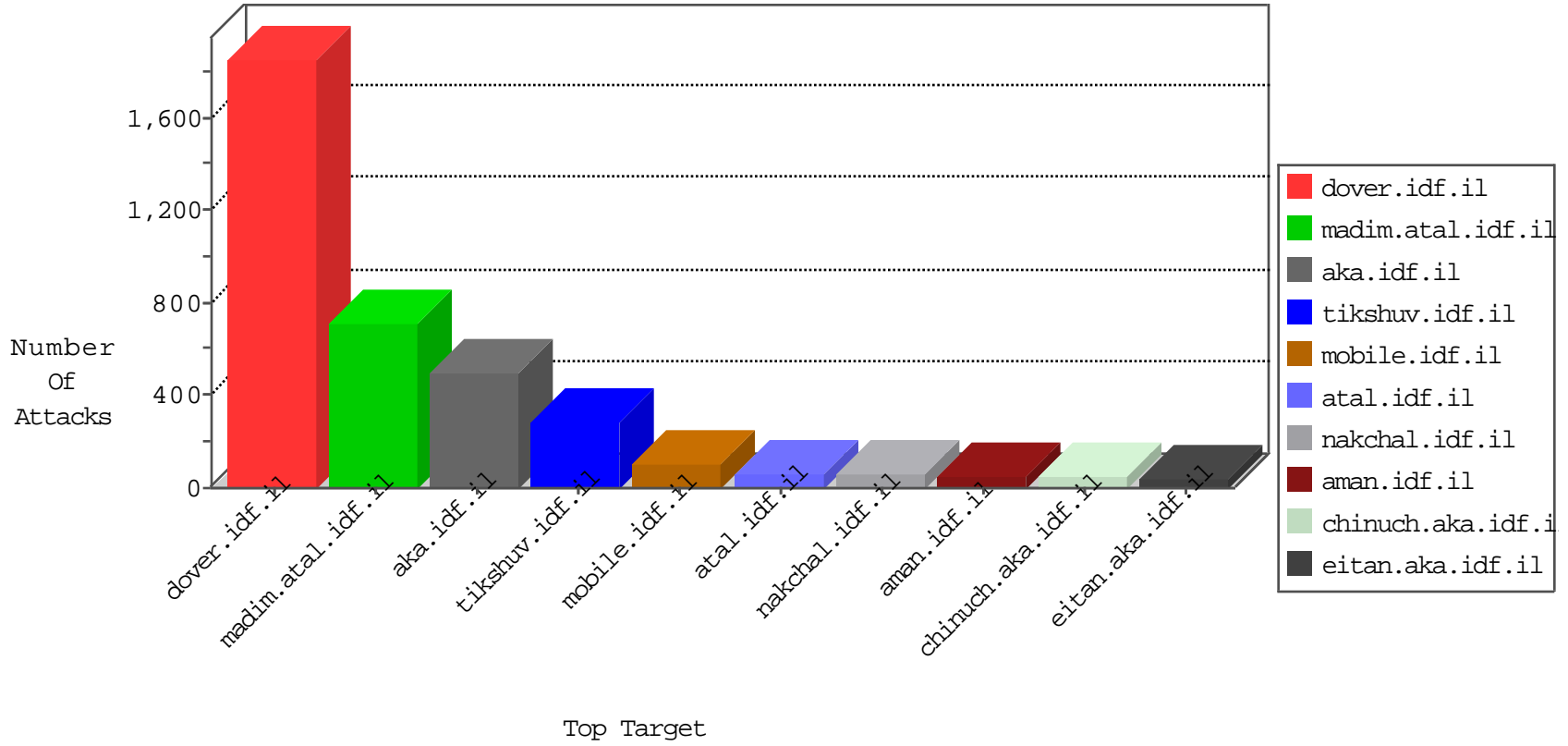


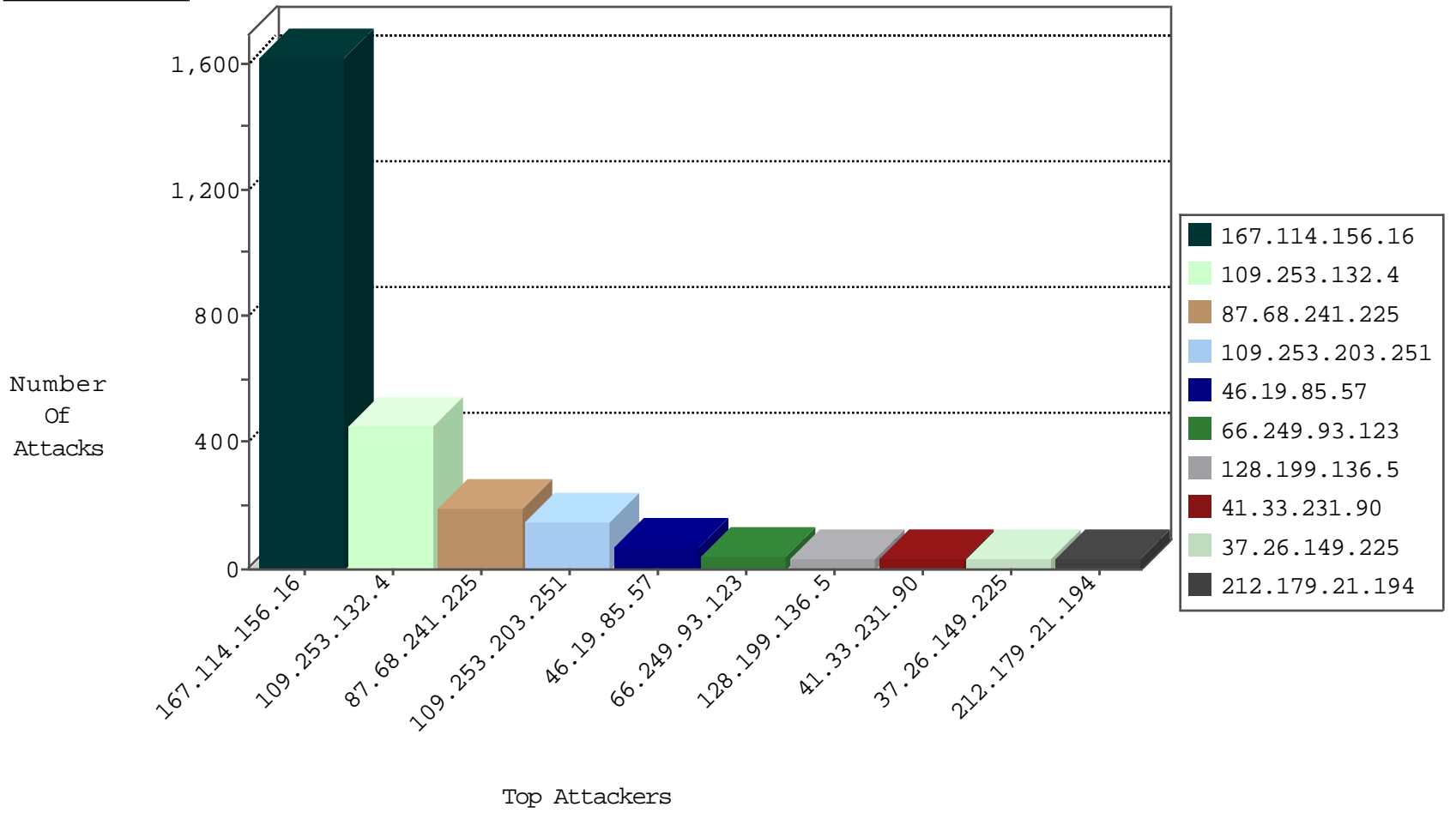
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3002
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
89.248.168.218	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
200.29.186.163	Chile	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Https	drop	1
89.248.168.218	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.158	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
89.248.168.218	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
85.104.115.34	Turkey	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

01-11-2016-14:04:02 to 01-11-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.57	147.237.0.34	Israel	tikshuv.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	32
183.60.252.84	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.224.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.162.131	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
74.68.55.15	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
119.164.254.57	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
93.99.204.29	147.237.8.50	Czech Republic	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.193.2.8	147.237.76.39	France	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
73.243.176.4	147.237.0.15	United States	kosher-kravi.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
46.19.85.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.34.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	37
37.26.149.225	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
46.19.85.57	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	30
2.54.139.31	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
62.128.48.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
87.68.83.144	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
46.19.85.200	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
62.0.219.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
112.198.103.92	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
2.54.186.164	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
109.253.212.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.182.202.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.179.220.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.5.174	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.64.152.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.168.241.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
80.179.211.135	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
2.54.166.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
109.253.129.79	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
40.77.167.81	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
77.127.220.175	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.52.49.255	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.146.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
82.81.66.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.39.169	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.179.5.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.200.205.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.146.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
132.70.66.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.116.241.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.179.169.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.243.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.70.66.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.155.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.145.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.203.251	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.47	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.47	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.168.241.38	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.0	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.189	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.132.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	254
87.68.241.225	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 87.68.241.225	Block	187
109.253.132.4	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.132.4	Block	94
109.253.203.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
109.253.132.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
109.253.203.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	52
109.253.132.4	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 109.253.132.4	Block	51
128.199.136.5	Singapore	147.237.76.147	chinuch.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	33
46.19.85.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
109.253.131.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
80.246.133.249	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 80.246.133.249	Block	20
82.166.24.184	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 82.166.24.184	Block	15
109.253.222.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
109.253.135.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
79.182.151.191	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	7
62.0.105.133	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
109.253.212.181	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
2.54.9.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.140.69	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
176.13.19.5	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
31.168.226.132	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	4
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
84.111.125.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.10.99.202	Switzerland	147.237.76.147	chinuch.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
80.246.136.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.129.79	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.3.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	3
176.13.10.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.130.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	3
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	2
109.65.96.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
147.236.16.190	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
85.250.238.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.129.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.203.251	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
193.41.209.2	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	2
166.171.184.23	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
73.243.176.4	United States	147.237.76.200	eitan.aka.idf.il	Access to: /cgi-bin/php	Block	1
132.70.66.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.224	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
94.230.84.253	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
46.19.85.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	1