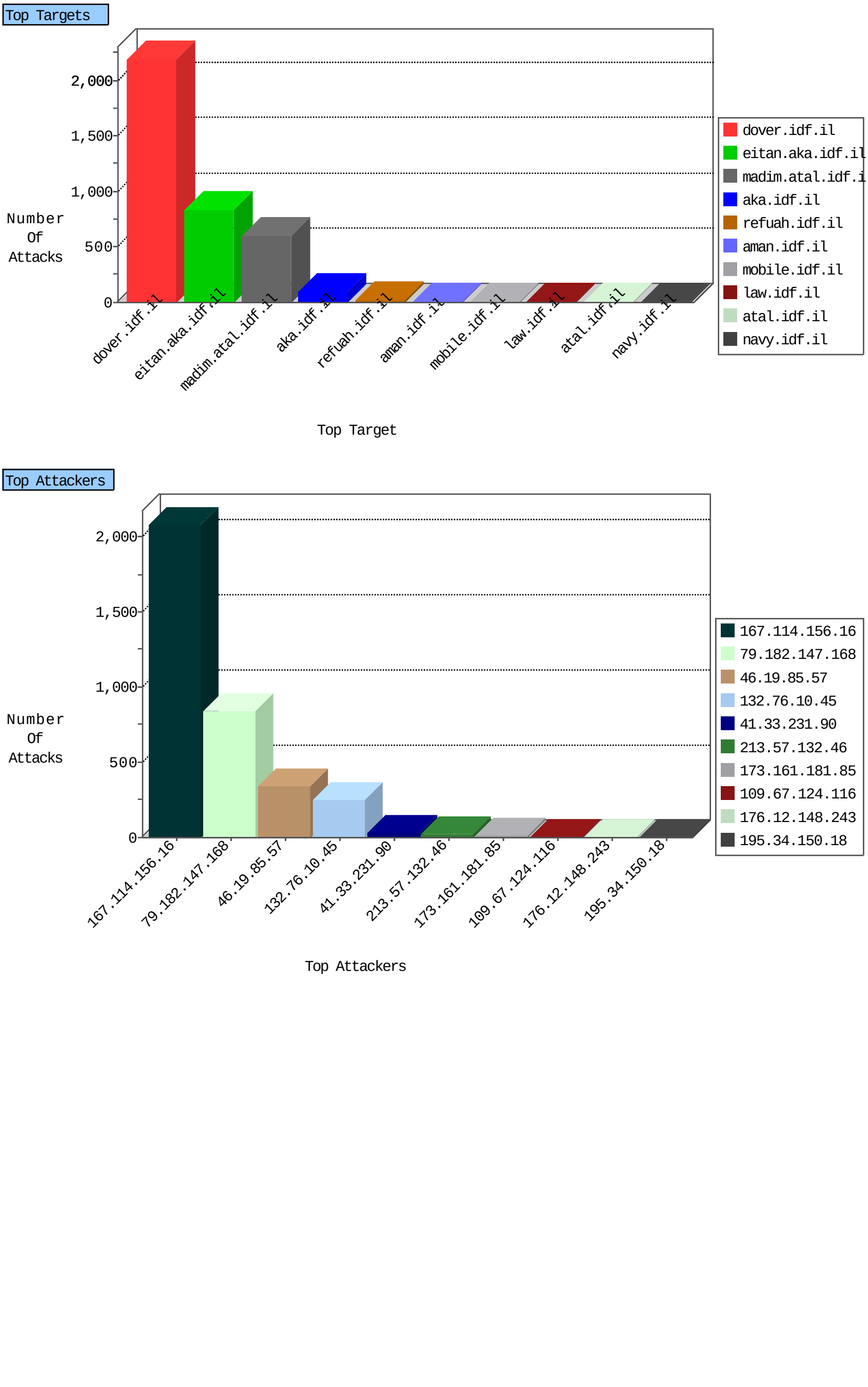
12-20-2015-01:04:04 to 12-20-2015-02:04:04

IDF Under Attack Daily Report



12-20-2015-01:04:04 to 12-20-2015-02:04:04

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	3180
58.46.64.46	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
40.77.167.73	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
58.46.64.46	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

12-20-2015-01:04:04 to 12-20-2015-02:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
176.65.26.124	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	13444: HTTP: WhatWeb User-Agent Header	Block	1

12-20-2015-01:04:04 to 12-20-2015-02:04:04

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
66.249.64.153	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
217.16.2.77	147.237.77.121	France	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
217.16.2.77	147.237.0.35	France	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.105.134.220	147.237.76.31	Sweden	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
58.253.96.122	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
5.39.222.253	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
217.16.2.77	147.237.76.177	France	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.253.96.122	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
5.39.222.253	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1

12-20-2015-01:04:04 to 12-20-2015-02:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.147.168	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	732
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.67.124.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.132.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
213.57.132.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
213.57.132.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
185.3.144.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
174.24.212.161	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.156.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.45.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	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
173.161.181.85	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
87.68.76.219	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
94.230.86.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.12.148.243	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.86.112	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
79.181.59.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.19.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.233	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.61.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.12.148.243	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
79.177.60.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.144.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.36	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
46.19.86.182	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.31	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.131.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
157.55.39.214	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.228.16.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
109.67.115.55	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
213.57.131.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
157.55.39.247	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
213.57.131.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.85.57	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.8.204.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
155.94.222.12	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
40.77.167.73	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
94.102.60.89	Netherlands	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
98.231.146.3	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.146.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.36	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
40.77.167.73	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.113.89	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.19.85.40	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
94.102.60.89	Netherlands	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.120.125.60		147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

12-20-2015-01:04:04 to 12-20-2015-02:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	182
132.76.10.45	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 132.76.10.45	Block	138
46.19.85.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
79.182.147.168	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.147.168	Block	107
132.76.10.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.85.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	45
132.76.10.45	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 132.76.10.45	Block	8
2.54.170.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.121.28.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.8.204.1	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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	2
213.8.204.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.117.18.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
173.161.181.85	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Query String â,ª×²â€ [[#18]][[#15]] on t.â€¦â,ªÂ´Â¿Ö±Ë†nz3Ö±g×©×ƒ6Â°Ã¿â€š×¡×¦Ö¶oÖµ×£fÂ?â„¢Â¨eÂ¡â,¬[[#26]]=×Ÿ×˜<Ö³[[#16]]×žÃ¶[[#25]]lÃŠ[[#17]]Â¸â,¬Ã¼	Block	1
93.172.153.167	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 93.172.153.167 (Unknown SSL Session)	None	1
173.161.181.85	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method Â¬[[#0]][[#0]][[#0]]BÂ¦Â•Ã?Ã€bXdÃ¯MRÃ¬Ã¾nÂ?Ã?Â¬Â£[[#27]]Â?{tÃ‡^Ã?[[#5]]Â§*Ã³ÃµÂ¦pÂ±\Ã¯Ã€Âœ"Ã³[[#14]]Â¸Â¿Â–[[#22]]Â'Ã´IÂ¹@RÂƒÃ±Ã„bEÃ–Â…Â¸Ã•	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.247	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/klali.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
46.166.186.210	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
173.161.181.85	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in URL t.â€¦â,ªÂ´Â¿Ö±Ë†nz3Ö±g×©×ƒ6Â°Ã¿â€š×¡×¦Ö¶oÖµ×£fÂ?â„¢Â¨eÂ¡â,¬[[#26]]=×Ÿ×˜<Ö³[[#16]]×žÃ¶[[#25]]lÃŠ[[#17]]Â¸â,¬Ã¼	Block	1
98.231.146.3	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
176.12.148.243	Israel	147.237.72.166	aka.idf.il	Too Many Cookies in a Request - 112 cookies	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/kesher	Block	1
173.161.181.85	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
109.67.115.55	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
80.246.62.135	Germany	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
207.46.13.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/klali/null	Block	1
46.166.188.248	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
173.161.181.85	United States	147.237.76.42	refuah.idf.il	Malformed URL t.â€¦â,ªÂ´Â¿Ö±Ë†nz3Ö±g×©×ƒ6Â°Ã¿â€š×¡×¦Ö¶oÖµ×£fÂ?â„¢Â¨eÂ¡â,¬[[#26]]=×Ÿ×˜<Ö³[[#16]]×žÃ¶[[#25]]lÃŠ[[#17]]Â¸â,¬Ã¼	Block	1
149.78.184.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	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
188.191.228.145	Russian Federation	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
46.19.86.60	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
173.161.181.85	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method Â¬[[#0]][[#0]][[#0]]BÂ¦Â•Ã?Ã€bXdÃ¯MRÃ¬Ã¾nÂ?Ã?Â¬Â£[[#27]]Â?{tÃ‡^Ã?[[#5]]Â§*Ã³ÃµÂ¦pÂ±\Ã¯Ã€Âœ"Ã³[[#14]]Â¸Â¿Â–[[#22]]Â'Ã´IÂ¹@RÂƒÃ±Ã„bEÃ–Â…Â¸Ã•	Block	1
80.246.62.135	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
173.161.181.85	United States	147.237.76.42	refuah.idf.il	NULL Character in Method Â¬[[#0]][[#0]][[#0]]BÂ¦Â•Ã?Ã€bXdÃ¯MRÃ¬Ã¾nÂ?Ã?Â¬Â£[[#27]]Â?{tÃ‡^Ã?[[#5]]Â§*Ã³ÃµÂ¦pÂ±\Ã¯Ã€Âœ"Ã³[[#14]]Â¸Â¿Â–[[#22]]Â'Ã´IÂ¹@RÂƒÃ±Ã„bEÃ–Â…Â¸Ã•	Block	1
54.153.32.246	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
157.55.39.214	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.187.129.166	France	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/1133-22638-he/dover.aspx.	Block	1
188.191.228.145	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/menu-ending.gif	Block	1
173.161.181.85	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Parameter Name â,ª×²â€ [[#18]][[#15]] in t.â€¦â,ªÂ´Â¿Ö±Ë†nz3Ö±g×©×ƒ6Â°Ã¿â€š×¡×¦Ö¶oÖµ×£fÂ?â„¢Â¨eÂ¡â,¬[[#26]]=×Ÿ×˜<Ö³[[#16]]×žÃ¶[[#25]]lÃŠ[[#17]]Â¸â,¬Ã¼	Block	1
132.76.10.45	Israel	147.237.0.19	madim.atal.idf.i	Too Many 403: Response Code per Session	Block	1
89.138.73.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

12-20-2015-01:04:04 to 12-20-2015-02:04:04