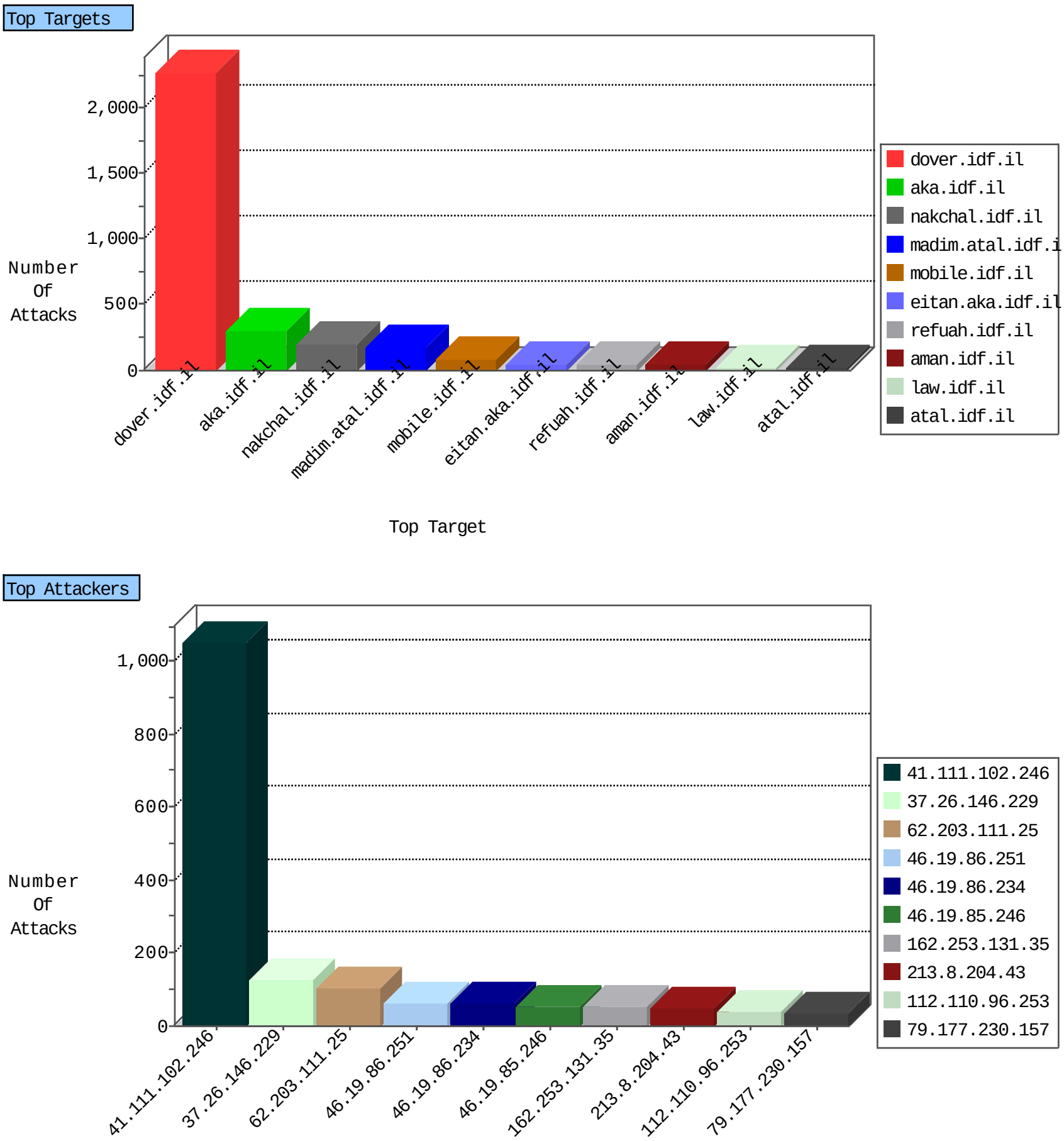
09-28-2016-16:04:05 to 09-28-2016-17:04:05

IDF Under Attack
Daily Report



09-28-2016-16:04:05 to 09-28-2016-17:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	687
176.13.237.193	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
2.53.45.19	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
79.176.91.95	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
93.174.94.235	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-28-2016-16:04:05 to 09-28-2016-17:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.178.197.44	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6

09-28-2016-16:04:05 to 09-28-2016-17:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
207.178.197.44	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	13
218.48.107.8	147.237.77.227	Korea, Republic of	e.hamaz.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
217.132.30.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.48.77.131	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	1
163.172.115.5	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
199.203.251.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.48.77.131	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
125.77.194.138	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
2.53.187.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.226.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.161.69	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
163.172.115.5	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
163.172.115.5	147.237.77.178	United Kingdom	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
80.178.145.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.115.5	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN Potential SSH Scan	1
77.124.37.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.115.5	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
62.219.138.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.115.5	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN Potential SSH Scan	1
217.132.111.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.111.102.246	147.237.77.216	Algeria	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.115.5	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
37.48.77.131	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
125.77.194.138	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
2.55.132.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.180.9.152	147.237.77.216	Cote D'Ivoire	dover.idf.il	ET SCAN NMAP -f -sS	1
93.190.90.226	147.237.77.234	Germany	halag.idf.il	ET SCAN Potential SSH Scan	1
176.13.4.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.161.69	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
163.172.115.5	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.161.69	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.115.5	147.237.77.74	United Kingdom	law.idf.il	ET SCAN Potential SSH Scan	1
79.178.197.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.115.5	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
62.219.240.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.115.5	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.116.100.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.115.5	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1

09-28-2016-16:04:05 to 09-28-2016-17:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	698
162.253.131.35	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
213.8.204.43	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
2.53.7.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.177.230.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	25
62.0.207.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
46.19.86.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	20
46.19.86.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
46.19.86.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
185.62.121.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
107.77.64.89	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	18
46.19.85.246	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
2.53.42.50	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
112.110.96.253	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
46.19.85.246	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
2.53.162.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
46.19.86.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
62.0.227.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.253.212.212	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.137.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.135.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.13.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
98.19.222.133	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	12
112.110.96.253	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
112.110.96.253	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
80.178.95.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.55.155.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.86.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
46.19.86.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
199.203.63.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	10
46.19.85.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
103.21.165.12	Sri Lanka	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.40	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.53.48.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9

09-28-2016-16:04:05 to 09-28-2016-17:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	125
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.111.102.246	Block	56
2.55.178.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
5.102.242.213	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.102.242.213	Block	18
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	7
46.120.190.190	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	6
77.138.10.183	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	5
2.53.42.50	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
185.32.176.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.212.212	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
77.138.147.31	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	3
37.26.146.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.139.108.223	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.143.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.22.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.137.185	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.120.190.190	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/6/	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
91.238.226.1	Belgium	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/sachar	Block	2
176.13.3.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.178.33.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 77.127.241.20 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
176.13.5.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
83.130.195.143	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
5.102.242.213	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
217.69.133.224	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/	Block	1
66.249.69.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8868-he/refuah.aspx	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
37.26.147.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.198.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/70002.doc	Block	1
84.109.116.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.120.190.190	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 46.120.190.190	Block	1
77.139.163.107	France	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 77.139.163.107 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
31.13.110.108	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar_blank	Block	1
109.253.194.242	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.5	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
2.53.188.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.69.222.212	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catIdF in www.aka.idf.il/main/giyus/general.aspx	None	1
77.139.163.107	France	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1415-he/dover.aspx	Block	1
66.249.64.8	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.64.8	Block	1
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Unauthorized Method POST for 147.237.77.216/	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
189.203.217.154	Mexico	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.120.240.129	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.120.240.129	Block	1

09-28-2016-16:04:05 to 09-28-2016-17:04:05