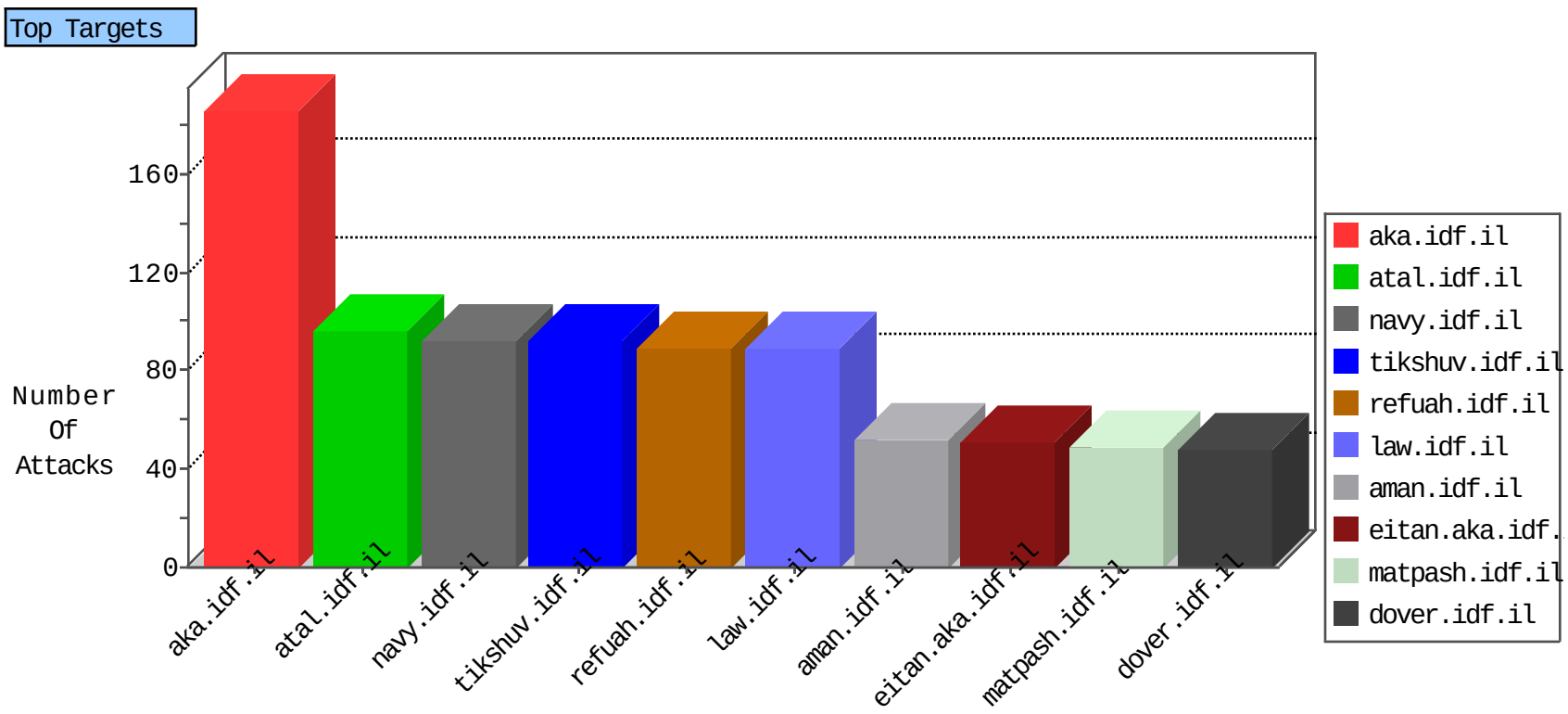
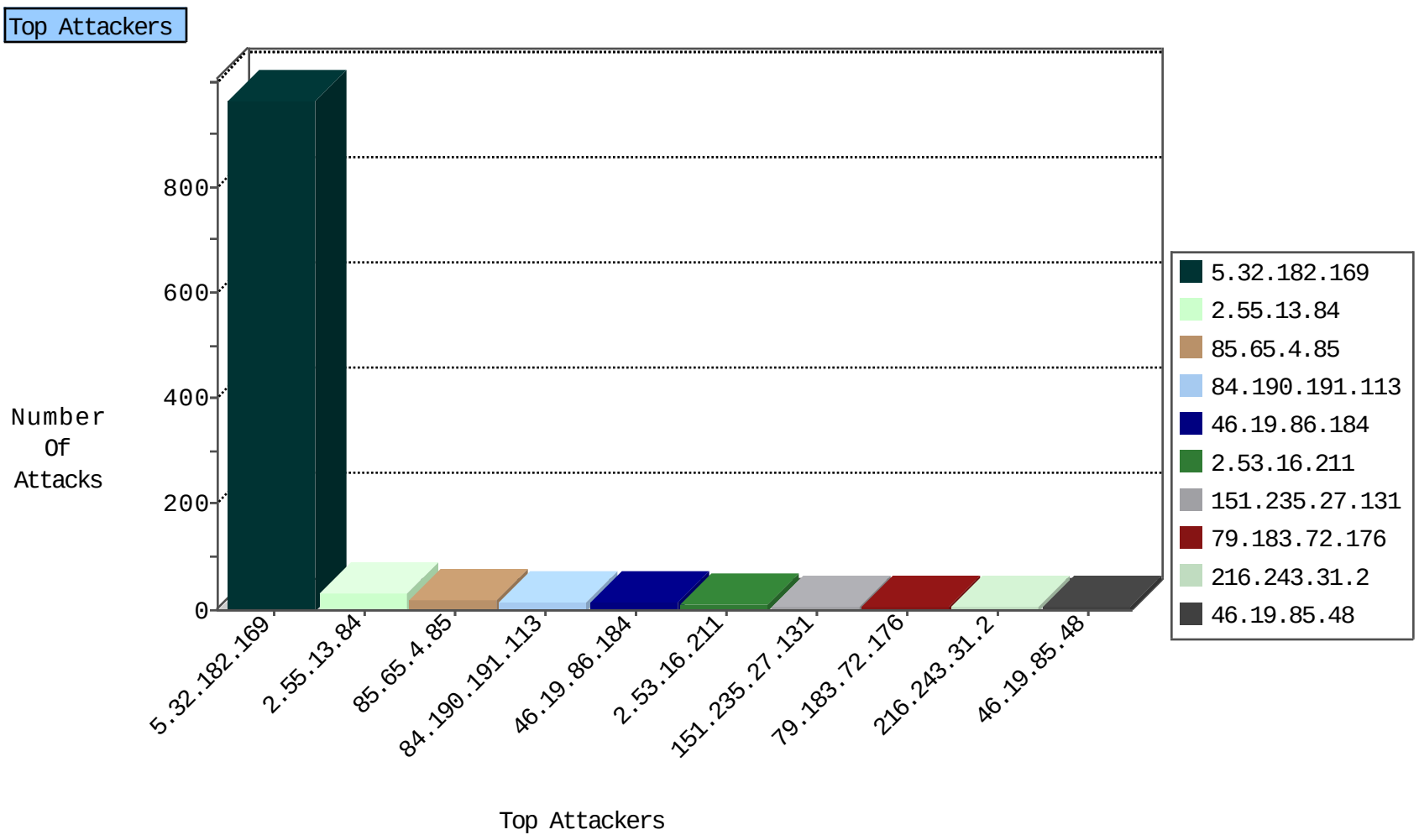
09-23-2016-21:04:03 to 09-23-2016-22:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-23-2016-21:04:03 to 09-23-2016-22:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.198	e.yohalan.idf.il	Black List	drop	2
142.54.174.85	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
213.202.233.188	Germany	147.237.76.42	refuah.idf.il	Black List	drop	1
84.229.49.217	Israel	147.237.76.86	navy.idf.il	Black List	drop	1
122.224.153.109	China	147.237.76.30	himush.idf.il	JLM_Purple_Con_Limit_Http	drop	1
213.202.233.188	Germany	147.237.76.44	e.refuah.idf.il	Black List	drop	1
104.238.146.105	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
104.238.146.105	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
69.30.226.220	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
104.238.147.7	United States	147.237.76.30	himush.idf.il	Black List	drop	1

09-23-2016-21:04:03 to 09-23-2016-22:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.0.34	tikshuv.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	84
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.233	atal.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	84
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.74	law.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	84
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.42	refuah.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	84
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.72.166	aka.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	84
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.86	navy.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	84
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.200	eitan.aka.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.39	mobile.meitav.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.72.156	aman.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.170	maarachot.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.176	matpash.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.72.167	ishurim.aka.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.147	chinuch.aka.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.0.15	kosher-kravi.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.226	www.chamatz.aka.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.31	nakchal.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42

09-23-2016-21:04:03 to 09-23-2016-22:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.166.92.132	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
45.63.28.189	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
183.9.38.91	147.237.77.74	China	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.134.160	147.237.77.74	United Kingdom	law.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.148.87	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
46.165.210.13	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
45.63.28.189	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
95.152.80.48	147.237.8.24	Switzerland	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
80.82.65.82	147.237.77.216	Netherlands	dover.idf.il	ET WEB_SERVER Poison Null Byte	1
58.220.2.5	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

09-23-2016-21:04:03 to 09-23-2016-22:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.65.4.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
2.53.16.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.190.191.113	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.183.72.176	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.55.13.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
2.55.13.84	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.55.13.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
2.55.13.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.86.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
213.57.70.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
151.235.27.131	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
151.235.27.131	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.190.191.113	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.53.28.128	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.53.18.0	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
196.64.93.103	Morocco	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
176.13.241.130	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.46.35.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
93.155.253.166	Bulgaria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
31.215.111.212	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
100.92.228.84		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
188.225.156.20	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.117.22.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
157.55.39.143	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.85.95	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.253.231.238	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.243.31.2	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.176.85.13	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.13.241.130	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
125.77.28.26	China	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.46.35.34	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.65.68.17	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.243.31.2	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
80.246.133.27	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.117.22.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
162.209.225.118	United States	147.237.0.35	akaws.idf.il	drop		drop	1
46.19.85.112	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
122.224.153.109	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
216.243.31.2	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.176.85.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.65.139.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	1
216.243.31.2	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.139.12.69	France	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-23-2016-21:04:03 to 09-23-2016-22:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 5.32.182.169	Block	4
46.121.150.234	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	4
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
46.117.246.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.32.182.169	Block	2
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.233	atal.idf.il	Unauthorized HTTP Method	Block	2
77.138.133.169	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	2
77.139.14.228	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.86	navy.idf.il	Unauthorized HTTP Method	Block	2
66.249.65.176	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/3/673.doc	Block	1
37.26.148.255	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
77.139.14.228	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	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
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
82.166.92.132	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.138.21.110	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	1
66.249.66.10	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/articles.aspx	Block	1
37.142.10.24	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.176	matpash.idf.il	Unauthorized HTTP Method	Block	1
79.176.85.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.100	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list7.htm	Block	1
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.39	mobile.meitav.idf.il	Admin Blocking	Block	1
66.249.64.66	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.0.34	tikshuv.idf.il	Unauthorized HTTP Method	Block	1
109.253.240.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.170	maarachot.idf.il	Multiple Admin Blocking from 5.32.182.169	Block	1
77.138.63.196	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
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.72.166	aka.idf.il	Unauthorized Method PROPFIND for www.aka.idf.il/	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
79.177.13.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.226	www.chamatz.aka.idf.il	Admin Blocking	Block	1
66.249.76.102	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.39	mobile.meitav.idf.il	Unauthorized HTTP Method	Block	1
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.72.156	aman.idf.il	Admin Blocking	Block	1
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/30112010masaiyot.aspx	Block	1
157.55.39.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 5.32.182.169	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2367.jpg	Block	1
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.0.15	kosher-kravi.idf.il	Unauthorized HTTP Method	Block	1
79.179.6.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 5.32.182.169	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmi	Block	1

09-23-2016-21:04:03 to 09-23-2016-22:04:03

09-23-2016-21:04:03 to 09-23-2016-22:04:03