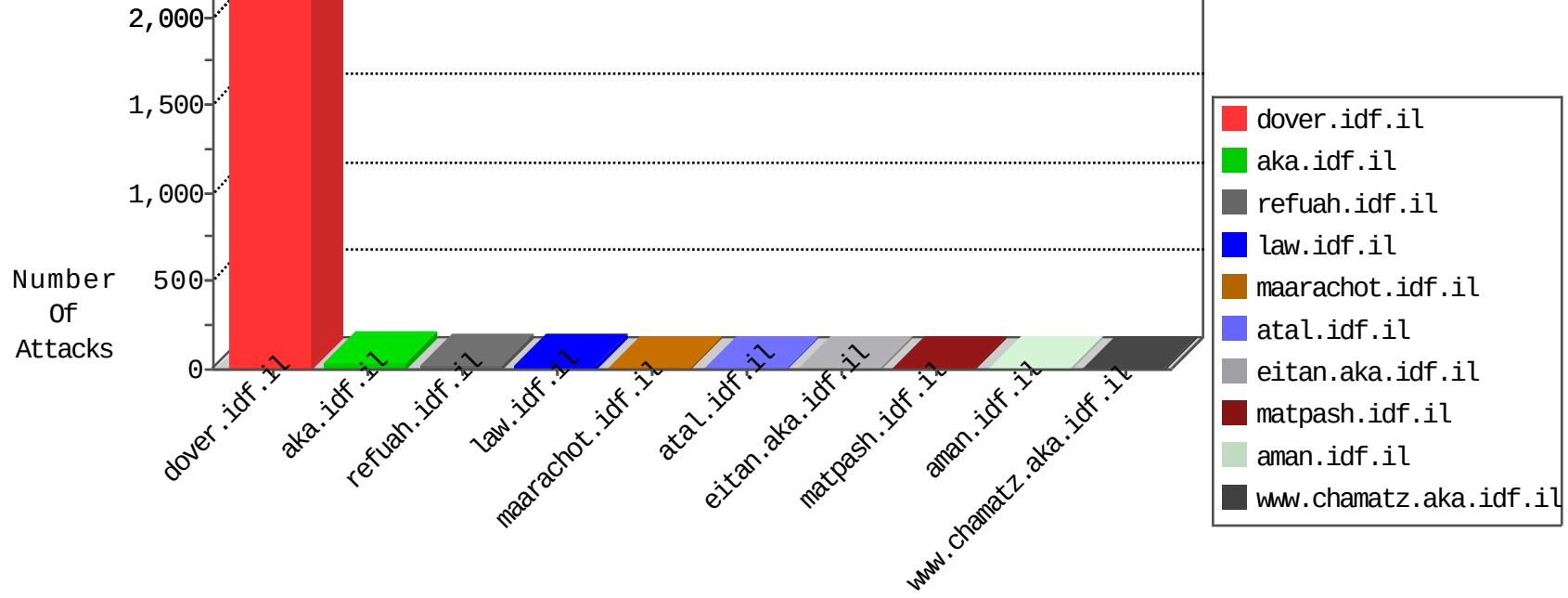
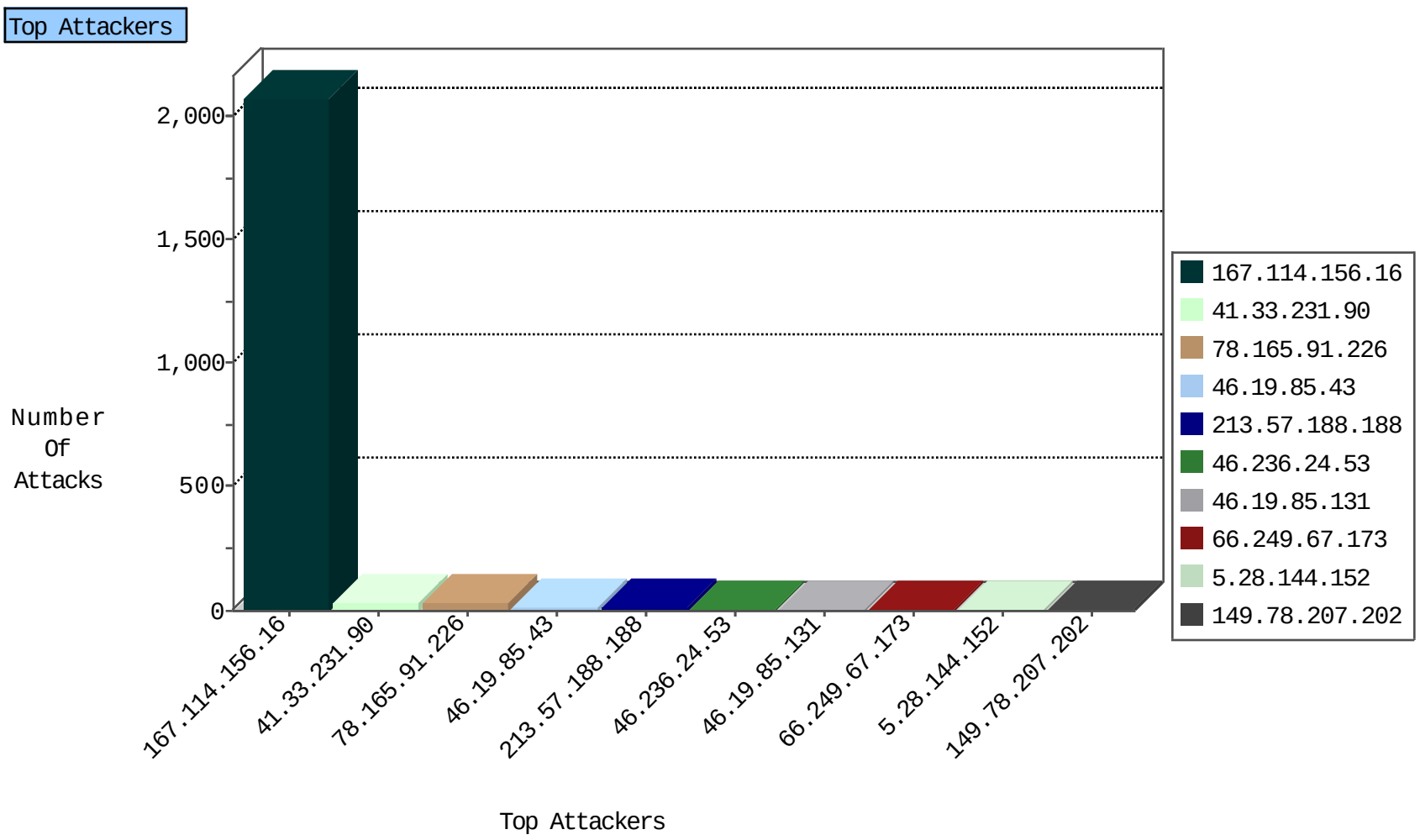
12-07-2015-01:05:03 to 12-07-2015-02:05:03

IDF Under Attack Daily Report





12-07-2015-01:05:03 to 12-07-2015-02:05:03

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	3380

12-07-2015-01:05:03 to 12-07-2015-02:05:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
78.165.91.226	Turkey	147.237.77.74	law.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
78.165.91.226	Turkey	147.237.76.42	refuah.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
78.165.91.226	Turkey	147.237.77.176	matpash.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
78.165.91.226	Turkey	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

12-07-2015-01:05:03 to 12-07-2015-02:05:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
78.165.91.226	147.237.77.74	Turkey	law.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	12
78.165.91.226	147.237.77.216	Turkey	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
78.165.91.226	147.237.77.176	Turkey	matpash.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
78.165.91.226	147.237.76.42	Turkey	refuah.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.102.8.139	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
91.218.246.103	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.0.15	Ukraine	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
74.117.209.135	147.237.77.233	United States	atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
159.122.238.133	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
159.122.238.133	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
142.54.163.74	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
91.218.246.103	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
81.169.251.74	147.237.0.35	Germany	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
213.57.188.188	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
185.106.94.91	147.237.76.200		eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
159.122.238.133	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
142.54.163.74	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1

12-07-2015-01:05:03 to 12-07-2015-02:05:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.236.24.53	United Kingdom	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.43	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.131	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
149.78.207.202	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
66.249.67.173	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.188.188	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.86	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.43	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
199.30.25.17	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.57.188.188	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.28.144.152	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.160.169.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.144.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.179.171.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.3.6	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	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
66.249.67.164	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.200	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
87.68.32.30	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.180	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.57.148.191	Uruguay	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.173.132.9	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
46.120.6.134	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
5.29.160.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.181	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.57.148.191	Uruguay	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.120.6.134	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
146.185.239.102	Russian Federation	147.237.0.35	akaws.idf.il	drop		drop	1
146.185.239.102	Russian Federation	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

12-07-2015-01:05:03 to 12-07-2015-02:05:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.39.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.184.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
46.120.98.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.147.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
195.154.146.225	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 195.154.146.225	Block	2
84.94.25.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
176.12.140.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
195.154.146.225	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/speakerofmatpash/pages/aavaratksafim18022010.aspx	Block	1
136.243.36.96	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 136.243.36.96	Block	1
40.77.167.57	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
93.173.2.32	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/xmlrpc.php	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza>Ñ?Ð¿ÐµÑ†Ð¸Ð°Ð»ÑŒ Ð½Ð¾Ñ?Ð°Ñ‚Ðµ, Ñ?Ð¾Ð·Ð´Ð°Ð½Ð½Ð¾Ñ? Ð´Ð»Ñ? Ñ?Ñ‚Ð¸Ñ…Ñ†Ð¸Ð¸.</p> <table cellspacing=	Block	1
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
107.178.195.163	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
5.9.36.66	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.183.115.163	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
136.243.36.96	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
40.77.167.75	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/319,	Block	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18764-en/	Block	1
54.152.228.19	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/asp	Block	1
176.13.6.25	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
37.26.149.156	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	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
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
41.109.176.44	Algeria	147.237.77.74	law.idf.il	PHP Attempt	Block	1
149.78.38.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.173.132.9	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8948-he/refuah.aspx	Block	1
54.175.3.91	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.10.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
40.77.167.8	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
207.46.13.155	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/talking_from_field/	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
41.109.176.44	Algeria	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
157.55.39.205	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
107.150.42.186	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.179.60.128	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
176.228.69.92	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.9	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/matehamatpash	Block	1
109.201.154.138	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
40.77.167.8	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
93.173.2.32	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.111.73	Block	1

12-07-2015-01:05:03 to 12-07-2015-02:05:03