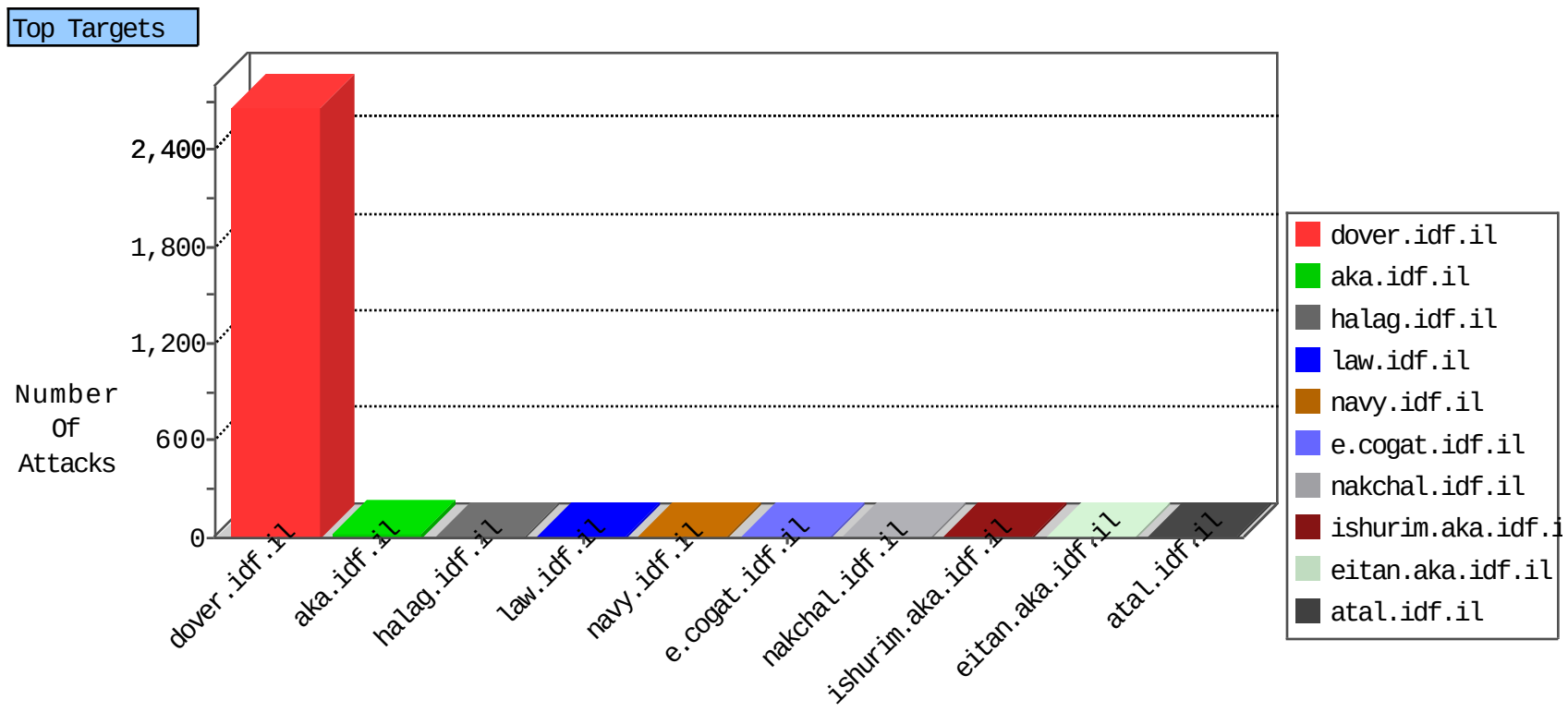
12-03-2015-03:04:07 to 12-03-2015-04:04:07

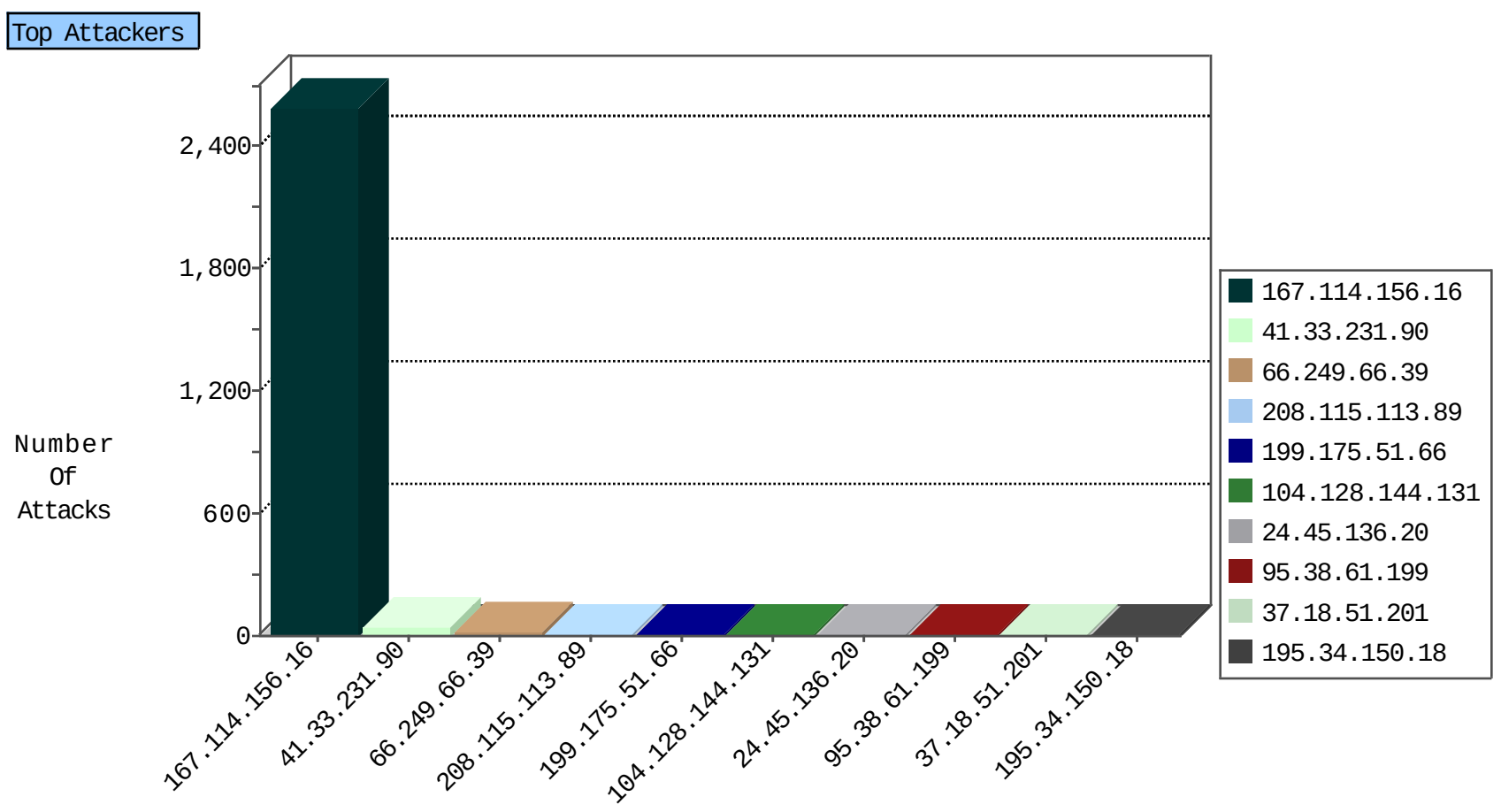
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-03-2015-03:04:07 to 12-03-2015-04:04:07

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	3359
189.38.57.42	Brazil	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
46.166.188.68	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

12-03-2015-03:04:07 to 12-03-2015-04:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.188.28	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

12-03-2015-03:04:07 to 12-03-2015-04:04:07

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
79.138.70.153	147.237.76.30	Sweden	himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
200.35.150.97	147.237.77.170	Panama	maarachot.idf.il	ET SCAN Potential SSH Scan	1
177.43.233.5	147.237.76.196	Brazil	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
159.147.148.28	147.237.77.226	Spain	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.0.33	Canada	idf.il	ET SCAN NMAP -sS window 2048	1
79.138.70.153	147.237.76.177	Sweden	ncore.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.0.34	Sweden	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
46.151.55.35	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
200.35.150.97	147.237.77.234	Panama	halag.idf.il	ET SCAN NMAP -sS window 1024	1
177.43.233.5	147.237.76.196	Brazil	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.0.34	Canada	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
104.128.144.131	147.237.0.33	Canada	idf.il	ET SCAN NMAP -f -sS	1

12-03-2015-03:04:07 to 12-03-2015-04:04:07

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
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
66.249.66.39	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	4
37.18.51.201	Russian Federation	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
87.68.70.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.1	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.113.89	United States	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
195.154.146.225	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
104.238.195.66		147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	2
208.115.113.89	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	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
209.141.43.84	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.229.239	United States	147.237.72.166	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	monitor	2
66.249.65.122	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
104.128.144.131	Canada	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.146.228	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
184.105.139.88	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.154.227.118	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
131.253.24.146	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.113.89	United States	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
184.105.139.123	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.55.211.245	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
197.37.49.160	Egypt	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
131.253.26.242	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
79.181.162.225	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
195.62.53.168	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
104.128.144.131	Canada	147.237.0.33	idf.il	drop		drop	1
216.72.41.121	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
207.46.13.4	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
82.221.105.7	Iceland	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
195.62.53.168	Russian Federation	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

12-03-2015-03:04:07 to 12-03-2015-04:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.175.51.66	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
79.176.122.228	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
199.175.51.66	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.php	Block	2
46.120.233.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
54.153.32.246	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	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
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/size220x0/13032.jpg	Block	1
24.45.136.20	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Name	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.26.146.228	Israel	147.237.72.167	ishurim.aka.idf.i	SSL Untraceable Connection - Open Mode	None	1
149.210.158.71	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/arabic/pages/default.aspx	Block	1
104.238.195.66		147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/clientscripts.js	Block	1
54.153.33.152	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
212.76.124.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter sig2 in www.aka.idf.il/main/giyus/general.aspx	None	1
199.30.16.170	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
24.45.136.20	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method Â,[[#0]][[#0]][[#0]][[#19]]Ã±[Ã‰Ã™ Ã?`Â¿ÂªÂ?Â¾ÂŸHfÃ”6[[#16]][[#7]]Â?Â¹,ÃƒÃ‚,Ã–ÃµSSÂ,6Ã€[[#30]]Â©Â’ [[#25]]ÂªÂ±VcKÂ¼Ã¼Â•Ã‹[[#16]]Â-Â½-$Lur8Ã¹Â²!Ã’ÃœÂƒ:[[#1]]Ã„ %Â?[[#12]]Ã§[[#28]]Ã?qÃ«Ã°Â?[[#29]]Â“Â?ÃŠÃ½Ã°[[#2]]Ãœ[[#25]]	Block	1
109.64.144.135	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
40.77.167.14	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	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
157.55.39.46	United States	147.237.77.233	atal.idf.il	PHP Attempt	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
66.249.64.166	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
217.132.9.108	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
24.45.136.20	United States	147.237.76.86	navy.idf.il	Illegal HTTP Version	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
79.112.105.50	Romania	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
40.77.167.78	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	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
157.55.39.46	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/load.php	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
218.7.170.190	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
66.249.66.1	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
199.175.51.66	United States	147.237.77.74	law.idf.il	Multiple Admin Blocking from 199.175.51.66	Block	1
24.45.136.20	United States	147.237.76.86	navy.idf.il	NULL Character in Method Â,[[#0]][[#0]][[#0]][[#19]]Ã±[Ã‰Ã™ Ã?`Â¿ÂªÂ?Â¾ÂŸHfÃ”6[[#16]][[#7]]Â?Â¹,ÃƒÃ‚,Ã–ÃµSSÂ,6Ã€[[#30]]Â©Â’ [[#25]]ÂªÂ±VcKÂ¼Ã¼Â•Ã‹[[#16]]Â-Â½-$Lur8Ã¹Â²!Ã’ÃœÂƒ:[[#1]]Ã„ %Â?[[#12]]Ã§[[#28]]Ã?qÃ«Ã°Â?[[#29]]Â“Â?ÃŠÃ½Ã°[[#2]]Ãœ[[#25]]	Block	1
149.88.94.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.112.105.50	Romania	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	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
157.55.39.115	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
24.45.136.20	United States	147.237.76.86	navy.idf.il	Abnormally Long Request method	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
66.249.66.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/rec.asp	Block	1
199.175.51.66	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 199.175.51.66	Block	1
37.26.146.228	Israel	147.237.72.167	ishurim.aka.idf.i	Multiple Untraceable SSL Sessions from 37.26.146.228 (Open Mode)	None	1
149.210.158.71	Netherlands	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 149.210.158.71	Block	1

12-03-2015-03:04:07 to 12-03-2015-04:04:07