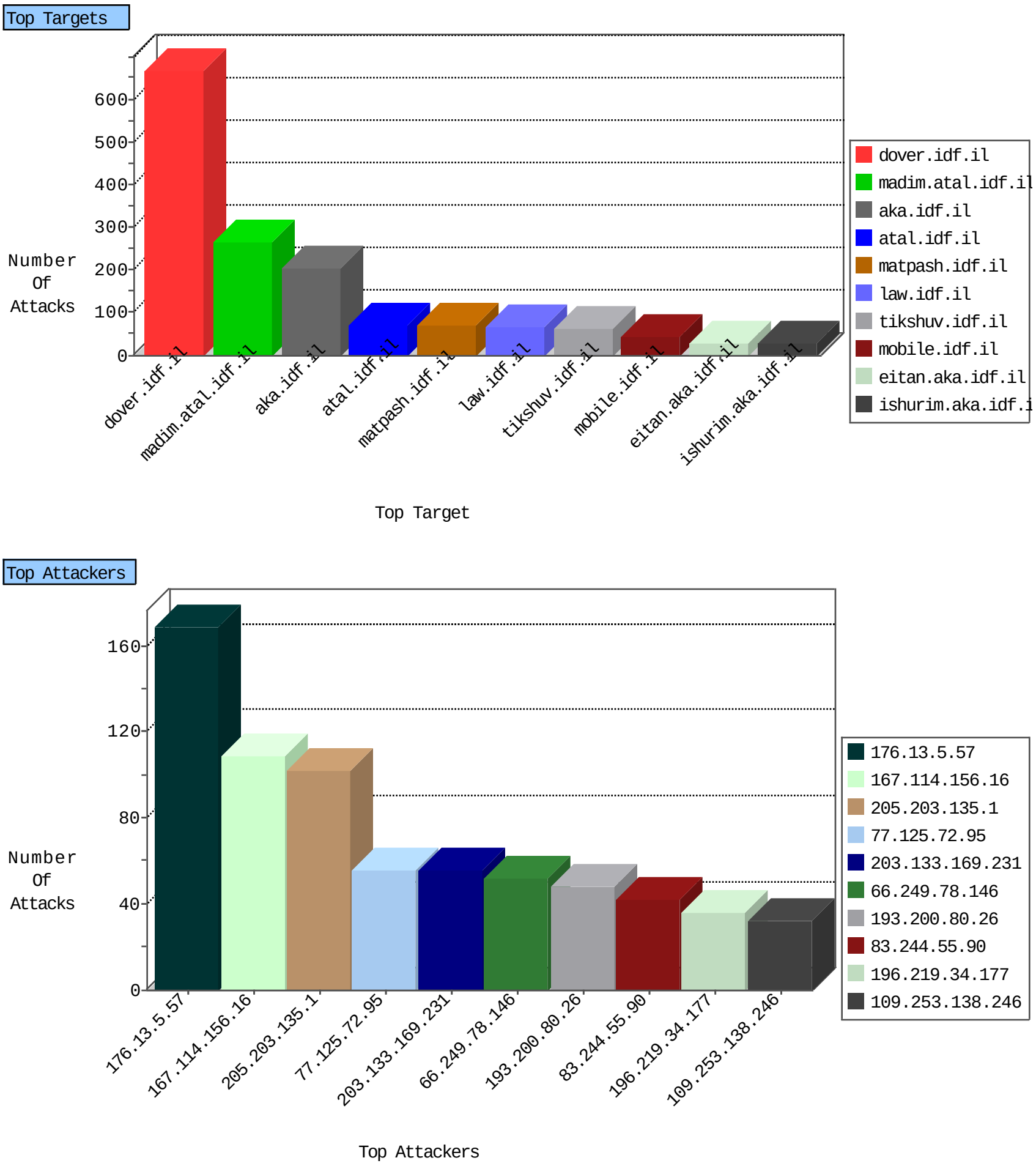
04-27-2016-09:04:03 to 04-27-2016-10:04:03

IDF Under Attack
Daily Report



04-27-2016-09:04:03 to 04-27-2016-10:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4850
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4016
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1053
82.145.218.138	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	13
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
128.69.180.109	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	1
172.251.45.17	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
71.6.158.166	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

04-27-2016-09:04:03 to 04-27-2016-10:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.205.0.49	Turkey	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
66.96.128.60	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
193.200.80.26	United Kingdom	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
93.89.19.29	Turkey	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
194.88.154.138	Poland	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
177.185.194.45	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
202.124.109.87	New Zealand	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
23.91.70.121	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
193.200.80.26	United Kingdom	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
193.200.80.26	United Kingdom	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

04-27-2016-09:04:03 to 04-27-2016-10:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
193.200.80.26	147.237.77.233	United Kingdom	atal.idf.il	SQL Injection - Select From	23
193.200.80.26	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	13
194.88.154.138	147.237.0.34	Poland	tikshuv.idf.il	SQL Injection - Select From	12
37.205.0.49	147.237.77.233	Turkey	atal.idf.il	SQL Injection - Select From	10
66.96.128.60	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	7
177.185.194.45	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	6
93.89.19.29	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	6
62.210.226.9	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	6
23.91.70.121	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
202.124.109.87	147.237.77.74	New Zealand	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
188.214.249.152	147.237.77.216	Romania	dover.idf.il	Xenu Link Sleuth User Agent	2
87.70.17.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.76.197		e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
174.37.194.144	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.141.210.203	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
84.94.64.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.240.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
174.37.194.144	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
174.37.194.144	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
58.218.204.211	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
89.248.167.131	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1

04-27-2016-09:04:03 to 04-27-2016-10:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
203.133.169.231	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
83.244.55.90	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	42
196.219.34.177	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
79.180.3.211	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
140.132.9.79	Taiwan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
168.159.160.54	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.176.92.29	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
199.203.152.235	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	13
109.173.59.185	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
87.71.48.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.9.17.118	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
93.80.217.121	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.179.19.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
98.232.163.119	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.106.46.74	Palestinian Territory, Occupied	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
36.70.199.50	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.146.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
208.81.64.248	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.145.218.189	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.46.39.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.93.243	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.70.130.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
217.132.63.11	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
209.88.157.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.3	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
217.132.63.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
87.70.36.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.211.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.227.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.92.29	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	5
5.22.135.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
217.132.63.11	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5

04-27-2016-09:04:03 to 04-27-2016-10:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.5.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	169
77.125.72.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	56
109.253.138.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	32
176.13.21.195	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	17
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.20.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
87.71.48.177	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
81.218.135.239	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.86.181	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
89.139.21.11	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3259.jpg	Block	1
5.39.222.159	Netherlands	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
84.111.244.200	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
54.86.175.219	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-6569-he/patzar.aspx.	Block	1
213.254.241.5	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
176.13.3.84	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	1
87.69.128.95	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
62.90.2.30	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
2.55.55.215	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
219.74.36.56	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
109.253.227.151	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/doctor	Block	1
87.70.82.35	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	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
5.29.234.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ei in www.aka.idf.il/	None	1
123.59.59.52	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.mafengwo.cn/894-he/nakhal.aspx	Block	1
66.249.66.50	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
5.29.234.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gfe_rd in www.aka.idf.il/main/home/default.aspx	None	1
164.132.161.7	Italy	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mail/kapats	Block	1

04-27-2016-09:04:03 to 04-27-2016-10:04:03