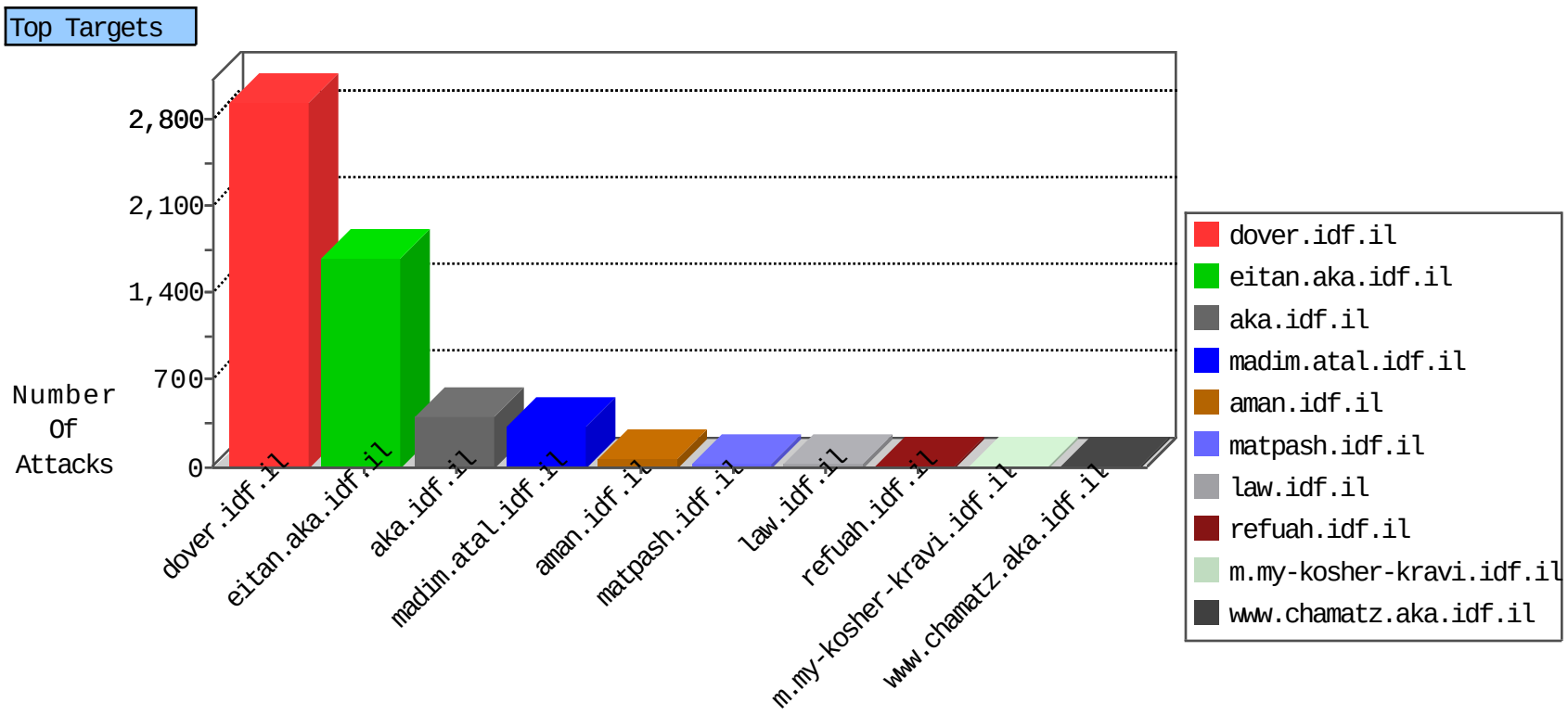
12-04-2015-13:04:08 to 12-04-2015-14:04:08

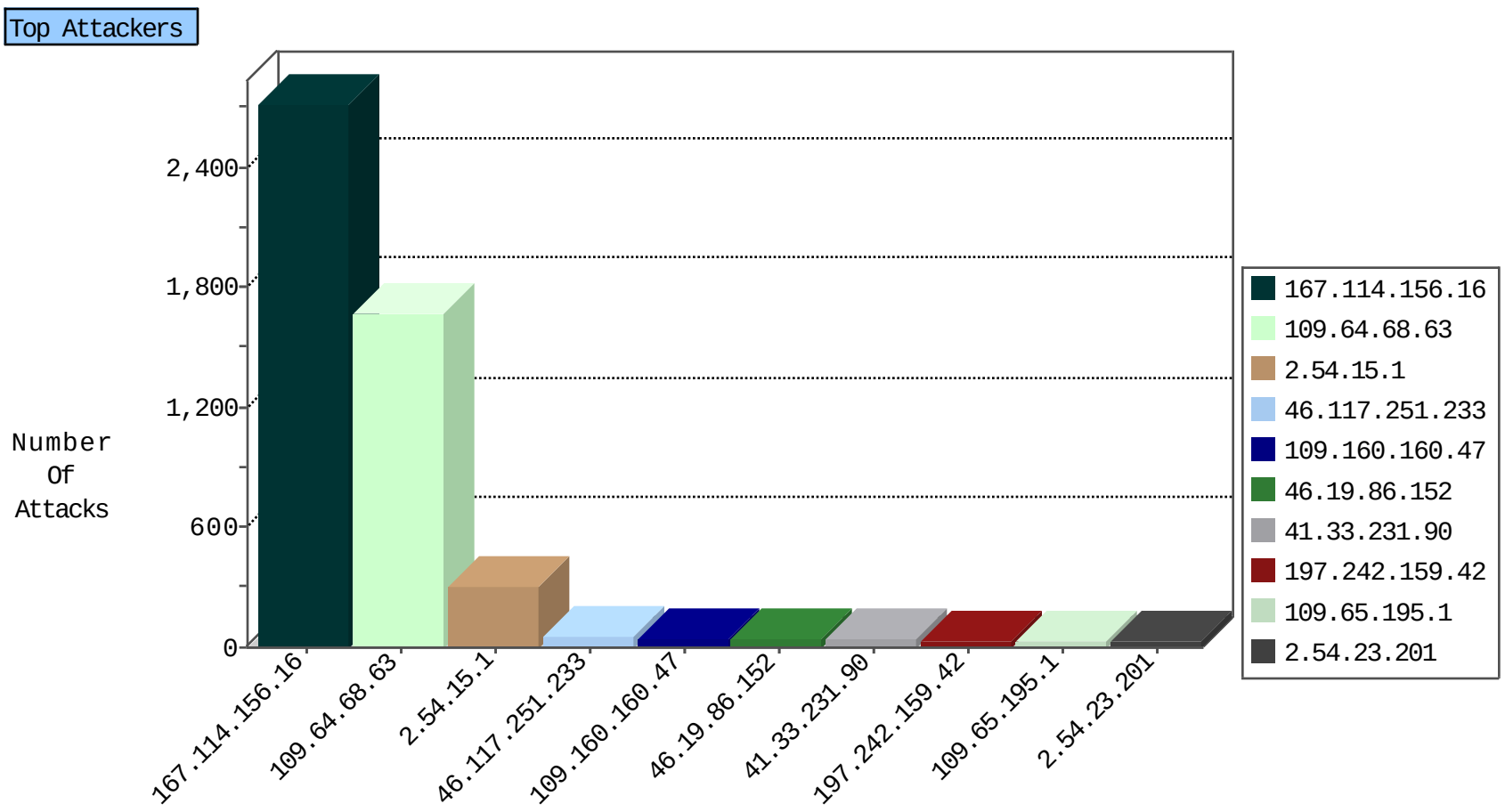
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-04-2015-13:04:08 to 12-04-2015-14:04:08

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	3339
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
118.193.21.98	China	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
54.67.60.7	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

12-04-2015-13:04:08 to 12-04-2015-14:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.242.159.42	South Africa	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
23.91.70.51	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
74.63.228.226	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1

12-04-2015-13:04:08 to 12-04-2015-14:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
197.242.159.42	147.237.72.166	South Africa	aka.idf.il	SQL Injection - Select From	24
66.249.64.165	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.1	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
196.47.173.21	147.237.77.176	Cote D'Ivoire	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
119.73.228.130	147.237.76.199	Singapore	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
91.218.246.103	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.77.176	Cote D'Ivoire	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
119.73.228.130	147.237.76.199	Singapore	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

12-04-2015-13:04:08 to 12-04-2015-14:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.68.63	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1338
109.160.160.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
46.19.86.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
100.100.53.141		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
213.57.128.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
109.65.195.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
84.228.217.52	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.195.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.23.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
100.100.125.211		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
217.132.2.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.212	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.157.55	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.110.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.94.54.95	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.142.110.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.114.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.23.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
100.100.125.211		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.3.146.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
217.132.2.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.23.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
149.78.37.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
2.54.23.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
217.132.2.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.120.124.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
213.57.128.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
217.132.2.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
149.78.37.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
149.78.37.175	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.54.23.181	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	4
2.54.130.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.35.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.147.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.80.178.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.32.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
158.169.40.8	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
5.28.186.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.116.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.37.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-04-2015-13:04:08 to 12-04-2015-14:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.68.63	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.64.68.63	Block	334
2.54.15.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	206
2.54.15.1	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.15.1	Block	70
2.54.15.1	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.15.1	Block	20
37.26.149.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.117.251.233	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 46.117.251.233	Block	5
46.117.251.233	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 46.117.251.233	Block	5
46.117.251.233	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 46.117.251.233	Block	5
46.117.251.233	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 46.117.251.233	Block	5
176.13.3.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.117.251.233	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in URL from 46.117.251.233	Block	4
79.179.59.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
84.228.15.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.251.233	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 46.117.251.233	Block	3
46.117.251.233	Israel	147.237.72.156	aman.idf.il	Multiple NULL Character in Header Name from 46.117.251.233	Block	2
2.54.189.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.195.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.13.43	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
5.29.110.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
71.65.240.113	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
176.228.128.6	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
46.117.251.233	Israel	147.237.72.156	aman.idf.il	Multiple Illegal HTTP Version from 46.117.251.233	Block	2
5.29.189.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
71.65.240.113	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	2
46.117.251.233	Israel	147.237.72.156	aman.idf.il	Multiple Malformed HTTP Header Line from 46.117.251.233	Block	2
46.117.251.233	Israel	147.237.72.156	aman.idf.il	Abnormally Long Request request version	Block	1
197.48.7.139	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
46.117.251.233	Israel	147.237.72.156	aman.idf.il	NULL Character in Method Ã€++k<Â¤ÃŒÂ„h[[#27]]"Â–h[[#8]]ÂšÂ‹ÃŽ [Ã?8Ã‰Ã›RÂ¥Â¬Â‰Â¿Â€ÃŸÃŸÃ²[[#17]]iÂ®Â‰]v$\[[#14]]Ã¶Ã–rÂ† qÃ»wÃ‡Ã?Â€Ã…O	Block	1
176.13.0.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.236.217	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.159.182.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.117.251.233	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Value from 46.117.251.233	Block	1
149.78.229.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
8.37.71.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18659-he/dover.aspx&usg=alkjrhivcyv3xtlz0ofuyrap2jxbvoqp_g	Block	1
80.246.137.154	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 80.246.137.154 (Open Mode)	None	1
77.126.96.94	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.8.174.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.117.251.233	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Query String [×¦×'×•m>NFÂ?#Ëœ Ö³%,,Ö¿[[#14]]×ƒ on Â¢[[#17]]m~×—Ö·Ã–Â¬=[[#5]]b[[#29]]â€œ Ö»Ö¾×²•[[#27]]{9×•(ÃšÂ¸ÃŠ[[#26]]Â¿Â»Â?#}m6Â?Â¥[[#19]]Â¶â€ž Â¼Ö¼$Âšr9`Ö¼v/-Ã›l[[#8]]bÖ°[[#25]]m(×ƒt[[#6]]ipn0 a[[#11]][[#28]]Âœ£-cuvÂ?-×¥Â¹â„¢Ã·Ö³Ö¿â€˜Ãž[[#30]][[#0]]	Block	1
109.66.24.160	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.19.86.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.120.144.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.3.144.101	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
37.142.109.252	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
157.55.39.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.117.251.233	Israel	147.237.72.156	aman.idf.il	Malformed URL Â¢[[#17]]m~×—Ö·Ã–Â¬=[[#5]]b[[#29]]â€œ Ö»Ö¾×²•[[#27]]{9×•(ÃšÂ¸ÃŠ[[#26]]Â¿Â»Â?#}m6Â?Â¥[[#19]]Â¶â€ž Â¼Ö¼$Âšr9`Ö¼v/-Ã›l[[#8]]bÖ°[[#25]]m(×ƒt[[#6]]ipn0 a[[#11]][[#28]]Âœ£-cuvÂ?-×¥Â¹â„¢Ã·Ö³Ö¿â€˜Ãž[[#30]][[#0]]	Block	1
141.212.121.176	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
2.54.178.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.101.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-04-2015-13:04:08 to 12-04-2015-14:04:08