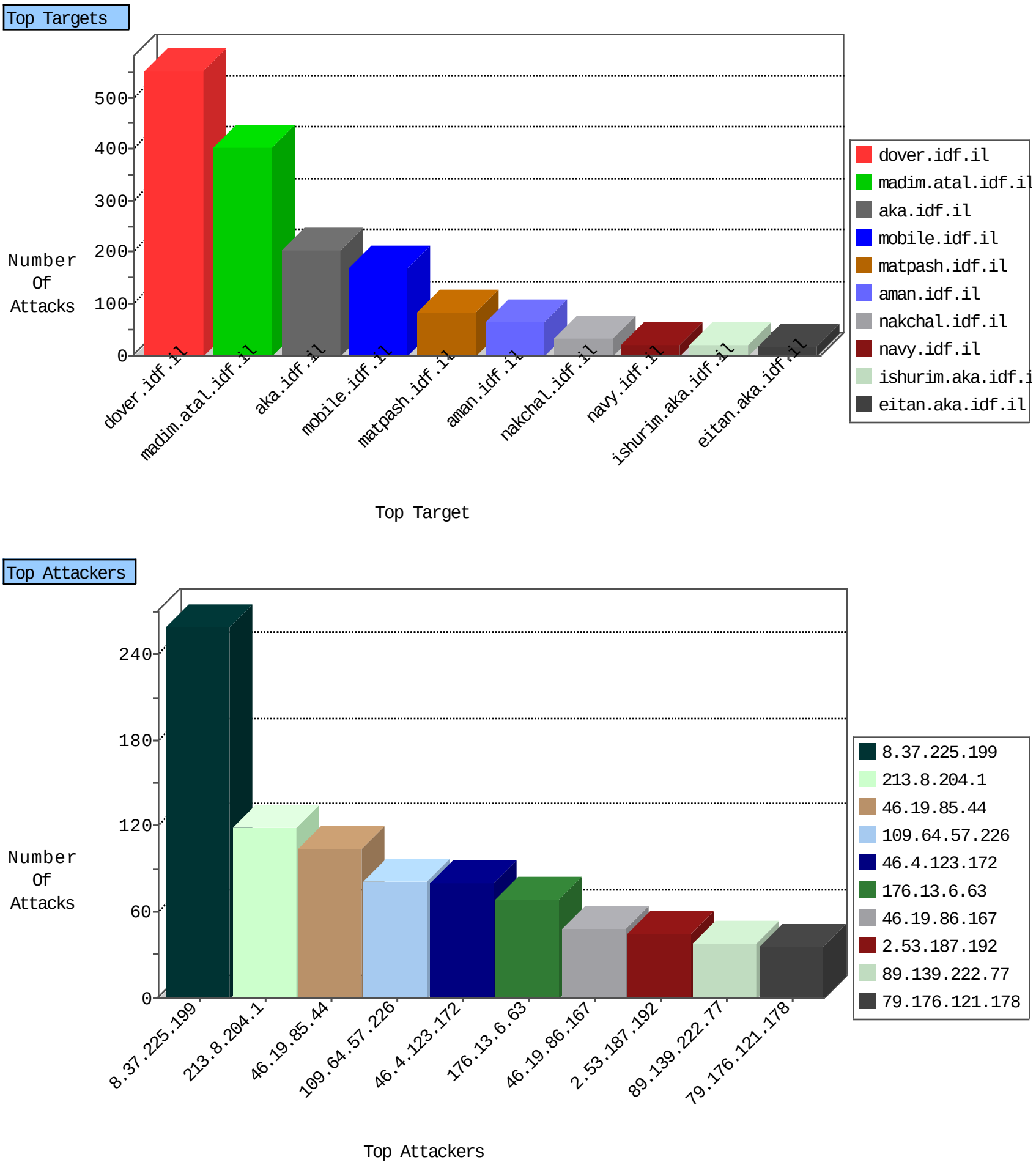
09-29-2016-21:04:00 to 09-29-2016-22:04:00

IDF Under Attack
Daily Report



09-29-2016-21:04:00 to 09-29-2016-22:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.139.64.157	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
8.37.225.199	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
142.54.174.82	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
198.204.255.78	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
173.208.198.12	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
63.141.231.210	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
192.187.109.59	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
141.212.122.57	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
63.141.242.195	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
142.54.180.69	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
89.248.172.16	Netherlands	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
192.187.118.68	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
69.30.226.221	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
173.208.150.116	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
63.141.231.198	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
142.54.174.85	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
109.253.215.203	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
208.67.1.248	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
142.54.174.86	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1

09-29-2016-21:04:00 to 09-29-2016-22:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.123.172	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	34
46.4.123.172	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	19
46.4.123.172	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	14
46.4.123.172	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.4.123.172	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.4.123.172	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	2
123.126.68.121	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-29-2016-21:04:00 to 09-29-2016-22:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	6
115.21.227.227	147.237.77.74	Korea, Republic of	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
62.210.113.183	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
118.44.6.52	147.237.77.234	Korea, Republic of	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
2.50.168.178	147.237.72.166	United Arab Emirates	aka.idf.il	ET SCAN NMAP -sS window 1024	1
180.213.5.205	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.37	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
46.172.91.21	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
13.79.155.79	147.237.8.27	Ireland	e.madim.atal.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
183.129.160.229	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
2.50.168.178	147.237.72.166	United Arab Emirates	aka.idf.il	ET SCAN NMAP -sS window 3072	1
180.213.5.205	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.162	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.91.21	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
8.37.225.199	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
180.213.5.205	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

09-29-2016-21:04:00 to 09-29-2016-22:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	255
79.176.121.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
223.24.113.233	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.132.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.19.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
154.241.215.74		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
89.139.222.77	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
46.19.86.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
66.102.6.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.65.80.110	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.44	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
185.3.147.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.44	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.44	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
89.139.222.77	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.85.44	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
185.3.147.186	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.44	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.85.44	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
66.249.73.170	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.120.243.61	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.102.6.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.129.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.139.222.77	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
46.4.123.172	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.84.77.34	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.73.174	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.226.28.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.13.166.140	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.102.9.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.165.79	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
66.102.6.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
94.230.86.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.102.6.17	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
79.177.192.252	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
176.13.244.158	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
46.116.118.186	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
66.102.6.17	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
68.180.231.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.69.83.182	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.102.6.17	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
87.197.164.92	Slovakia	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
66.102.6.17	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

09-29-2016-21:04:00 to 09-29-2016-22:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.204.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
109.64.57.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
176.13.6.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
2.53.187.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
46.19.86.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
79.178.227.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.109.212.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.127.23.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.18.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
84.95.214.180	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
109.226.28.96	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	4
46.19.86.20	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.20	Block	4
46.19.86.20	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
77.138.16.100	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.159.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.216.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.183	Block	3
164.138.118.33	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar/faq.aspx	Block	2
2.53.31.178	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.132	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	2
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.168.75	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.132	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
77.138.166.87	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.166.87	Block	1
37.142.88.204	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.54	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
46.121.73.40	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.64.32.71	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.10.182	France	147.237.72.166	aka.idf.il	Unauthorized Request Content Type text/ping	Block	1
176.13.250.227	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/favicon.ico	Block	1
109.253.129.133	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
85.64.210.209	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
46.116.42.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.166.87	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/popups/markivsachar.aspx	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.102.9.8	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
109.64.56.239	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
46.19.86.107	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
213.57.153.73	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
84.95.214.180	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 84.95.214.180	Block	1
183.129.160.229	China	147.237.76.31	nakchal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.69.251	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/mobile/	Block	1
87.69.216.31	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1
46.120.110.234	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
204.79.180.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
79.176.88.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1

09-29-2016-21:04:00 to 09-29-2016-22:04:00