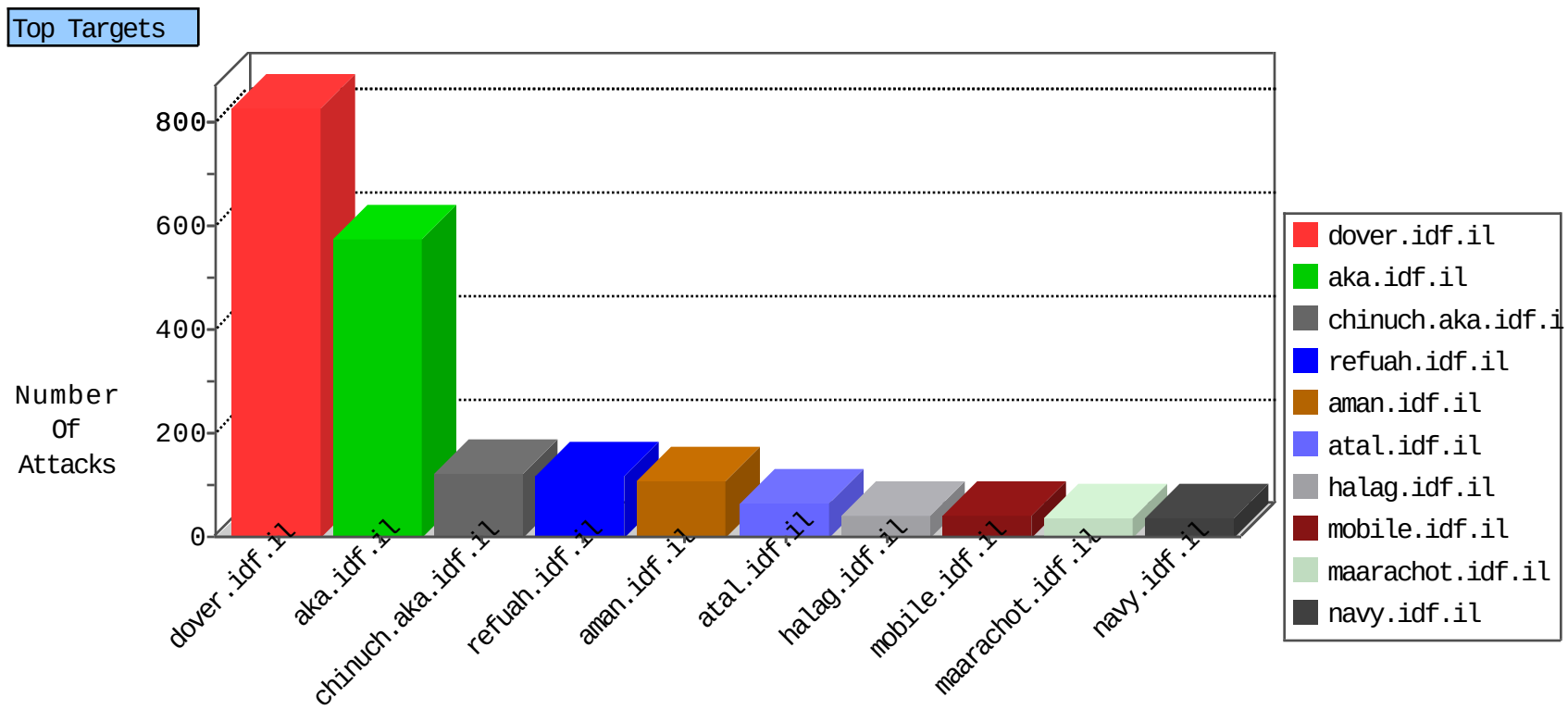
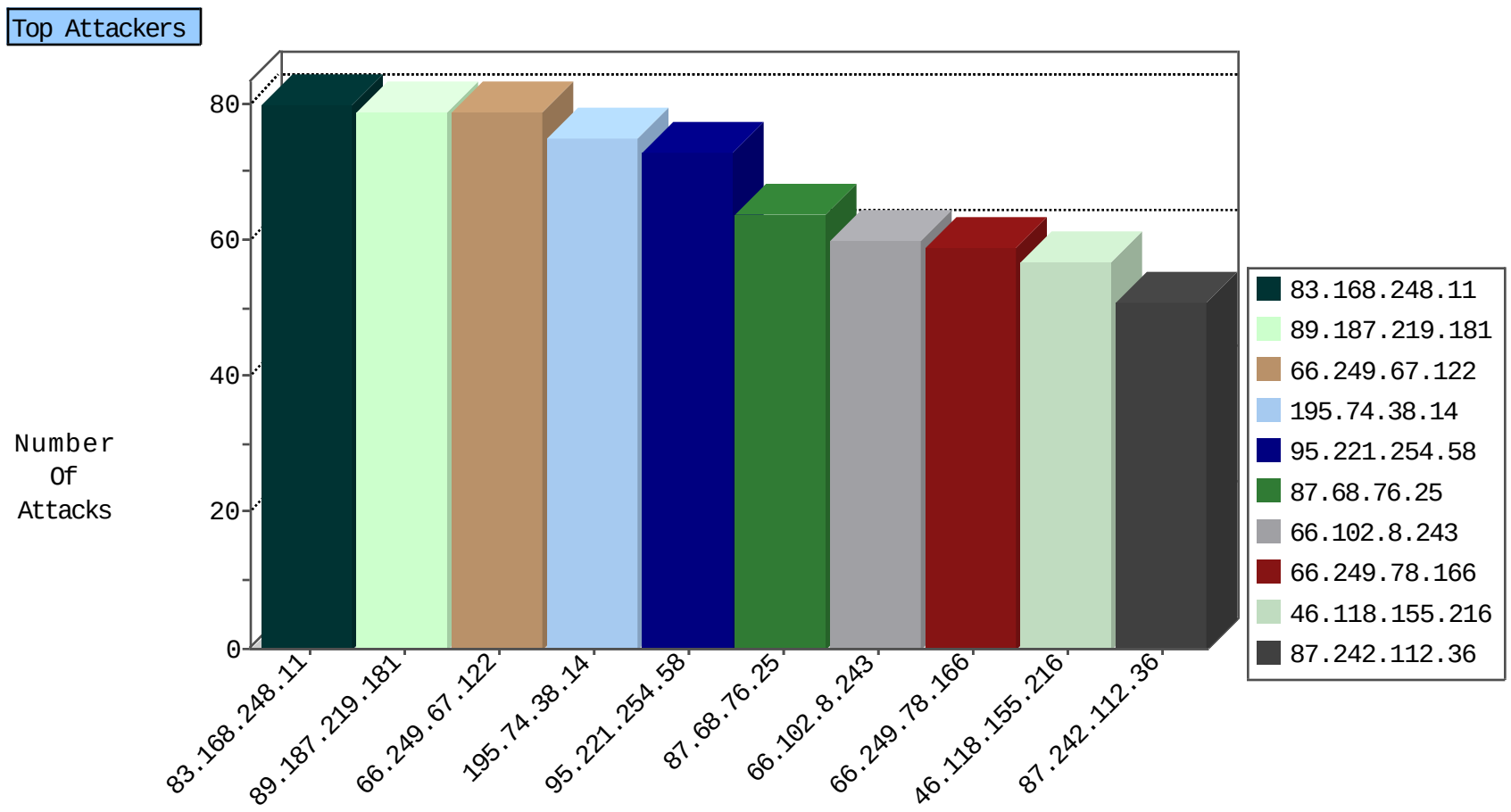
10-31-2015-02:04:05 to 10-31-2015-03:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-31-2015-02:04:05 to 10-31-2015-03:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4866
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3246
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3058
66.249.69.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2575
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	773
220.181.108.93	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	255
50.116.30.23	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	61
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	5
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
85.250.3.123	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
66.103.79.166	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
181.166.222.246	Argentina	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.102.8.237	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-31-2015-02:04:05 to 10-31-2015-03:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.168.248.11	Sweden	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	20

10-31-2015-02:04:05 to 10-31-2015-03:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
83.168.248.11	147.237.72.166	Sweden	aka.idf.il	SQL Injection - Select From	60
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.84.67	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.75.106	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
37.49.226.136	147.237.0.19	Netherlands	madim.atal.idf.i	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.76.42	United States	refuah.idf.il	ET DROP Dshield Block Listed Source	1
98.102.200.172	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
58.253.96.122	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
37.49.226.136	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
201.191.71.86	147.237.76.31	Costa Rica	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-31-2015-02:04:05 to 10-31-2015-03:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
95.221.254.58	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
89.187.219.181	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
66.102.8.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
93.80.91.58	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
2.92.219.149	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
2.92.137.32	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
66.102.8.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.78.51	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
63.234.66.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
195.74.38.14	Sweden	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
195.74.38.14	Sweden	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	22
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
95.215.227.115	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
87.242.112.36	Russian Federation	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
173.68.157.64	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.65.42.61	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
40.77.167.37	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
73.161.45.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
157.55.39.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
95.25.195.146	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.176.23.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.67.41	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.187.191	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.127.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.137.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
220.255.97.166	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.8.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.44	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
199.30.24.183	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.8.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.221.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.8.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
65.130.210.195	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
181.166.222.246	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
65.55.210.22	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

10-31-2015-02:04:05 to 10-31-2015-03:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.67.122	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.64.75	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.122	Block	45
87.68.76.25	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation searchText in www.atal.idf.il/1367-he/atal.aspx	Block	45
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	45
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	30
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	30
66.249.78.128	Israel	147.237.76.147	chinuch.aka.idf.i	Suspicious Response Code_Custom_Temporary	Block	30
176.12.137.35	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
66.249.78.59	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1149-he/chinuch.aspx	Block	15
95.215.227.115	United Kingdom	147.237.72.166	aka.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	15
87.68.76.25	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.6	Block	15
66.249.78.135	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to chinuch.aka.idf.il/404.htm	Block	15
149.78.25.181	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	15
66.249.67.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim1/maind9ea.html	Block	15
94.245.88.217	United Kingdom	147.237.72.166	aka.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	15
66.249.78.66	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15
177.81.248.152	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	15
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/112327.pdf	Block	15
95.215.227.115	United Kingdom	147.237.72.166	aka.idf.il	Multiple signatures from 95.215.227.115	Block	15
87.242.112.36	Russian Federation	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/925-he/chinuch.aspx	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	15
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/giyus/qanda/default.asp	None	15
66.249.75.70	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	15
94.245.88.217	United Kingdom	147.237.72.166	aka.idf.il	Multiple signatures from 94.245.88.217	Block	15
64.14.68.11	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	15
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/62532.pdfg2=whvq9jgvov3igm-oflegda	Block	15
66.249.78.121	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on chinuch.aka.idf.il/404.htm	Block	15
195.74.38.14	Sweden	147.237.72.156	aman.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
96.30.50.236	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	15
87.242.112.36	Russian Federation	147.237.72.166	aka.idf.il	Multiple signatures from 87.242.112.36	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	15
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/displayallsoldiers.asp	None	15
66.249.78.4	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list1.htm	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
94.245.88.250	United Kingdom	147.237.72.166	aka.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	15
66.249.64.190	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums.frm/frmuserdetails.aspx	Block	15
66.249.78.128	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on chinuch.aka.idf.il/404.htm	Block	15
195.74.38.14	Sweden	147.237.72.156	aman.idf.il	Multiple signatures from 195.74.38.14	Block	15
109.65.42.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	15
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
94.245.88.135	United Kingdom	147.237.72.166	aka.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
37.230.106.78	Turkey	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	15