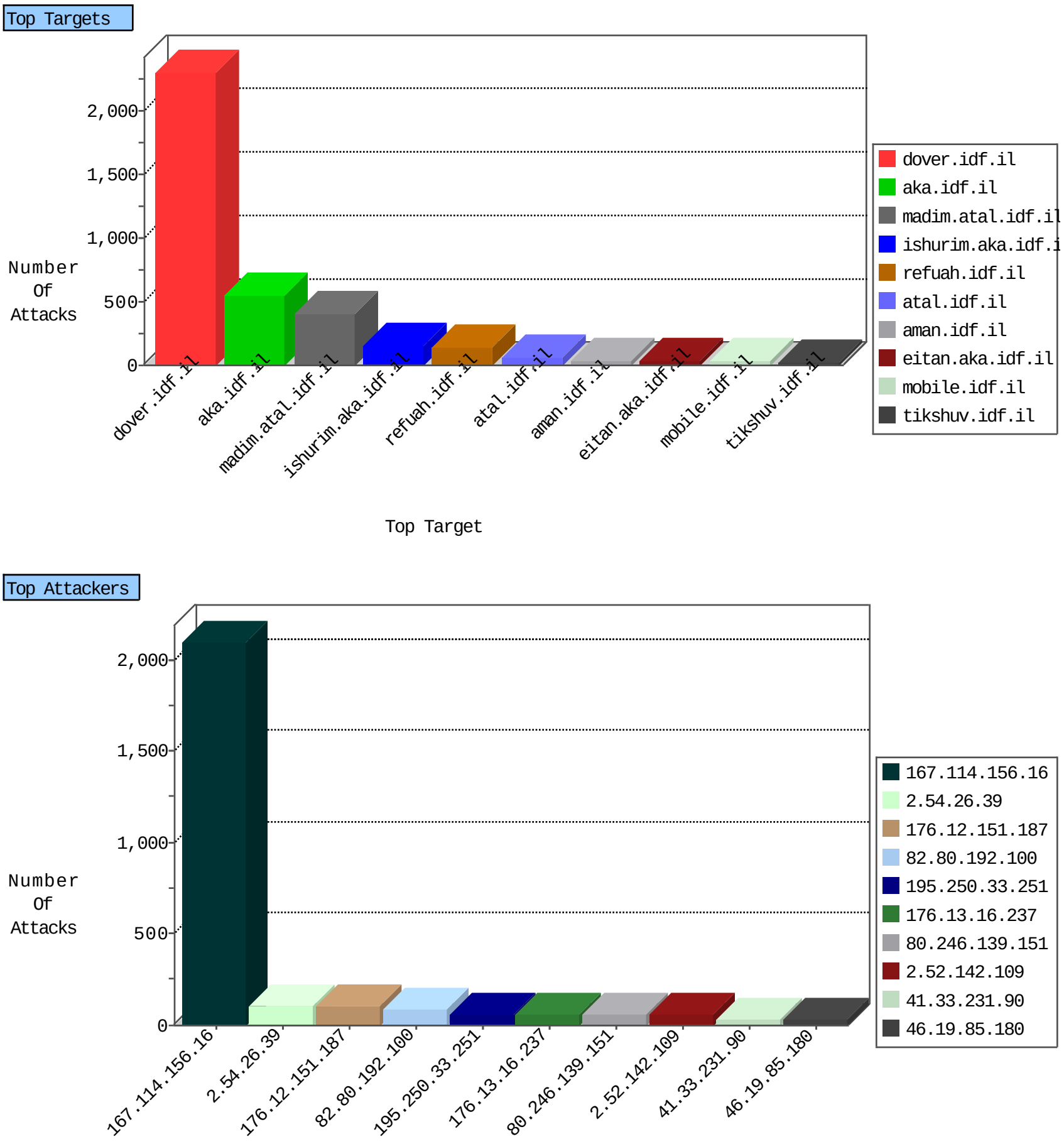
12-27-2015-10:04:01 to 12-27-2015-11:04:01

IDF Under Attack Daily Report



12-27-2015-10:04:01 to 12-27-2015-11:04:01

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	3411
134.147.203.115	Germany	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	3
212.109.216.112	Russian Federation	147.237.77.178	e.matpash.idf.il	Frk_Under_Attack_Con_Tcp	drop	2

12-27-2015-10:04:01 to 12-27-2015-11:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-27-2015-10:04:01 to 12-27-2015-11:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.8.204.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.88	147.237.77.74		law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.56	147.237.76.197		e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.31	147.237.8.28		e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
94.188.161.41	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.62.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.169.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.12.142.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.88	147.237.76.177		ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.31	147.237.77.227		e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
114.215.111.222	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-27-2015-10:04:01 to 12-27-2015-11:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.250.33.251	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	61
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
79.182.56.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
46.19.86.176	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
2.52.142.109	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
109.128.238.147	Belgium	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	23
2.54.29.116	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
195.160.240.11	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
46.19.85.95	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
192.118.22.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
2.54.181.58	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.19.85.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.130.110	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
109.253.158.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.27	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
79.183.131.11	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	11
46.19.85.132	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
2.52.142.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
80.246.130.104	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
2.52.142.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
80.246.139.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
109.253.158.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
109.64.67.249	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
185.120.126.111		147.237.77.176	matpash.idf.il	drop	SAM rule	drop	8
128.127.107.123	Netherlands	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
2.52.142.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.179.21.194	Israel	147.237.76.202	e.halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.97	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.187	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.228.188.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
146.185.61.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.233	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.168.138.173	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.233	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.40.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.5.92	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
176.13.1.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.185.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.58.99	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.62.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.232	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.26.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	97
82.80.192.100	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	91
176.13.16.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
176.12.151.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
176.12.151.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
80.246.139.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
176.13.2.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
41.102.74.200	Algeria	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 41.102.74.200	Block	25
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
80.246.139.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
2.54.26.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
82.81.160.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
193.108.195.249	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	4
5.102.222.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
197.134.254.87	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
192.116.55.253	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	3
128.127.107.123	Netherlands	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
197.134.254.87	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	3
80.246.136.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.219.187.94	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
109.253.216.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.94.7	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.94.7	Block	3
176.13.19.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.219.24.52	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
213.8.204.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.40.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	2
46.19.86.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.109.64.103	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in www.refua.atal.idf.il/926-he/refuah.aspx	Block	2
176.13.4.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.115.130.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
109.186.119.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.142.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.130.110	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
73.136.215.236	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
176.13.5.92	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
37.26.147.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.250.237.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.166.77.241	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/langstyle.css	Block	1
2.54.37.122	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.246.136.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.60.232.66	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
124.146.201.2	Japan	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
37.26.149.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
101.100.0.41	New Zealand	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.182.56.210	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
185.32.179.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.4.248	Israel	147.237.77.243	mobile.idf.il	Illegal HTTP Version	Block	1