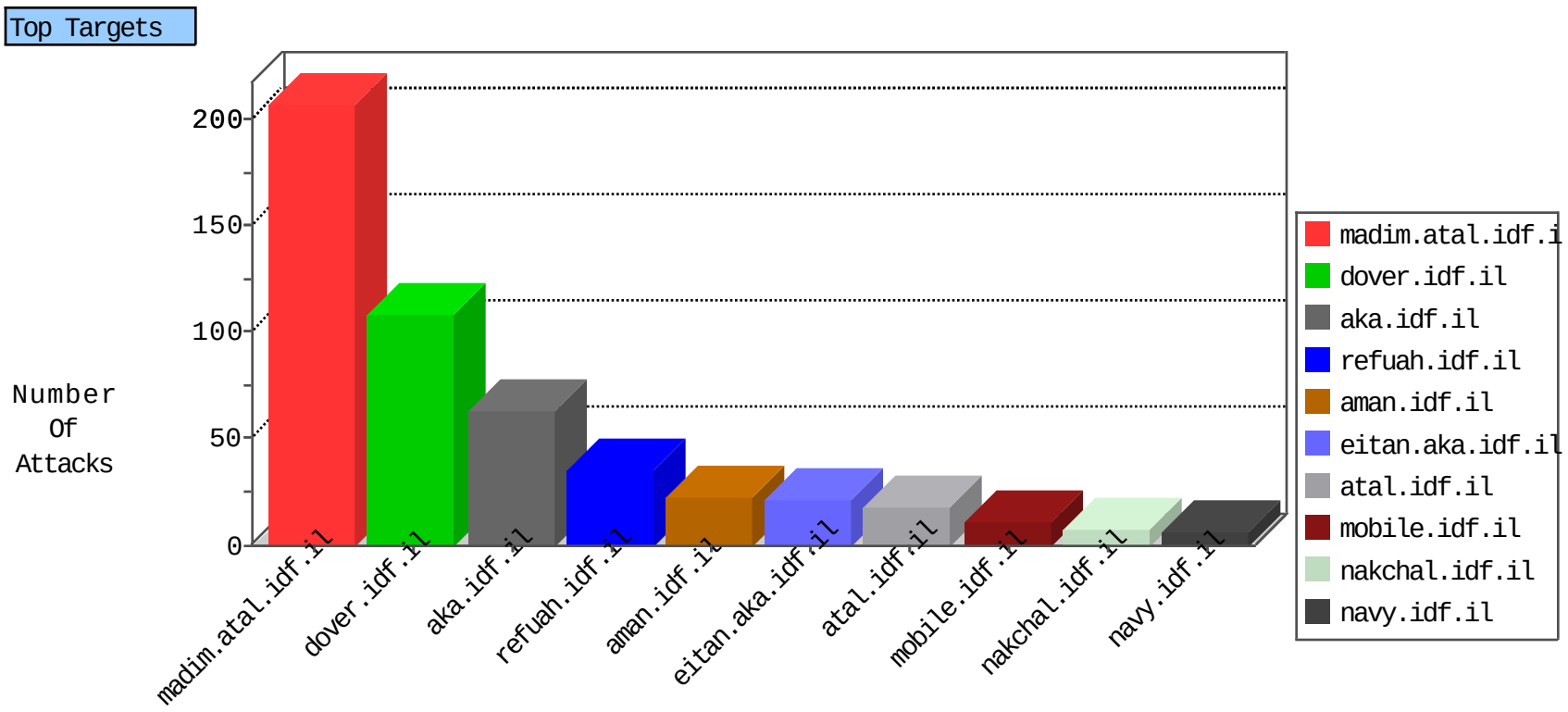
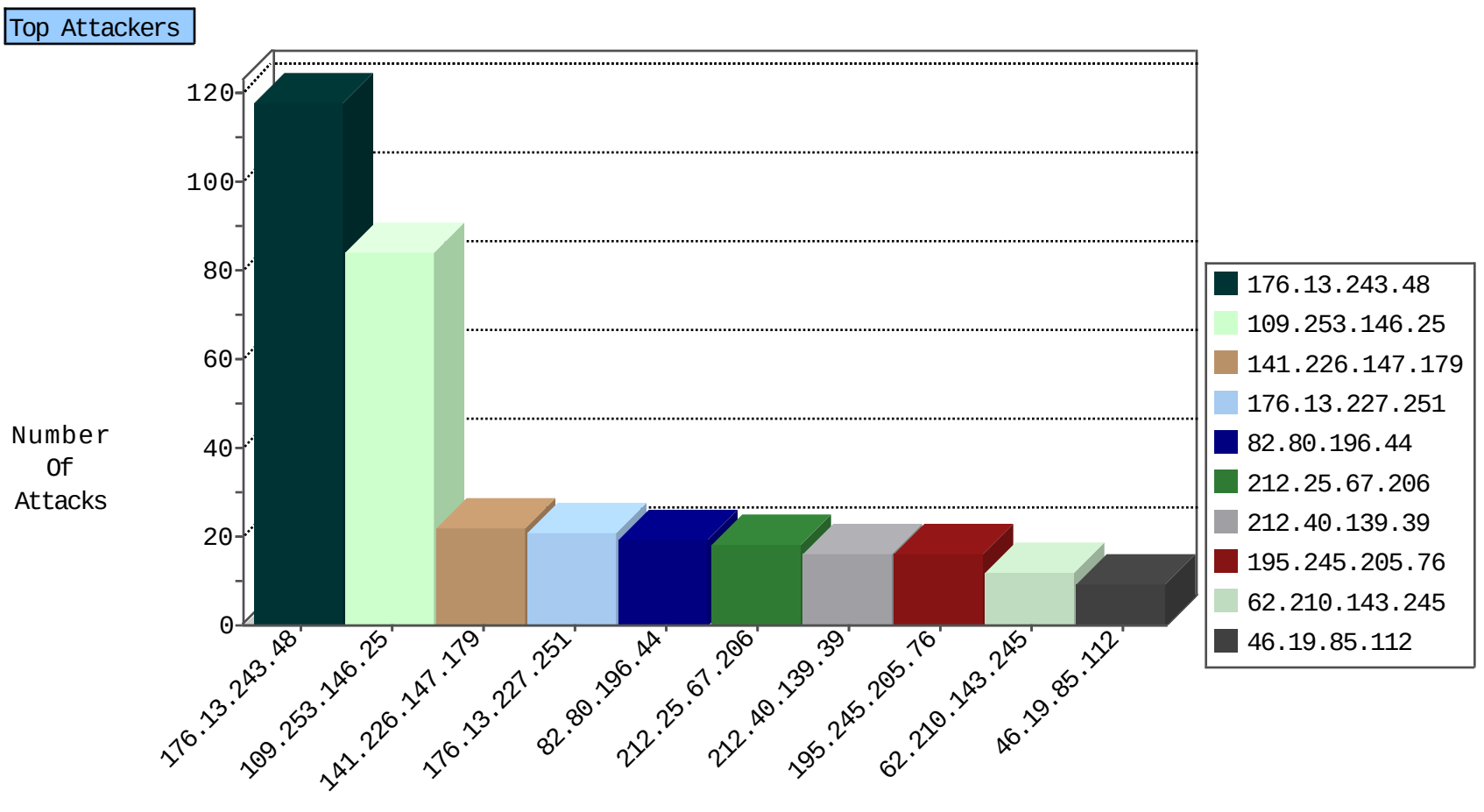
09-05-2016-11:04:23 to 09-05-2016-12:04:23

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-05-2016-11:04:23 to 09-05-2016-12:04:23

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.112	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	31
176.13.243.48	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	8
109.236.84.10	Netherlands	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
73.97.140.187	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.177	ncore.idf.il	Black List	drop	1
83.142.230.136	United Kingdom	147.237.77.205	prisha.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Black List	drop	1

09-05-2016-11:04:23 to 09-05-2016-12:04:23

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.143.245	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	12
139.193.40.129	Indonesia	147.237.77.176	matpash.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1

09-05-2016-11:04:23 to 09-05-2016-12:04:23

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.245.205.76	147.237.0.19	Russian Federation	madim.atal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
46.120.50.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.216	Russian Federation	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
82.81.214.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.238.38	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.205	Russian Federation	prisha.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
79.178.163.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.164.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
141.226.147.179	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	1
195.245.205.76	147.237.76.199	Russian Federation	e.nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
79.176.51.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.48.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.167.6.84	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
77.124.24.9	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.39	Russian Federation	mobile.meitav.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
93.157.86.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.210.250.111	147.237.0.19	France	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
195.245.205.76	147.237.76.30	Russian Federation	himush.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
87.71.246.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.227.67.172	147.237.77.170	Sweden	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
195.245.205.76	147.237.72.167	Russian Federation	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
85.64.11.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.148.16.146	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
195.245.205.76	147.237.8.45	Russian Federation	e.eitan.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
84.94.208.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.8.14	Russian Federation	e.orchot.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
46.148.16.146	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
82.146.49.51	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
213.8.83.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.114.3.241	147.237.77.226	Israel	www.chamatz.aka.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
46.19.86.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.212	Russian Federation	e.dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
81.218.76.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
161.18.199.151	147.237.77.179	Colombia	e.mazi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.55.4.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.121	Russian Federation	e.navy.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
79.178.54.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.61.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.42.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.81.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.196	Russian Federation	e.sviva.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
104.128.144.131	147.237.8.50	Canada	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
62.210.250.111	147.237.77.19	France	law-forum.idf.il	ET SCAN Potential SSH Scan	1
195.245.205.76	147.237.76.34	Russian Federation	yohalan.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
87.236.194.161	147.237.76.38	Czech Republic	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
195.245.205.76	147.237.72.217	Russian Federation	e.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
85.250.234.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.227.67.172	147.237.77.121	Sweden	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1

09-05-2016-11:04:23 to 09-05-2016-12:04:23

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
176.13.227.251	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
141.226.147.179	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
109.67.237.24	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
109.65.123.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.90	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
141.226.147.179	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.43.111.234	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
176.13.243.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
84.110.176.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.147.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.110.176.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
192.116.92.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.148.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.70	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.96.190.166	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.65.18.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.6	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
84.95.85.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.70	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
79.179.15.4	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.25.102.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.207.224	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.118	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.29.202.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
176.13.234.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
109.253.215.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
85.130.219.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
72.5.195.133	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
45.56.74.212	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
139.162.225.219	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.130.219.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
72.5.195.133	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
195.60.235.57	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.226.218.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
212.179.218.166	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	1
46.120.122.219	Israel	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
176.13.244.9	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.82	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
85.130.219.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-05-2016-11:04:23 to 09-05-2016-12:04:23

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.243.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
109.253.146.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
212.40.139.39	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	16
212.25.67.206	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized HTTP Method	Block	13
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
132.72.33.69	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	5
213.8.204.40	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
212.25.67.206	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 212.25.67.206	Block	4
213.57.165.51	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	4
176.13.227.251	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	3
132.72.33.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	3
220.255.103.184	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
195.62.18.235	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
165.72.200.11	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	2
176.13.12.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.140.82	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
141.226.147.179	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
77.124.33.160	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
212.25.102.63	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
46.19.85.170	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
203.127.58.229	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.227.109	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
217.194.198.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
64.62.219.164	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.2.126	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.115.177.202	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
157.55.39.118	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
77.124.247.188	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.120.73.198	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
203.127.58.237	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
219.75.81.166	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
2.53.163.106	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.62.18.235	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 195.62.18.235	Block	1
165.72.200.11	Europe	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 165.72.200.11	Block	1
77.138.30.213	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
212.179.28.34	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/110192.pdf	Block	1
203.127.96.232	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
64.62.219.71	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.97	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/869-3860-he/patzar.aspx	Block	1
37.26.148.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.109.234	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
207.46.13.36	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/main/giyus/general.aspx	Block	1
64.62.219.150	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.249.6	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
212.25.67.206	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/1/	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.19.85.90	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
195.62.18.235	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1

09-05-2016-11:04:23 to 09-05-2016-12:04:23