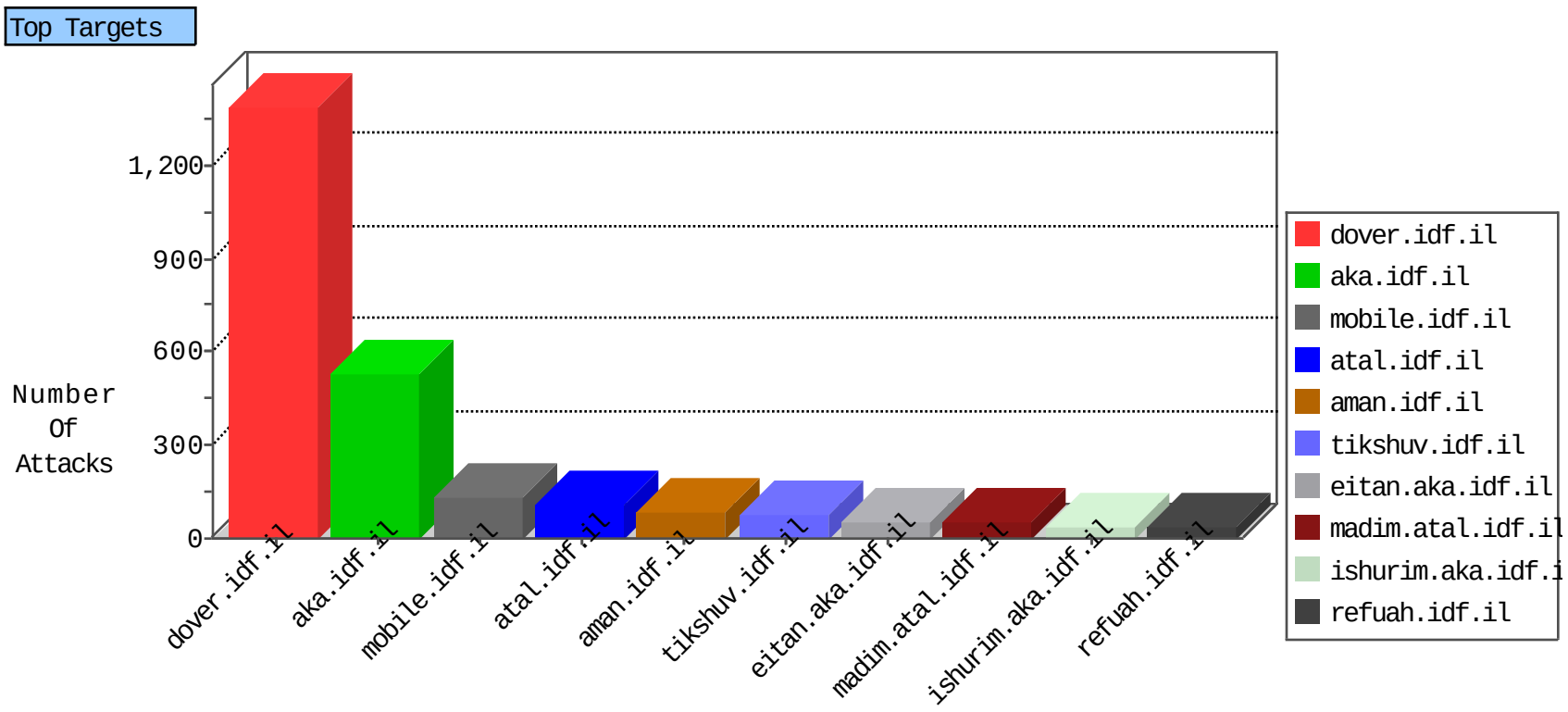
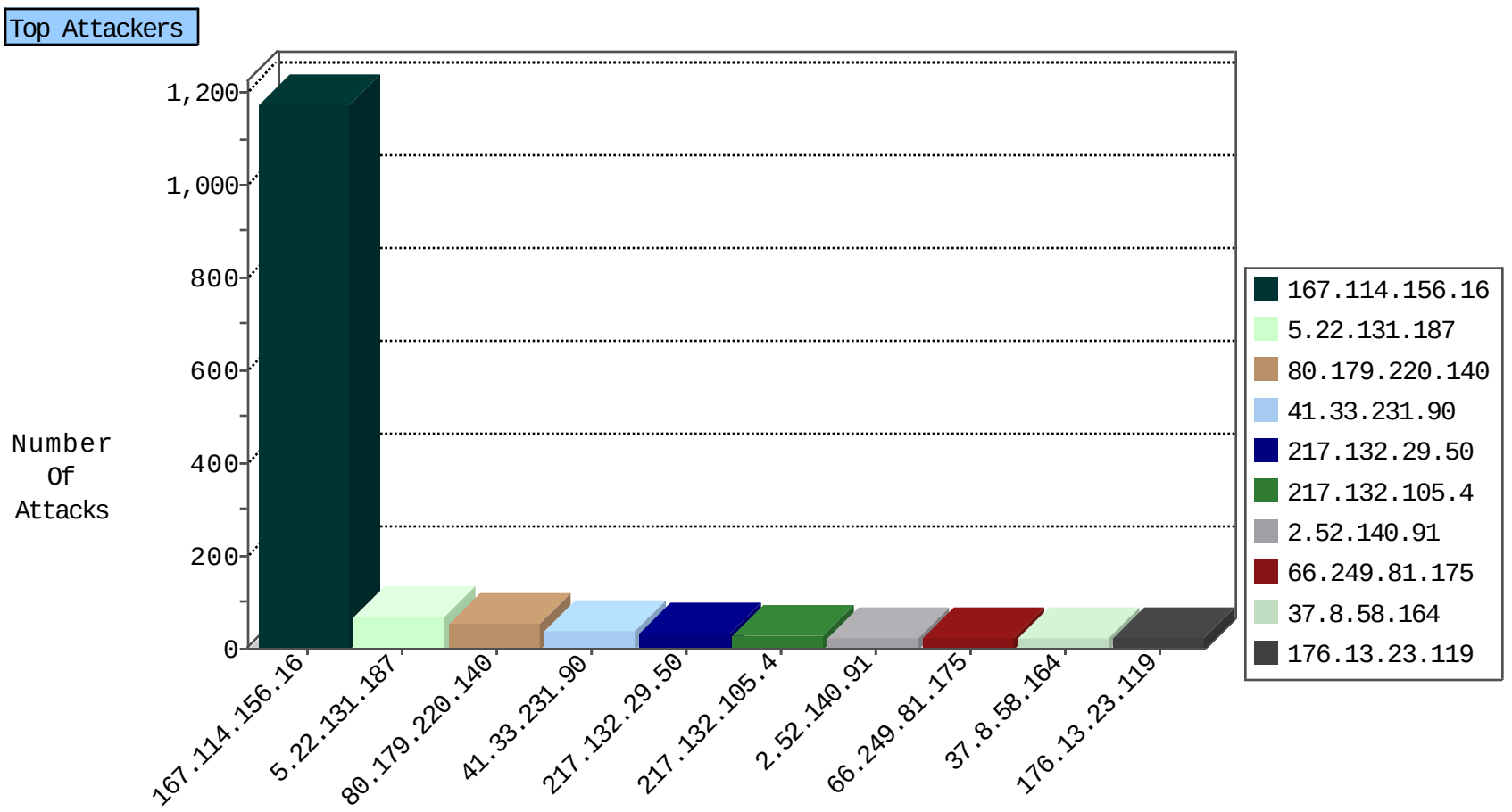
12-30-2015-13:04:02 to 12-30-2015-14:04:02

IDF Under Attack Daily Report





12-30-2015-13:04:02 to 12-30-2015-14:04:02

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	3924
212.179.210.163	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
212.25.121.195	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.25.121.195	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3

12-30-2015-13:04:02 to 12-30-2015-14:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-30-2015-13:04:02 to 12-30-2015-14:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.179.32.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.81.175	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
104.236.56.95	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.28.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.23.10.190	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
61.216.2.14	147.237.8.27	Taiwan	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
213.8.62.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.7.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.183.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
81.23.10.190	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
80.178.222.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
218.77.79.38	147.237.76.86	China	navy.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
149.88.141.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-30-2015-13:04:02 to 12-30-2015-14:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.179.220.140	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	22
46.19.86.199	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
2.52.32.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
84.228.197.3	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.150.90	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
37.8.58.164	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
176.13.10.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.143.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.8.58.164	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
176.13.23.119	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
176.13.23.119	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
217.132.105.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.249.81.183	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
46.117.89.158	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
80.178.189.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.86.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.14.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
217.132.105.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.117.89.158	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
79.181.189.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.134.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
37.26.147.152	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
213.57.129.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
2.52.140.91	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.165.179	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
217.132.29.50	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.0.217.1	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.13.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.217.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.4	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.131.62	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
108.171.128.161	United Kingdom	147.237.72.166	aka.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
79.180.143.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.4	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.102.62	Israel	147.237.72.166	aka.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
213.57.139.222	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.189	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.160.147.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.142.151.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.83	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.137.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

12-30-2015-13:04:02 to 12-30-2015-14:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.22.131.187	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
46.19.86.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
80.246.136.245	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
176.13.4.219	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	8
46.19.86.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.54.128.146	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/registrationwizard/register.aspx parameter	None	4
176.13.2.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.21.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.12.143.178	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Email in mobile.idf.il/sachar/createaccount	Block	4
2.54.163.215	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
66.249.66.61	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.253.146.247	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
176.13.9.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.232	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
2.54.1.121	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
109.160.147.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.55	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.142.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.9.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.176.104.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
157.55.39.179	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.203.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.14.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.1.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
141.8.142.82	Russian Federation	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.128.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.3	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
212.143.240.218	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
37.26.147.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.119.130	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	2
82.80.131.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.179.220.140	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	2
176.13.3.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.186.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
149.78.166.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.10.159	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.67.122.3	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	2
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/registrationwizard/register.aspx parameter	None	2
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.120.237.2	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	2
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	2
79.181.129.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.1.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.149.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
2.54.44.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.129.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.115.165	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-30-2015-13:04:02 to 12-30-2015-14:04:02