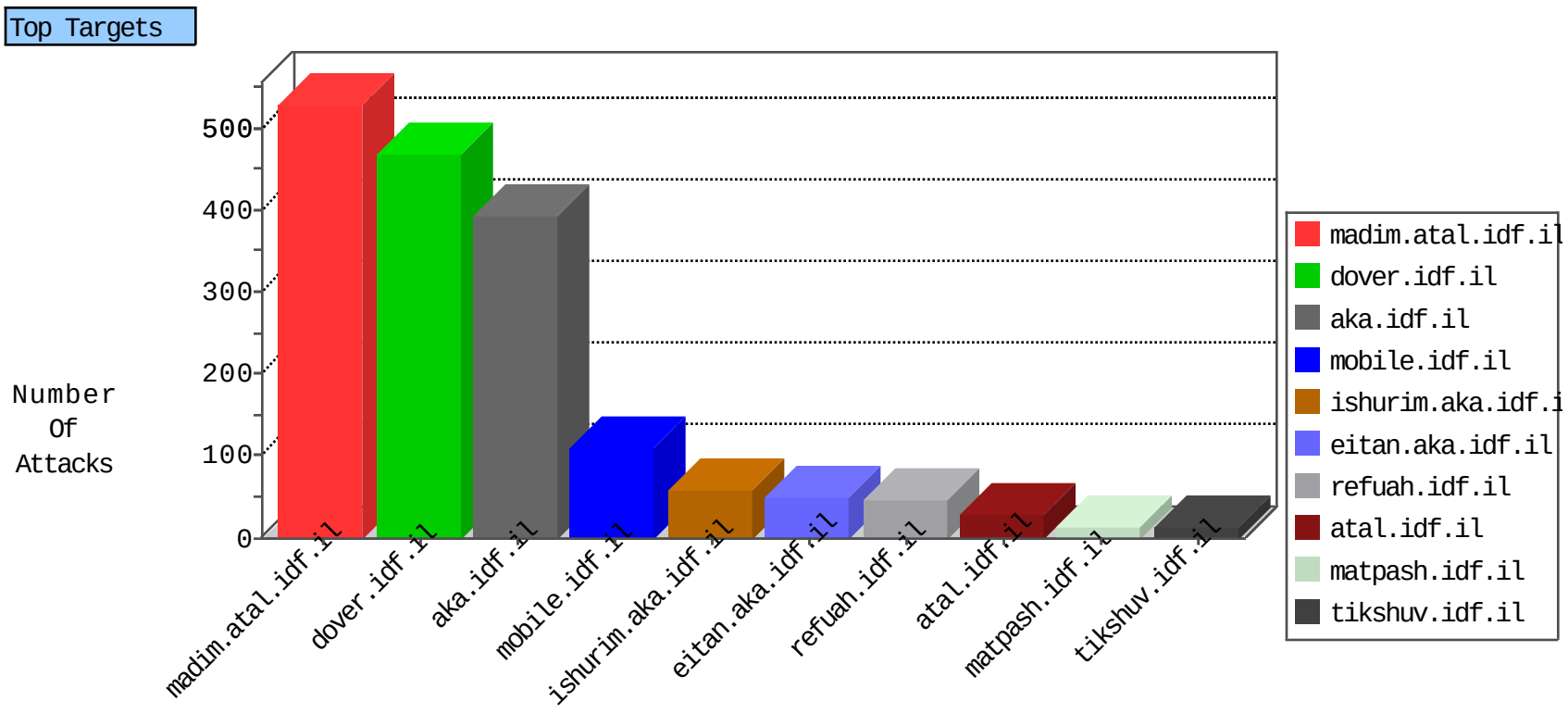
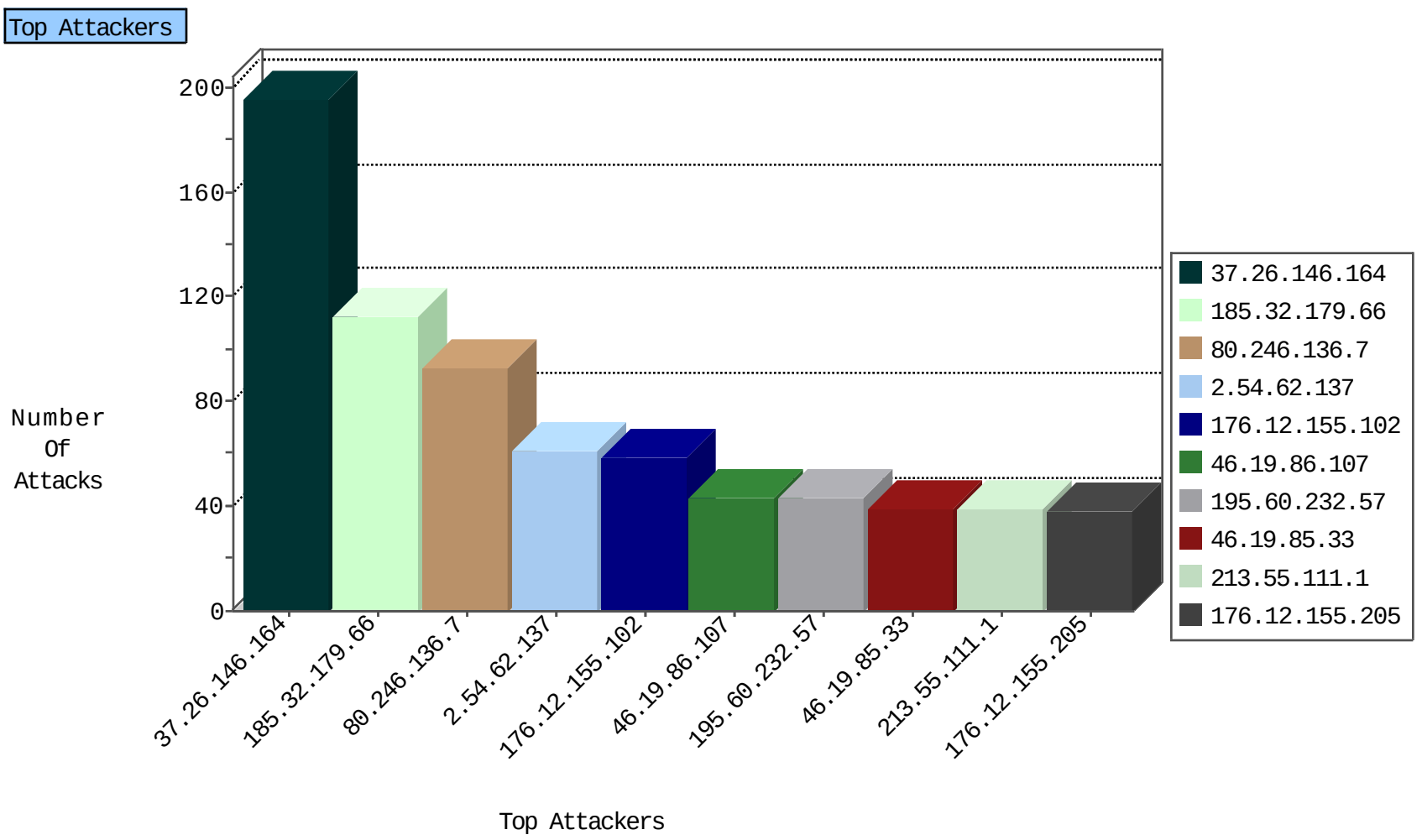
02-02-2016-09:04:08 to 02-02-2016-10:04:08

IDF Under Attack Daily Report





02-02-2016-09:04:08 to 02-02-2016-10:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
80.246.136.215	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
2.54.170.217	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
213.8.204.80	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2

02-02-2016-09:04:08 to 02-02-2016-10:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-02-2016-09:04:08 to 02-02-2016-10:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.60.232.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
212.143.186.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.225.171.194	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
109.186.182.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.177.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.25.112.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.110.132.54	147.237.76.148		gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
109.64.6.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.96.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-02-2016-09:04:08 to 02-02-2016-10:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.33	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	39
213.55.111.1	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
185.32.179.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
2.54.62.137	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	27
176.12.154.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
185.32.179.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	26
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
2.54.62.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
46.19.85.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
185.32.179.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
185.32.179.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
87.69.232.227	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
82.166.140.117	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.12.154.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.117.155.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
37.26.146.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.179.114.27	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
185.32.179.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
46.19.85.71	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
213.57.94.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.179.114.27	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
37.26.147.198	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
79.178.229.125	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.115.83.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
79.178.229.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.246.140.174	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.31	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
109.65.66.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.8.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.114.3	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.194.206.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.38.95	Israel	147.237.77.243	mobile.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
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
192.115.83.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.173	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.65.217.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.194.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.138.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.156	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.62.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.85.156	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.54.48.144	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.32.179.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	128
80.246.136.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
37.26.146.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	66
176.12.155.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
46.19.86.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
176.12.155.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
176.12.154.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
37.26.146.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
80.246.136.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
176.12.155.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
213.151.36.149	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.151.36.149	Block	5
37.26.146.189	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 37.26.146.189	Block	5
176.12.154.122	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.54.184.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.154.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
89.138.65.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
76.115.96.90	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.154.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
40.77.167.32	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/main/home/default.aspx	Block	3
37.26.147.160	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.147.160	Block	2
2.54.2.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.147.160	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	2
37.26.147.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.154.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.117.143.250	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
37.26.148.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	2
2.54.155.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	2
2.52.20.6	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.12.155.76	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.66.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/109222.pdf	Block	1
93.173.250.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
176.126.252.12	Romania	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
84.228.62.113	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
40.77.167.33	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
79.178.14.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.25.112.2	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.67	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/109172.pdf	Block	1
46.19.86.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/guys	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
213.151.36.149	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/&sa=u&ved=0ahukewjbonidxdjkahuehhokhsgocmsqfggomam&usg=afqjcneeywysowwcocycbntx0qxav9lbkw	Block	1