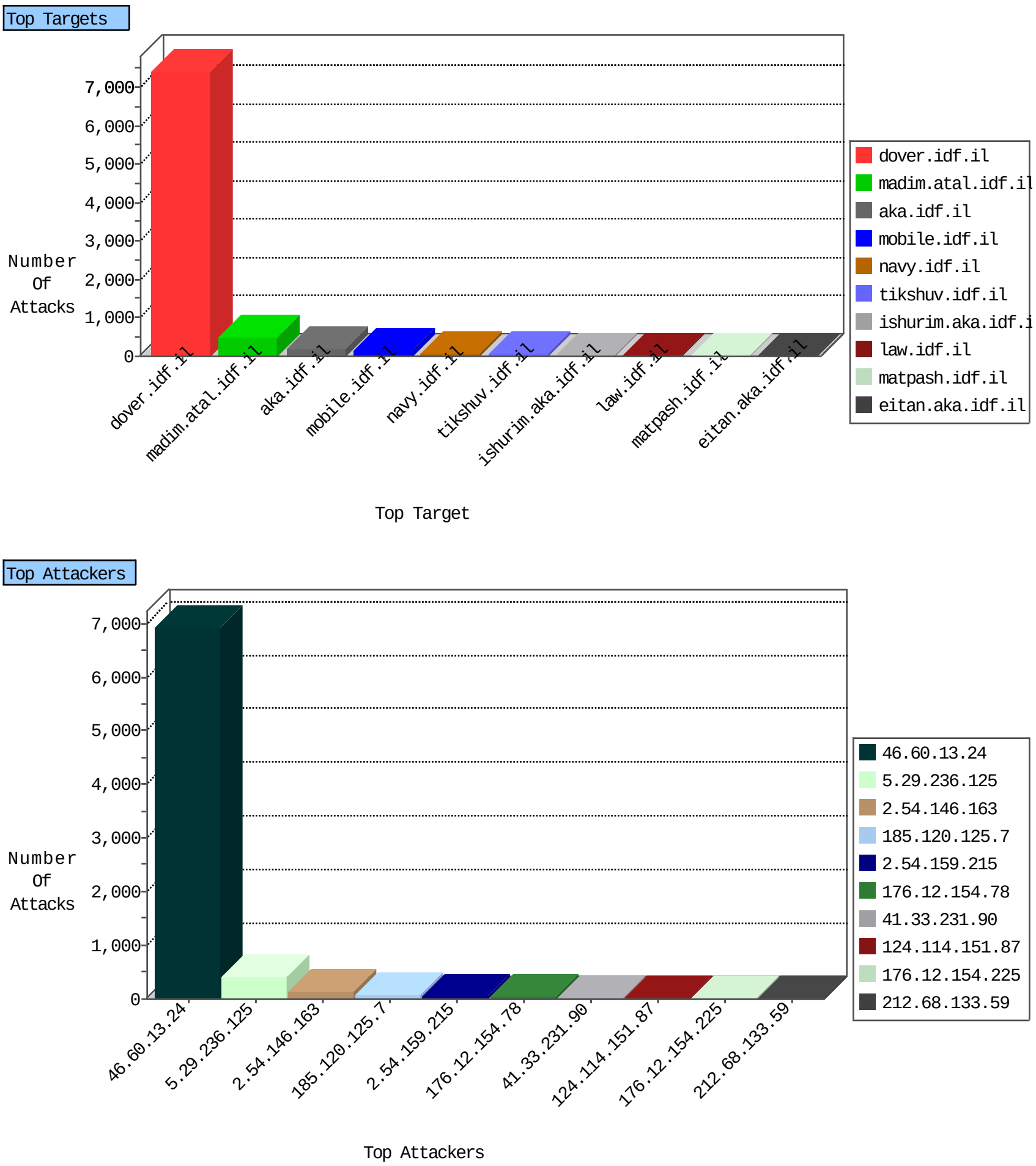
02-01-2016-22:04:05 to 02-01-2016-23:04:05

IDF Under Attack Daily Report



02-01-2016-22:04:05 to 02-01-2016-23:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	14
79.180.200.166	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
198.48.92.104	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
142.54.169.163	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
167.114.92.57	Canada	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
74.91.28.60	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
185.130.5.224		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

02-01-2016-22:04:05 to 02-01-2016-23:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.45.30.212	Egypt	147.237.77.216	dover.idf.il	C158: HTTP(S): Hacked in the Payload	Block	7
151.80.31.154	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
194.181.124.40	Poland	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	1
109.186.169.78	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
151.80.31.150	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.151	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-01-2016-22:04:05 to 02-01-2016-23:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.60.13.24	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	6942
124.114.151.87	147.237.0.34	China	tikshuv.idf.il	ET WEB_SERVER Possible SQL Injection (varchar)	10
41.45.30.212	147.237.77.216	Egypt	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.93.123	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.193.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.63.209.14	147.237.72.166	Pakistan	aka.idf.il	ET SCAN NMAP -sS window 4096	1
109.235.254.181	147.237.77.234	Turkey	halag.idf.il	ET SCAN NMAP -sS window 3072	1
202.63.209.14	147.237.72.166	Pakistan	aka.idf.il	ET SCAN NMAP -f -sS	1
109.235.254.181	147.237.77.234	Turkey	halag.idf.il	ET SCAN NMAP -f -sS	1
195.62.52.41	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
109.65.214.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.62.52.41	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
195.62.52.41	147.237.0.19	Russian Federation	madim.atal.idf.i	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.72.217	Sweden	e.idf.il	ET SCAN NMAP -sS window 1024	1
178.62.14.193	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
213.151.42.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
202.63.209.14	147.237.72.166	Pakistan	aka.idf.il	ET SCAN NMAP -sS window 2048	1
109.235.254.181	147.237.77.234	Turkey	halag.idf.il	ET SCAN NMAP -sS window 2048	1
195.62.52.41	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Potential SSH Scan	1
109.160.151.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.62.52.41	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN Potential SSH Scan	1
79.178.145.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.62.52.41	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
5.255.253.46	147.237.72.166	Russian Federation	aka.idf.il	portscan: TCP Distributed Portscan	1
188.143.232.24	147.237.72.166	Russian Federation	aka.idf.il	portscan: TCP Distributed Portscan	1
178.62.14.193	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1

02-01-2016-22:04:05 to 02-01-2016-23:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
2.54.146.163	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	50
2.54.159.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.54.146.163	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	27
46.19.86.244	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	24
2.54.146.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
2.54.146.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
2.54.146.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	22
212.68.133.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
141.0.15.216	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
5.29.96.248	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.68.74.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.87.65.14	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
124.114.151.87	China	147.237.0.34	tikshuv.idf.il	SQL Injection	SQL injection detected in URL: 'varChar'	monitor	10
176.12.155.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.182.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.12.155.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.87.65.14	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
109.65.223.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.18		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.36.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.155.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.221.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.76.127.10	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.26.149.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.5.223.35	Palestinian Territory, Occupied	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
79.181.169.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.160.247.82	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.112.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
37.46.39.243	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.110.7.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
76.10.170.182	Canada	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
80.246.137.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.49.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
141.0.14.193	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
178.52.148.106	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
84.108.13.216	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
178.52.148.106	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.64.124.131	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
41.202.84.45	Cote D'Ivoire	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.46.38.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.143.232.24	Russian Federation	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
87.68.73.82	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
5.29.236.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	233
5.29.236.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	155
176.12.154.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
5.29.236.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	33
176.12.154.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
37.26.147.201	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.201	Block	14
2.54.159.215	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
124.114.151.87	China	147.237.0.34	tikshuv.idf.il	Multiple Illegal Byte Code Character in Parameter Value from 124.114.151.87	Block	9
94.199.151.22	United Kingdom	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 94.199.151.22	Block	7
188.143.232.24	Russian Federation	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.143.232.24	Block	5
176.12.155.136	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.12.155.136	Block	4
212.68.133.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.182.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
149.78.30.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.154.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.121.136.195	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	3
176.12.155.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.155.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
88.203.124.144	Malta	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
79.180.219.98	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1679-18967/dover.aspx	Block	2
87.68.74.144	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.127.84.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.116.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.143.232.24	Russian Federation	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 188.143.232.24	Block	2
188.143.232.24	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 188.143.232.24	Block	2
188.143.232.24	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.24	Block	2
5.102.213.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.23.159	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
188.143.232.24	Russian Federation	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 188.143.232.24	Block	2
65.208.151.119	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	2
46.19.86.228	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.177.23.159	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
188.143.232.24	Russian Federation	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 188.143.232.24	Block	2
176.35.166.207	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
77.125.150.166	Israel	147.237.72.166	aka.idf.il	Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.66.67	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/111642.pdf	Block	1
163.247.46.239	Chile	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/spanish/	Block	1
196.40.97.170	South Africa	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/test/wp-admin/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	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
37.26.149.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
188.143.232.24	Russian Federation	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/926-he/	Block	1
185.120.125.18		147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/home/default.aspx	Block	1
66.249.66.126	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/106611.pdf	Block	1
93.172.239.139	Israel	147.237.77.74	law.idf.il	Illegal Byte Code Character in URL /602-2265-he/patzar.aspx	Block	1
79.181.55.126	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1
5.61.27.86	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wordpress/wp-admin/	Block	1
188.143.232.24	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/900-he/	Block	1