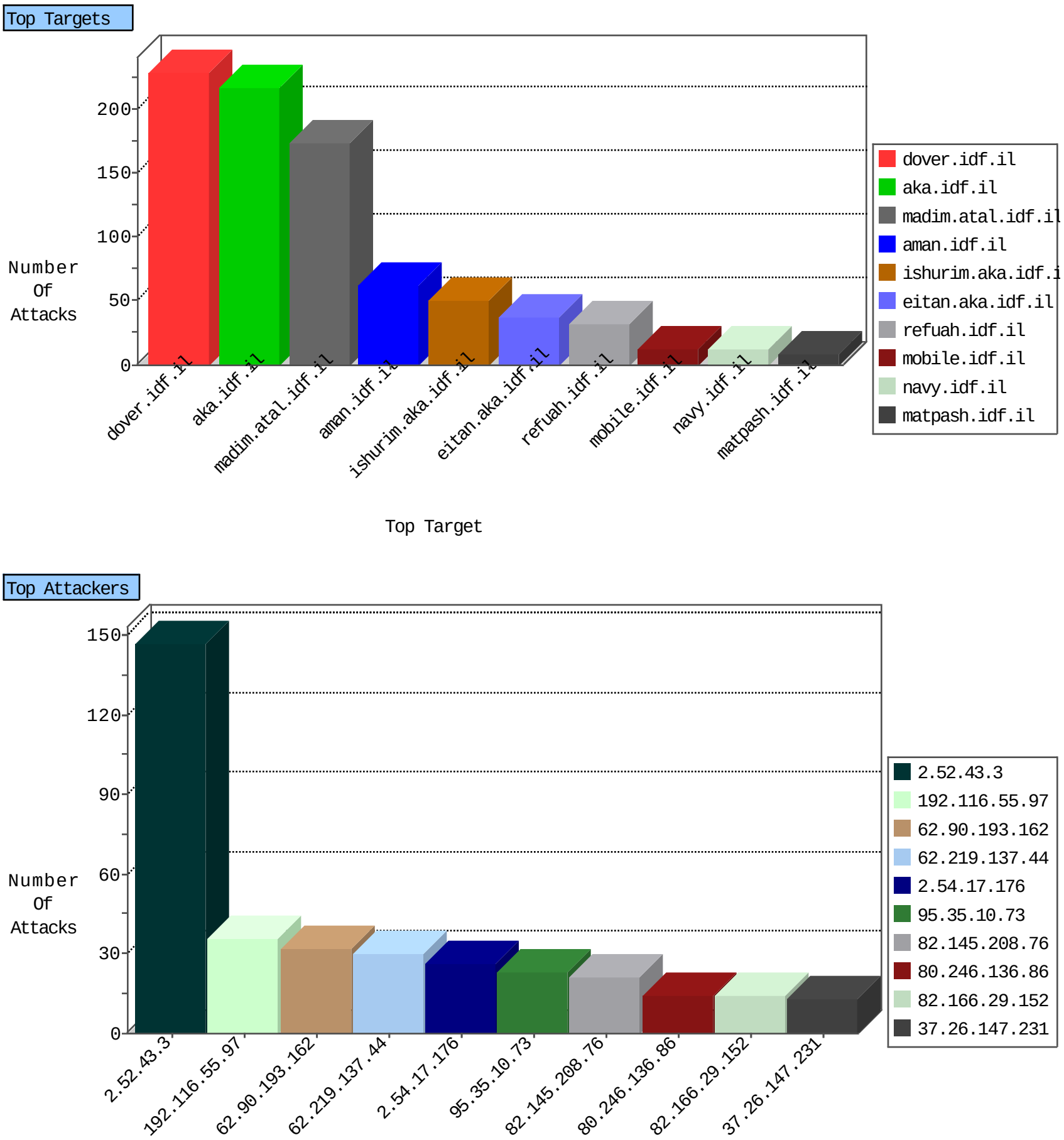
03-10-2016-09:04:08 to 03-10-2016-10:04:08

IDF Under Attack Daily Report



03-10-2016-09:04:08 to 03-10-2016-10:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.208.76	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	21
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
184.105.139.118	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.207	Netherlands	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
10.218.220.1		147.237.77.243	mobile.idf.il	L4 Source or Dest Port Zero	drop	1
185.130.5.246		147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.98	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
158.255.6.130	Russian Federation	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
58.97.74.88	Thailand	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.103	United States	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.102	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
61.21.168.82	Japan	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1

03-10-2016-09:04:08 to 03-10-2016-10:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.121.101.78	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.154	Italy	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
37.26.146.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.151	Italy	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.152	Italy	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-10-2016-09:04:08 to 03-10-2016-10:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
122.227.180.99	147.237.76.198	China	e.yohalan.idf.il	GPL SCAN nmap TCP	2
84.228.29.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.198.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.66.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.238	147.237.76.176		test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
45.35.64.142	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.186.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.248.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
108.170.20.114	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
87.68.153.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.14.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.14.228.126	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.68.98.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.203.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.50.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
108.170.20.114	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.205	Canada	prisha.idf.il	ET SCAN NMAP -sS window 3072	1

03-10-2016-09:04:08 to 03-10-2016-10:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.116.55.97	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
62.219.137.44	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
62.90.193.162	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
62.90.193.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	14
147.236.34.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.186.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.66.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.2.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
96.47.68.190	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
82.166.29.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
95.35.10.73	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.118.48.248	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.17.176	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.24.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.35.10.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.176.119	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
82.166.29.152	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
176.13.7.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.194.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.17.176	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
37.8.57.83	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.142	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.10.198	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.17.176	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.136.86	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.17.176	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.67.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
37.46.39.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.189.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.17.176	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.88	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
95.35.10.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.11.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.142.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.232	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
87.70.28.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.115.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.34.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.137.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.120.125.9		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.127.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
154.72.166.39	Cameroon	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
213.8.125.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.177.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.40.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.203.129	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.16.255	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
2.52.43.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	147
37.26.147.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.253.214.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	3
46.19.85.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
199.30.24.94	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.162	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
62.90.193.162	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
37.26.148.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
157.55.12.92	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.156	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.19.85.156	Block	2
199.30.24.162	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
154.72.166.39	Cameroon	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.133.99	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.116	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.2.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl111 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
195.146.61.5	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.107.230.216	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
37.26.148.199	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ishurim.	Block	1
207.46.13.70	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
65.55.210.155	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.2.157	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
94.230.93.244	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
2.54.19.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.33	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/107975.pdf	Block	1
114.124.3.208	Indonesia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.107.230.216	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
37.26.148.222	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.232.28.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mains/sachar	Block	1
77.87.228.69	Germany	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.2.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
94.230.93.251	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.156	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl79 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
2.54.186.103	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/109575.pdf	Block	1
123.125.71.114	China	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.166.53.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.126.7.92	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
212.76.96.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
65.55.210.228	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1