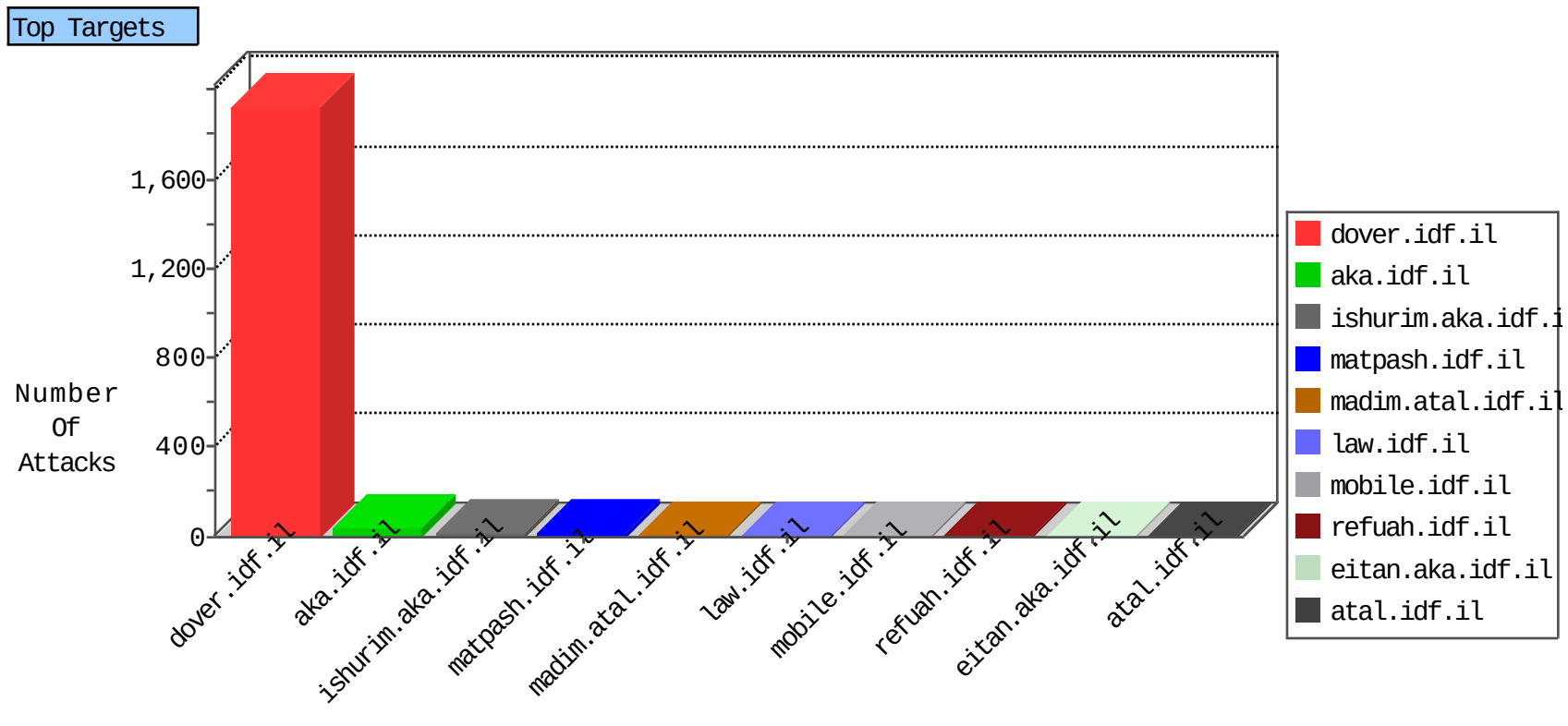
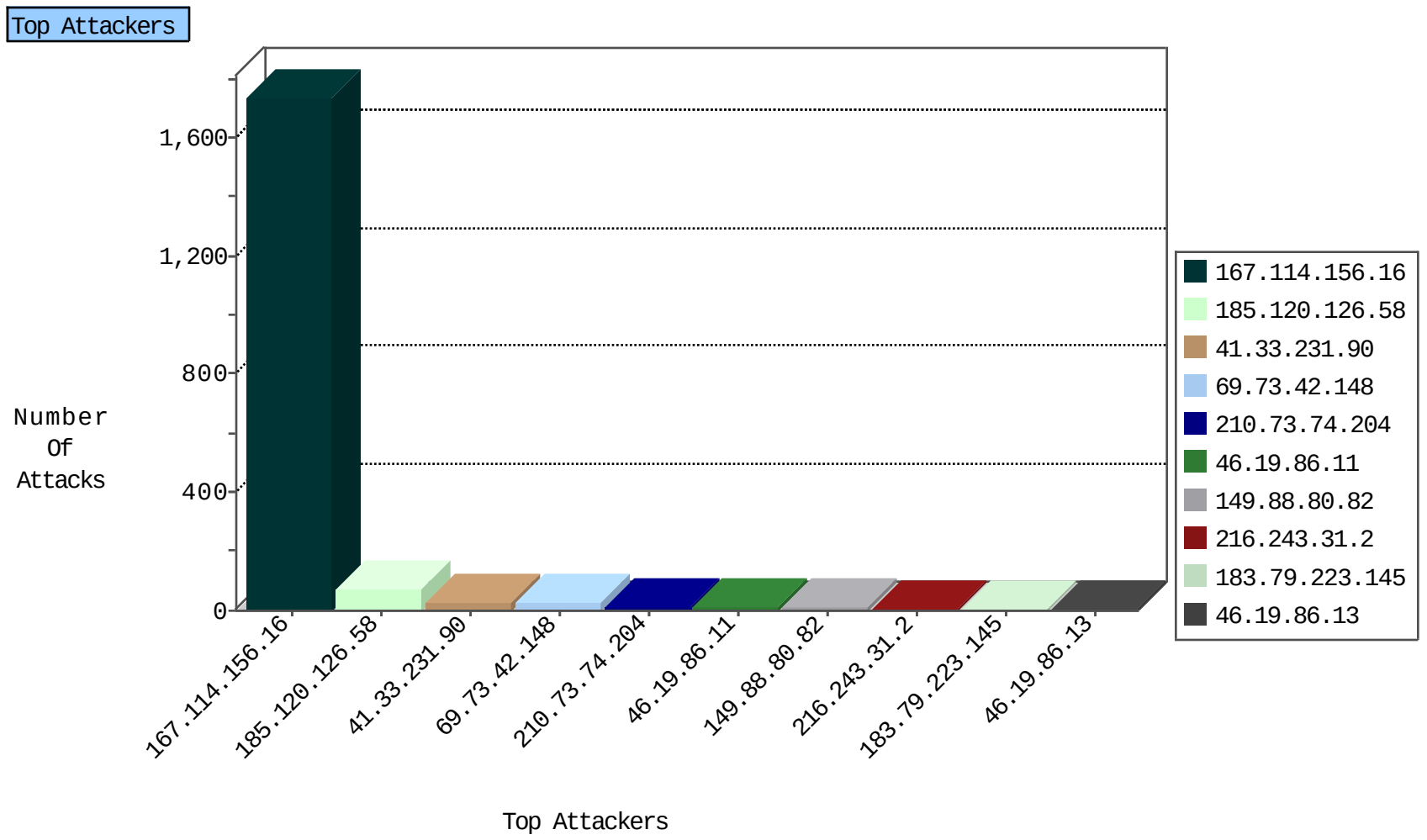
12-14-2015-02:04:01 to 12-14-2015-03:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-14-2015-02:04:01 to 12-14-2015-03:04:01

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	3301
52.53.222.9	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.201		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

12-14-2015-02:04:01 to 12-14-2015-03:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.100	United States	147.237.77.233	atal.idf.il	C1000106: HTTP: majestic bot	Block	1

12-14-2015-02:04:01 to 12-14-2015-03:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
210.73.74.204	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
210.73.74.204	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
210.73.74.204	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
187.160.47.63	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
210.73.74.204	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
115.29.2.4	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
210.73.74.204	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
115.29.2.4	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
210.73.74.204	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
210.73.74.204	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
210.73.74.204	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
210.73.74.204	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
210.73.74.204	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
210.73.74.204	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
120.24.100.212	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
210.73.74.204	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
115.29.2.4	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
210.73.74.204	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
115.29.2.4	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
210.73.74.204	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
210.73.74.204	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1

12-14-2015-02:04:01 to 12-14-2015-03:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	50
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
69.73.42.148	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
46.19.86.11	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.88.80.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
149.88.80.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.13	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
65.55.210.50	United States	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.141.35	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
79.183.54.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.44.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.11	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	3
216.105.170.98		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.183.155.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.148.207	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
91.200.12.18	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
176.12.139.103	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
209.133.111.211	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
37.34.83.155	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
91.200.12.18	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
108.176.155.12	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
188.120.148.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.12.139.103	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.184.193.78	Iran, Islamic Republic of	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
128.199.87.148	Singapore	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.120.46.224	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.149	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
130.193.50.10	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.243.31.2	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.52.42.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.153	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.144	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.243.31.2	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.199.87.148	Singapore	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.184.193.78	Iran, Islamic Republic of	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
167.88.7.232	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.149	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
130.207.203.56	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.243.31.2	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.52.42.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.157	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.145	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.199.87.148	Singapore	147.237.76.34	yohalan.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.79.223.145	Japan	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 183.79.223.145	Block	5
46.19.86.28	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	4
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.19.86.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.147.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.142.228.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
207.241.226.39	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
207.241.226.39	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 207.241.226.39	Block	2
37.26.147.180	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.178.38.106	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
207.241.226.39	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19485-he/kkkkkkk=f8e62612kkkkkkk_f8e62612	Block	1
95.185.215.40	Saudi Arabia	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
207.46.13.169	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templates/www.behazdaa.org.il	Block	1
141.212.122.97	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /x	Block	1
80.230.21.177	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.241.226.39	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/dynamic_map/piwik.php	Block	1
107.178.195.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
207.46.13.187	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
150.70.173.10	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.108.230.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/home	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
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8868-he/refuah.aspx	Block	1
183.79.223.145	Japan	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/files/9/× ×• ×©×?1	Block	1
107.178.195.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-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/1133-he/dover.aspx	Block	1
38.111.147.88	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/homepage/shared/usercontrols/headerupper/	Block	1
150.70.173.10	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
89.38.150.47	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/1923.pdf	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
69.73.42.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-23001-he/dover	Block	1
40.77.167.77	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/matehamatpash/pages/dover.aspx	Block	1
157.55.39.132	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/captcha.ashx	Block	1
89.38.150.47	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-signup.php	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1

12-14-2015-02:04:01 to 12-14-2015-03:04:01