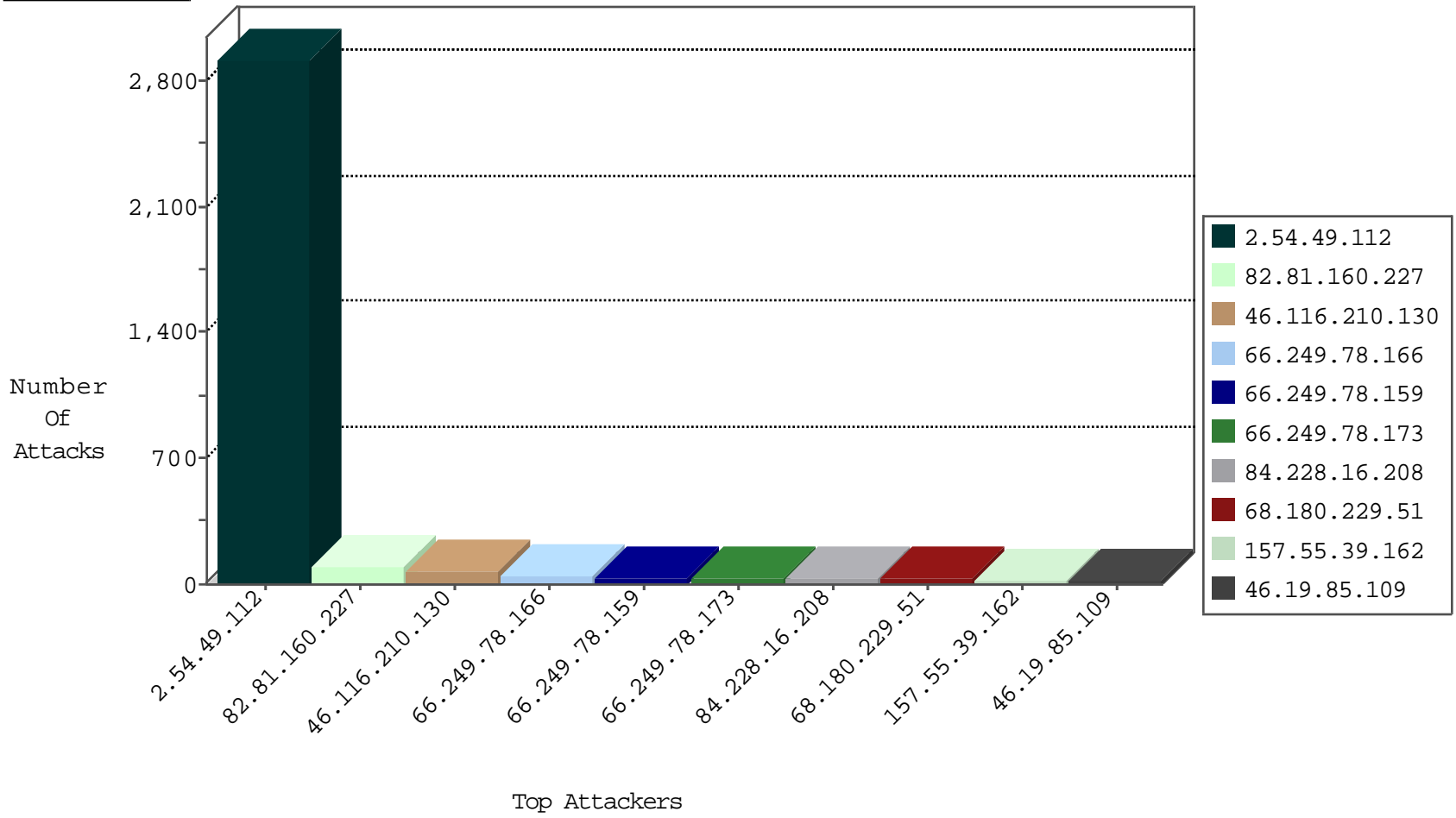




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
84.228.16.208	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	267
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
204.42.253.132	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
61.165.201.21	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
195.142.179.50	Turkey	147.237.77.216	dover.idf.il	12373: HTTP: WordPress admin Login	Block	4
46.19.85.143	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.116.210.130	Israel	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	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	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
46.166.186.237	Netherlands	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.148	ggcenter.aka.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
93.120.27.62	Romania	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.42	refuah.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	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1
71.6.167.142	United States	147.237.76.199	e.nakchal.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	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
87.69.191.205	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	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
186.158.218.212	Argentina	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
79.180.162.53	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	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
92.253.21.242	Jordan	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
130.211.183.28		147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.81.136	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
217.132.213.111	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
112.84.178.36	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
157.7.237.231	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.67	China	147.237.77.74	law.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
116.228.152.154	China	147.237.76.42	refuah.idf.il	ET DROP Dshield Block Listed Source	1
61.240.144.64	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
116.121.137.2	Korea, Republic of	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.158.162.40	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
221.235.205.123	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
116.121.137.2	Korea, Republic of	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
61.158.162.40	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
116.121.137.2	Korea, Republic of	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
112.84.178.36	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
162.248.10.134	Canada	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.9.56.243	Germany	147.237.76.42	refuah.idf.il	Tehila - Perl LWP with fake user agent	1
112.84.178.36	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
157.7.237.231	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
112.84.178.36	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
157.7.237.231	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.77.205	prisha.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
121.46.0.125	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.67	China	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
116.121.137.2	Korea, Republic of	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
116.121.137.2	Korea, Republic of	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
221.235.205.123	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.158.162.40	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
116.121.137.2	Korea, Republic of	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
196.41.123.120	South Africa	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
112.84.178.36	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
162.248.10.134	Canada	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
60.18.162.244	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
112.84.178.36	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
162.248.10.134	Canada	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -f -sS	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.49.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2792
82.81.160.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	96
46.116.210.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	68
2.54.49.112	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	42
2.54.49.112	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	42
2.54.49.112	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	42
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
93.173.4.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
85.64.210.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
109.64.43.52	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	17
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
82.145.210.28	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
69.121.142.251	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
2.52.61.167	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
157.55.39.162	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
213.57.42.90	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
87.68.246.107	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
94.230.86.212	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
79.180.117.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	9
209.133.111.211	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
176.12.139.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
82.145.223.43	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
108.29.0.76	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
37.73.221.244	Ukraine	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
5.29.69.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
66.249.64.178	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
84.109.5.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
58.178.137.50	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
5.29.55.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.64.178	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
84.143.215.196	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
85.65.84.220	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
93.172.53.249	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
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	5
130.211.183.28		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fr&	Block	3
5.9.56.243	Germany	147.237.76.42	refuah.idf.il	PHP Attempt	Block	3
109.65.52.69	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
85.64.119.110	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to ww.aka.idf.il/https://www.aka.idf.il/	Block	2
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
138.134.102.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/atal1/izkor/view_pictures.asp	Block	1
46.121.195.214	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.124	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
109.186.173.134	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.81.239	Israel	147.237.76.30	himush.idf.il	URL is Above Root Directory ww.himush.atal.idf.il/./favicon.ico	Block	1
184.56.116.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/030.stm	Block	1
66.249.65.1	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/speakerofmatpash/pages/summaryofgazainternationalorganizations.aspx	Block	1
37.142.11.120	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.43.52	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
216.218.206.66	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
52.17.71.65	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.161	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
130.211.183.28		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 130.211.183.28	Block	1
80.246.133.112	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.99	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0326-2.stm	Block	1
66.249.67.218	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1236-he/refuah.aspx	Block	1
38.99.96.162	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	1
130.211.183.28		147.237.77.216	dover.idf.il	Multiple signatures from 130.211.183.28	Block	1
2.54.144.158	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.109.244.159	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
188.165.15.117	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/news/www.idf.il/mivtza	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
46.19.86.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
109.160.184.175	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.240	Block	1
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/catalog.asp	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to ww.aka.idf.il/sachar/faq.aspx	Block	1
130.211.183.28		147.237.77.216	dover.idf.il	PHP Attempt	Block	1
5.9.56.243	Germany	147.237.76.42	refuah.idf.il	CVE-2014-8770: MAGMI Unauthorized File Upload	Block	1
85.64.94.191	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
188.165.15.230	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8675-he/refuah.aspx	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
46.117.248.136	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/matash	Block	1
109.160.184.175	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 109.160.184.175	None	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
176.12.145.222	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.64.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1