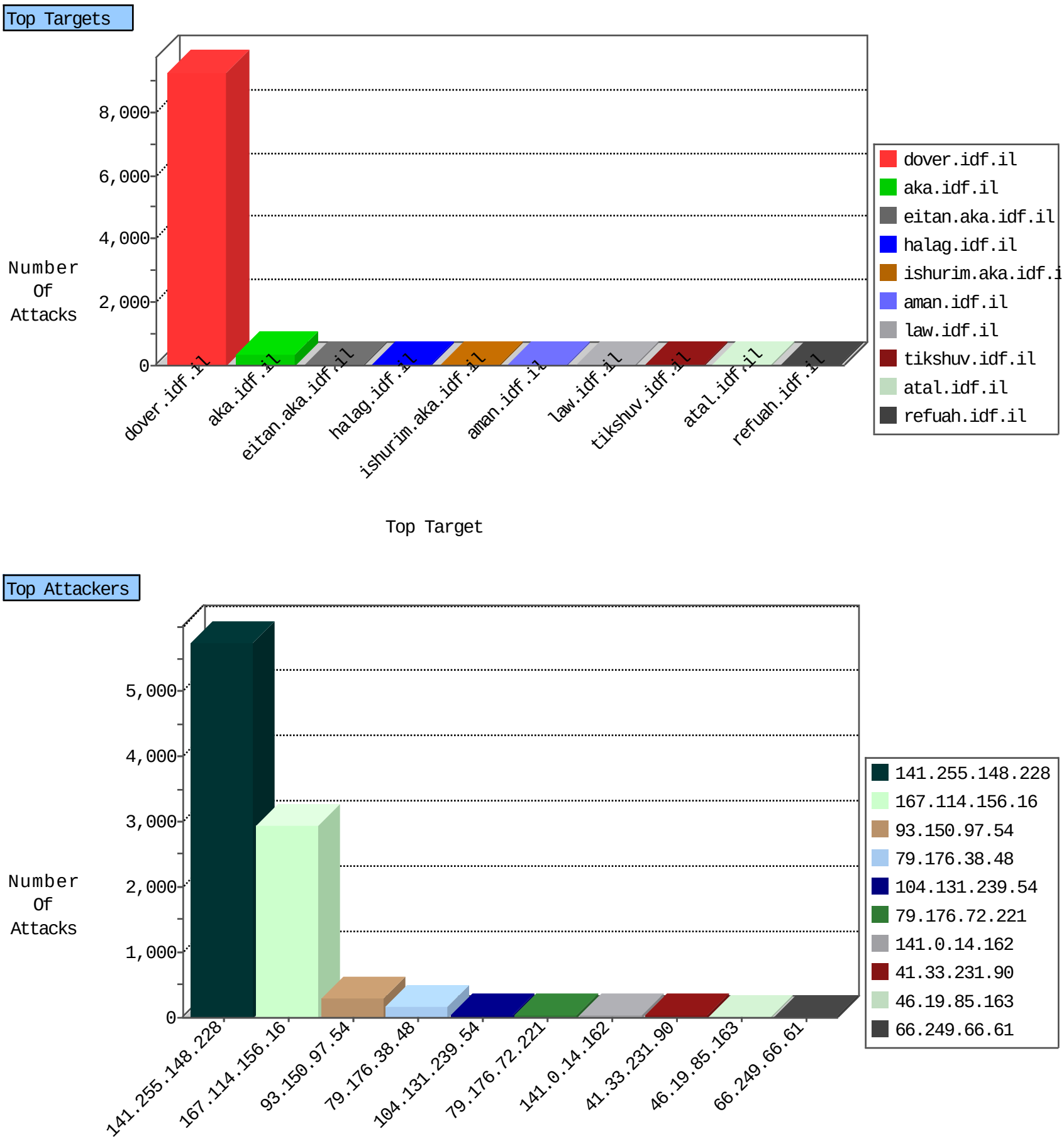
12-04-2015-20:04:04 to 12-04-2015-21:04:04

IDF Under Attack
Daily Report



12-04-2015-20:04:04 to 12-04-2015-21:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	115667
141.255.148.228	Netherlands	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	17299
141.255.148.228	Netherlands	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	12579
141.255.148.228	Netherlands	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	4707
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3533
141.255.148.228	Netherlands	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1940
141.255.148.228	Netherlands	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	463
141.255.148.228	Netherlands	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	213
141.255.148.228	Netherlands	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	40
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
66.249.66.28	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
90.61.6.72	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
66.249.66.31	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
104.131.147.112	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
141.255.148.228	Netherlands	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
199.30.16.160	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
146.185.239.100	Russian Federation	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
141.255.148.228	Netherlands	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Htps	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

12-04-2015-20:04:04 to 12-04-2015-21:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.156.69.180	Morocco	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
141.255.148.228	Netherlands	147.237.77.216	dover.idf.il	10725: TCP: LOIC DDoS Tool	Block	1

12-04-2015-20:04:04 to 12-04-2015-21:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.129	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
43.229.53.89	147.237.0.15	Japan	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
37.230.212.125	147.237.72.166	Russian Federation	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.239.126.72	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.77.216	United States	dover.idf.il	ET DROP Dshield Block Listed Source	1
98.119.105.221	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
98.119.105.221	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
91.218.246.103	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
43.229.53.89	147.237.0.35	Japan	akaws.idf.il	ET SCAN Potential SSH Scan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
209.126.116.147	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
91.236.120.178	147.237.72.166	Russian Federation	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
88.247.111.112	147.237.76.31	Turkey	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.151.55.35	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1

12-04-2015-20:04:04 to 12-04-2015-21:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.255.148.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3804
141.255.148.228	Netherlands	147.237.77.216	dover.idf.il	drop		drop	679
93.150.97.54	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	286
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	174
79.176.38.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
141.255.148.228	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	129
141.255.148.228	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	107
104.131.239.54	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
141.0.14.162	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	38
79.176.72.221	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
46.19.85.163	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	23
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
176.127.22.15	Switzerland	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
100.100.54.210		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
79.177.19.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.69.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.72.221	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.143.91.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.46.148.234	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.67.113.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.91.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.120.148.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.237.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
93.150.97.54	Italy	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.178.182.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
188.120.148.206	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.16.45.251	Italy	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
93.150.97.54	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.150.200.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.161.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.110.208.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.20.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.101.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.168.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.137.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.187.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.114	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.170.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.184	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.57.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.159.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.64.198	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	3

12-04-2015-20:04:04 to 12-04-2015-21:04:04

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.46.148.234	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

12-04-2015-20:04:04 to 12-04-2015-21:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.131.100.197	Egypt	147.237.77.74	law.idf.il	PHP Attempt	Block	4
41.131.100.197	Egypt	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	4
149.78.250.122	Israel	147.237.0.17	m.my-kosher-kravi .idf.il	Distributed Illegal Parameter Encoding	None	2
84.108.220.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.65.138.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.102.254.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.146.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.125	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
105.156.69.180	Morocco	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-8021-he/dover.aspx	Block	1
82.166.233.197	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
61.135.190.72	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/reset.css	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
37.142.68.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.114.212.166	Romania	147.237.76.86	navy.idf.il	Malformed URL dÂ±[[#27]]"Â?×£Â½â€°Ö¶Â´×š[[#1]]×¦u[[#16]]hÂŒ i6zÂ¡![[#4]]Â¨×±5Â?Â¿[[#23]]ÂžÂµ×ž×˜[[#31]]â€¦Ã™×'Â-×• Â´z[[#14]][[#8]]Ã—â€¹[k^l•Ã¼Ö¹q×£Â·ÃŠ-qcË†×'pn6Â¼[[#28]]Â»v<va	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/16122010masaiyot.aspx	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/br><brothers/skira/default.asp	Block	1
94.230.84.59	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/chinuch/klali/	None	1
79.182.219.62	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
46.120.169.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1108-he/nakhal.aspx	Block	1
2.52.52.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.64	United States	147.237.0.19	madim.atal.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
105.156.69.180	Morocco	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.43	Block	1
61.135.190.197	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/layoutdev.css	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
40.77.167.14	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.137.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.114.212.166	Romania	147.237.76.86	navy.idf.il	NULL Character in Method Â,[[#0]][[#0]][[#0]]!lAÂ€Â•?UÃ€Ã'&J}^rÃ—Ã´Â«[Â²Ã¤+[[#0]]Ã·Â¥4qÂ¼Â—Â™[[#28]][[#15]]Â•Â?Ã·ÂŸÃ¿Â"Â?;Ã—Â»ÃˆÂˆÂ˜	Block	1
66.249.67.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
94.230.86.162	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
79.182.219.62	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
46.120.179.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 195.154.146.225	Block	1
141.212.122.64	United States	147.237.77.19	law-forum.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
79.114.212.166	Romania	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
2.54.141.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
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	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
61.135.190.198	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/1.he/960.css	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
84.111.224.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.106.226.71	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
79.114.212.166	Romania	147.237.76.86	navy.idf.il	Unknown HTTP Request Method Â,[[#0]][[#0]][[#0]]!lAÂ€Â•?UÃ€Ã' &J}^rÃ—Ã´Â«[Â²Ã¤+[[#0]]Ã·Â¥4qÂ¼Â—Â™[[#28]][[#15]]Â•Â?Ã·ÂŸÃ¿Â" Â?;Ã—Â»ÃˆÂˆÂ˜ in URL dÂ±[[#27]]"Â?×£Â½â€°Ö¶Â´×š [[#1]]×¦u[[#16]]hÂŒi6zÂ¡![[#4]]Â¨×±5Â?Â¿[[#23]]ÂžÂµ×ž×˜[[#31]]â€ ¦Ã™×'Â-×•Â´z[[#14]][[#8]]Ã—â€¹[k^l•Ã¼Ö¹q×£Â·ÃŠ-qcË†×' pn6Â¼[[#28]]Â»v<va	Block	1
66.249.67.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
117.78.13.55	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/robots.txt	Block	1

12-04-2015-20:04:04 to 12-04-2015-21:04:04