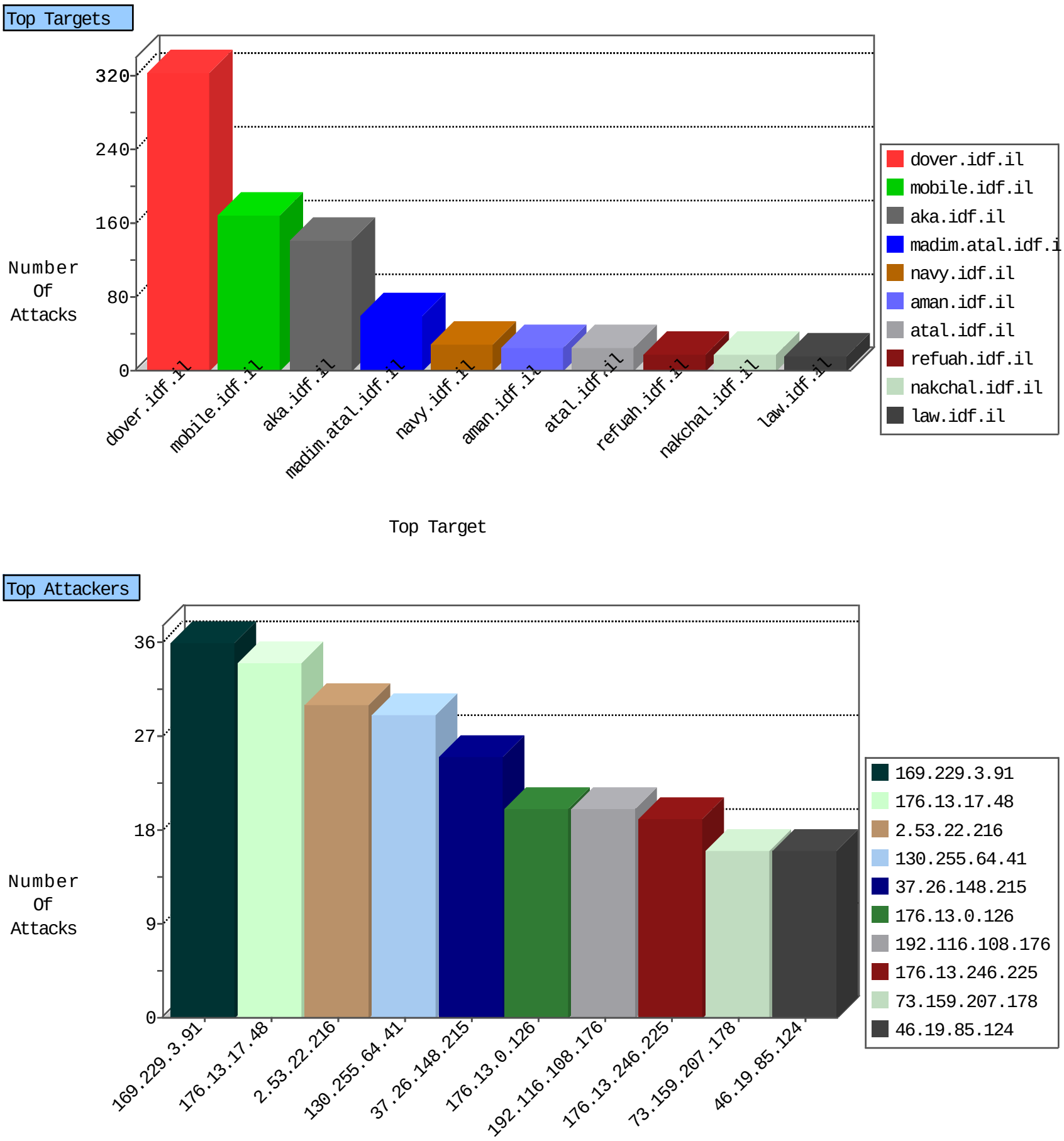
09-29-2016-15:04:07 to 09-29-2016-16:04:07

IDF Under Attack
Daily Report



09-29-2016-15:04:07 to 09-29-2016-16:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.209.87	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
5.102.242.160	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
79.179.55.62	Israel	147.237.72.166	aka.idf.il	Black List	drop	3
198.204.247.220	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
63.141.231.197	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
63.141.231.194	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
142.54.180.69	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
198.204.247.220	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
63.141.231.196	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
204.12.217.6	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
198.148.116.133	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
173.208.150.114	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
63.141.250.154	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
192.187.118.22	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
198.148.116.133	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
173.208.198.10	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
69.30.193.253	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
46.19.86.52	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
198.204.255.77	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
192.187.118.66	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
89.248.167.131	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
63.141.231.210	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
198.148.116.133	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1
173.208.207.131	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
69.30.227.222	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
198.204.255.77	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
198.44.110.12	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
63.141.231.214	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
192.187.101.234	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	1

09-29-2016-15:04:07 to 09-29-2016-16:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-29-2016-15:04:07 to 09-29-2016-16:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
216.218.206.102	147.237.76.86	United States	navy.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
46.121.26.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
200.58.214.138	147.237.76.86	Colombia	navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
125.85.67.79	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.85.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
120.27.116.133	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.146.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.97.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.58.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.8.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.192.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.124.29.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.172.91.21	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.118.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.20.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.242.167.44	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
120.63.143.13	147.237.76.31	India	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.85.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.130.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.50.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.5.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.47.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.116.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.7.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.56.212	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.161.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-29-2016-15:04:07 to 09-29-2016-16:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.22.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
130.255.64.41	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
176.13.17.48	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	18
73.159.207.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
176.13.0.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.18	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.116.108.176	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
176.13.246.225	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.86.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
188.120.148.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
31.168.83.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.246.225	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	8
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.168	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.17.48	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
77.139.173.141	France	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.17.48	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.55.34.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.55.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.139.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.237.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.161.6	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
2.55.183.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.212.201	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
81.218.66.107	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
109.253.136.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
82.80.255.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
207.46.13.176	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.134	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.132.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.178.215.146	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

09-29-2016-15:04:07 to 09-29-2016-16:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
46.19.86.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
31.168.4.193	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 31.168.4.193	Block	9
176.13.0.126	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.213.17.10	Russian Federation	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 176.213.17.10	Block	5
77.138.104.232	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	5
79.176.89.212	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.176.89.212	Block	4
109.253.220.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.8	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.179.55.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.63.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.138.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.134.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.20.117	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
46.19.86.188	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
188.120.148.171	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.138.164.106	France	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
2.53.134.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
79.176.89.212	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/golani/	Block	1
185.32.179.16	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/69039.pdf	Block	1
176.13.246.225	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
84.94.48.88	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.94.48.88	Block	1
5.28.177.25	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
77.139.173.141	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
207.46.13.151	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	NULL Character in Method	Block	1
157.55.39.149	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/brothers/news/	None	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	1
183.129.160.229	China	147.237.77.234	halag.idf.il	Distributed Unknown HTTP Request Method	Block	1
93.172.111.146	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method [[#16]]'•±[[#15]][[#11]]ìÁ¿yŽ2ïmjNÌ¸•ü[[#5]]"Q•[[#20]]Å2œ¯—•€$+c!:[[#25]]´#â•¤Ó•2″·VŸš¿?[[#15]]í[[#29]]» in URL	Block	1
79.178.140.154	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
77.138.9.203	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/ishurim	Block	1
185.32.179.132	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	NULL Character in URL	Block	1
46.19.86.240	Israel	147.237.76.31	nakchal.idf.il	Distributed Malformed URL	Block	1
116.15.138.254	Singapore	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
84.94.105.221	Israel	147.237.77.176	matpash.idf.il	Unauthorized HTTP Method	Block	1
31.168.4.193	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
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
77.139.249.120	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/kadatz/default.asp	Block	1
207.46.13.176	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/2/62532.pdf	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
157.55.39.175	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1

09-29-2016-15:04:07 to 09-29-2016-16:04:07