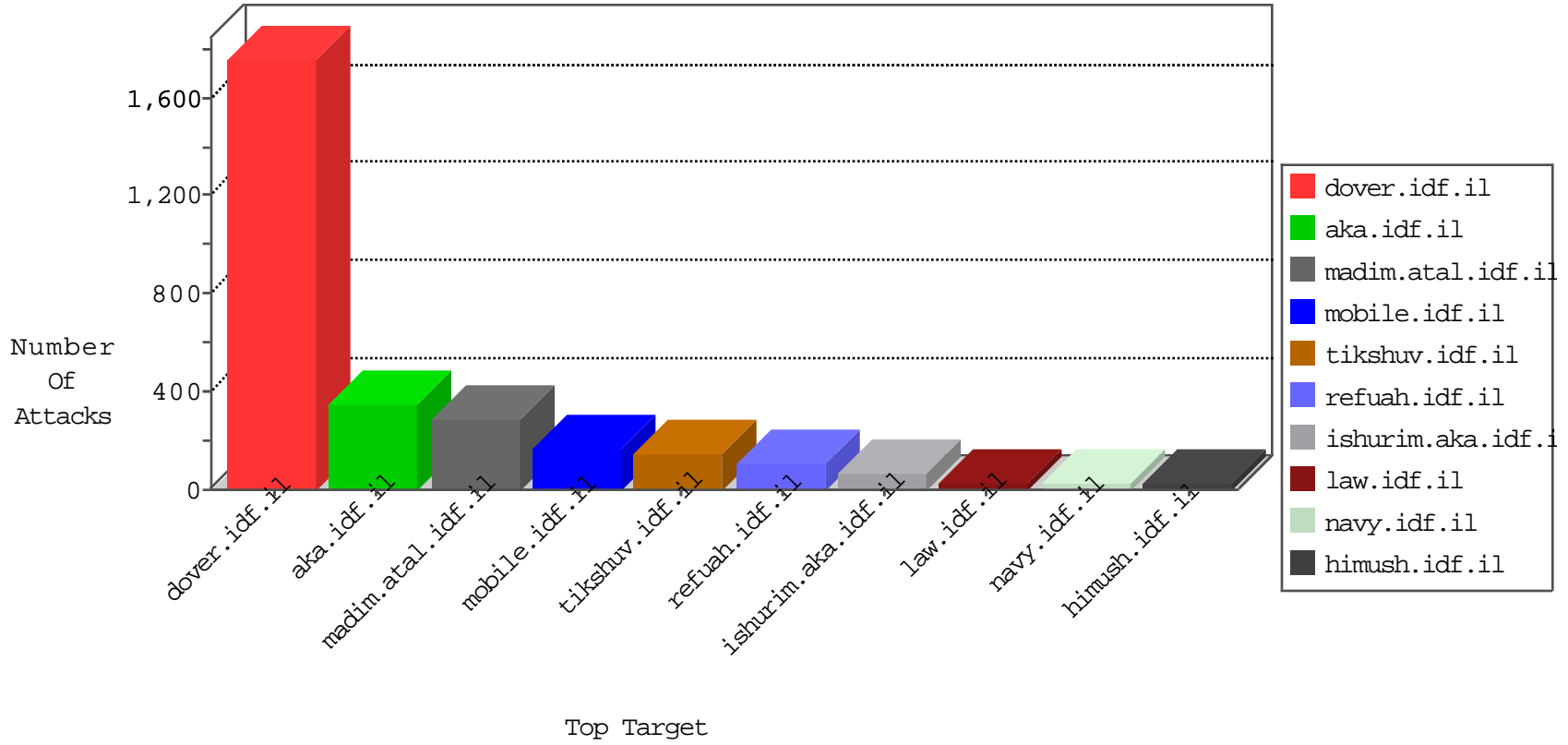


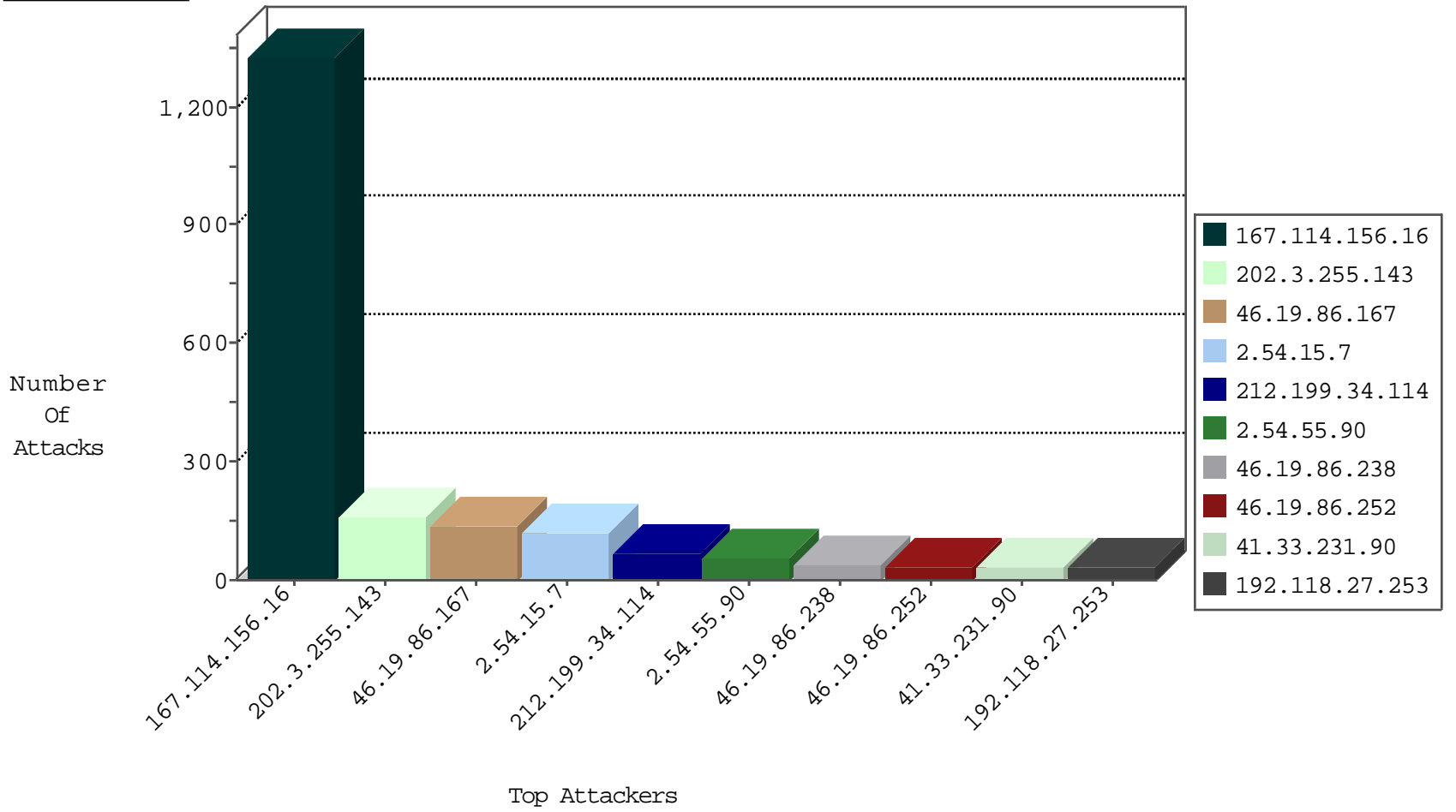
IDF Under Attack Daily Report



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	3000
2.54.175.175	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
176.13.23.39	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.64.68.161	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
84.95.252.113	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
89.248.174.4	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
193.41.247.4	Romania	147.237.76.34	yohalan.idf.il	I4 Source or Dest Port Zero	drop	1

01-17-2016-13:04:08 to 01-17-2016-14:04:08

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
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	128
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.246.136.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.60	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
46.19.86.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.234	147.237.8.46		e.chinuch.idf.i	ET SCAN Potential SSH Scan	1
149.88.164.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.188.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.161.40.120	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.200.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.118.73.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.40	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.76.200	United States	eitan.aka.idf.i	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.199.34.114	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	65
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.86.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.55.90	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
192.118.27.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.41	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.86.62	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
176.13.18.16	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
109.253.210.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
66.249.69.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.47.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
194.90.252.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.175.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.55.90	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	12
80.246.133.60	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.66.144.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.178.219.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
80.246.133.60	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
79.178.219.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.41	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.118.27.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
2.54.55.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
85.65.51.96	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.54.55.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.55.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.86.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.117.242.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.65.16	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.118.27.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.42	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.242.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.65.51.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.179.168.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.118	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.70	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.146.35	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.229.56	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.118	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.130.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.167	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	136
2.54.15.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	88
46.19.86.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
2.54.15.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	31
46.19.85.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
2.54.46.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
216.35.195.247	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	14
176.13.17.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
46.19.86.113	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	11
46.19.86.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
46.19.86.252	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
46.19.86.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
46.19.85.154	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
212.150.215.254	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.150.215.254	Block	4
46.19.86.113	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.210.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
212.179.185.157	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
2.54.175.175	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
37.26.148.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.166.240.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.50.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	3
176.13.18.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.6.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.216.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	3
212.150.215.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	2
87.69.32.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.195	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.181.56.191	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
46.19.85.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.2.20	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
212.150.215.8	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.150.215.8	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
80.246.136.73	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.220.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.178.219.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
220.181.132.216	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
46.19.85.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.60	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/mailbox.aspx&sa=u&ved=0ahukewj3v8u0rp_jahum arqkhf4zbrqqfeggmay&sig2=eadgnuats1qp1d-1ft4fxg&usg=afqjcnfw8xbjdj46 aa_ieeng07gs79p8hq	Block	1
109.66.144.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
54.173.223.170	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
2.54.47.6	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.250.227.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1