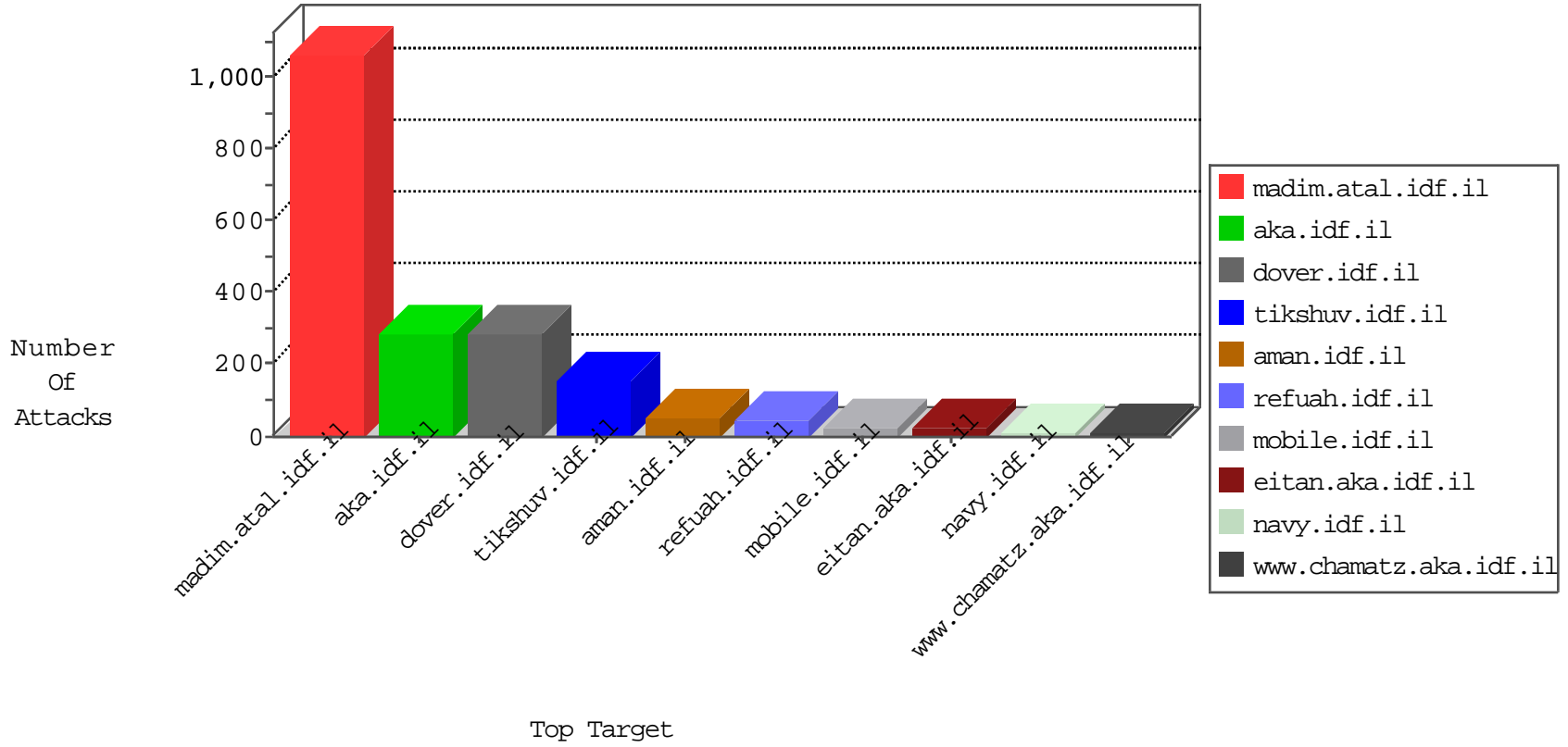


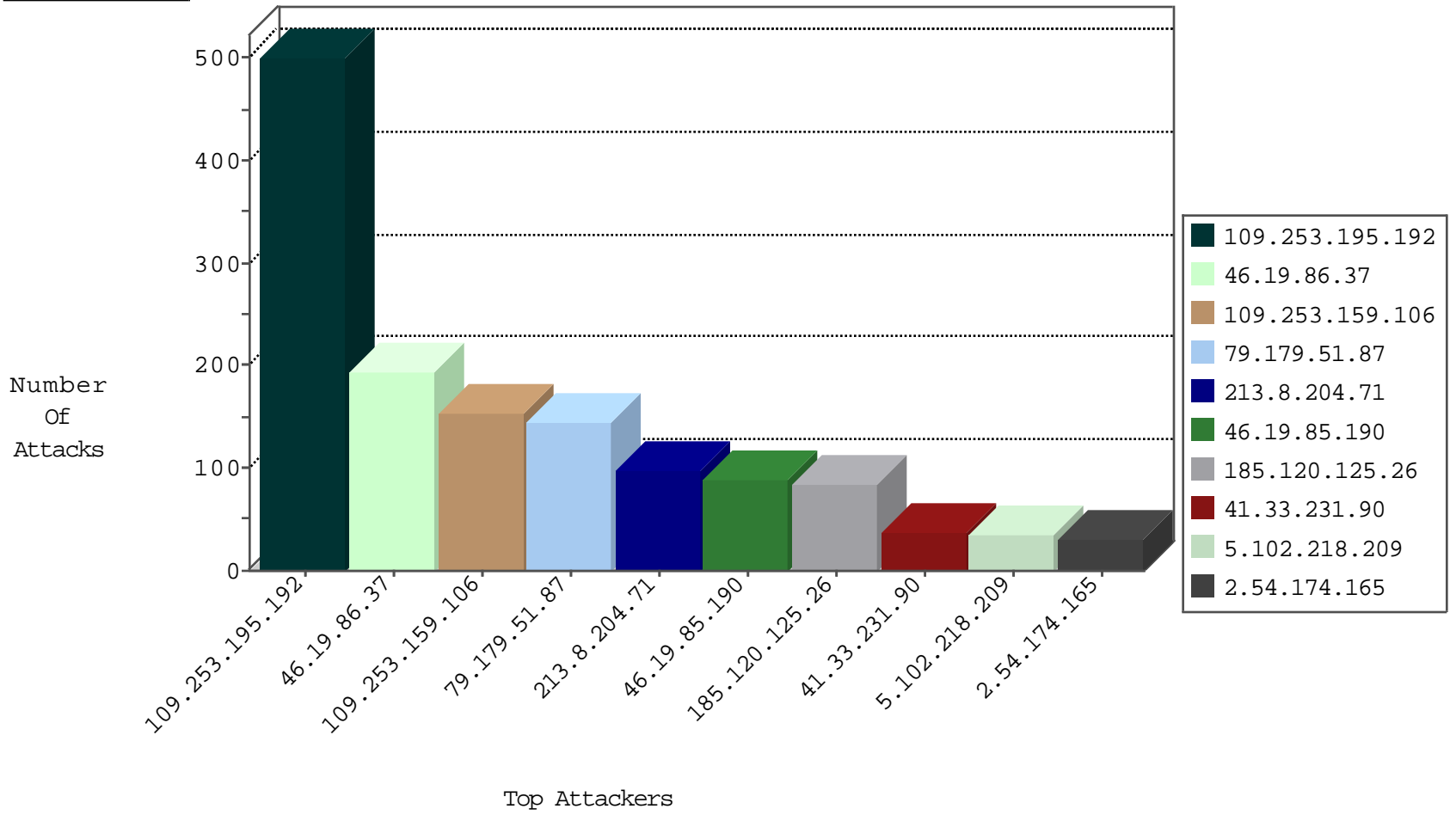
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.202.128.149	Ukraine	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
31.202.128.149	Ukraine	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
31.202.128.149	Ukraine	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
31.202.128.149	Ukraine	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
31.202.128.149	Ukraine	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.98.3.81	Netherlands	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2

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
59.46.193.114	147.237.0.200	China	m4u.idf.il	GPL SCAN nmap TCP	2
218.24.171.223	147.237.0.200	China	m4u.idf.il	GPL SCAN nmap TCP	2
218.246.0.97	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.204.71	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
1.189.209.194	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
1.189.209.194	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
128.199.53.63	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
1.189.209.194	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
125.212.232.144	147.237.76.201	Vietnam	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
1.189.209.194	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
104.131.139.20	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP Lizard Cart CMS SQL injection in detail.php id attempt	1
104.130.169.225	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
91.207.60.30	147.237.76.148	Ukraine	ggcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.180.54.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
1.189.209.194	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.77.233	United States	atal.idf.il	ET DROP Dshield Block Listed Source	1
1.189.209.194	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
188.120.148.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
1.189.209.194	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
125.212.232.144	147.237.76.201	Vietnam	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
1.189.209.194	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
109.186.173.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
1.189.209.194	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
104.130.169.225	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
104.130.169.225	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.207.60.30	147.237.76.147	Ukraine	chimuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
5.102.218.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
46.117.7.140	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
2.54.174.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
213.57.87.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.46.39.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.88	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.202.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
94.230.86.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.229.32.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.11.237	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.174.197	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
188.120.152.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.145.219.180	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.174.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.229.32.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.176.242	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
2.54.174.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.174.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.67.11.237	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
87.69.120.243	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.78.170	United States	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.210.186.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.39.213	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.117.58.169	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
31.210.187.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.135.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.139.208	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
149.78.14.94	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.178.57.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.38.215	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.158.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.6.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.67.6.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.232.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.22.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.245.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.140.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.6.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
82.81.45.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.195.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	257
79.179.51.87	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.179.51.87	Block	145
109.253.195.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	140
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	108
109.253.159.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
109.253.195.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
213.8.204.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
46.19.85.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
109.253.159.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
46.19.85.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
89.138.175.137	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 89.138.175.137	Block	19
213.8.204.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	19
89.139.24.74	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.139.24.74	Block	16
80.246.136.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
188.143.232.43	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$ucArticleLobbyControl\$datepicker in www.idf.il/1283-en/dover.aspx	Block	7
84.109.80.130	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	5
80.246.137.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
65.208.151.113	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	3
80.246.136.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.128.35.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
65.208.151.117	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	2
87.71.2.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
95.86.121.186	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1141-he/dover.aspx&sa=u&ved=0ahukewjtlvvywebkahwha3ik hxjobs0qfggkmac&usg=afqjcnhkhqezgvtly8qaaymujs8oe2kqhva	Block	1
77.126.221.138	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
178.57.208.101	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
65.208.151.116	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripts/{1}	Block	1
109.160.164.214	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$TochenPlaceHolder\$ct138\$ct101\$ct103\$cb1Question \$6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
87.68.157.97	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.121.44.39	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$TochenPlaceHolder\$ct138\$ct101\$ct103\$cb1Question \$0 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
198.58.102.156	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
37.26.146.220	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.69.112	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/general/general.aspx	Block	1
65.208.151.114	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	1
95.86.127.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/61998	Block	1
84.109.80.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	1
77.126.221.138	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 77.126.221.138	Block	1
109.253.138.239	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$TochenPlaceHolder\$ct138\$ct101\$ct103\$cb1Question \$2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1769	Block	1
65.208.151.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	1
104.131.139.20	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
84.229.32.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.127.63.81	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
65.208.151.118	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 65.208.151.118	Block	1
65.208.151.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 65.208.151.112	Block	1
41.82.92.179	Senegal	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
128.194.131.235	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1