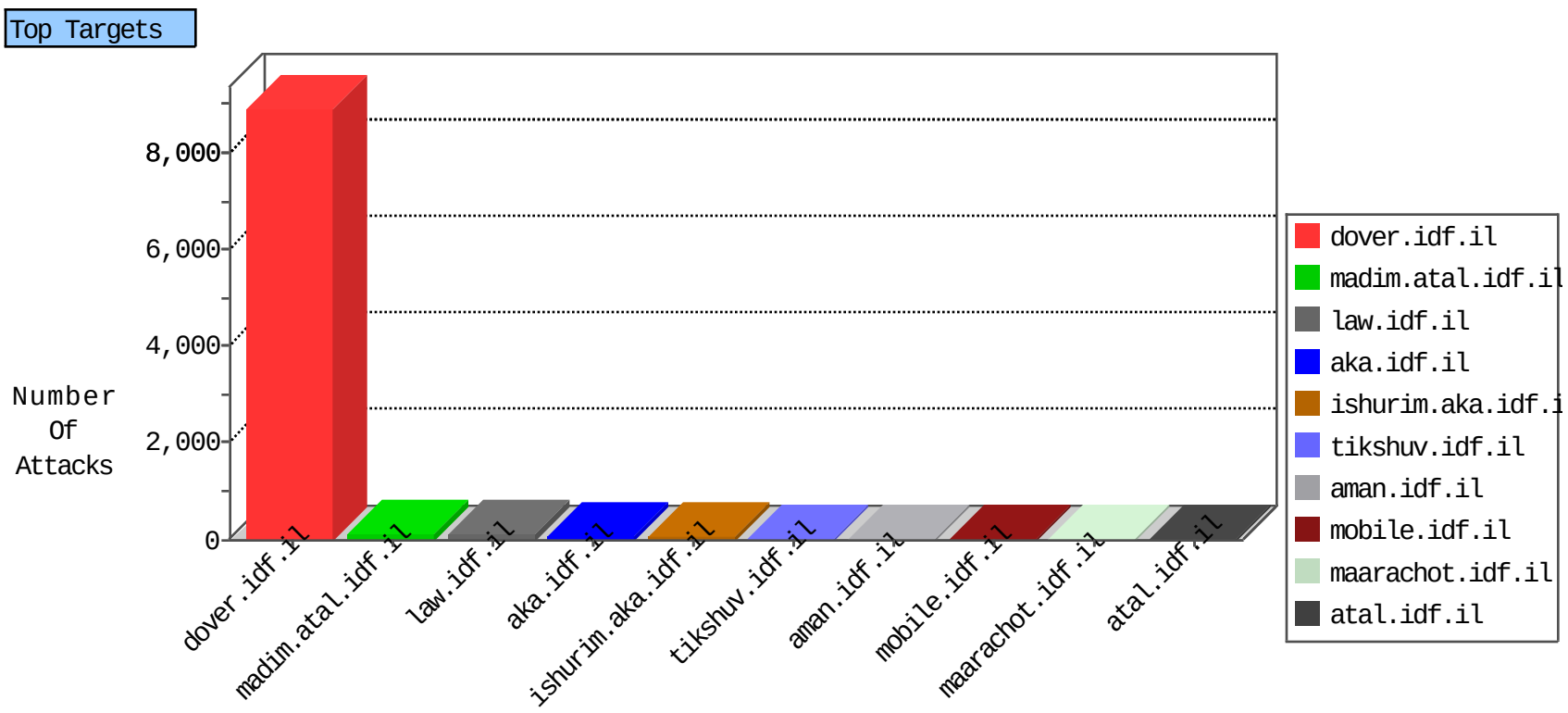
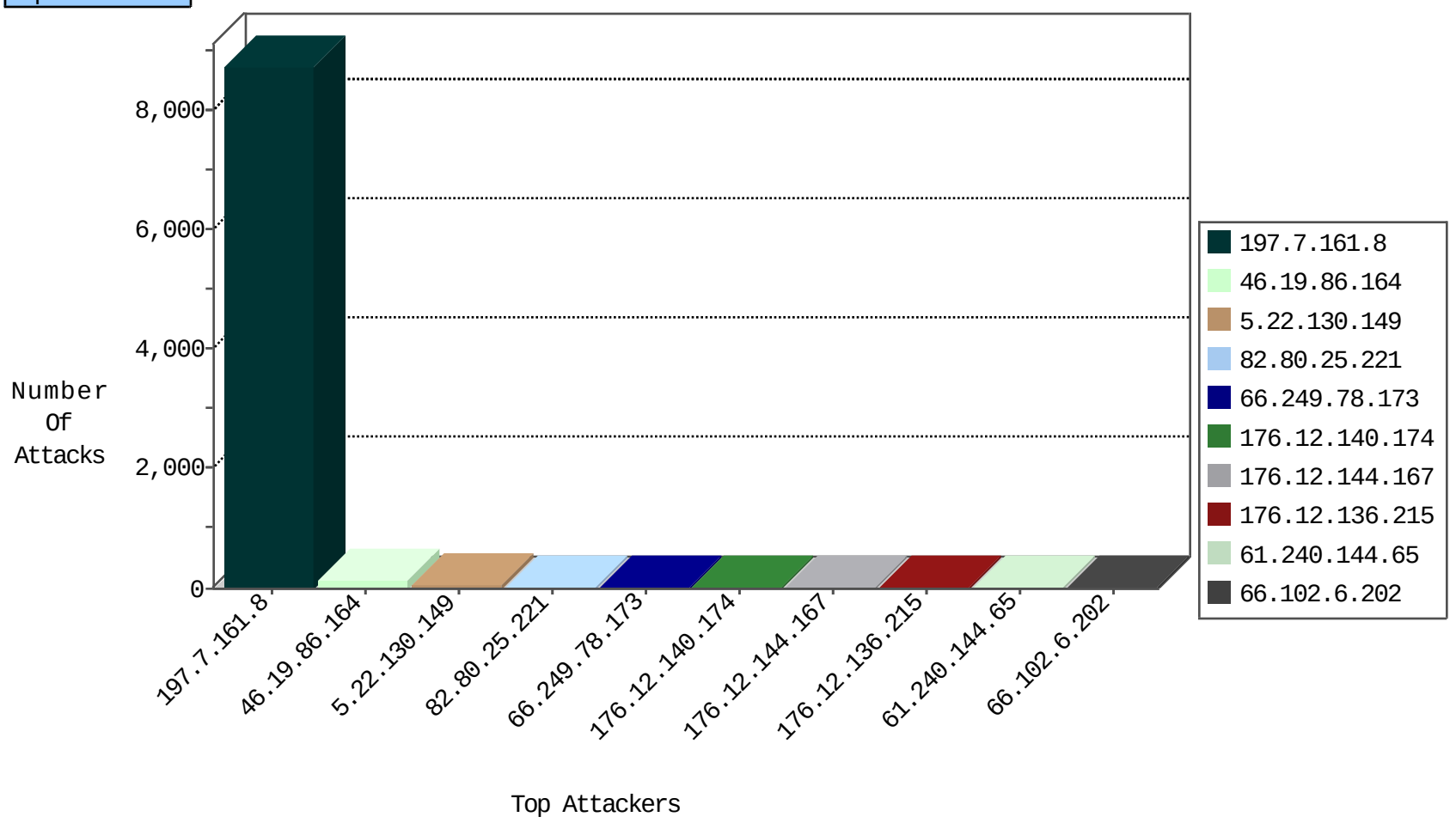
03-28-2015-20:03:04 to 03-28-2015-21:03:04

IDF Under Attack
03-28-2015-20:03:04

Top Targets



Top Attackers



03-28-2015-20:03:04 to 03-28-2015-21:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count

03-28-2015-20:03:04 to 03-28-2015-21:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.182.187.217	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
84.153.66.198	Germany	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
31.223.188.113	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.153.66.198	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.125.87.37	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

03-28-2015-20:03:04 to 03-28-2015-21:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
5.22.130.149	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
80.246.133.80	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
194.114.146.227	Israel	147.237.72.167	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
80.246.133.237	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.125.223.164	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.170	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
218.50.2.105	Korea, Republic of	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
41.231.53.25	Tunisia	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
218.50.2.105	Korea, Republic of	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	United States	147.237.76.148	gqcenter.aka.idf.il	ET DROP Dshield Block Listed Source	1
41.231.53.25	Tunisia	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
41.231.53.25	Tunisia	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
131.104.106.84	Canada	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.170	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
218.50.2.105	Korea, Republic of	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
41.231.53.25	Tunisia	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
211.138.34.58	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
41.231.53.25	Tunisia	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
41.231.53.25	Tunisia	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
111.203.22.56	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.170	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1

03-28-2015-20:03:04 to 03-28-2015-21:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il		drop	drop	2843
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il	SAM rule	drop	drop	2473
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2270
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il	Data received before SYN-ACK was acknowledged. Stripping all packet data.	Streaming Engine: TCP SYN Modified Retransmission	drop	441
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	150
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	146
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il		Bad TCP sequence	monitor	105
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	26
5.22.130.149	Israel	147.237.72.167	ishurim.aka.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	23
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
176.12.144.167	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.136.215	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
5.22.130.149	Israel	147.237.72.167	ishurim.aka.idf.i	First packet isn't SYN	drop	drop	12
176.12.140.174	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il	Anonymous DoSer Denial of Service Tool	Web Server Enforcement Violation	reject	12
66.102.6.202	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.140.234	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
217.132.108.246	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	7
188.120.148.135	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
66.102.6.194	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.186.228.68	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.64	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	6
176.12.151.191	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.186.228.31	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.27	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.186.228.67	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	6
109.253.129.154	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.186.228.57	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.92	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	5
5.22.130.149	Israel	147.237.72.167	ishurim.aka.idf.i	SYN retransmit with different window scale	Bad TCP sequence	alert	5
31.210.186.139	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	5
5.102.254.171	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
31.186.228.94	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	4
132.66.231.57	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	4
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il	Network quota was exceeded	Network Quota Violation	monitor	4
31.186.228.58	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.134	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
89.138.200.219	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
31.186.228.30	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.95	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.86	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.59	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	4
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il	Unexpected post SYN packet - RST or SYN expected	drop	drop	4
37.247.36.83	Netherlands	147.237.76.197	e.himush.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
46.19.85.105	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
31.186.228.23	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.61	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.93	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.62	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	205
46.19.86.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	130
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	4
2.54.55.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	4
207.46.13.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.16	Block	3
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il	Multiple Malformed URL from 197.7.161.8	Block	3
194.114.146.227	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Untraceable SSL Sessions from 194.114.146.227 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	2
79.180.111.203	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.183.37.122	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	2
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	2
87.69.1.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.65.13.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
77.126.40.235	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/home.aspx	None	1
176.12.150.62	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
54.145.180.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/iaf/present2.stm	Block	1
93.172.153.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.13.110.122	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
198.20.69.74	United States	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.78.109	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.109	Block	1
188.165.15.176	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9773-he/refuah.aspx	Block	1
37.26.147.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
132.66.231.57	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
85.65.228.31	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
77.127.126.143	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/default.aspx	None	1
176.12.151.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
62.212.82.33	Netherlands	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
31.23.6.114	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
95.58.129.135	Kazakstan	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
198.20.69.74	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
79.182.171.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-15693-he/dover.aspx	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	1
38.107.189.136	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
145.255.161.143	Kazakstan	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
85.250.24.38	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
2.52.38.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/statistics/gens.stm	Block	1
197.7.161.8	Tunisia	147.237.77.216	dover.idf.il	Malformed URL are	Block	1
77.127.126.143	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/forgotpassword.aspx	None	1
176.12.151.235	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
62.212.82.33	Netherlands	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
31.129.117.199	Ukraine	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
95.86.81.88	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
190.232.28.2	Peru	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/documents.asp	Block	1
46.19.86.116	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication	Block	1
85.250.87.207	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
77.237.138.51	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
178.120.153.132	Belarus	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.64.141	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-7237-he/atal.aspx	Block	1