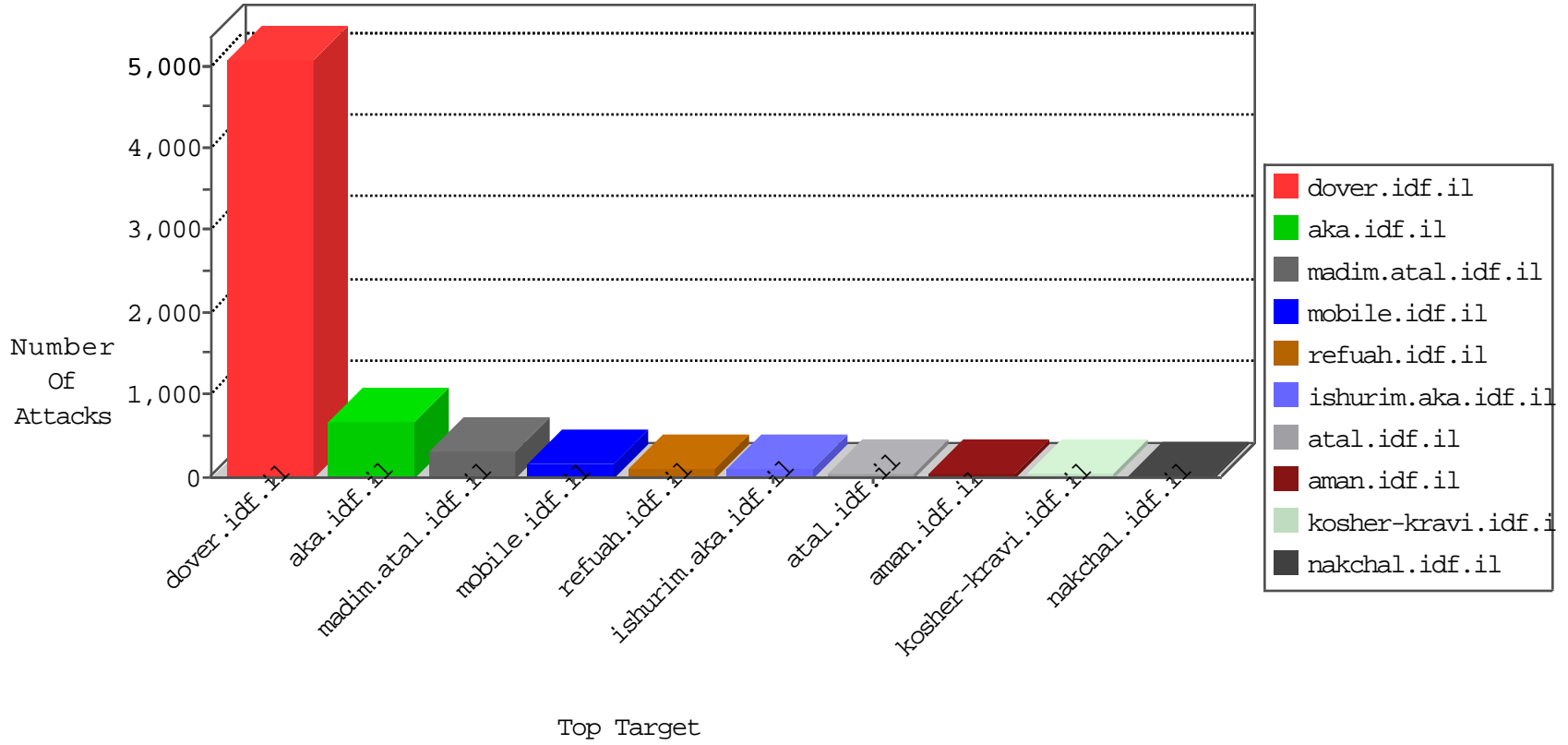


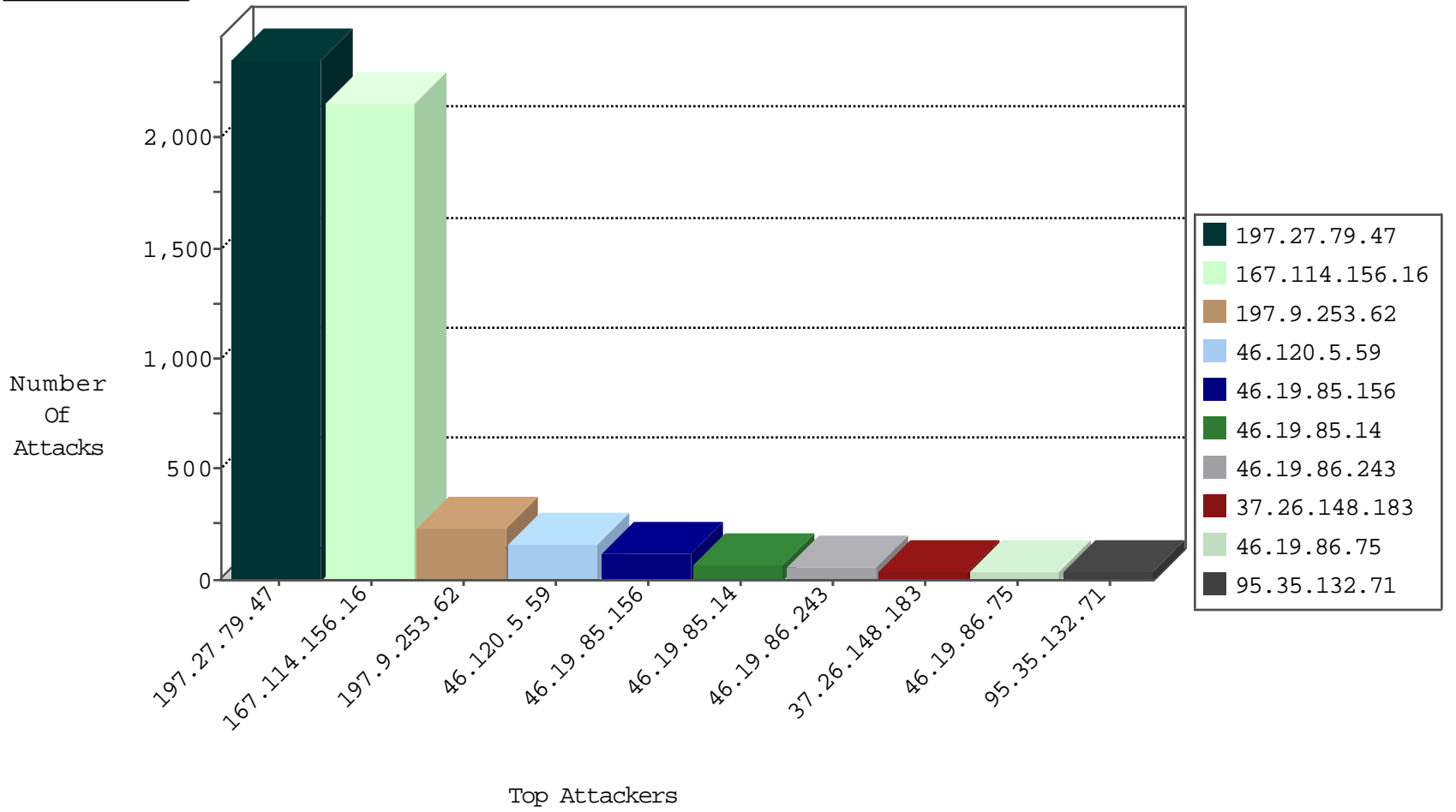
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.27.79.47	Tunisia	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	12143
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3140
0.0.0.0		147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1026
197.27.79.47	Tunisia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	469
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	149
197.9.253.62	Tunisia	147.237.77.216	dover.idf.il	HTTP-MISC-WebLogic-Str-BO	dest-reset	93
197.27.79.47	Tunisia	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	24
197.27.79.47	Tunisia	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	23
2.54.32.229	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
85.64.86.208	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
37.26.146.231	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
173.252.90.230	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
40.77.167.8	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.106.120.54		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
41.41.74.22	Egypt	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
41.41.74.22	Egypt	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
192.116.218.146	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
41.41.74.22	Egypt	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
41.41.74.22	Egypt	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.9.253.62	Tunisia	147.237.77.216	dover.idf.il	C1000203: HTTP: Thorshammer - Post to root dir	Block	105
79.177.191.17	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
84.108.139.66	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
197.27.79.47	147.237.77.216	Tunisia	dover.idf.il	portscan: TCP Distributed Portscan	1
94.159.152.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.77.176	Sweden	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.34	China	ychalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.229.184.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
80.246.133.146	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
162.222.185.165	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
79.177.109.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.36	147.237.76.196		e.sviva.idf.il	ET SCAN Potential SSH Scan	1
217.132.126.39	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.162.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.76.201	Cote D'Ivoire	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
94.102.48.195	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
194.8.88.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.167.155	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.65.71.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
84.111.225.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
79.181.27.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
5.29.200.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.36	147.237.77.233		atal.idf.il	ET SCAN Potential SSH Scan	1
109.64.184.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.27.79.47	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	939
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	163
46.19.86.243	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55
46.120.5.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	46
46.120.5.59	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	42
46.19.86.75	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	39
95.35.132.71	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
197.27.79.47	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
185.32.179.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
80.178.134.53	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
212.179.220.37	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
46.120.5.59	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	26
176.13.7.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.126	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.120.5.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
46.120.5.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
79.181.21.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.108.15.130	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
31.168.239.154	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	14
37.26.148.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	12
79.183.60.67	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
213.57.247.100	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.205.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	11
2.54.20.213	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
185.120.126.111		147.237.72.166	aka.idf.il	drop	SAM rule	drop	10
46.120.5.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
191.38.38.229	Brazil	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
176.13.1.236	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.52.53.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.120.71.126	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
213.57.137.128	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
2.52.144.29	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
66.249.66.145	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
84.108.181.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
176.13.1.236	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
94.230.86.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.148.183	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
85.130.238.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.178.59.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.81.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.221.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.133.146	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.144.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.161.246.51	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
46.19.85.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
46.19.85.156	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.156	Block	29
185.32.179.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
176.13.14.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
197.9.253.62	Tunisia	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 197.9.253.62	Block	20
84.229.158.235	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	16
176.13.7.74	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
157.55.39.98	United States	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.98	Block	8
185.32.179.217	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.56.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
41.238.106.134	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.238.106.134	Block	4
2.52.23.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
185.32.179.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.174.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.166.122.247	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/'	Block	3
176.13.13.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.4.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.42.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.6.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
98.218.127.89	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.2.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.205.250	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.181.4.195	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
2.54.135.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
171.25.193.132	Sweden	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/faq.aspx	Block	2
197.9.253.62	Tunisia	147.237.77.216	dover.idf.il	Multiple Malformed URL from 197.9.253.62	Block	2
37.26.148.137	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
46.19.86.44	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
197.9.253.62	Tunisia	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 197.9.253.62	Block	2
109.253.142.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.14	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.151.52	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
5.102.246.116	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	2
2.54.45.132	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.94.41.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.133.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.197.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.78.62.97	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
37.26.147.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.230.24.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.92.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
93.173.60.21	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
208.84.202.19	Saint Vincent and the Grenadines	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/	Block	1