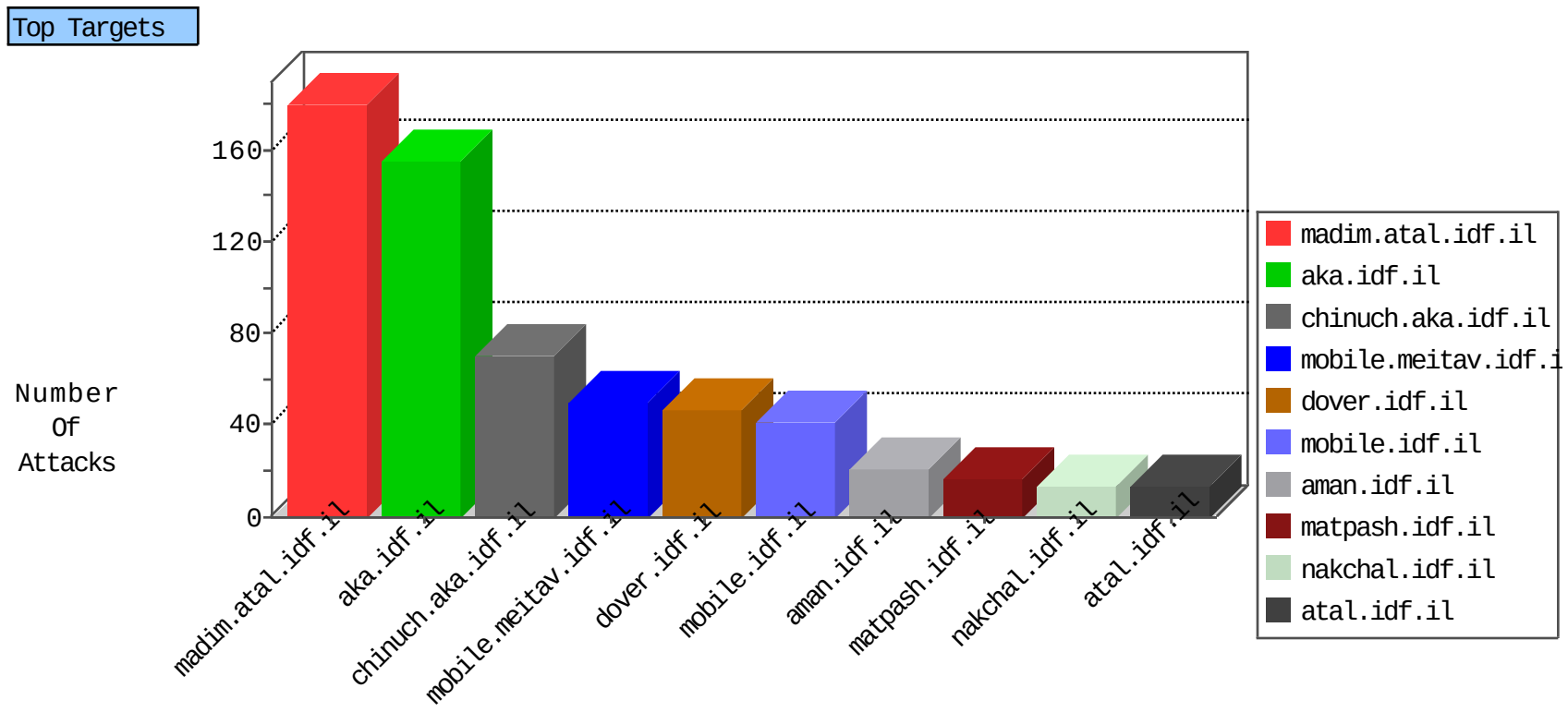
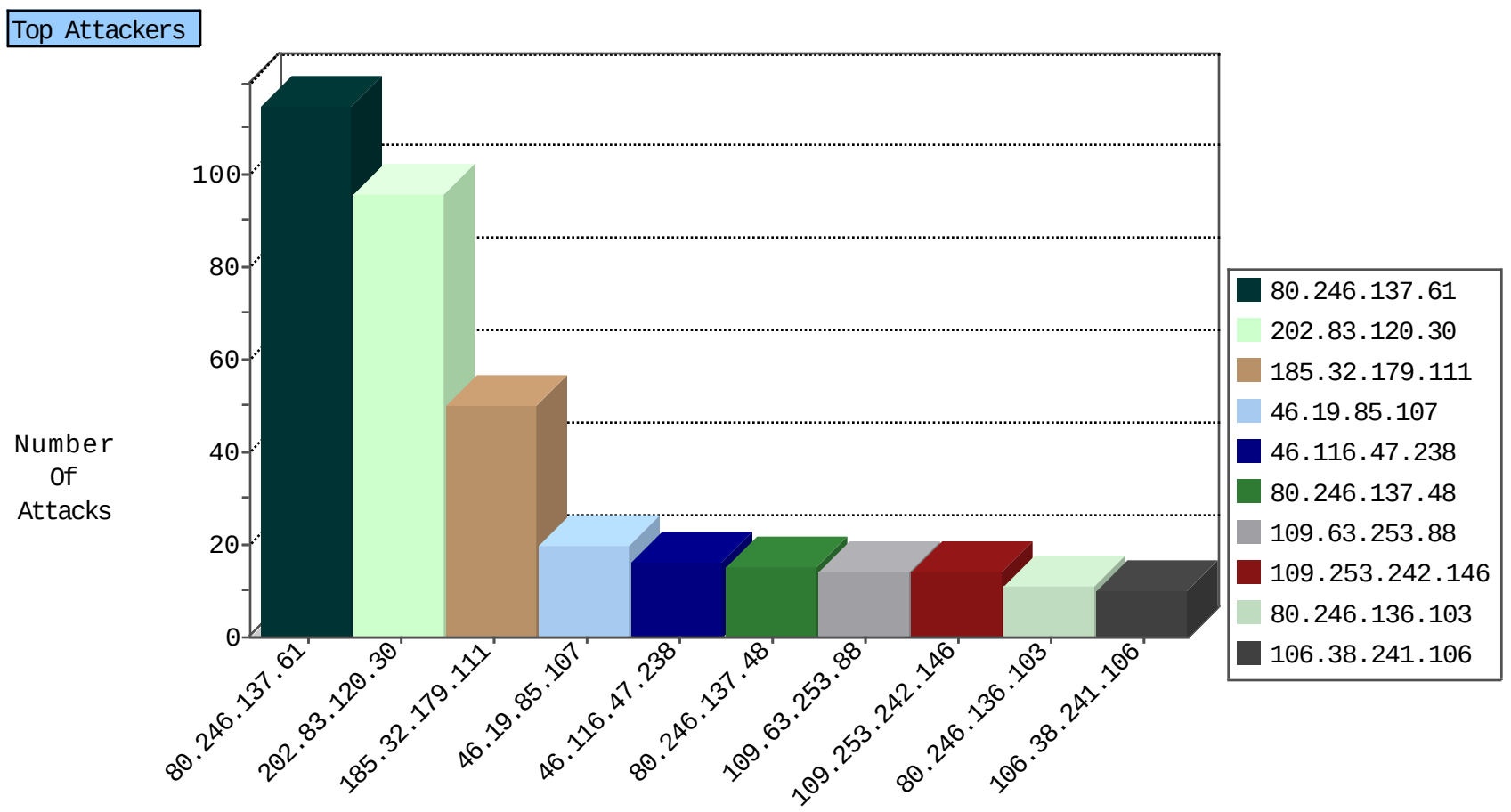
09-25-2016-18:04:09 to 09-25-2016-19:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-25-2016-18:04:09 to 09-25-2016-19:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.31	nakchal.idf.il	Black List	drop	4
212.179.247.58	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
183.60.48.25	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
63.141.231.212	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
208.110.84.66	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
69.30.227.221	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
63.141.231.197	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
122.224.153.109	China	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Http	drop	1
63.141.231.211	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
69.30.193.253	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
208.110.84.69	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	1
208.110.84.66	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
69.30.227.218	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
63.141.231.194	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
208.110.84.70	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
142.54.174.84	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
66.240.236.119	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
212.179.247.58	Israel	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
142.54.174.84	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
69.30.193.250	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
208.110.84.67	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1

09-25-2016-18:04:09 to 09-25-2016-19:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	10
85.14.244.113	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-25-2016-18:04:09 to 09-25-2016-19:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.139.98.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
109.64.109.217	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
103.235.104.148	147.237.72.166	India	aka.idf.il	SQL Injection - Update (POST)	1
80.246.137.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.215.36.46	147.237.77.19	Kenya	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
210.212.207.80	147.237.0.34	India	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.129.148.230	147.237.0.200	Latvia	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
115.47.12.162	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
109.67.202.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN NMAP -sS window 1024	1
103.235.104.148	147.237.72.166	India	aka.idf.il	ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 1	1
82.102.169.113	147.237.76.31	Israel	nakchal.idf.il	LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file	1
54.144.119.103	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
201.7.217.249	147.237.77.121	Brazil	e.navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
115.47.12.162	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1

09-25-2016-18:04:09 to 09-25-2016-19:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.63.253.88	Russian Federation	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
80.246.137.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	10
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	8
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
77.124.18.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.242.146	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
5.22.134.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.174	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.238.115	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.253.146.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.107	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.107	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.253.242.146	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.185	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.174	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.55.11.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
80.246.136.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.130.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
46.19.85.214	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.201.194.211	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.246.136.103	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
37.26.148.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.66	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
80.246.136.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
176.13.234.222	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.130.231.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.245.9	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.116.19.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
185.32.179.238	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
80.246.136.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
213.57.236.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
87.69.149.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.180.254.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.116.47.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.252.93.89	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
147.235.8.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
213.57.236.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.134.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.4	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

09-25-2016-18:04:09 to 09-25-2016-19:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.137.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
185.32.179.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50
46.116.47.238	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	14
87.69.87.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.87.20	Block	4
31.154.81.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
192.114.105.254	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/forms.aspx	Block	3
46.19.85.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.137.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.137.48	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.181.207.212	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	3
46.19.85.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.121.97.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.139.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
82.102.169.113	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	2
77.139.21.23	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugtafkidim.aspx	Block	2
109.253.159.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.76.121	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/english/pages/default.aspx	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
77.139.30.230	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
185.120.125.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-23188-he/dover.aspx	Block	1
109.253.134.56	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
82.102.169.113	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/1682.doc	Block	1
80.179.9.115	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1
2.53.136.199	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.242.146	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
67.19.79.218	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /robots.txt	Block	1
87.69.87.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/61353.jpg	Block	1
80.246.138.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.44.181	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/kiosk	Block	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1672	Block	1
109.253.135.143	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
80.179.9.115	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
2.55.145.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
67.82.20.229	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
103.235.104.148	India	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/user/login/	Block	1
77.139.154.236	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
212.150.200.166	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/.giyus/	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
85.64.118.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
64.251.27.99	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /robots.txt	Block	1
5.22.134.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.130.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/guyus	Block	1
185.32.179.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
66.249.69.14	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.14	Block	1

09-25-2016-18:04:09 to 09-25-2016-19:04:09