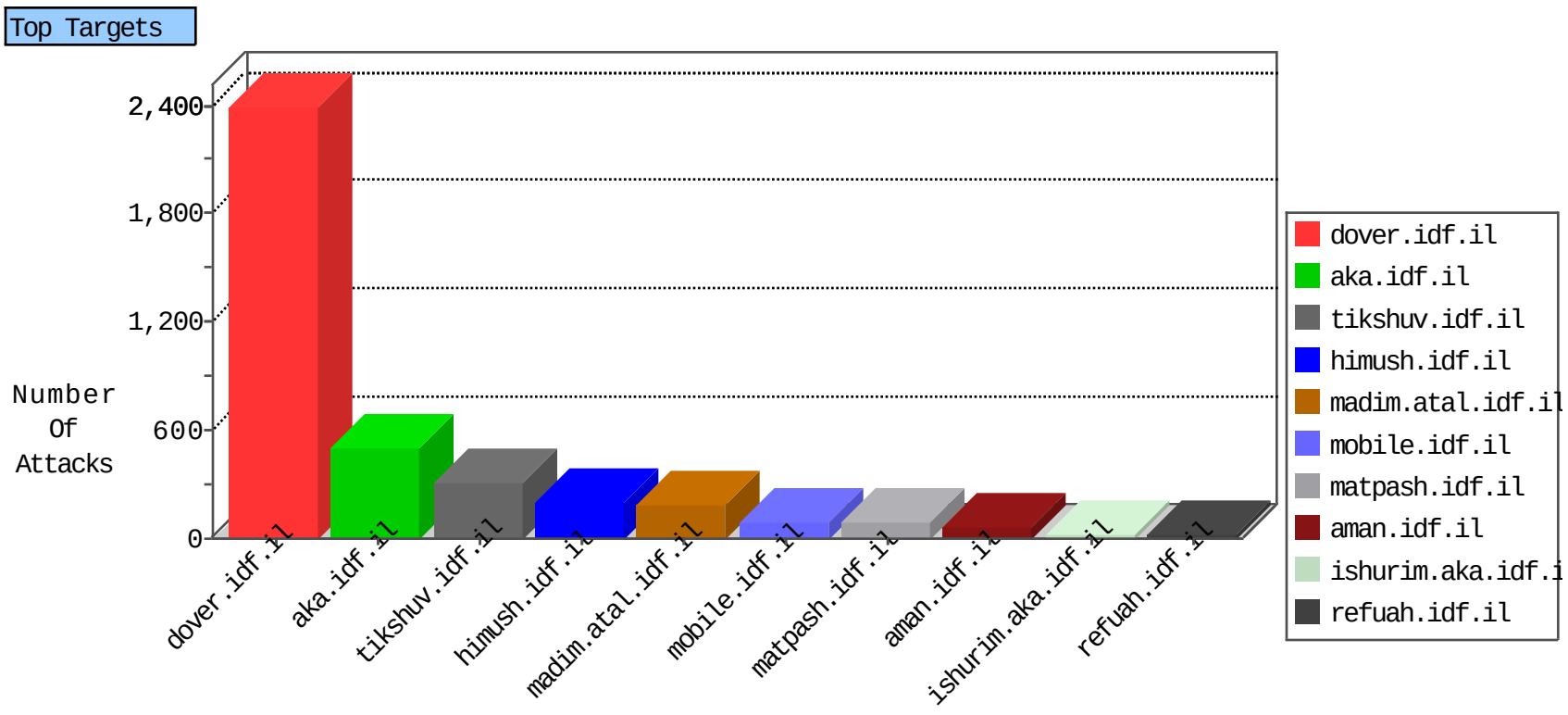
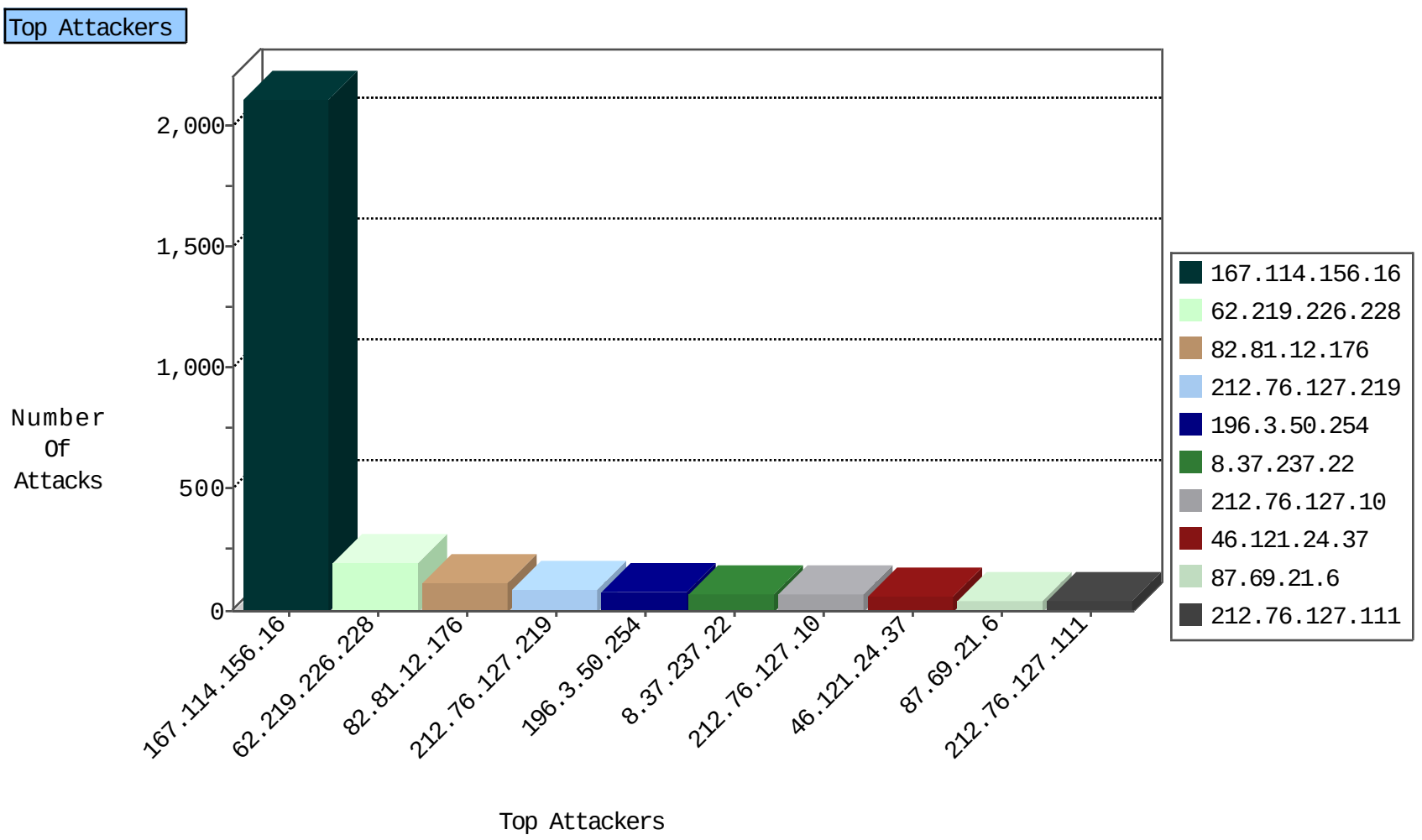
01-25-2016-13:04:01 to 01-25-2016-14:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-25-2016-13:04:01 to 01-25-2016-14:04:01

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	3007
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	120
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
8.37.237.22	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
109.66.205.39	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
107.167.108.144	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
8.37.237.22	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
182.96.195.239	China	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
42.118.243.249	Vietnam	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
8.37.237.22	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1

01-25-2016-13:04:01 to 01-25-2016-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-25-2016-13:04:01 to 01-25-2016-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.179.197.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
79.181.34.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.1.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.183.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.234.17	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.72.134.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.99.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.14.151.180	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.167.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
109.160.193.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.75.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-25-2016-13:04:01 to 01-25-2016-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	84
196.3.50.254	Switzerland	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	78
212.76.127.10	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	65
212.76.127.111	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	45
107.167.108.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	41
109.253.142.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.253.141.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
107.167.97.221	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
107.167.98.168	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
8.37.237.22	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
2.54.52.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
109.67.51.88	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
149.62.200.153	Bulgaria	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
85.130.216.49	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
94.230.86.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
79.179.190.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
66.249.78.147	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
37.26.149.249	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
93.173.249.116	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
80.74.97.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.217	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
217.194.197.154	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
82.80.30.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.194.197.154	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.181.202.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.8.156	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.51.88	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
194.90.76.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.173.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.123.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.119.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.29.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.76.127.44	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.182.219.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.215.118	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.45.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.8.57.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
213.57.196.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
85.65.154.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.246.130.21	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	4
80.246.130.21	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.250.227.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.78.226.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.29.16	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.183.36.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.219.226.228	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	196
46.121.24.37	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	62
87.69.21.6	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 87.69.21.6	Block	45
2.54.167.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
46.19.85.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
8.37.237.22	United States	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
2.54.24.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	24
46.19.85.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
109.65.59.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.253.141.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
37.26.148.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.7.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.0.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.246.137.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.4.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
31.154.4.18	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.154.4.18	Block	5
109.253.207.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.21.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.215	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.209.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.67.51.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
80.246.139.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
103.248.80.3	India	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	2
80.246.136.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.179.59.103	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
103.248.80.3	India	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	2
176.13.7.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.149.234	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in URL Â¨Ã?[[#16]]0]â€™â„¢Â£Â?×¤Â¹Âš [[#25]]np×¥Ö»[[#1]]	Block	1
2.54.37.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
37.142.64.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.219.121	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.25.84.200	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/smalim/scriptresource.axd	None	1
79.114.249.57	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.114.249.57	Block	1
176.13.18.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.154.4.18	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/sip_storage/files/2/61222.gif	None	1
105.109.165.177	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
2.54.178.250	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
85.64.243.192	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
80.246.136.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.237.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$btnSubmit.y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.67.150.32	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
79.178.212.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.52.161.99	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /shop/admin/orders.php/login.php	Block	1
31.154.4.18	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/main/smalim/scriptresource.axd	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1