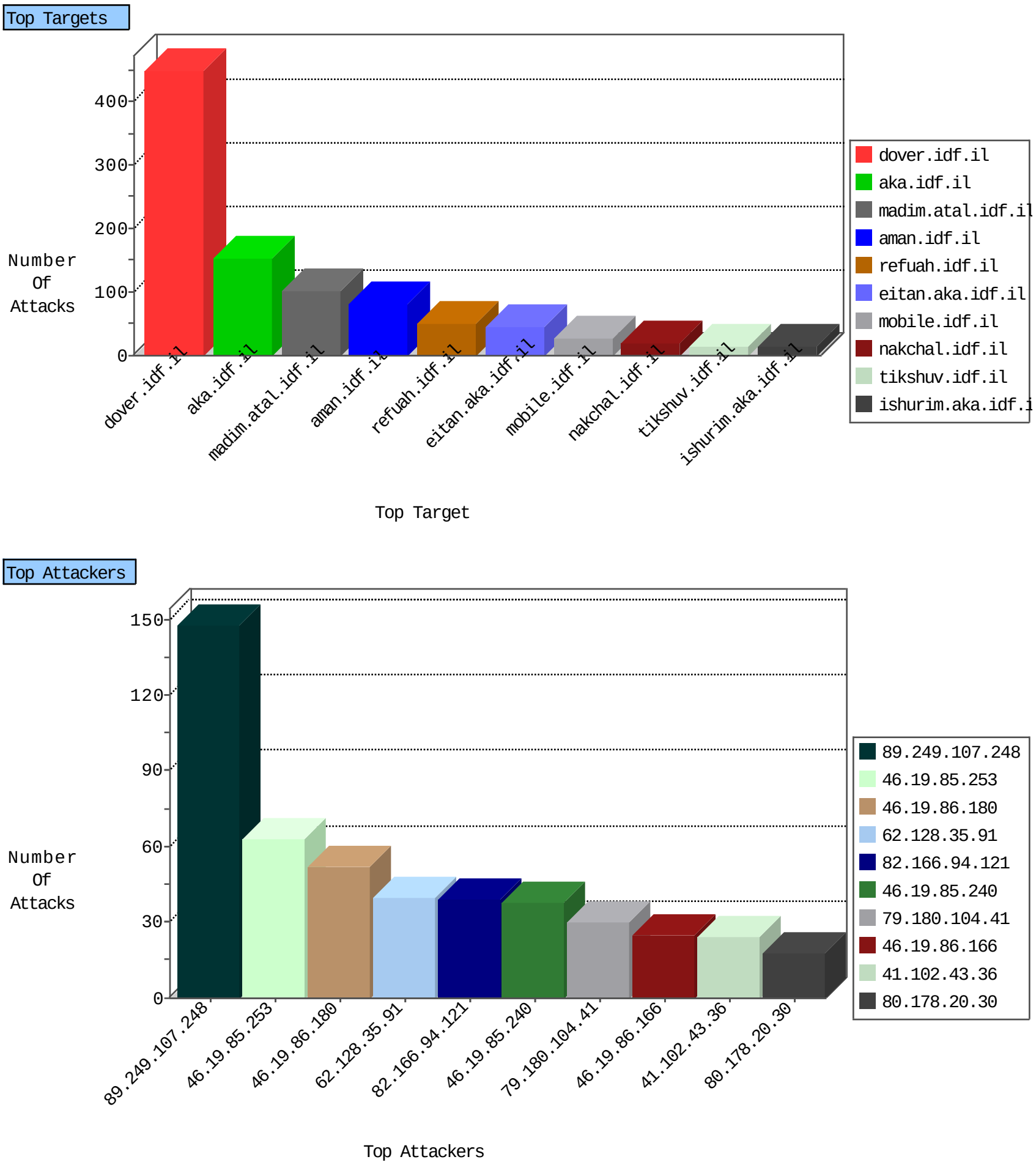
09-01-2016-15:04:01 to 09-01-2016-16:04:01

IDF Under Attack Daily Report



09-01-2016-15:04:01 to 09-01-2016-16:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.106.235	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
5.189.186.243	Germany	147.237.76.86	navy.idf.il	Black List	drop	2
5.189.186.243	Germany	147.237.76.34	yohalan.idf.il	Black List	drop	2
5.189.186.243	Germany	147.237.76.38	e.e.meitav.idf.il	Black List	drop	2
5.189.186.243	Germany	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	2
117.21.227.62	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
5.189.186.243	Germany	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
87.106.189.34	Germany	147.237.77.234	halag.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
5.189.186.243	Germany	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.31	nakchal.idf.il	Black List	drop	1
117.144.202.195	China	147.237.76.196	e.sviva.idf.il	Black List	drop	1
61.172.176.242	China	147.237.76.196	e.sviva.idf.il	Black List	drop	1
93.158.200.97	Netherlands	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
175.179.114.100	Japan	147.237.76.176	test.ncore.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
93.158.200.97	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.201	e.atal.idf.il	Black List	drop	1
222.69.159.254	China	147.237.76.196	e.sviva.idf.il	Black List	drop	1
82.221.105.7	Iceland	147.237.76.177	ncore.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.30	himush.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.202	e.halag.idf.il	Black List	drop	1

09-01-2016-15:04:01 to 09-01-2016-16:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-01-2016-15:04:01 to 09-01-2016-16:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.178.15.247	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	4
79.182.106.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.116.144.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.213.5.204	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
5.22.135.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
117.21.227.62	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
117.21.227.62	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
88.206.207.85	147.237.77.216	Sweden	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.50.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.204.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.117.182.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.200.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
79.178.15.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
182.203.167.71	147.237.72.14	China	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.142.213.178	147.237.77.216	Morocco	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.5.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.47.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
117.21.227.62	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
117.21.227.62	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
84.108.192.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.54.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.139.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.69.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.6.226	147.237.72.156	Lithuania	aman.idf.il	ET SCAN Potential SSH Scan	1

09-01-2016-15:04:01 to 09-01-2016-16:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.249.107.248	Croatia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	148
82.166.94.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
62.128.35.91	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
80.178.20.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
46.19.86.180	Israel	147.237.77.216	dover.idf.il	SYN Attack		monitor	17
46.19.85.240	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
46.19.85.240	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
46.19.86.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
41.102.43.36	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
193.191.219.80	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.53.3.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
188.120.148.14	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
89.139.111.192	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
156.194.70.75	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
185.86.6.139	Turkey	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
91.135.102.163	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.71.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
156.194.70.75	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.130.160.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.154.9.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
85.130.160.21	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.53.14.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
85.130.160.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.180	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.84	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
2.55.61.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.186.77.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
212.179.146.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.86.180	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.67.124.224	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
84.111.32.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.253.134.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.67.216.249	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
41.102.43.36	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
46.19.86.180	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
100.92.43.120		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
41.102.43.36	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.46.41.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
173.255.211.75	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
91.151.139.73	Georgia	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
5.102.242.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.76.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
108.29.54.177	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
46.117.25.1	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
46.19.86.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
47.16.86.41	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	4
37.26.148.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
62.200.229.135	Europe	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	3
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
178.210.146.51	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/robots.txt	Block	3
2.53.133.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.180.104.41	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.180.104.41	Block	2
199.30.16.185	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.27.106.3	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	2
79.180.104.41	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 79.180.104.41	Block	2
199.30.25.21	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.14.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.111.64.59	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar/newsarchive.aspx	Block	2
199.30.25.34	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.40	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.180.104.41	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 79.180.104.41	Block	2
79.180.104.41	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 79.180.104.41	Block	2
79.180.104.41	Israel	147.237.72.156	aman.idf.il	Multiple Illegal HTTP Version from 79.180.104.41	Block	2
80.178.20.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.127.51.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
206.71.242.130	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 206.71.242.130	Block	1
79.180.104.41	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 79.180.104.41 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
62.128.35.91	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
185.3.147.235	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.14	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.109.118.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.104.41	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Value	Block	1
213.8.41.250	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
79.181.179.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.104.41	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 79.180.104.41	Block	1
176.13.10.111	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.104.41	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in URL •[[#5]]s½•‘	Block	1
2.55.61.34	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
109.67.216.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.178.204.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.234.212	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
206.71.242.130	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
79.180.104.41	Israel	147.237.72.156	aman.idf.il	NULL Character in Header Name at	Block	1
46.19.85.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.104	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.57.178.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.111.32.27	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.180.104.41	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method G•lGñ[[#20]]˜ÃTÃ³•¸ìéâ¹dþõ[[#21]]ÉØ¸•	Block	1
79.183.98.95	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.180.104.41	Israel	147.237.72.156	aman.idf.il	Multiple NULL Character in Header Name from 79.180.104.41	Block	1
46.116.81.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1