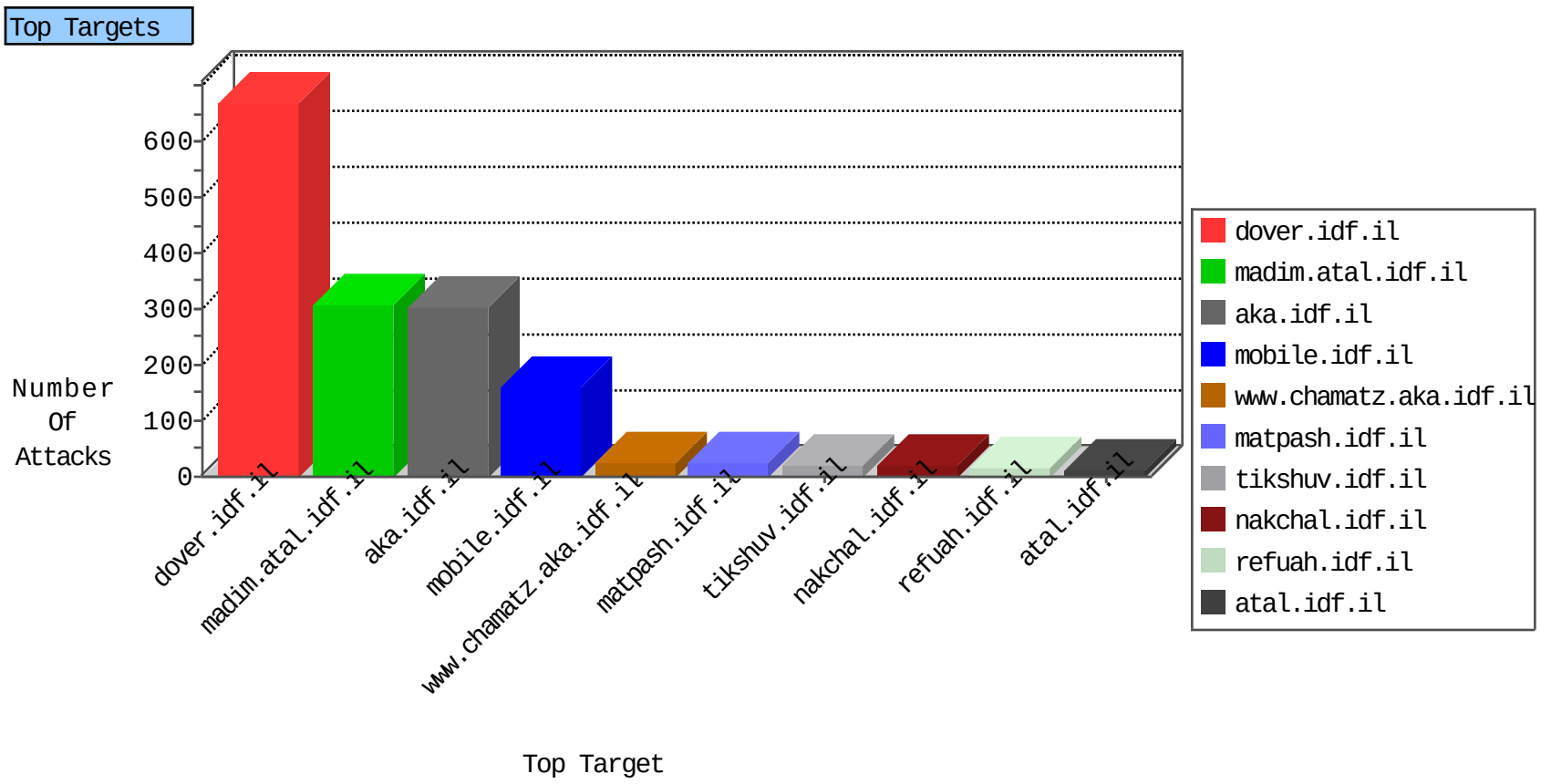
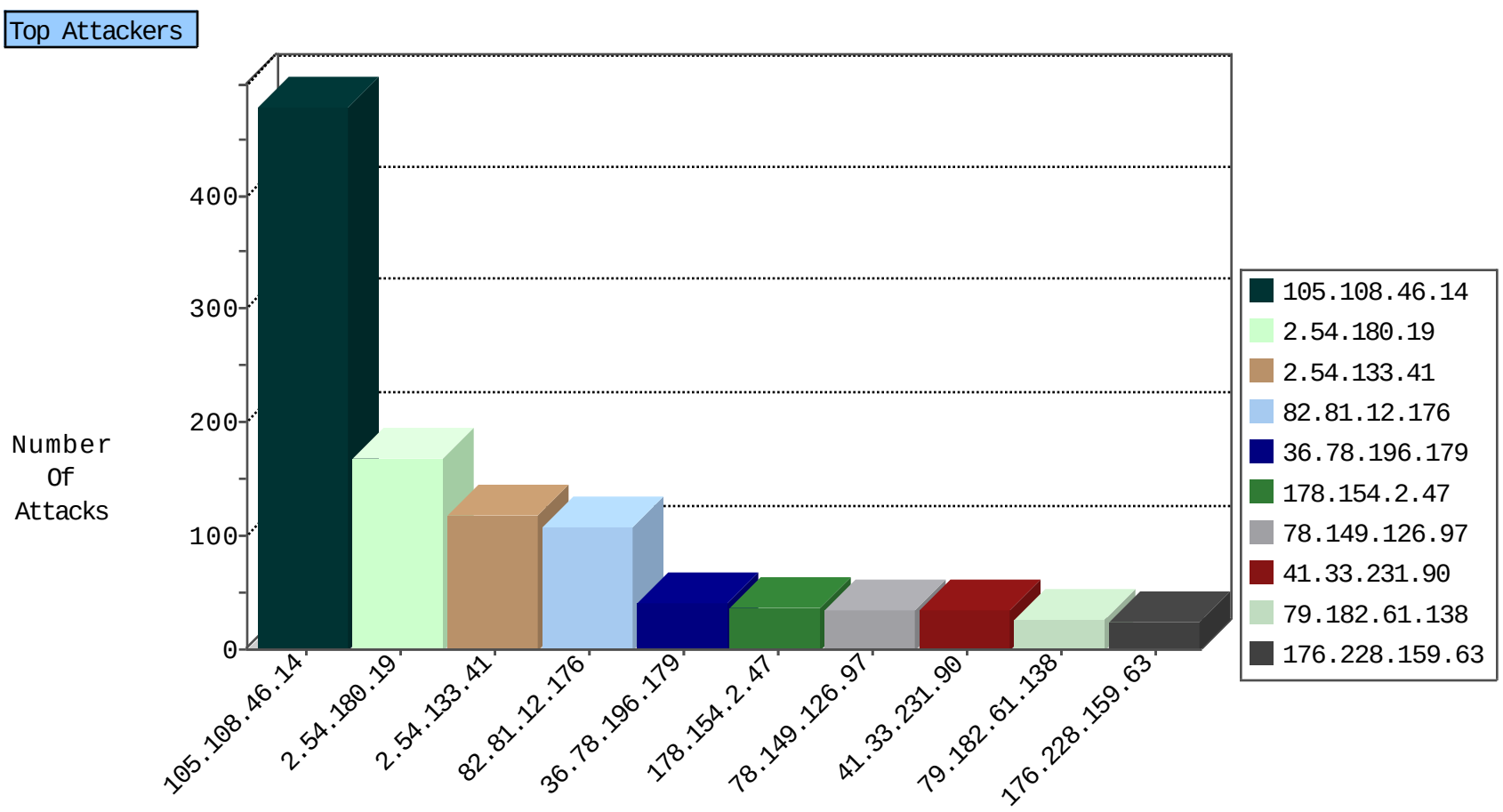
01-30-2016-12:04:00 to 01-30-2016-13:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-30-2016-12:04:00 to 01-30-2016-13:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	108
105.108.46.14	Algeria	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-dun	dest-reset	17
105.108.46.14	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	11
183.238.143.73	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

01-30-2016-12:04:00 to 01-30-2016-13:04:00

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	C103: HTTP: User Agent Sogou+web+spider	Block	1
144.76.12.78	Germany	147.237.77.176	matpash.idf.il	C106: HTTP: majestic bot	Block	1

01-30-2016-12:04:00 to 01-30-2016-13:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
13.75.42.200	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
188.0.236.123	147.237.72.14	Moldova, Republic of	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
139.196.57.234	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.160.196	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.77.227	Turkey	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
13.75.42.200	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
119.146.221.68	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.120.164.239	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
46.45.137.67	147.237.77.61	Turkey	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1

01-30-2016-12:04:00 to 01-30-2016-13:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.108.46.14	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	167
105.108.46.14	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	159
105.108.46.14	Algeria	147.237.77.216	dover.idf.il	SYN Attack		reject	44
36.78.196.179	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	41
178.154.2.47	Belarus	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
78.149.126.97	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.182.61.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
105.108.46.14	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
105.108.46.14	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	26
37.26.148.155	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	22
2.54.158.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.228.159.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
105.108.46.14	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
109.253.193.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.67.3.26	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
109.67.59.166	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
185.6.56.52	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
5.144.59.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.228.131.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.135.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.139.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.198.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.159	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.210.187.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
105.108.46.14	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.76	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.185.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.181.30.192	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.179.26.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.253.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.123.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
105.108.46.14	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.176.113.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.201.224.8	Ukraine	147.237.76.86	navy.idf.il	drop	SAM rule	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.13.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.12.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-30-2016-12:04:00 to 01-30-2016-13:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
157.55.39.44	United States	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
105.108.46.14	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
2.54.58.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.152.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.111.111.59	Israel	147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.180.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	167
2.54.133.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
149.78.240.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.240.44	Block	14
84.111.111.59	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	8
176.228.159.63	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
2.54.158.151	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
46.121.214.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
31.24.33.250	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.24.33.250	Block	5
84.111.111.59	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 84.111.111.59	Block	5
157.55.39.44	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/main/home/default.aspx	Block	4
109.253.193.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.186.186.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.212.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.111.111.59	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	3
79.180.200.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.142.209.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.109.163.122	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
109.253.206.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
195.154.189.197	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
84.109.107.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.222.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.65.150.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.64.18.79	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	2
109.253.198.159	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
89.138.246.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.94.48.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.54.133.41	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.13.15.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1781-he/dover.aspx	Block	1
46.19.85.117	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.57.209.195	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
109.65.48.123	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.65.48.123	Block	1
23.254.138.210	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
188.120.148.59	Israel	147.237.76.30	himush.idf.il	PHP Attempt	Block	1
79.178.126.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.88.34.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.64.48	Block	1
93.172.52.45	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
37.26.146.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.228.128.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.70.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
46.120.196.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.132.104.132	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
109.65.48.123	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
188.120.148.59	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/xmlrpc.php	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/headers/tfasim.gif	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
195.154.189.197	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/license.php	Block	1
77.75.77.101	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/25/	Block	1