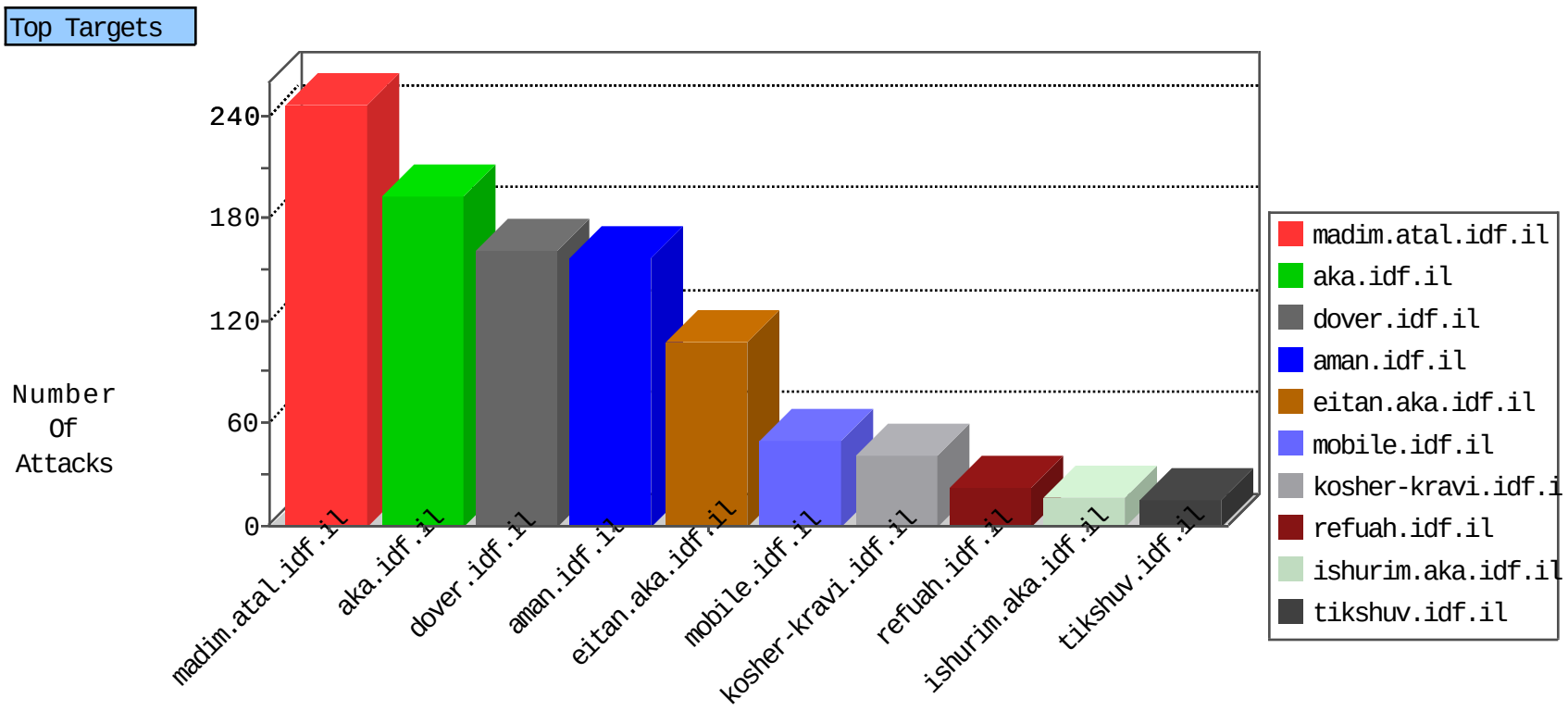
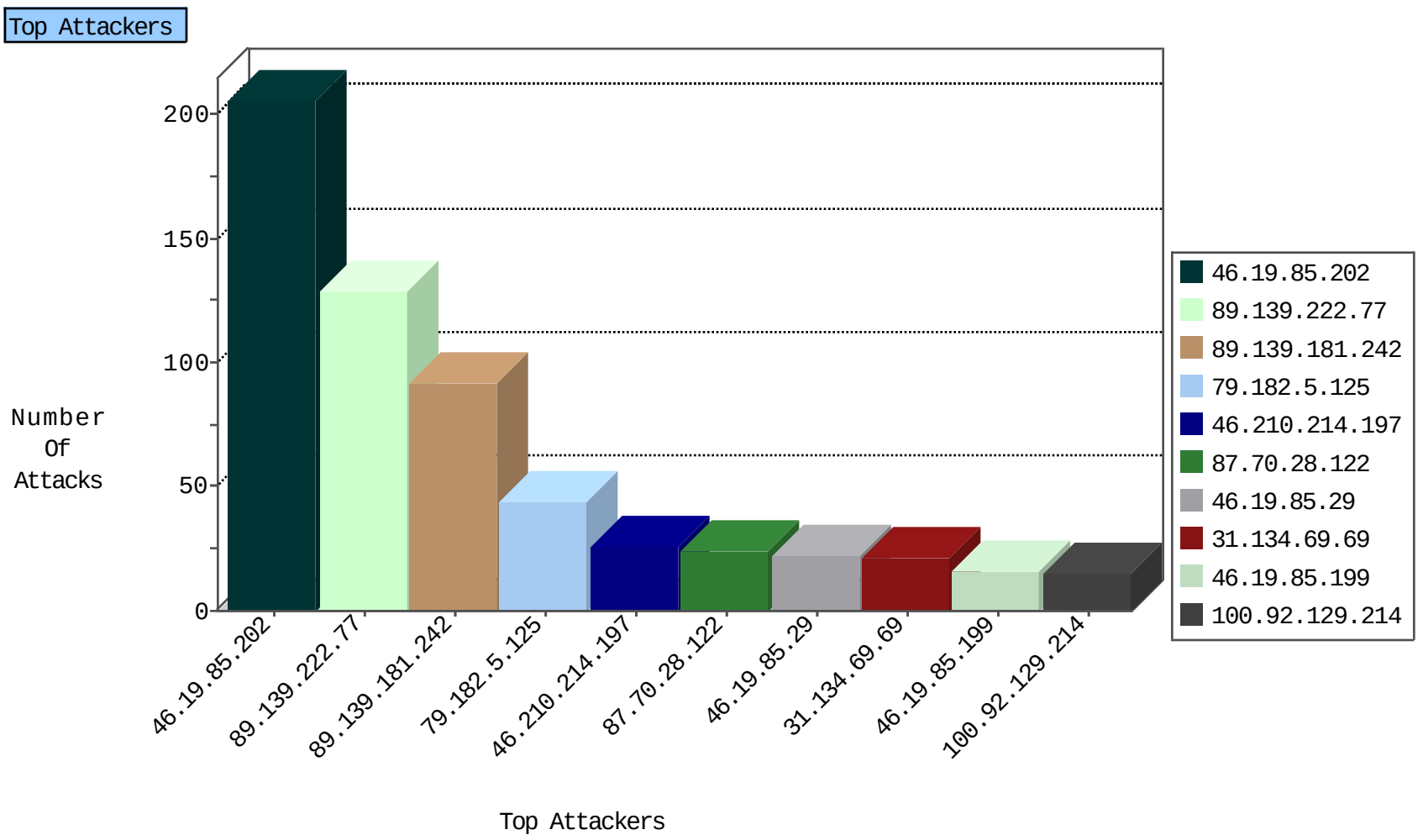
09-29-2016-20:04:05 to 09-29-2016-21:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-29-2016-20:04:05 to 09-29-2016-21:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.193.254	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
173.208.213.194	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
173.208.213.198	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
63.141.250.154	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
209.126.136.2	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
173.208.150.115	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
192.187.101.238	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	1
209.126.136.2	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
173.208.207.130	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
198.204.247.219	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
69.30.227.222	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
212.24.153.38	Czech Republic	147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	1
198.204.255.76	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
142.54.174.86	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1

09-29-2016-20:04:05 to 09-29-2016-21:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-29-2016-20:04:05 to 09-29-2016-21:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
31.134.69.69	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
31.134.69.69	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Potential SSH Scan	2
31.134.69.69	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
31.134.69.69	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.162	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
31.134.69.69	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
31.134.69.69	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.39	United Kingdom	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
31.134.69.69	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
31.134.69.69	147.237.76.197	Ukraine	e.himush.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
31.134.69.69	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
31.134.69.69	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
188.161.84.19	147.237.77.170	Palestinian Territory, Occupied	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
31.134.69.69	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
31.134.69.69	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
31.134.69.69	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
31.134.69.69	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
31.134.69.69	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
31.134.69.69	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN Potential SSH Scan	1
31.134.69.69	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN Potential SSH Scan	1
31.134.69.69	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1

09-29-2016-20:04:05 to 09-29-2016-21:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.139.181.242	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	92
89.139.222.77	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	36
89.139.222.77	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	29
89.139.222.77	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	23
100.92.129.214		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
79.182.5.125	Israel	147.237.0.15	kosher-kravi.idf.i	drop	First packet isn't SYN	drop	14
89.139.222.77	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
89.139.222.77	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
89.139.222.77	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.182.5.125	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
87.70.28.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
87.70.28.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
37.19.119.7	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
156.33.252.37	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
79.182.5.125	Israel	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.28.136.158	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
79.177.32.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.42.217	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
66.108.152.81	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
176.13.229.105	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.5.125	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.248.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.133	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.32.71	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
79.178.138.209	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
66.249.93.85	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.53.152.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.235.191	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.254	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.254	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.117.56.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.149.177	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.231.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.147.129	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.61.54	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.79	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.246.138.58	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.0	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.64.32.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
93.172.199.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.253.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
131.253.27.31	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

09-29-2016-20:04:05 to 09-29-2016-21:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	203
46.210.214.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
46.121.14.166	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	7
46.19.85.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
88.15.241.70	Spain	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	3
46.117.56.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.53.182.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.117.128.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.248.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
141.226.161.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.120.168.75	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
87.69.216.31	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
2.53.55.207	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
93.172.199.55	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.177.32.195	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
204.79.180.129	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	1
157.55.39.11	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/news/news.in.aspx	Block	1
87.69.216.31	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
68.180.228.44	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter PageNum in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
46.19.86.68	Israel	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method , in URL sdch	Block	1
109.64.32.71	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.218.179.41	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.210.144.159	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx	Block	1
87.197.164.92	Slovakia	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.127.61.54	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
46.19.86.146	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.132	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper	Block	1
2.53.185.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.6.32	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
213.57.171.216	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.248.130	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.47.68	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
192.243.55.132	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.26.147.157	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
141.226.217.240	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
87.69.216.31	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 87.69.216.31	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
192.116.175.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$rptEmai in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	1
46.19.86.68	Israel	147.237.0.34	tikshuv.idf.il	Illegal HTTP Version	Block	1
93.172.111.51	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.229.201	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
192.243.55.136	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper	Block	1
37.26.147.249	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
157.55.39.11	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 157.55.39.11	Block	1
66.249.69.228	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1764	Block	1
192.116.175.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.68	Israel	147.237.0.34	tikshuv.idf.il	Malformed URL sdch	Block	1

09-29-2016-20:04:05 to 09-29-2016-21:04:05