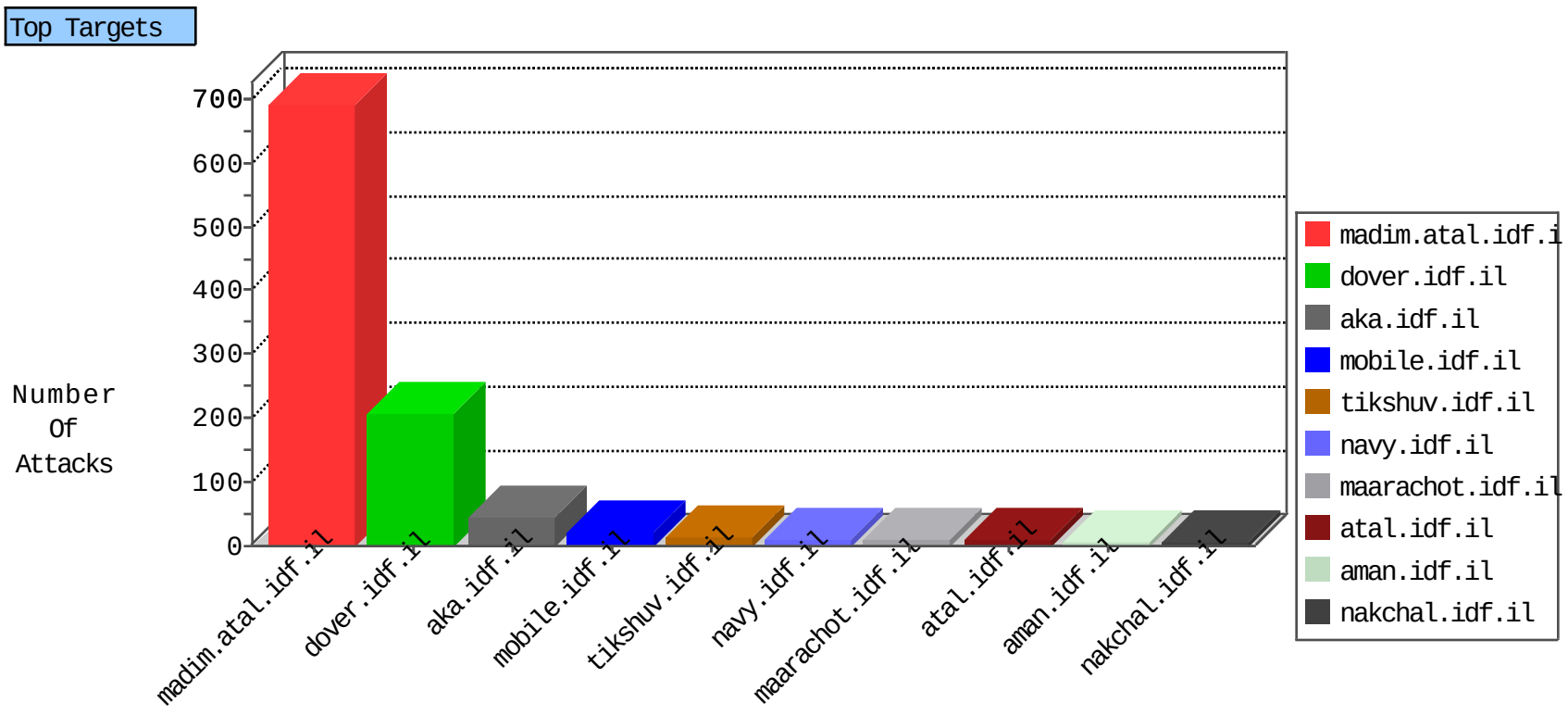
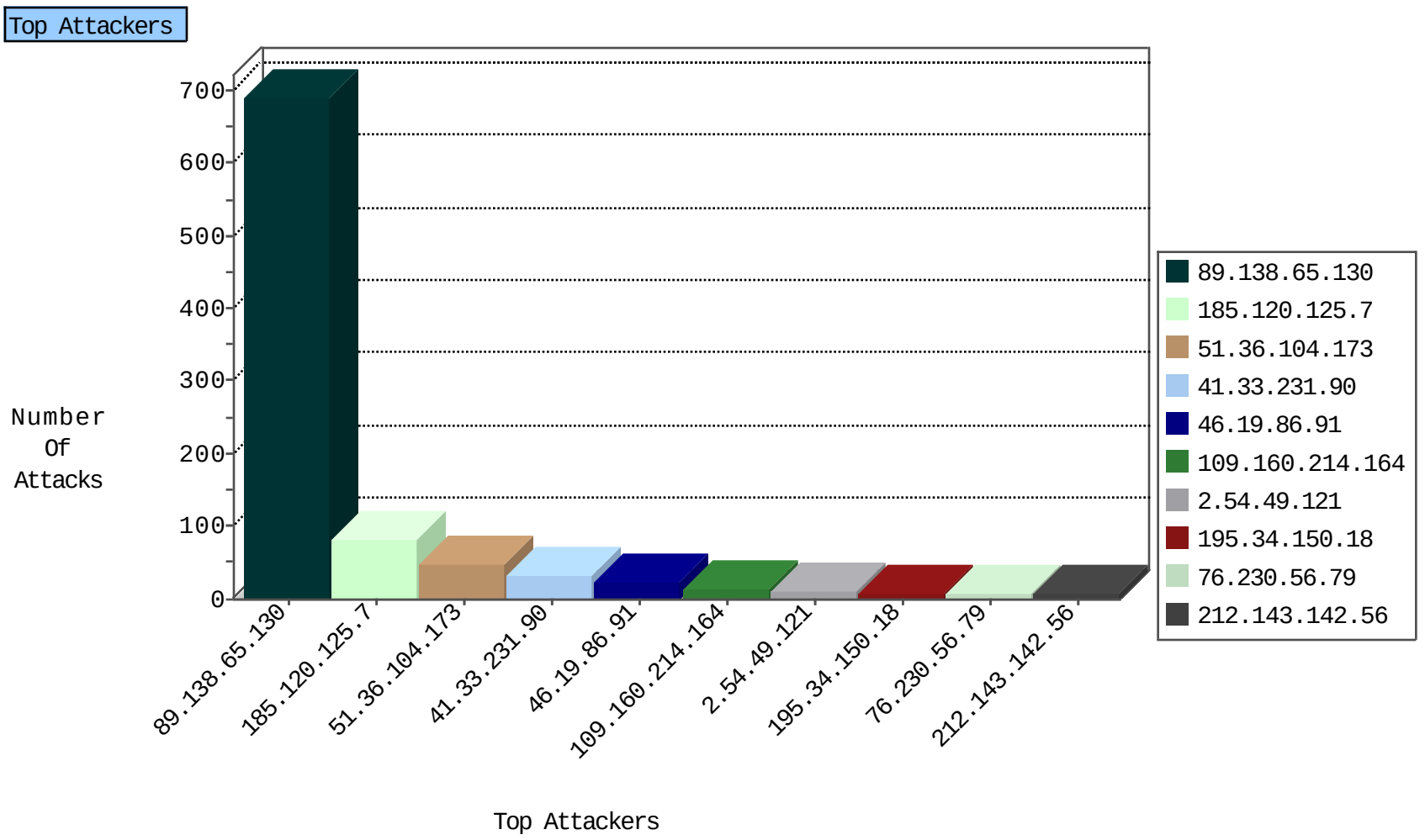
02-02-2016-01:07:15 to 02-02-2016-02:07:15

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-02-2016-01:07:15 to 02-02-2016-02:07:15

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	drop	4
178.239.62.139	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
178.239.62.139	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
178.239.62.139	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
178.239.62.139	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
178.239.62.139	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

02-02-2016-01:07:15 to 02-02-2016-02:07:15

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.111	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-02-2016-01:07:15 to 02-02-2016-02:07:15

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
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
183.61.109.189	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
173.55.32.113	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
121.201.27.61	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
108.228.245.226	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
198.20.69.74	147.237.77.235	United States	sviva.idf.il	ET DROP Dshield Block Listed Source	1
183.61.109.189	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
183.61.109.189	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
168.62.238.153	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
114.119.5.2	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
98.119.105.221	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1

02-02-2016-01:07:15 to 02-02-2016-02:07:15

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	54
51.36.104.173	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	43
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	27
46.19.86.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.49.121	Israel	147.237.0.34	tikshuv.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
194.90.89.5	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
66.249.78.161	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.160.214.164	Israel	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
5.102.254.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.78.147	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.160.214.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.183.173.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
198.71.227.53	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
185.120.125.56		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
51.36.104.173	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.46.38.171	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
51.36.104.173	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
76.115.96.90	United States	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.85.119	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
87.69.2.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
46.19.85.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.5.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
87.69.2.183	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
136.243.67.234	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
40.78.146.128	United States	147.237.77.216	dover.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
157.55.39.85	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
123.125.71.113	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
198.20.69.74	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.134.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.157	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.209.188.207	United States	147.237.77.216	dover.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
195.28.180.101	Israel	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
176.12.155.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
124.114.36.5	China	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
84.110.184.105	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.158	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.17.130	Germany	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
124.114.36.5	China	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.110.184.105	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
190.215.128.81	Chile	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

02-02-2016-01:07:15 to 02-02-2016-02:07:15

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.65.130	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 89.138.65.130	Block	374
89.138.65.130	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 89.138.65.130	Block	212
89.138.65.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
109.160.214.164	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	5
46.19.86.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
76.115.96.90	United States	147.237.77.170	maarachot.idf.il	Distributed Suspicious Response Code	Block	3
68.180.228.112	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/â€Ž	Block	1
76.230.56.79	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in URL Ö·\[[#31]]Öµ;$×°â€¢sÃ™–Ö³wâ€¦×,×±•×žÖ°[[#8]]t×?Æ'Ö±â€¦,â€"×§r/{Â?.Â¶dq×?â€“Ö»×´Ãš×²×¢Âœ×¤-n×œÂœÂ²,"Â°ÃžÃ¿Â¢l×³Â¨[[#2]]ÂŒiÖ·Ö»[[#18]]Ö¹Ã™k@×°Â¹s×¨×€Â¼Â d2â€š	Block	1
46.120.97.101	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
76.230.56.79	United States	147.237.77.233	atal.idf.il	Illegal HTTP Version	Block	1
66.249.69.11	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/templates/news/null	Block	1
89.138.65.130	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
76.230.56.79	United States	147.237.77.233	atal.idf.il	Abnormally Long Request method	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
76.230.56.79	United States	147.237.77.233	atal.idf.il	Malformed URL Ö·\[[#31]]Öµ;$×°â€¢sÃ™–Ö³wâ€¦×,×±•×žÖ°[[#8]]t×?Æ'Ö±â€¦,â€"×§r/{Â?.Â¶dq×?â€“Ö»×´Ãš×²×¢Âœ×¤-n×œÂœÂ²,"Â°ÃžÃ¿Â¢l×³Â¨[[#2]]ÂŒiÖ·Ö»[[#18]]Ö¹Ã™k@×°Â¹s×¨×€Â¼Â d2â€š	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149	Block	1
89.138.65.130	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
76.230.56.79	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Header Name	Block	1
40.77.167.32	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20235-he/kkkkkkk=342052f7kkkkkkk_342052f7	Block	1
76.230.56.79	United States	147.237.77.233	atal.idf.il	NULL Character in Method Â¼[[#0]][[#0]][[#0]]KÂ¬[[#11]]Ã†ÃœÃ€7[[#12]]Â?Â'Ã?Â½ÃƒÃŒÃ…Ã?Ã˜ZÃ"p6Â§Ã®Â§vWnJ7Â©4{Â¬Â-Â°Ã"M[[#31]]kÂ½Ã]W*[[#27]]Ã»0Ã-DÂ¨XeÃš[[#20]]Â¶JA	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
76.230.56.79	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Method Â¼[[#0]][[#0]][[#0]]KÂ¬[[#11]]Ã†ÃœÃ€7[[#12]]Â?Â'Ã?Â½ÃƒÃŒÃ…Ã?Ã˜ZÃ"p6Â§Ã®Â§vWnJ7Â©4{Â¬Â-Â°Ã"M[[#31]]kÂ½Ã]W*[[#27]]Ã»0Ã-DÂ¨XeÃš[[#20]]Â¶JA	Block	1
198.20.69.74	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/robots.txt	Block	1
76.230.56.79	United States	147.237.77.233	atal.idf.il	Unknown HTTP Request Method Â¼[[#0]][[#0]][[#0]]KÂ¬[[#11]]Ã†ÃœÃ€7[[#12]]Â?Â'Ã?Â½ÃƒÃŒÃ…Ã?Ã˜ZÃ"p6Â§Ã®Â§vWnJ7Â©4{Â¬Â-Â°Ã"M[[#31]]kÂ½Ã]W*[[#27]]Ã»0Ã-DÂ¨XeÃš[[#20]]Â¶JA in URL Ö·\[[#31]]Öµ	Block	1

02-02-2016-01:07:15 to 02-02-2016-02:07:15