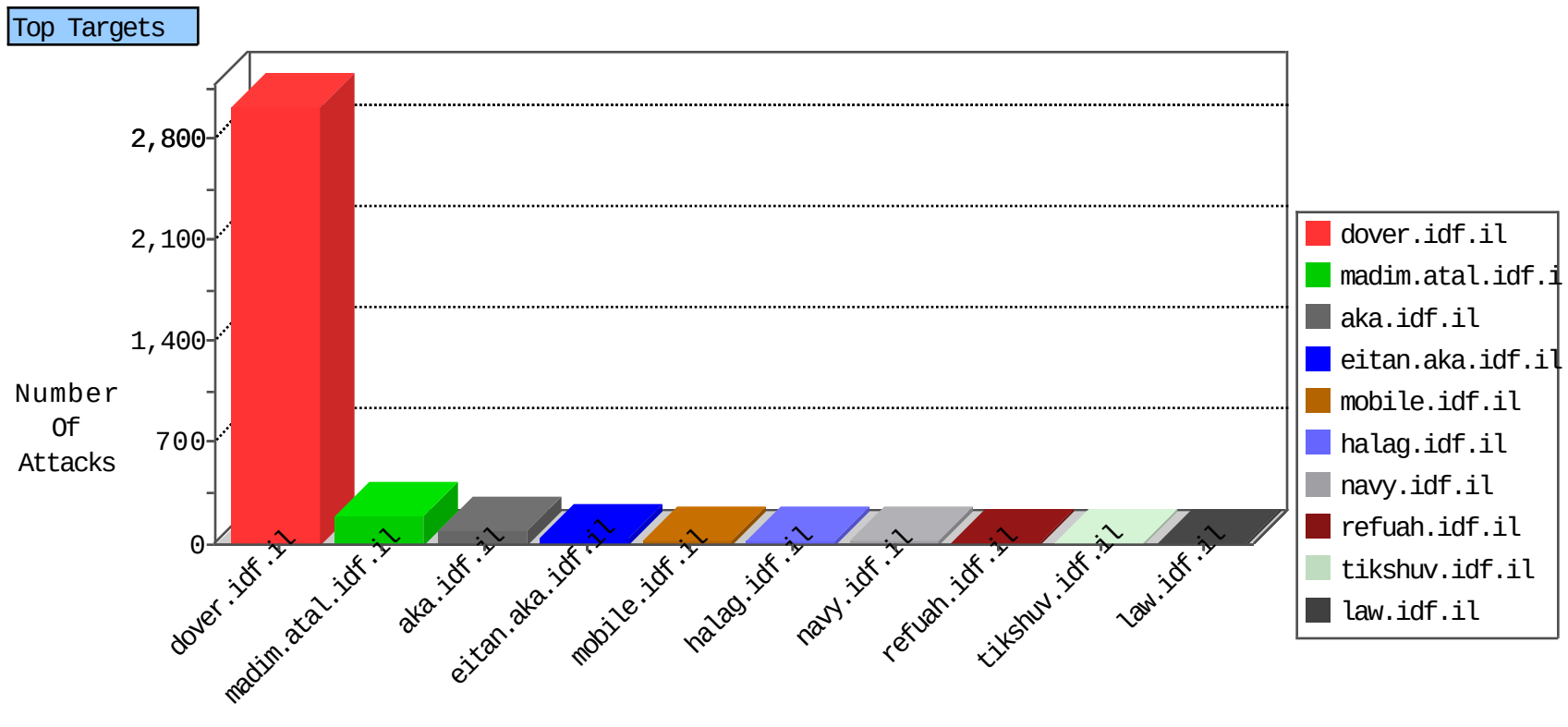
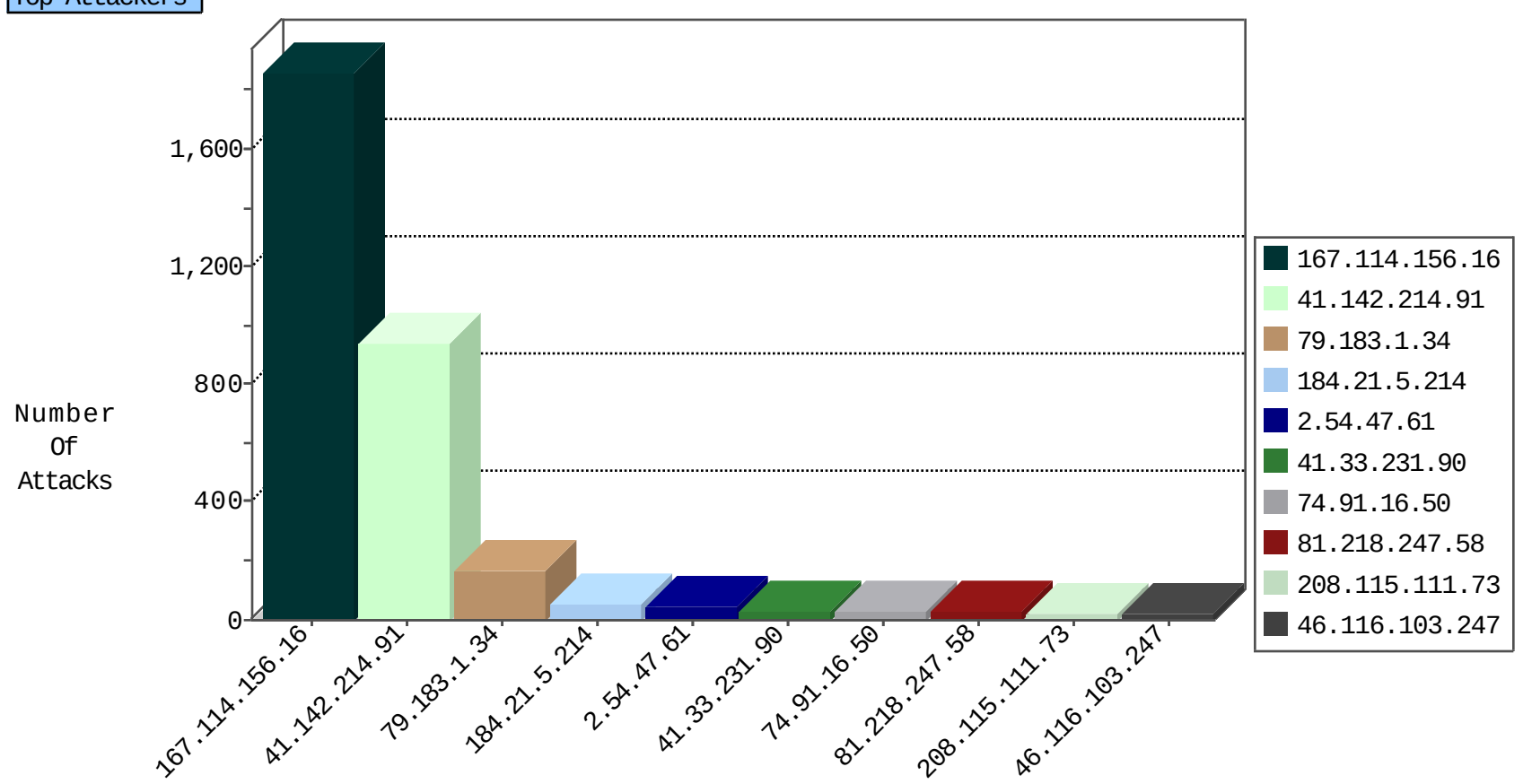
12-25-2015-22:04:02 to 12-25-2015-23:04:02

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-25-2015-22:04:02 to 12-25-2015-23:04:02

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	3092
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	975
41.142.214.91	Morocco	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	597
41.142.214.91	Morocco	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	261
184.21.5.214	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
46.166.188.68	Netherlands	147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

12-25-2015-22:04:02 to 12-25-2015-23:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.91.16.50	United States	147.237.77.216	dover.idf.il	C014: HTTP: Fuck in url	Block	26

12-25-2015-22:04:02 to 12-25-2015-23:04:02

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	3
81.218.247.58	147.237.8.28	Israel	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
81.218.247.58	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
169.55.120.153	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.247.58	147.237.76.196	Israel	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
87.197.159.157	147.237.8.45	Slovakia	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.247.58	147.237.76.86	Israel	navy.idf.il	ET SCAN Potential SSH Scan	1
81.218.247.58	147.237.77.235	Israel	sviva.idf.il	ET SCAN Potential SSH Scan	1
81.218.247.58	147.237.76.31	Israel	nakchal.idf.il	ET SCAN Potential SSH Scan	1
218.108.132.58	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.247.58	147.237.77.226	Israel	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
202.124.48.157	147.237.76.202	Japan	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
81.218.247.58	147.237.77.179	Israel	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.201	Cote D'Ivoire	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
81.218.247.58	147.237.0.35	Israel	akaws.idf.il	ET SCAN Potential SSH Scan	1
81.218.247.58	147.237.77.121	Israel	e.navy.idf.il	ET SCAN Potential SSH Scan	1
178.169.143.78	147.237.76.177	Bulgaria	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
81.218.247.58	147.237.76.202	Israel	e.halag.idf.il	ET SCAN Potential SSH Scan	1
178.169.143.78	147.237.76.177	Bulgaria	ncore.idf.il	ET SCAN NMAP -f -sS	1
81.218.247.58	147.237.76.200	Israel	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
169.55.120.153	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
81.218.247.58	147.237.76.198	Israel	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.232.52.14	147.237.0.33	Russian Federation	idf.il	ET SCAN NMAP -sS window 1024	1
81.218.247.58	147.237.76.148	Israel	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.77.176		matpash.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.247.58	147.237.76.39	Israel	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
81.218.247.58	147.237.77.234	Israel	halag.idf.il	ET SCAN Potential SSH Scan	1
81.218.247.58	147.237.72.167	Israel	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
218.108.132.58	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.247.58	147.237.77.216	Israel	dover.idf.il	ET SCAN Potential SSH Scan	1
202.124.48.157	147.237.76.202	Japan	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.247.58	147.237.8.24	Israel	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
81.218.247.58	147.237.77.176	Israel	matpash.idf.il	ET SCAN Potential SSH Scan	1
81.218.247.58	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
81.218.247.58	147.237.77.19	Israel	law-forum.idf.il	ET SCAN Potential SSH Scan	1
178.169.143.78	147.237.76.177	Bulgaria	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
81.101.206.244	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.247.58	147.237.76.201	Israel	e.atal.idf.il	ET SCAN Potential SSH Scan	1
31.44.67.178	147.237.76.34	Albania	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.245.28.46	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
81.218.247.58	147.237.76.199	Israel	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1

12-25-2015-22:04:02 to 12-25-2015-23:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.142.214.91	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	637
41.142.214.91	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	131
184.21.5.214	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	47
2.54.47.61	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
41.142.214.91	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
41.142.214.91	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	18
41.142.214.91	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
212.150.214.130	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
199.30.24.89	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	7
109.65.35.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
41.142.214.91	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
5.102.254.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.142.214.91	Morocco	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Anonymous DoSer Denial of Service Tool	reject	4
84.108.90.89	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.108.90.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.116.103.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
87.69.231.58	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
185.3.146.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.181.203.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.7.11	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.102.254.245	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.190.60	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
157.55.39.47	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.182.51.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.174.169	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.176.50.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.117	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.179.98	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
188.120.148.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.54.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.179.98	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
84.221.146.157	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.135.33	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
87.69.106.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
128.232.110.28	United Kingdom	147.237.76.199	e.nakchal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	2
77.125.109.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.54.48.63	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2

12-25-2015-22:04:02 to 12-25-2015-23:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.1.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
79.183.1.34	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.183.1.34	Block	58
41.142.214.91	Morocco	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.142.214.91	Block	24
2.52.41.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.116.103.247	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.116.103.247	Block	6
79.183.1.34	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 79.183.1.34	Block	4
2.54.128.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.116.103.247	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	4
46.116.103.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.181.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.120.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	2
176.13.5.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.133.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
81.215.95.51	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.215.95.51	Block	2
2.52.7.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
87.68.56.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.251.99	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
5.22.131.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
157.55.39.178	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/yassin7.	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
109.67.71.87	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.86	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	1
207.46.13.183	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kamlar/	Block	1
81.215.95.51	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
77.127.65.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.3.146.117	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 185.3.146.117	Block	1
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/size100x0/3493.jpg	Block	1
128.232.110.29	United Kingdom	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
87.69.193.92	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
50.87.43.17	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
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	1
31.168.208.53	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	Unauthorized URL Access to www.aka.idf.il/lomdim/forum/	Block	1
109.160.209.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.76.124.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.95.58.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.177.114.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.17.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.3.146.117	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
128.232.110.29	United Kingdom	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3350.jpg	Block	1
89.46.101.168	Romania	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
50.87.43.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
37.26.147.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.21	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
176.13.8.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-25-2015-22:04:02 to 12-25-2015-23:04:02