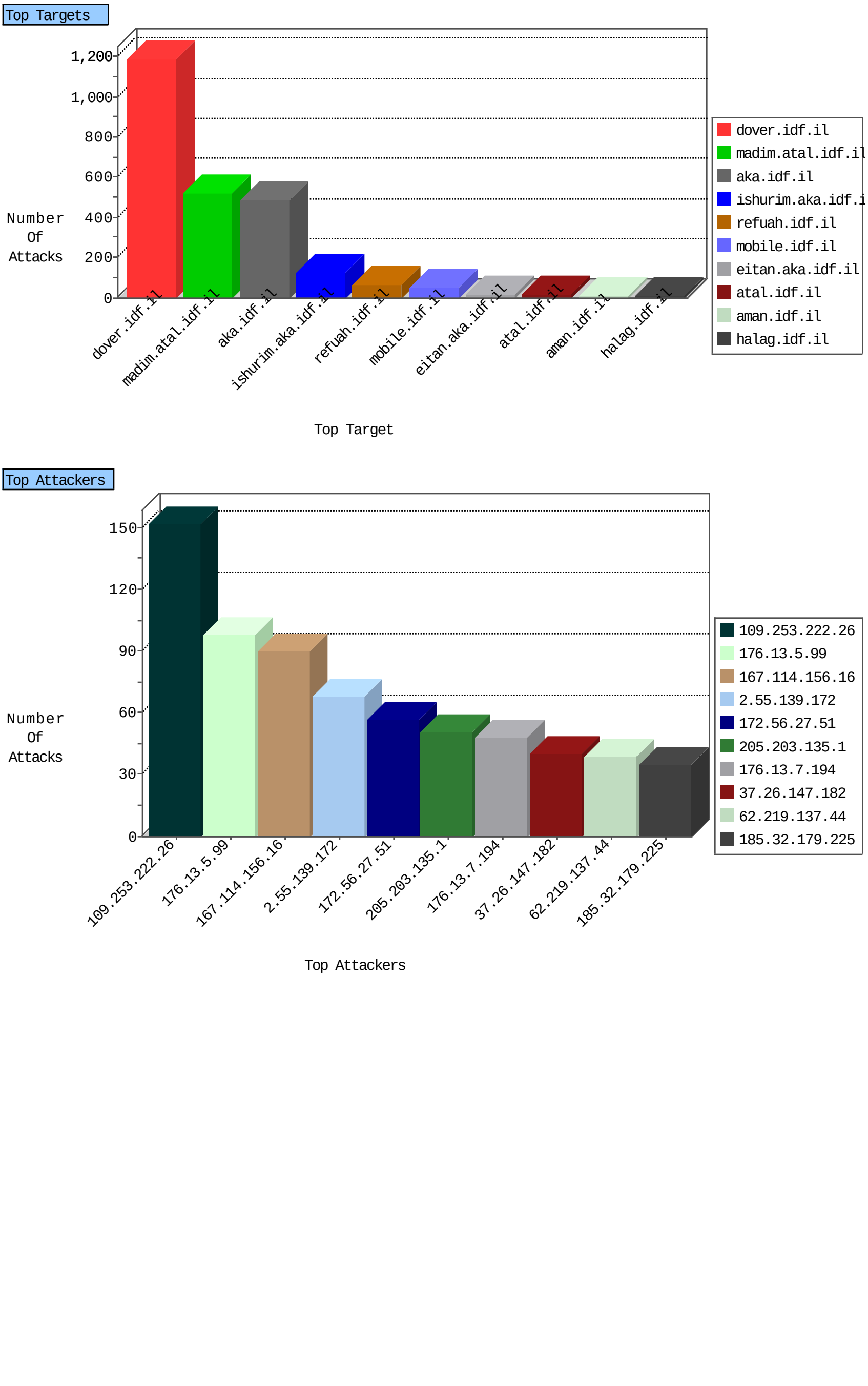
05-01-2016-16:04:04 to 05-01-2016-17:04:04

IDF Under Attack Daily Report



05-01-2016-16:04:04 to 05-01-2016-17:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3096
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2604
2.53.15.125	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
185.120.125.132	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
185.32.179.141	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
5.22.129.132	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
2.55.18.60	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
193.47.165.251	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
46.117.20.12	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.53.165.158	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
2.55.177.249	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
2.55.191.190	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
2.53.2.249	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
183.60.48.25	China	147.237.0.15	kosher-kravi.idf.il	Frk_Under_Attack_Con_Tcp	drop	1
80.246.139.53	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.53.152.234	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
141.212.122.206	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
2.55.176.158	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
31.210.186.9	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
79.176.70.222	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.53.55.66	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
123.151.42.61	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Udp	drop	1
31.210.186.9	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.53.170.148	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.53.1.66	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
80.246.137.141	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.53.132.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
132.73.200.179	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

05-01-2016-16:04:04 to 05-01-2016-17:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.143.180.166	United States	147.237.0.19	madim.atal.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
223.73.252.238	China	147.237.77.216	dover.idf.il	0872: HTTP: Apache .htaccess Access	Block	1

05-01-2016-16:04:04 to 05-01-2016-17:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.i	Tehila - Perl LWP with fake user agent	2
62.98.35.13	147.237.77.216	Italy	dover.idf.i	Xenu Link Sleuth User Agent	2
106.38.241.106	147.237.76.86	China	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

05-01-2016-16:04:04 to 05-01-2016-17:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
172.56.27.51	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
176.13.7.194	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
62.219.137.44	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
46.208.31.157	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
176.31.117.76	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
87.90.15.132	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
109.65.172.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
37.26.146.194	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
74.108.128.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
93.172.144.92	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
185.46.212.70	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
83.244.54.142	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.81.212	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
185.32.179.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
80.246.136.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
213.8.204.15	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
147.236.34.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
50.116.28.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.239.134.51	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.32.179.225	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
2.53.2.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
50.112.219.207	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.188.213.250	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
185.32.179.225	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.244.89.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
199.207.253.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.168.13.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.168.13.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.18.149	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
81.218.38.70	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
213.8.204.16	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
176.13.5.241	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.130.253.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7

05-01-2016-16:04:04 to 05-01-2016-17:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.222.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	152
176.13.5.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
2.55.139.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
37.26.147.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
109.253.150.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
109.64.126.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.53.25.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
37.26.146.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
176.13.5.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
217.132.63.190	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	8
2.53.150.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.146.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.53.0.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.212.20	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	3
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	3
46.19.86.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.11.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.159.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.211.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	3
176.13.8.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.200.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.75	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 46.19.85.75	Block	2
185.3.146.227	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	2
133.130.102.240	Japan	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
51.254.200.12	France	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
82.81.208.162	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatusDay in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.73	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.8.204.36	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
176.13.18.149	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
79.178.235.164	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gws_rd in www.aka.idf.il/main/home/default.aspx	None	1
138.134.102.15	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 138.134.102.15	Block	1
106.38.241.106	China	147.237.76.86	navy.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
195.154.15.227	France	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
79.182.36.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.5.118	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
51.254.200.12	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/index.php	Block	1
82.166.148.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.204.77	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
141.212.122.113	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /x	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/71580.pdf	Block	1
46.19.86.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14322-he/dover.aspx'½¬¿¬¯¬'₪½¬¿¬¯¬'×'	Block	1
79.182.120.104	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
68.180.230.184	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
109.253.225.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
51.255.65.68	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
84.95.198.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

05-01-2016-16:04:04 to 05-01-2016-17:04:04