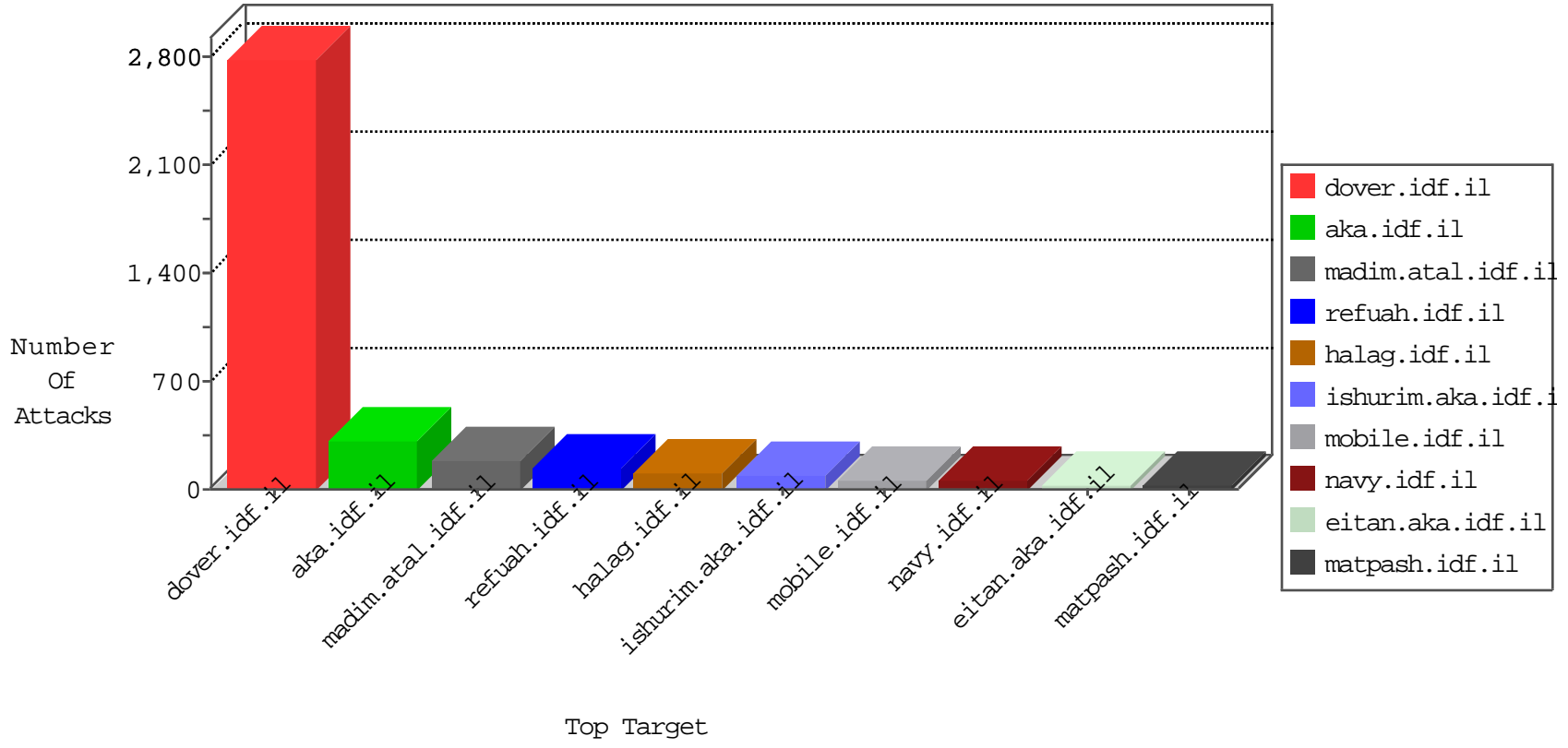


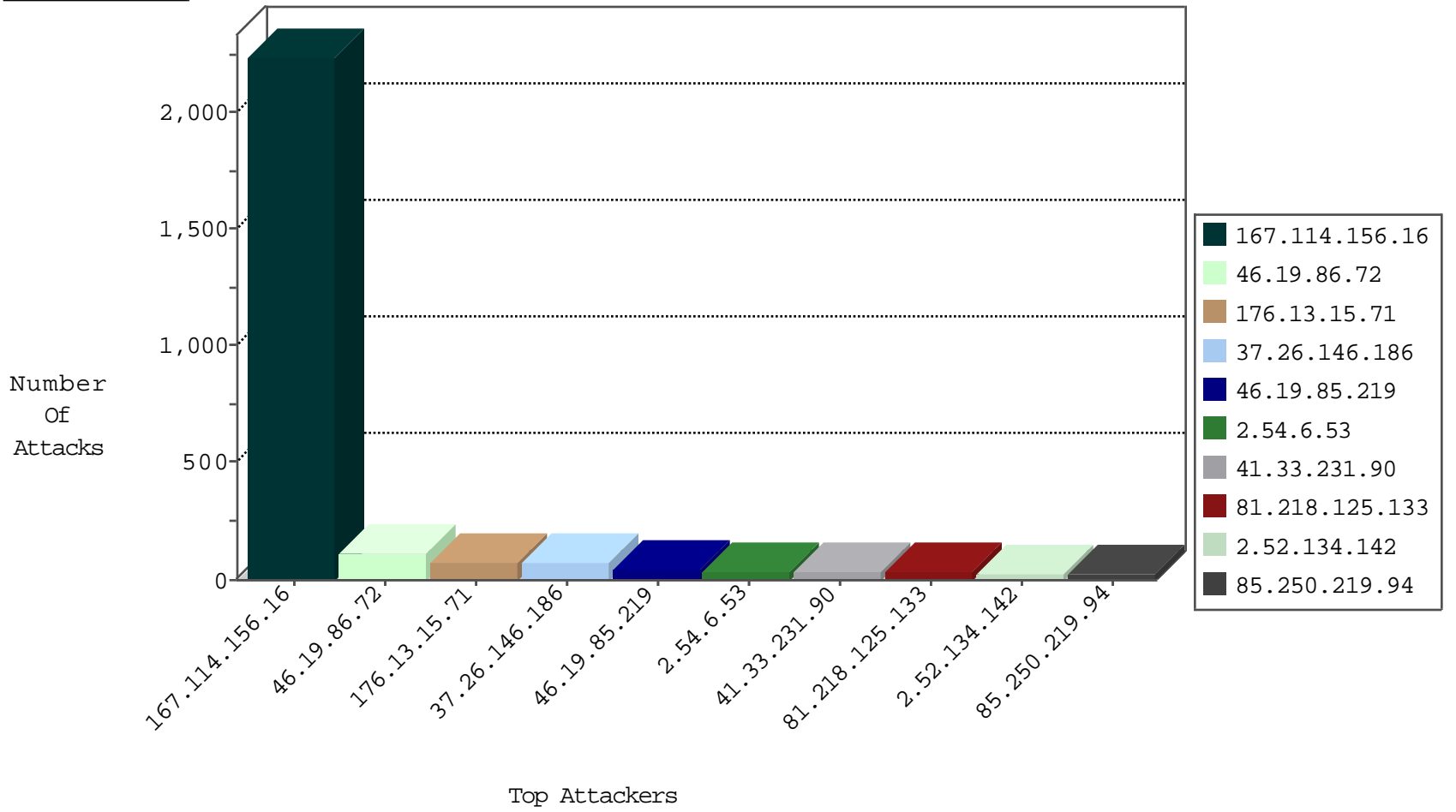
IDF Under Attack Daily Report



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	3268
80.82.78.8	Netherlands	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
134.147.203.115	Germany	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	2
89.248.172.110	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
37.26.149.212	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	1
89.248.172.110	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.110	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
52.53.222.9	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
71.6.158.166	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.110	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.148.233	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
198.27.82.153	Canada	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	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	1
46.19.85.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.136.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.77.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.17.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
58.218.213.44	147.237.77.216	China	dover.idf.il	SQL Injection - Select From	1
58.218.213.44	147.237.77.216	China	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	1
58.218.213.44	147.237.77.216	China	dover.idf.il	ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt	1
212.25.83.133	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.194.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.3.146.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
36.45.199.14	147.237.8.46	China	e.chimuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
149.88.71.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.225.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.25.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.213.44	147.237.77.216	China	dover.idf.il	SQL generic sql with comments injection attempt - GET parameter	1
58.218.213.44	147.237.77.216	China	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	1
58.218.213.44	147.237.77.216	China	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	1
212.25.84.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.192.77	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
37.26.146.186	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	73
46.19.86.72	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	47
46.19.86.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
81.218.125.133	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
85.250.219.94	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
79.176.145.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.86.72	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
2.52.134.142	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
37.26.146.174	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
80.179.9.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.114	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
162.243.220.220	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.228.75.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.108.27.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.249	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.166	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
46.19.85.229	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
212.235.22.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.87.48.181	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
2.54.8.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.178.150.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.96	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.228.128.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.149.212	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
79.179.27.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
46.19.86.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
162.243.3.70	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
81.218.162.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
176.13.17.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.129.246	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.219	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.138.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.27.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.86.63	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.163.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.219	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.180.12.88	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.116.239.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.15.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
2.54.6.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
2.52.167.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
2.54.156.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
176.13.17.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
79.176.103.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	3
46.116.132.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.20.208	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/7/	Block	3
37.26.149.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.226.32.70	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/7/	Block	3
2.54.8.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.167.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.186.95.68	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
176.13.3.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
162.243.3.70	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.243.3.70	Block	2
79.178.20.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2
46.116.35.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.177.57.242	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
45.55.211.95		147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /	Block	1
37.26.149.188	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
85.250.136.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/x'x'x*xj	Block	1
2.54.85.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.140.145	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
109.186.102.229	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.35.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.143.85.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.116.149.197	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
37.60.46.153	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
93.173.42.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
58.218.213.44	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/news/html/	Block	1
176.13.4.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.168.213.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
46.19.86.20	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
149.88.136.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.67	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
46.19.85.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
85.250.219.94	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1