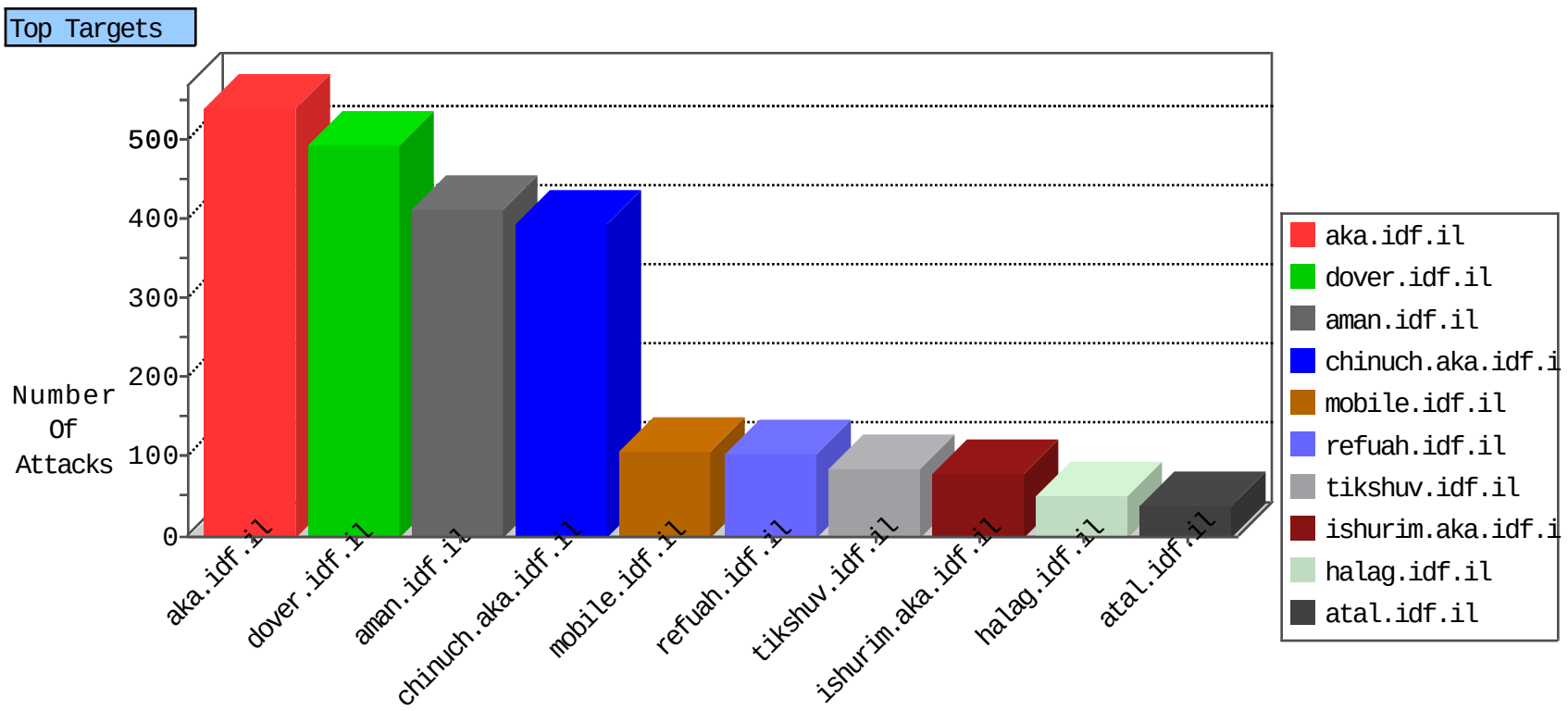
02-02-2016-17:04:08 to 02-02-2016-18:04:08

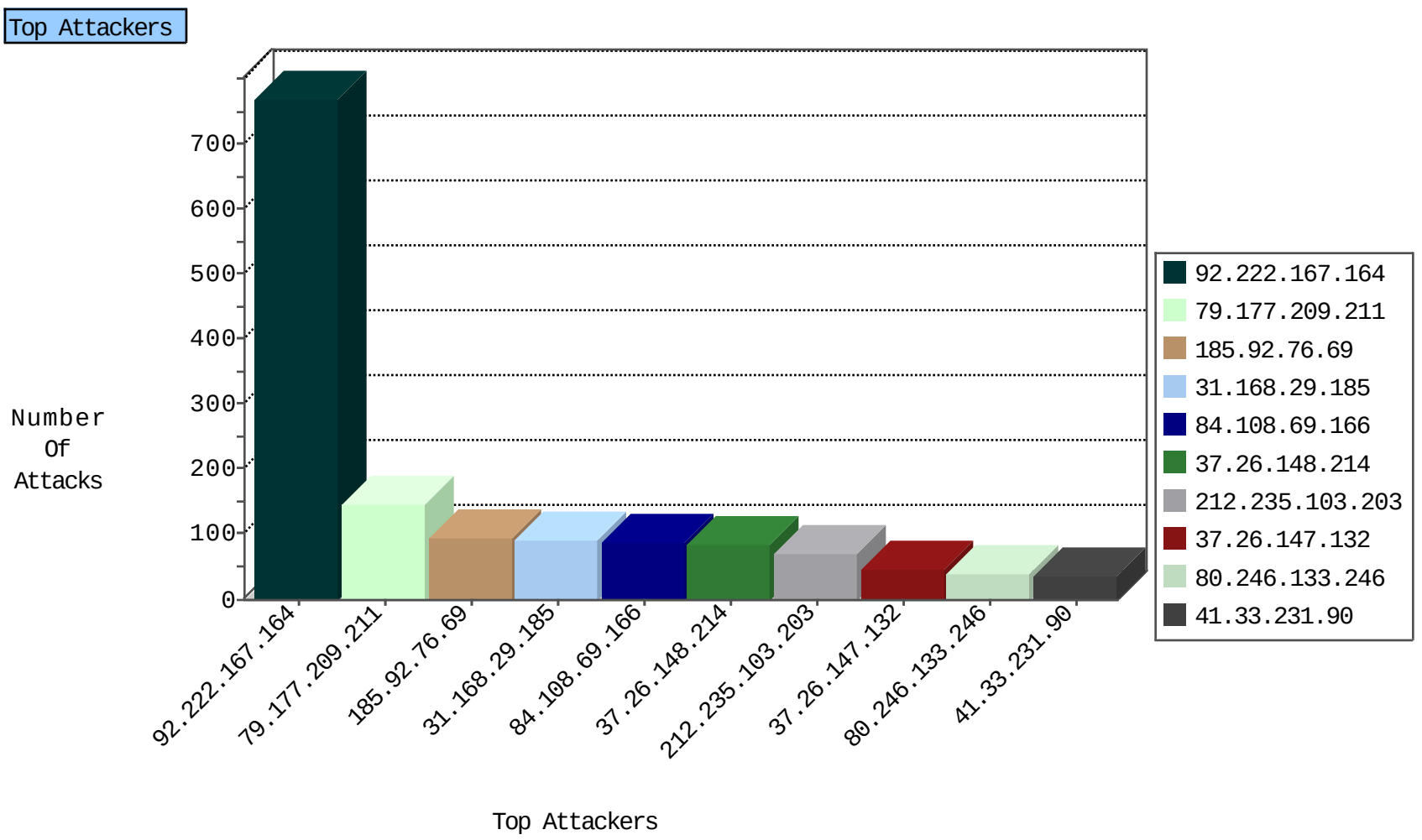
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-02-2016-17:04:08 to 02-02-2016-18:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
70.192.135.153	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1709
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	35
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	10
164.138.122.32	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
46.19.86.195	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
183.60.48.25	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
74.143.58.3	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
61.160.215.88	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

02-02-2016-17:04:08 to 02-02-2016-18:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-02-2016-17:04:08 to 02-02-2016-18:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

02-02-2016-17:04:08 to 02-02-2016-18:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
92.222.167.164	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	379
92.222.167.164	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	274
79.177.209.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	147
92.222.167.164	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	99
185.92.76.69		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
31.168.29.185	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	89
37.26.148.214	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
212.235.103.203	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	69
37.26.147.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
80.246.133.246	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
132.66.235.215	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
46.19.86.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.115	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
89.138.27.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.12.155.51	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
46.19.85.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.52.23.161	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
92.222.167.164	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.120.134.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
80.246.133.104	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.22	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	7
31.210.186.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
54.151.42.39	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
84.94.40.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
2.54.29.82	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
176.12.154.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.69.104	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.168.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.15.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.130.192	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.133.104	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
176.12.155.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.97	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	4
149.78.172.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.226.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
31.210.187.152	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
2.52.148.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.23.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.46.38.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.117.221.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

02-02-2016-17:04:08 to 02-02-2016-18:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 84.108.69.166	Block	10
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 84.108.69.166	Block	9
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 84.108.69.166	Block	9
2.54.49.113	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 84.108.69.166	Block	8
80.178.97.72	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	7
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 84.108.69.166	Block	6
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 84.108.69.166	Block	4
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.95	Block	4
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 84.108.69.166	Block	4
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.95	Block	4
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 84.108.69.166	Block	4
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 84.108.69.166	Block	4
176.12.155.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.139.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.24.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/footerback.gif"	Block	3
176.12.154.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 84.108.69.166	Block	3
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Url from 84.108.69.166	Block	3
176.12.154.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
116.203.6.195	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
212.143.124.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
188.143.232.70	Russian Federation	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 188.143.232.70	Block	2
212.150.215.254	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/0/112410.pdf	Block	2
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 84.108.69.166	Block	2
185.32.179.218	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
188.143.232.22	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.22	Block	2
116.203.6.195	India	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
80.246.136.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.155.51	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.95	Block	2
79.182.55.241	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
46.19.86.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
37.26.149.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.136.217	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.108.69.166	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
166.63.123.145	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.95	Block	1
31.168.29.185	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
109.66.10.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.166.98.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
213.151.42.213	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	1
79.194.87.199	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
84.108.69.166	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 84.108.69.166 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
46.120.134.17	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 46.120.134.17	Block	1

02-02-2016-17:04:08 to 02-02-2016-18:04:08