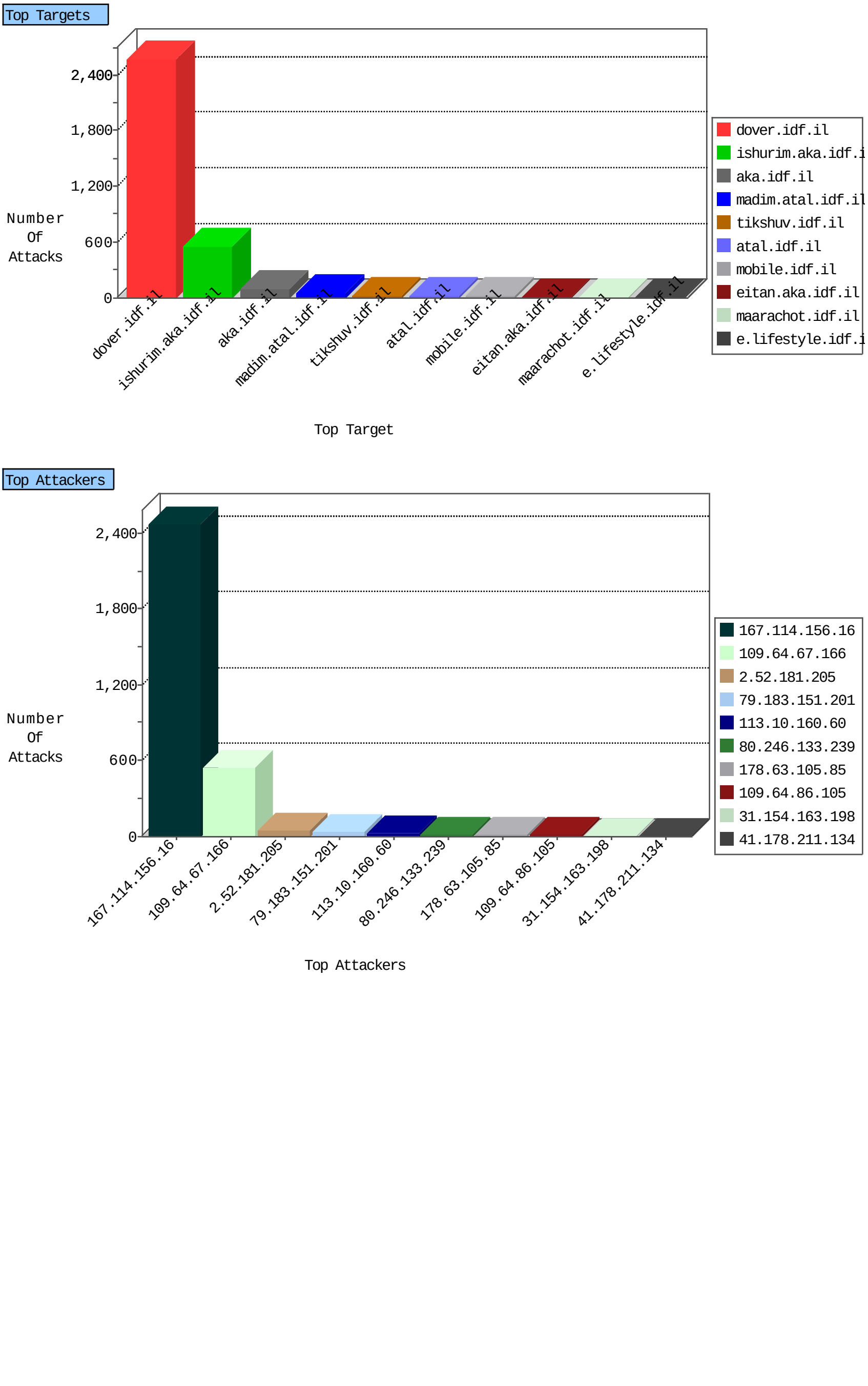
03-14-2016-00:04:08 to 03-14-2016-01:04:08

IDF Under Attack Daily Report



03-14-2016-00:04:08 to 03-14-2016-01:04:08

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	3355
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
82.145.217.86	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1
94.102.49.206	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
212.143.254.66	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

03-14-2016-00:04:08 to 03-14-2016-01:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.163.198	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
176.13.9.251	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
97.104.98.214	United States	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
113.10.160.60	Hong Kong	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

03-14-2016-00:04:08 to 03-14-2016-01:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.133.239	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
180.97.81.71	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
128.199.128.167	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
122.114.117.177	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
122.114.117.177	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
52.11.196.117	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
23.96.219.55	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
23.96.219.55	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
5.160.14.250	147.237.76.34	Iran, Islamic Republic of	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
184.80.10.136	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
139.217.27.204	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
122.114.117.177	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
122.114.117.177	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
40.117.103.99	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
23.96.219.55	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
23.96.219.55	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

03-14-2016-00:04:08 to 03-14-2016-01:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.67.166	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	552
79.183.151.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
109.64.86.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.43.51.144	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
80.246.133.239	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.66.60.75	Denmark	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
149.88.251.52	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.120.49.103	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	4
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	4
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	3
79.176.115.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.154.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.184.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.186.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.154.189.8	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.1.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.17.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.172.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.26.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.12.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.31.110	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.182.161.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.138.202.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.178.211.134	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	2
89.138.202.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	2
79.176.241.211	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
68.180.231.54	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.178.211.134	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
41.178.211.134	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.46.39.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.125	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.194	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
41.43.51.144	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.68	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.102.254.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.77	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.146.192	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
109.253.134.52	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

03-14-2016-00:04:08 to 03-14-2016-01:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.181.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
113.10.160.60	Hong Kong	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 113.10.160.60	Block	25
66.220.145.245	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.64.86.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
157.55.39.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
71.166.97.130	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
131.253.25.192	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.179.99.65	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method KA+$ZÐƒ§Ì±é¼)üËú/d¢±¤ç–[[#16]]Š5iA !¼oÞ8[[#16]]3è2‹Ü²¨DÆiªOãžHäCÚ[[#16]]›·»[[#28]]”tW‹"ÝºŸÍáN1,"*™V7[[#3]],Ä•[[#24]]yÈ¸4kn:è•Ú¾¬—•2à–S=3õÄ²*[[#19]]álÑÉ¨[[#21]]@Ò¨’³aö_³ÌY¿<[[#6]]_Òw[[#28]]gLŠúíf#012A[[#20]]—¬ãè•(ì{q[[#22]]N-Å„¶Ø_[[#4]]á'¬²ùìˆ[[#1]]ôlÌ²[[#12]]uÜŽxˆ¹ÞžžlßÕ^AÜ}¶^È[[#20]]ŽÙ±LêzM•¸B¡òË[[#12]]78T	Block	1
207.46.13.172	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.69.85	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/english/pages/default.aspx	Block	1
141.212.122.64	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /x	Block	1
87.71.9.228	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
79.179.99.65	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name C”Gwž!Á×ë•[[#3]]}³_[[#16]][[#4]]tÖŠú±U[[#17]]+l0#011K[[#8]]ŒÒiG€"•z³63B¬¿tœÜÄNîKut–-àÖó[[#7]]è]1fñNkN+ó"šUïGŸq3ÆŠ	Block	1
113.10.160.60	Hong Kong	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 113.10.160.60	Block	1
79.179.99.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
141.212.122.64	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /x	Block	1
37.26.148.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
92.77.138.187	Germany	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 92.77.138.187 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
79.179.99.65	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xyzzy	Block	1
87.71.9.228	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
77.66.60.75	Denmark	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-en	Block	1
149.88.251.52	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
37.237.192.104	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
95.91.192.120	Germany	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.99.65	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method KA+$ZÐƒ§Ì±é¼)üËú/d¢±¤ç–[[#16]]Š5iA !¼oÞ8[[#16]]3è2‹Ü²¨DÆiªOãžHäCÚ[[#16]]›·»[[#28]]”tW‹"ÝºŸÍáN1,"*™V7[[#3]],Ä•[[#24]]yÈ¸4kn:è•Ú¾¬—•2à–S=3õÄ²*[[#19]]álÑÉ¨[[#21]]@Ò¨’³aö_³ÌY¿<[[#6]]_Òw[[#28]]gLŠúíf#012A[[#20]]—¬ãè•(ì{q[[#22]]N-Å„¶Ø_[[#4]]á'¬²ùìˆ[[#1]]ôlÌ²[[#12]]uÜŽxˆ¹ÞžžlßÕ^AÜ}¶^È[[#20]]ŽÙ±LêzM•¸B¡òË[[#12]]78T	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
198.58.102.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
113.10.160.60	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fck/	Block	1
2.52.42.253	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.71.9.228	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
79.179.99.65	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
156.199.152.250		147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.7.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
79.179.99.65	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
66.249.64.198	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1763	Block	1
207.46.13.160	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.52.181.205	Israel	147.237.0.19	madim.atal.idf.i	Cookie Tampering on cookie Login: Expected ********** *, Observed **********	None	1
87.71.9.228	Israel	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
79.179.99.65	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
46.19.86.129	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
157.55.39.112	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1

03-14-2016-00:04:08 to 03-14-2016-01:04:08