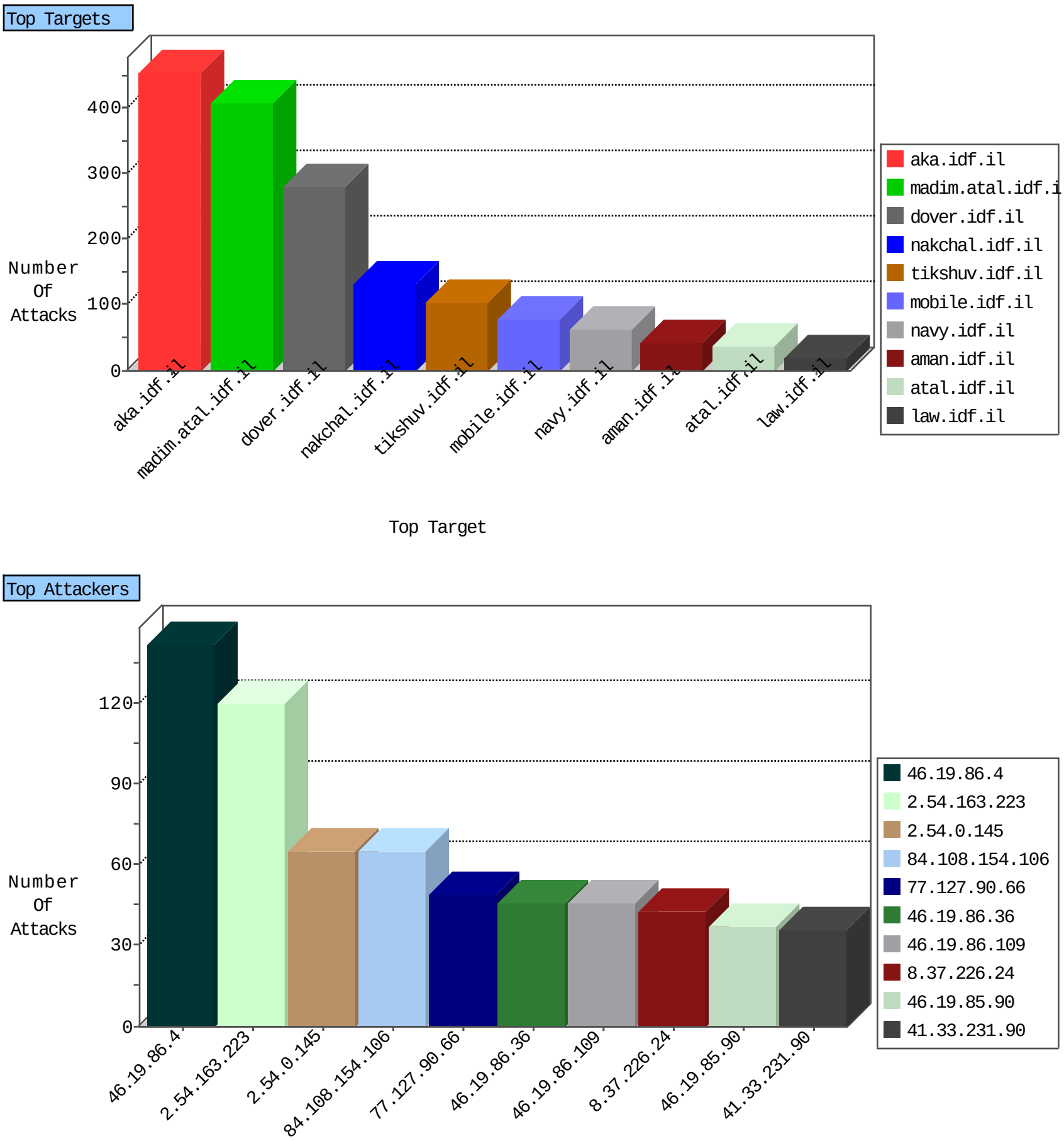
02-09-2016-20:04:09 to 02-09-2016-21:04:09

IDF Under Attack Daily Report



02-09-2016-20:04:09 to 02-09-2016-21:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	409
84.110.211.103	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
105.98.93.121	Algeria	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
158.130.6.191	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
66.249.82.94	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
142.54.160.211	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
142.54.169.165	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
142.54.169.166	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
8.37.226.24	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1

02-09-2016-20:04:09 to 02-09-2016-21:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
155.94.254.143	United States	147.237.0.17	m.my-kosher-kravi.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
155.94.254.143	United States	147.237.76.200	eitan.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
172.246.104.194	United States	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	1
45.63.97.227		147.237.72.166	aka.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	1
209.15.196.170	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
85.203.16.57	Netherlands	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

02-09-2016-20:04:09 to 02-09-2016-21:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.15.196.170	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	3
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
74.73.166.84	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
125.26.22.199	147.237.76.34	Thailand	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.228.138.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.218.185.120	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.117.185.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.140.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.52.34.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
176.13.2.213	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
85.64.46.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.218.185.120	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
58.218.185.120	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
46.72.16.219	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
8.37.226.24	147.237.77.216	Anonymous Proxy	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.7.88.57	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-09-2016-20:04:09 to 02-09-2016-21:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.163.223	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
8.37.226.24	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	41
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.109	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.177.174.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
79.178.126.73	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
46.19.86.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
46.19.86.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.150	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.36	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
109.64.17.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.154.178.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.94	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
46.19.85.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
178.248.90.71	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.13.2.213	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
109.66.57.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.2.213	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
84.228.216.120	Israel	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
149.88.93.100	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.3.147.216	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.44.79	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.181.116.58	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
197.40.42.198	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
205.155.141.254	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.64.66.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.8.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.69.77.91	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
94.230.86.200	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.76	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.66.169.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.79.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.100.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.106.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.230.55.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.139.12.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.2.213	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
82.69.77.91	United Kingdom	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
147.236.38.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.82.183	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.66.159.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.22.131.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.62.236	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
68.53.56.130	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.182.217.220	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.52.170.189	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

02-09-2016-20:04:09 to 02-09-2016-21:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	103
84.108.154.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
2.54.0.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
77.127.90.66	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.85.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
84.109.24.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
2.54.0.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
109.65.196.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
5.28.130.2	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
31.210.178.175	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 31.210.178.175	Block	15
84.108.103.113	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
46.19.86.109	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
109.253.207.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.228.205.254	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/main/sachar	Block	3
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
176.13.6.57	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
84.109.24.99	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/1088-he/meretz.aspx	Block	3
172.246.104.194	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 172.246.104.194	Block	3
46.19.85.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.87.32	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.86.87.32	Block	2
95.86.87.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-7791-he/dover.aspx&sa=u&ved=0ahukewjphnhsquvkahwme5okhssubkgqfggwmaq&usg=afqjcnf-g8tivzdlyydslnhtnkpvnptmja	Block	2
46.120.230.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
99.10.189.251	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
89.139.178.103	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	2
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	2
176.13.10.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$83 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.121.84.169	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyu×“	Block	2
2.54.21.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.187.127	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
31.168.17.13	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
213.251.182.114	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-admin/	Block	1
68.180.231.40	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/540-he/	Block	1
179.156.103.50	Brazil	147.237.77.216	dover.idf.il	Distributed eMail Hoarding	Block	1
54.167.183.116	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
84.228.138.53	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.54.176.53	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
207.59.201.18	United States	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.102.169.113	Block	1
176.13.2.213	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3416.jpg	Block	1
46.116.55.62	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
31.210.178.175	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
75.119.200.110	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/old/wp-admin/	Block	1
184.154.174.162	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wordpress/wp-admin/	Block	1
141.212.122.177	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.64.149	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding)![Fi}(&X-FO_PdXK/L0-[xhX1YtKq1 in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
2.54.179.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
207.59.201.18	United States	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1

02-09-2016-20:04:09 to 02-09-2016-21:04:09