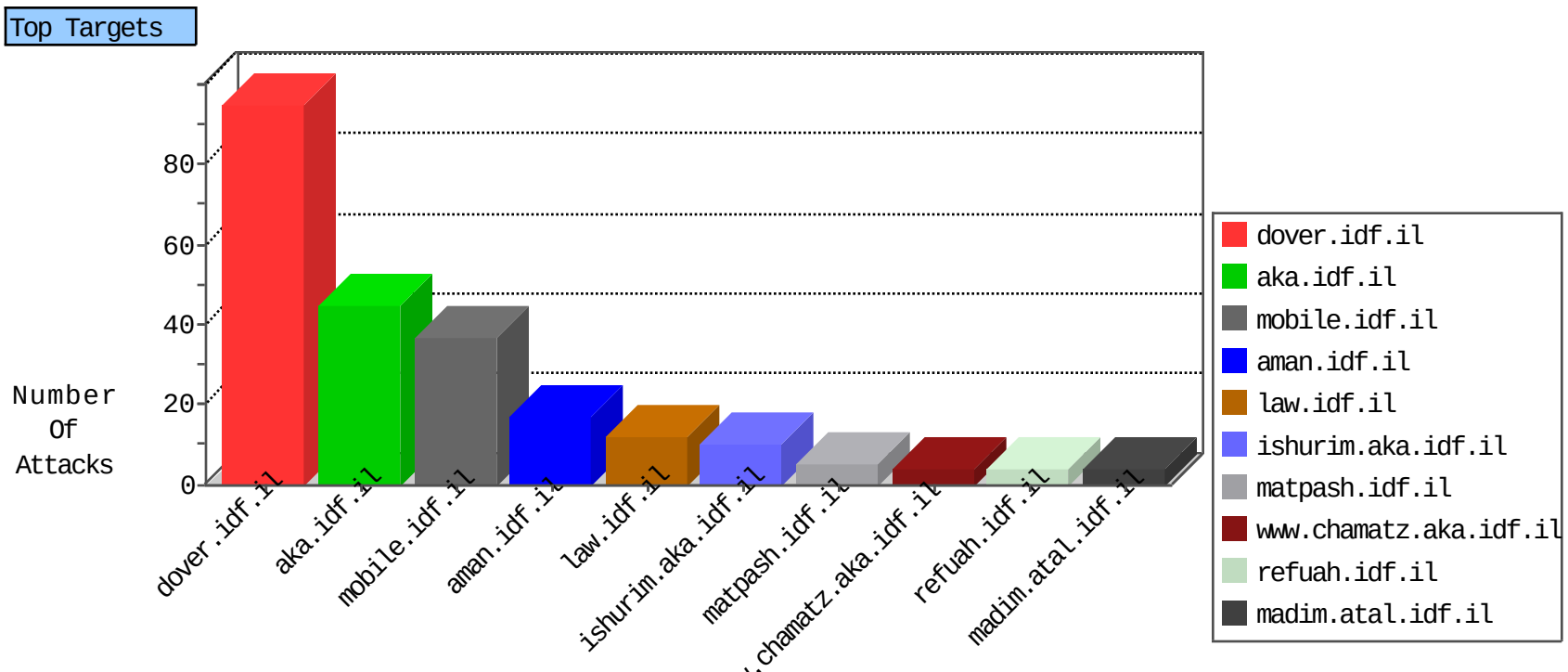
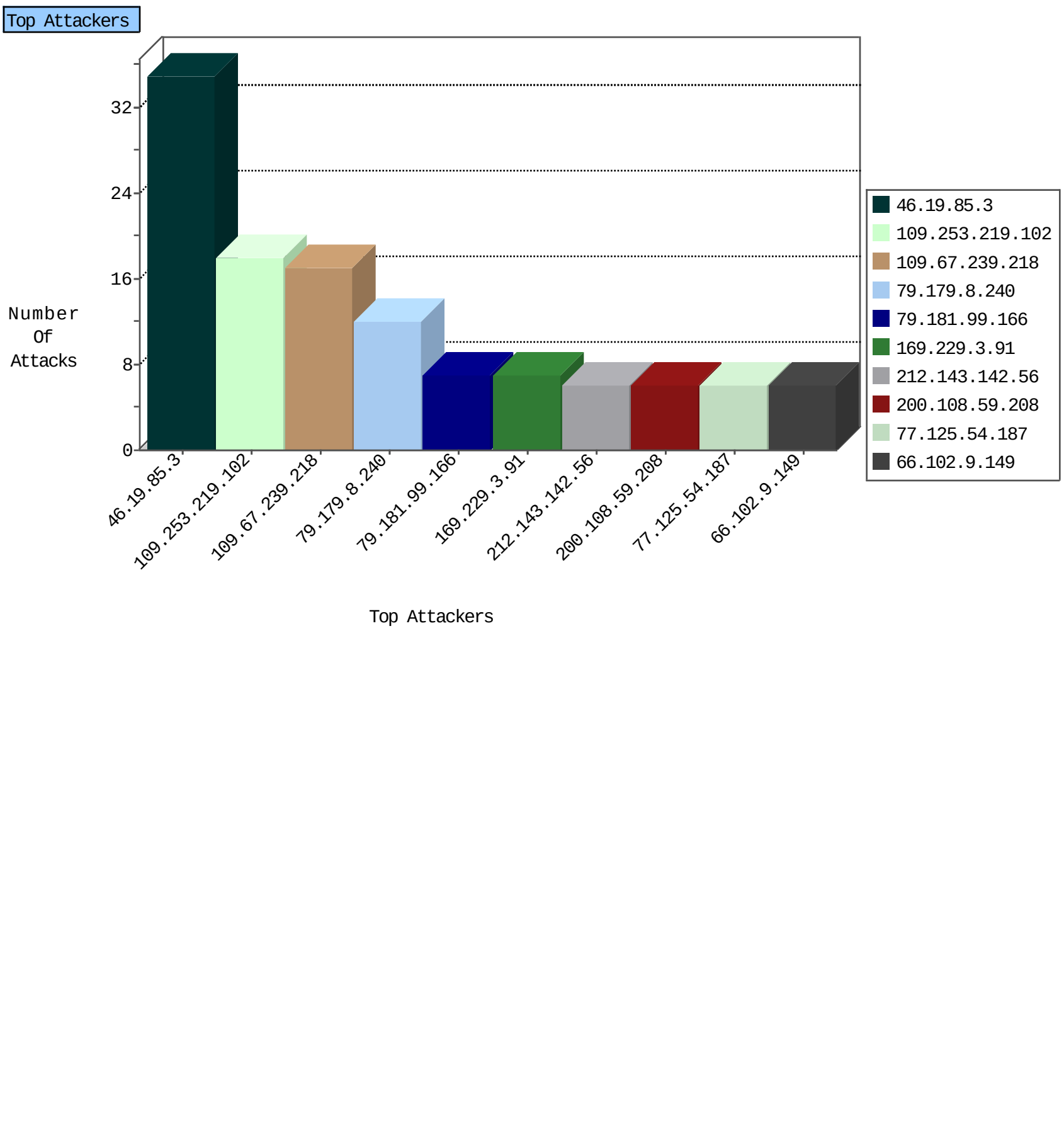
10-01-2016-00:04:06 to 10-01-2016-01:04:06

IDF Under Attack Daily Report





10-01-2016-00:04:06 to 10-01-2016-01:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
116.255.205.9	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Black List	drop	2
139.162.13.205	Singapore	147.237.72.166	aka.idf.il	block-sp-traf1	forward	2
58.218.200.137	China	147.237.0.17	m.my-kosher-kravi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
191.96.249.116	Chile	147.237.76.200	eitan.aka.idf.il	Black List	drop	1

10-01-2016-00:04:06 to 10-01-2016-01:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-01-2016-00:04:06 to 10-01-2016-01:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.67.239.218	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	6
109.67.239.218	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	6
194.224.101.170	147.237.77.234	Spain	halag.idf.il	ET SCAN NMAP -sS window 1024	1
176.47.31.13	147.237.77.176	Saudi Arabia	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
122.230.146.84	147.237.77.61	China	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.207.141.110	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
93.190.90.226	147.237.76.177	Germany	ncore.idf.il	ET SCAN Potential SSH Scan	1
84.111.2.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
194.224.101.170	147.237.77.233	Spain	atal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.8.46	United Kingdom	e.chinuch.idf.i	ET SCAN NMAP -sS window 1024	1
112.35.0.254	147.237.76.38	China	e.e.meitav.idf.i	ET SCAN Potential SSH Scan	1
104.207.141.110	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
88.249.106.23	147.237.77.243	Turkey	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
14.152.59.11	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

10-01-2016-00:04:06 to 10-01-2016-01:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
109.253.219.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.179.8.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
85.65.246.136	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
66.102.9.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
189.160.121.5	Mexico	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	5
46.117.82.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.215.37	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
176.13.7.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.34.20.31	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
108.178.44.182	United States	147.237.72.167	ishurim.aka.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3
85.64.21.33	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
95.134.178.107	Ukraine	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
109.64.16.48	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.26	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.53.164.85	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.125.54.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.153.195	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.86.34	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
200.108.59.208	Panama	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
213.57.153.195	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.31.124	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
84.109.242.51	Israel	147.237.0.16	my-kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
80.246.137.125	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.125.54.187	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.93.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
136.0.98.93	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
200.108.59.208	Panama	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.172.255.31	Poland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
84.108.40.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
176.13.8.184	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
77.125.54.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.29	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
65.19.167.130	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
169.229.3.91	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.249.93.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
139.162.13.205	Singapore	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
106.38.241.106	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
200.108.59.208	Panama	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
84.108.40.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

10-01-2016-00:04:06 to 10-01-2016-01:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.239.218	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.67.239.218	Block	3
2.53.22.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.219.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.67.239.218	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.67.239.218	Block	2
198.20.69.74	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/robots.txt	Block	1
108.178.44.182	United States	147.237.72.167	ishurim.aka.idf.il	Illegal Parameter Encoding RegNum in www.ishurim.aka.idf.il/	None	1
46.117.82.72	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
139.162.13.205	Singapore	147.237.72.166	aka.idf.il	NULL Character in Method	Block	1
68.180.230.216	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
204.79.180.141	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-	Block	1
77.138.104.63	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
207.46.13.108	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.102.6.21	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
141.226.217.240	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
84.109.242.51	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
220.181.108.152	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.64.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
180.76.15.158	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9366-he/refuah.aspx	Block	1
85.243.8.12	Portugal	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/general.aspx	None	1
2.53.22.107	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
139.162.13.205	Singapore	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8804-he/refuah.aspx	Block	1

10-01-2016-00:04:06 to 10-01-2016-01:04:06