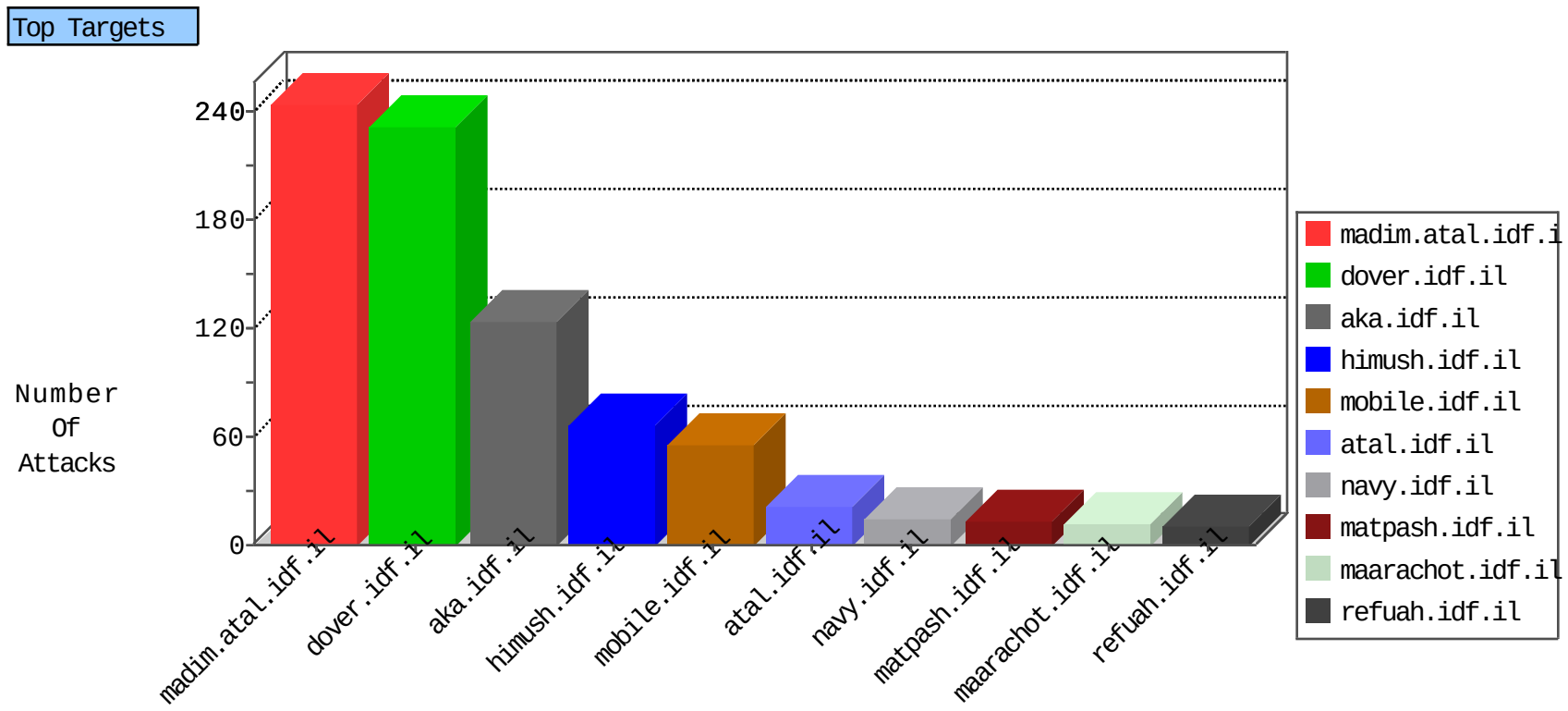
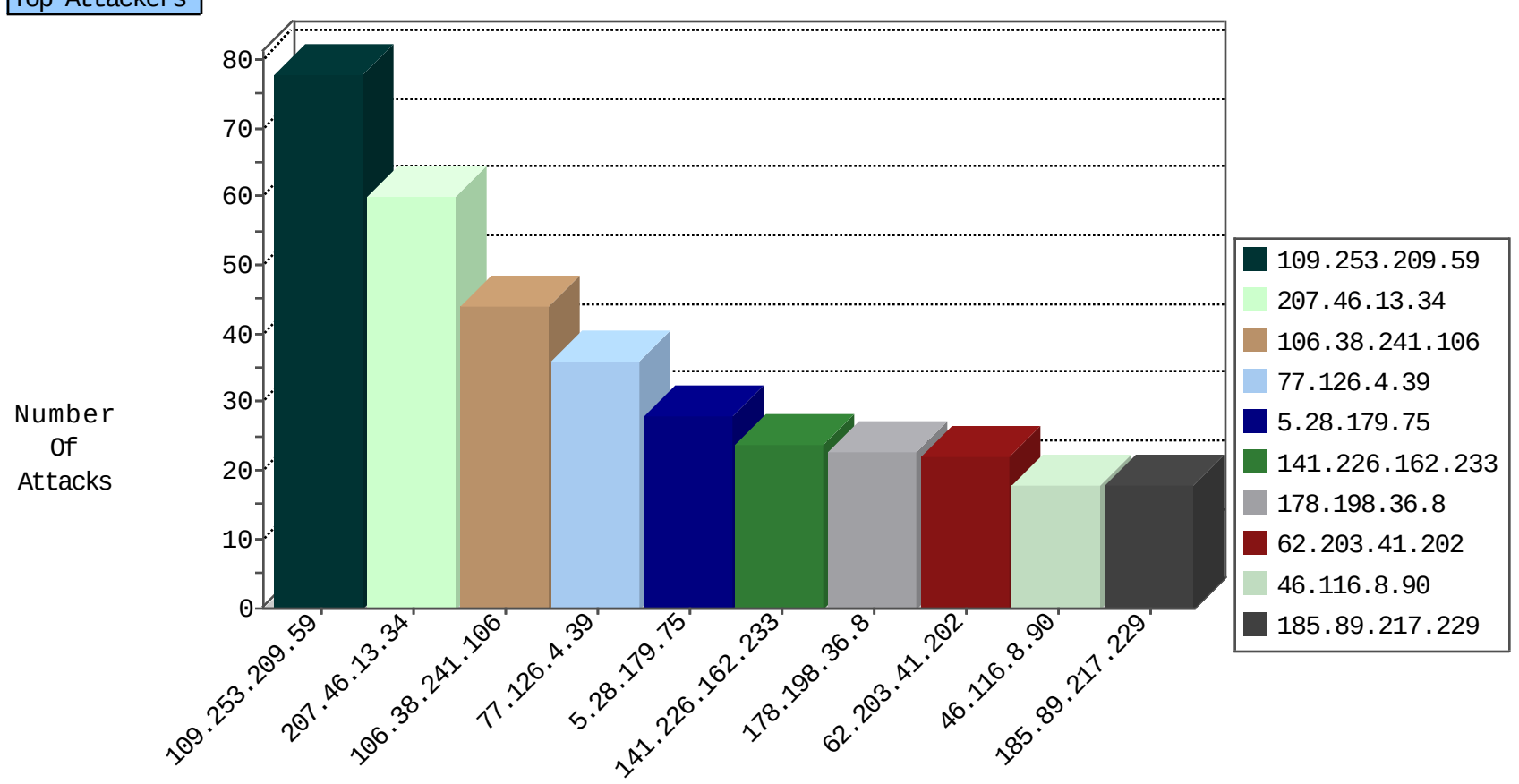
10-03-2016-17:04:04 to 10-03-2016-18:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-03-2016-17:04:04 to 10-03-2016-18:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	8
46.19.86.6	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.248.174.4	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
115.47.12.162	China	147.237.72.156	aman.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.197	e.himush.idf.il	Black List	drop	1
78.129.171.175	United Kingdom	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

10-03-2016-17:04:04 to 10-03-2016-18:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	15
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	11
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	11
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	5
106.38.241.106	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	5
106.38.241.106	China	147.237.76.86	navy.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

10-03-2016-17:04:04 to 10-03-2016-18:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
146.200.148.0	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
208.100.26.228	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
213.42.28.185	147.237.0.33	United Arab Emirates	idf.il	ET SCAN NMAP -sS window 2048	1
208.100.26.228	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
180.150.177.188	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
14.152.59.11	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
213.42.28.185	147.237.0.33	United Arab Emirates	idf.il	ET SCAN NMAP -sS window 4096	1
213.42.28.185	147.237.0.33	United Arab Emirates	idf.il	ET SCAN NMAP -f -sS	1

10-03-2016-17:04:04 to 10-03-2016-18:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	57
77.126.4.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
5.28.179.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	28
66.249.65.53	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
109.75.78.10	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
141.226.162.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
141.226.162.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.8.204.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
109.65.84.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
62.203.41.202	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
80.246.136.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
62.114.217.99	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
196.207.93.186	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.3.147.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.166.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
62.203.41.202	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
213.8.204.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
84.108.227.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
87.70.38.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
85.64.21.155	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
146.185.56.162	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
62.203.41.202	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
62.203.41.202	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
128.179.184.22	Switzerland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
84.108.227.208	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
62.203.41.202	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
141.226.217.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.223.65	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.32.123.251	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.29.202.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
185.3.147.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.117.75.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
85.114.119.3	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	3
5.29.202.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
187.253.122.9	Mexico	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
187.253.122.9	Mexico	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.53.15.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
195.142.92.32	Turkey	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
37.26.148.178	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.24.184.193	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
178.199.205.188	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2

10-03-2016-17:04:04 to 10-03-2016-18:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.209.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
46.116.8.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
185.89.217.229	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
185.89.217.225	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
185.89.217.232	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
185.89.217.228	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
185.89.217.230	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
185.89.217.234	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
185.89.217.227	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
185.89.217.226	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
185.89.217.235	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
80.246.136.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
185.89.217.233	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.108.5.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
116.24.250.26	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 116.24.250.26	Block	6
2.53.2.121	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	5
185.89.217.231	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
82.80.249.158	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.80.249.158	Block	4
79.178.13.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
95.35.169.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.249.158	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	3
116.24.250.26	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
85.64.16.23	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.182.118.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.64.182	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1246-he/atal.aspx	Block	1
116.24.250.26	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
31.13.113.81	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he/dover.aspxفارو	Block	1
82.80.249.211	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
192.52.250.229	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general	Block	1
46.121.83.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.65.10	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json	Block	1
136.243.67.234	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
40.77.167.66	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/modules/shared/usercontrols/navmenu/	Block	1
82.205.30.61	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he/dover.aspxفارو	Block	1
207.161.164.179	Canada	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
68.180.230.216	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
51.174.220.1	Norway	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
66.249.65.12	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
157.55.39.92	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/g/yus	Block	1
46.19.85.215	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 46.19.85.215 (Open Mode)	None	1
84.95.208.20	Israel	147.237.72.167	ishurim.aka.idf.il	PHP Attempt	Block	1
207.161.164.179	Canada	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
66.249.64.100	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.73.133	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-22488-he/dover.aspx	Block	1
46.19.85.215	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.182.118.43	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.180	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1
82.80.249.158	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/71004.pdf	Block	1

10-03-2016-17:04:04 to 10-03-2016-18:04:04