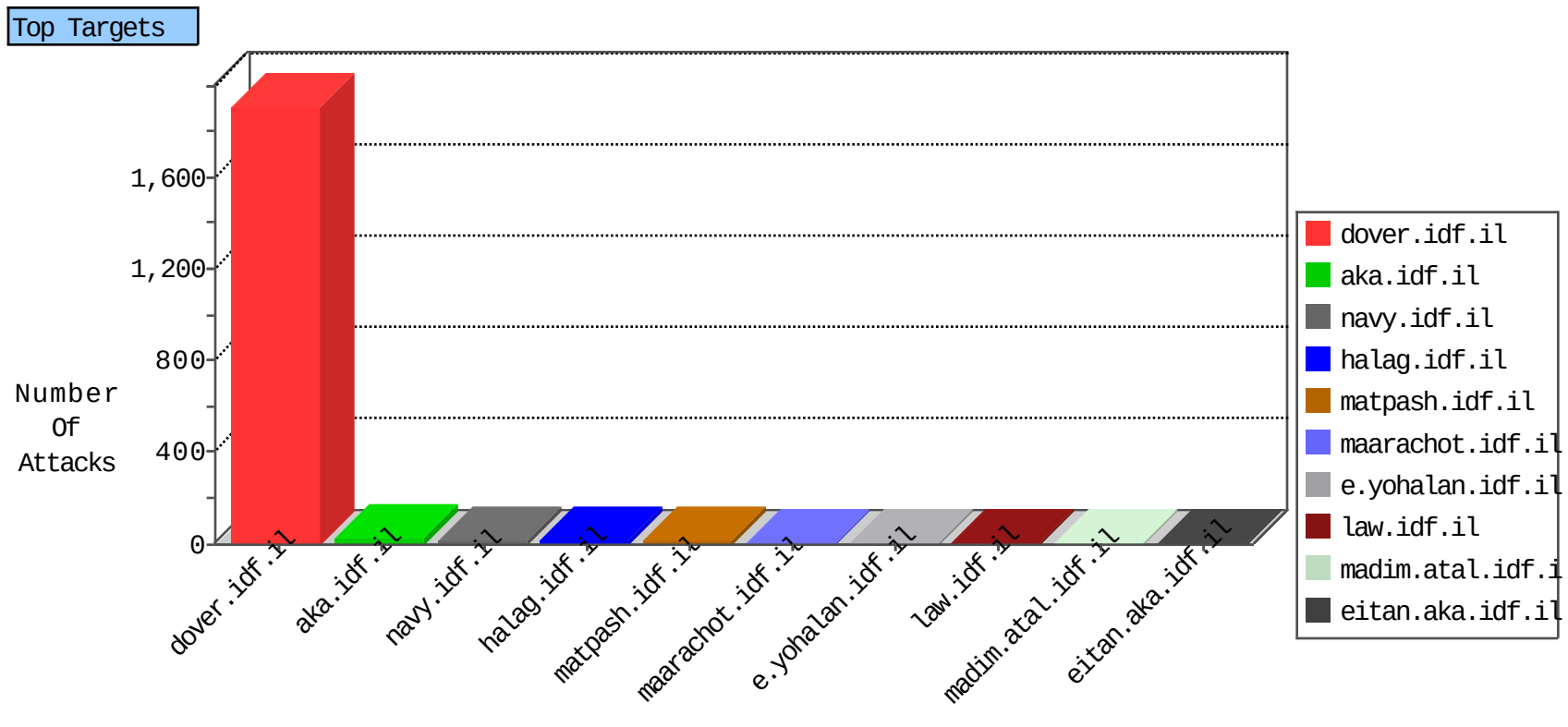
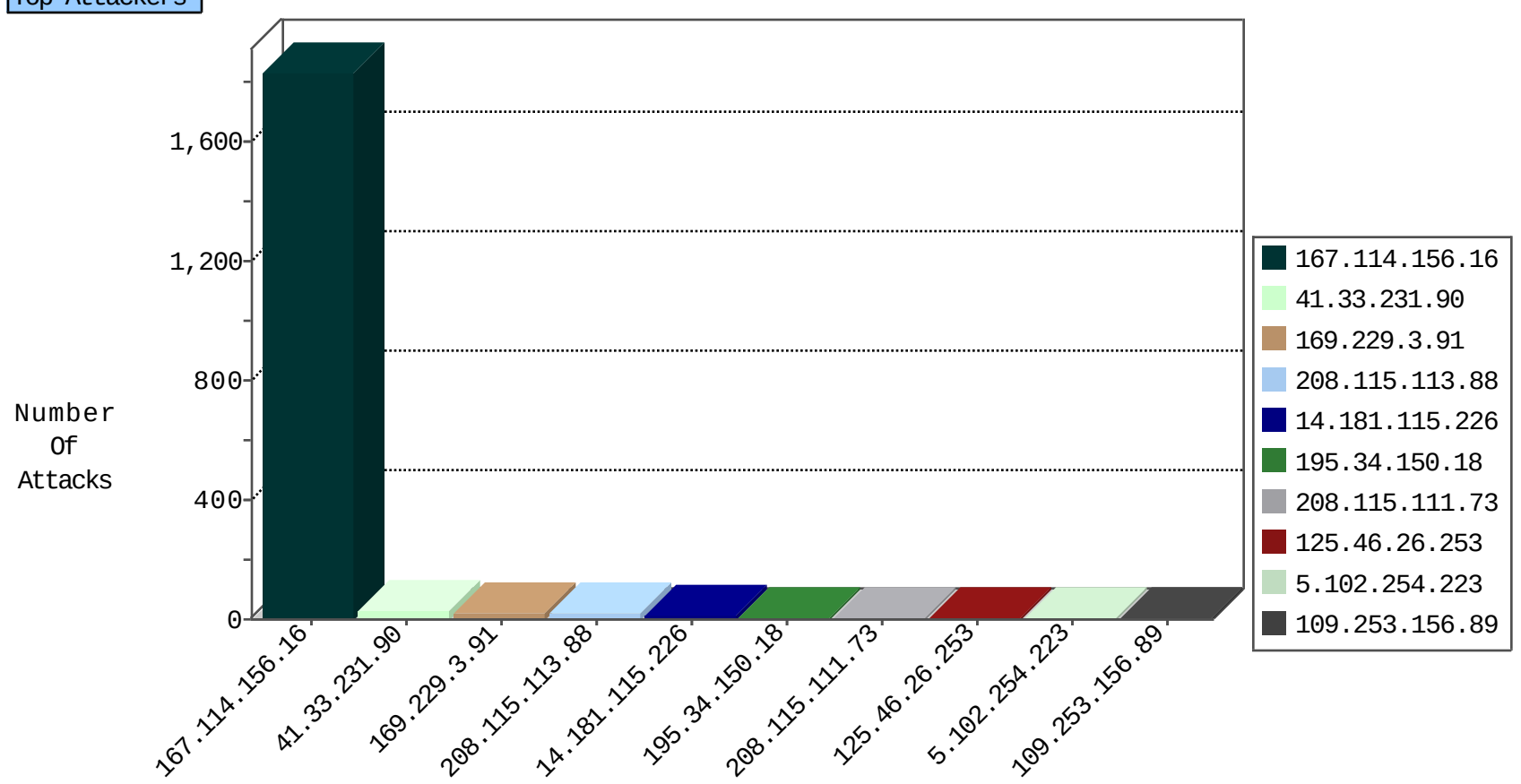
01-12-2016-02:04:06 to 01-12-2016-03:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-12-2016-02:04:06 to 01-12-2016-03:04:06

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	3051

01-12-2016-02:04:06 to 01-12-2016-03:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-12-2016-02:04:06 to 01-12-2016-03:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
183.47.98.72	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
146.185.250.2	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN NMAP -sS window 1024	1
113.171.23.126	147.237.76.201	Vietnam	e.atal.idf.il	ET SCAN Potential SSH Scan	1
104.193.172.73	147.237.76.198	Canada	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
104.193.172.73	147.237.76.198	Canada	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
1.165.7.57	147.237.8.27	Taiwan	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.106.92.44	147.237.77.74		law.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.219.238.10	147.237.8.24		e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
104.193.172.73	147.237.76.198	Canada	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1

01-12-2016-02:04:06 to 01-12-2016-03:04:06

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	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
14.181.115.226	Vietnam	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	6
14.181.115.226	Vietnam	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
40.77.167.68	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
157.55.2.157	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
5.102.254.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.210.187.226	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
208.115.111.73	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.10	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.46.39.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
207.46.13.14	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.211	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
185.3.147.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.219	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
159.203.218.135	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
131.253.35.149	United States	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
37.26.147.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.85	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
159.203.218.135	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
137.116.71.170	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.170	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
81.18.165.229	Netherlands	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
27.46.137.52	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
137.116.71.170	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.171	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.250.205.24	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.111.73	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.81	United States	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1

01-12-2016-02:04:06 to 01-12-2016-03:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	19
109.253.156.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
88.198.48.46	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/shared/usercontrols/headerupper/	Block	2
125.46.26.253	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
77.125.73.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.102.254.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
125.46.26.253	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-admin/admin-ajax.php	Block	2
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	2
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
173.238.242.217	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
73.234.145.235	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 73.234.145.235	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Abnormally Long Request method	Block	1
125.46.26.253	China	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 125.46.26.253	Block	1
40.77.167.62	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/sachar/faq.aspx	None	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Malformed URL â€¹Â¾Ö±Â¿Ö»%[[#15]]Ö·sÖ¾[[#14]]â,ª×²[[#14]][[#30]]â€” -×?Â¥Ã»[[#4]]Ã¼â€ -â€ ×'Ö¸	Block	1
150.70.173.51	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.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
180.243.123.30	Indonesia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
73.234.145.235	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in Method	Block	1
89.247.32.200	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/console/core/doc_mgr/undefined	Block	1
46.166.190.146	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
150.70.173.51	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
198.20.69.78	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Query String on â€ ¹Â¾Ö±Â¿Ö»%[[#15]]Ö·sÖ¾[[#14]]â,ª×²[[#14]][[#30]]â€” -×?Â¥Ã»[[#4]]Ã¼â€ -â€ ×'Ö¸	Block	1
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
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	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1756	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Unknown HTTP Request Method Â‰[[#26]]Â§Ã£vÃ¥X[[#28]]5NÃ‡ [[#19]]Â´, in URL â€¹Â¾Ö±Â¿Ö»%[[#15]]Ö·sÖ¾[[#14]]â, ª×²[[#14]][[#30]]â€"-×?Â¥Ã»[[#4]]Ã¼â€ -â€ ×'Ö¸	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Abnormally Long Request method	Block	1
80.82.215.199	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
8.37.70.83	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/1048-he/tikshuv.aspx&usg=alkjrhgta4ofqm_k3igc77nollu4q-3x_w	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in URL â€¹Â¾Ö±Â¿Ö»%[[#15]]Ö·sÖ¾[[#14]]â, ª×²[[#14]][[#30]]â€"-×?Â¥Ã»[[#4]]Ã¼â€ -â€ ×'Ö¸	Block	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method	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
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
125.46.26.253	China	147.237.77.176	matpash.idf.il	Admin Blocking	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
84.111.248.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
14.181.115.226	Vietnam	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal URL Path Encoding â€¹Â¾Ö±Â¿Ö»%[[#15]]Ö·sÖ¾[[#14]]â, ª×²[[#14]][[#30]]â€"-×?Â¥Ã»[[#4]]Ã¼â€ -â€ ×'Ö¸	Block	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1

01-12-2016-02:04:06 to 01-12-2016-03:04:06