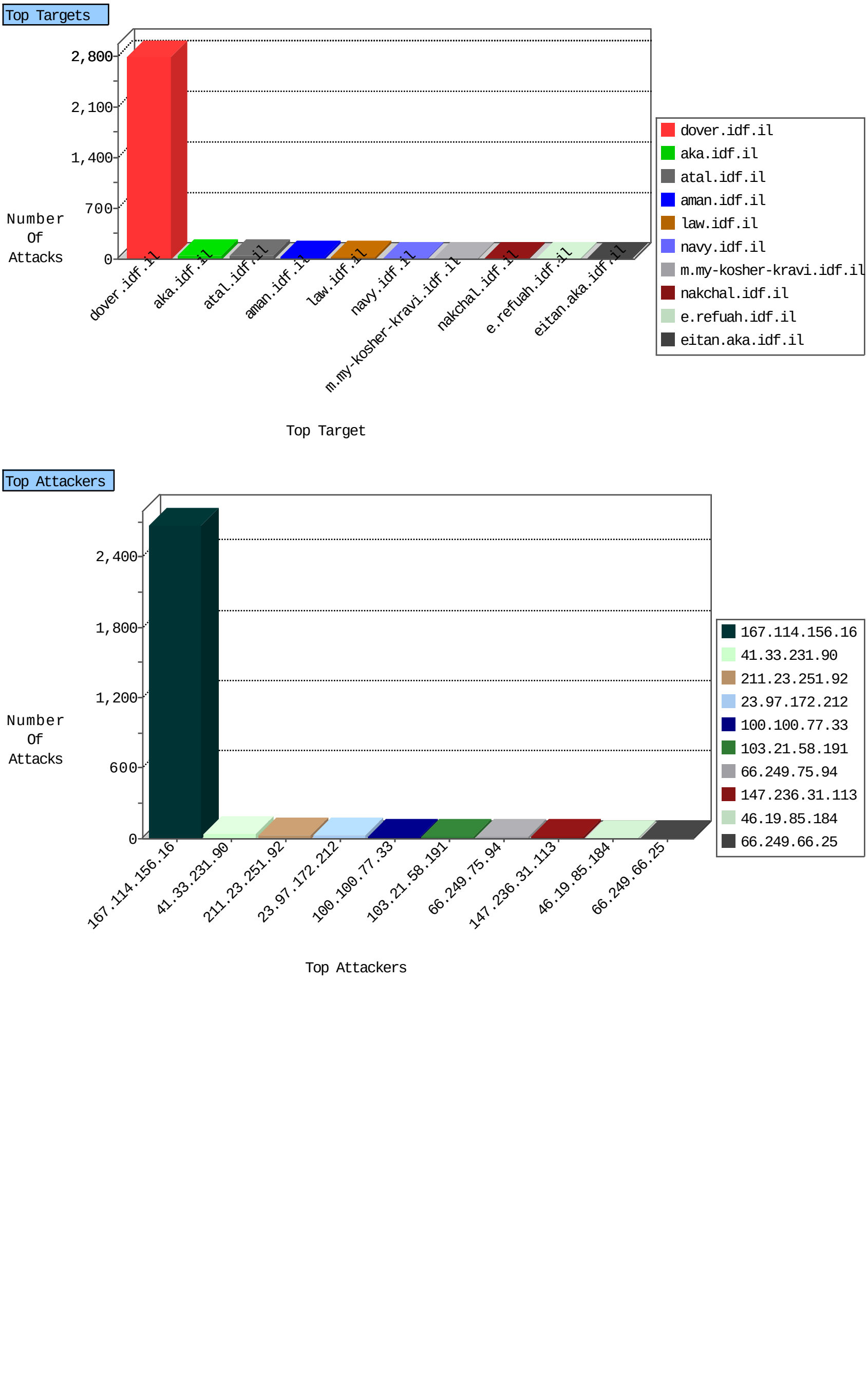
12-01-2015-05:04:08 to 12-01-2015-06:04:08

IDF Under Attack Daily Report



12-01-2015-05:04:08 to 12-01-2015-06:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3375
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	233
115.230.124.164	China	147.237.76.176	test.ncore.idf.i	JLM_Under_Attack_Con_Tcp	drop	2
202.112.51.96	China	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
93.158.203.169	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.106.92.7		147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
185.106.92.7		147.237.76.38	e.e.meitav.idf.i	Block_Ntp_All_Net	drop	1
125.175.19.197	Japan	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

12-01-2015-05:04:08 to 12-01-2015-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
103.21.58.191	India	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
211.23.251.92	Taiwan	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	7
59.120.255.127	Taiwan	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1

12-01-2015-05:04:08 to 12-01-2015-06:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
211.23.251.92	147.237.77.233	Taiwan	atal.idf.il	SQL Injection - Select From	21
103.21.58.191	147.237.77.74	India	law.idf.il	SQL Injection - Select From	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
59.120.255.127	147.237.77.233	Taiwan	atal.idf.il	SQL Injection - Select From	3
150.164.225.30	147.237.76.202	Brazil	e.halag.idf.il	ET SCAN Potential SSH Scan	1
23.92.216.183	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
150.164.225.30	147.237.76.177	Brazil	ncore.idf.il	ET SCAN Potential SSH Scan	1
150.164.225.30	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
149.202.186.50	147.237.76.31	Germany	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
119.247.127.191	147.237.76.197	Hong Kong	e.himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.240.250.155	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
61.130.145.216	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
150.164.225.30	147.237.77.216	Brazil	dover.idf.il	ET SCAN Potential SSH Scan	1
31.6.71.154	147.237.76.34	Poland	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
150.164.225.30	147.237.76.200	Brazil	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
150.164.225.30	147.237.76.44	Brazil	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
149.202.186.50	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
149.202.186.50	147.237.76.30	Germany	himush.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
189.254.90.133	147.237.72.14	Mexico	dover.idf.il(old	ET SCAN NMAP -sS window 3072	1

12-01-2015-05:04:08 to 12-01-2015-06:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	22
23.97.172.212	United States	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	18
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
147.236.31.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.66.154.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
23.97.172.212	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.183.170.106	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.183.36.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.106.94.2		147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
79.183.170.106	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
66.249.75.110	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
180.76.15.29	China	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
157.55.12.75	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
199.30.25.235	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
113.240.250.155	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	2
184.105.139.116	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.132	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
64.125.239.125	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.218	United States	147.237.0.35	akaws.idf.il	drop		drop	1
213.57.128.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.199	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
137.116.71.170	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
188.138.17.205	France	147.237.0.35	akaws.idf.il	drop		drop	1
64.125.239.170	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
174.89.181.249	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.218	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
106.38.241.106	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
216.218.206.102	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.199	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
151.44.165.180	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.214	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.138.17.205	France	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.125.239.227	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.148	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.219	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.218.206.102	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.59	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	7
157.55.39.238	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.238	Block	3
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.28	Block	3
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.31	Block	2
79.177.132.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.169.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
79.180.49.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
2.54.4.230	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
197.35.119.105	Egypt	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.208	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/0/111450.pdf	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/1133-he/dover.aspx	Block	1
197.35.119.105	Egypt	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/xmlrpc.php	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/927-he/atal.aspx	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
184.105.247.195	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.173	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/links.aspx	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
197.35.117.192	Egypt	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
84.109.106.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/haredim/general.aspx	None	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2317.png	Block	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
141.212.122.128	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Malformed URL from 141.212.122.128	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8948-he/refuah.aspx	Block	1
216.218.206.66	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
197.35.117.192	Egypt	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
95.108.158.144	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
66.249.64.153	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
149.88.86.255	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1