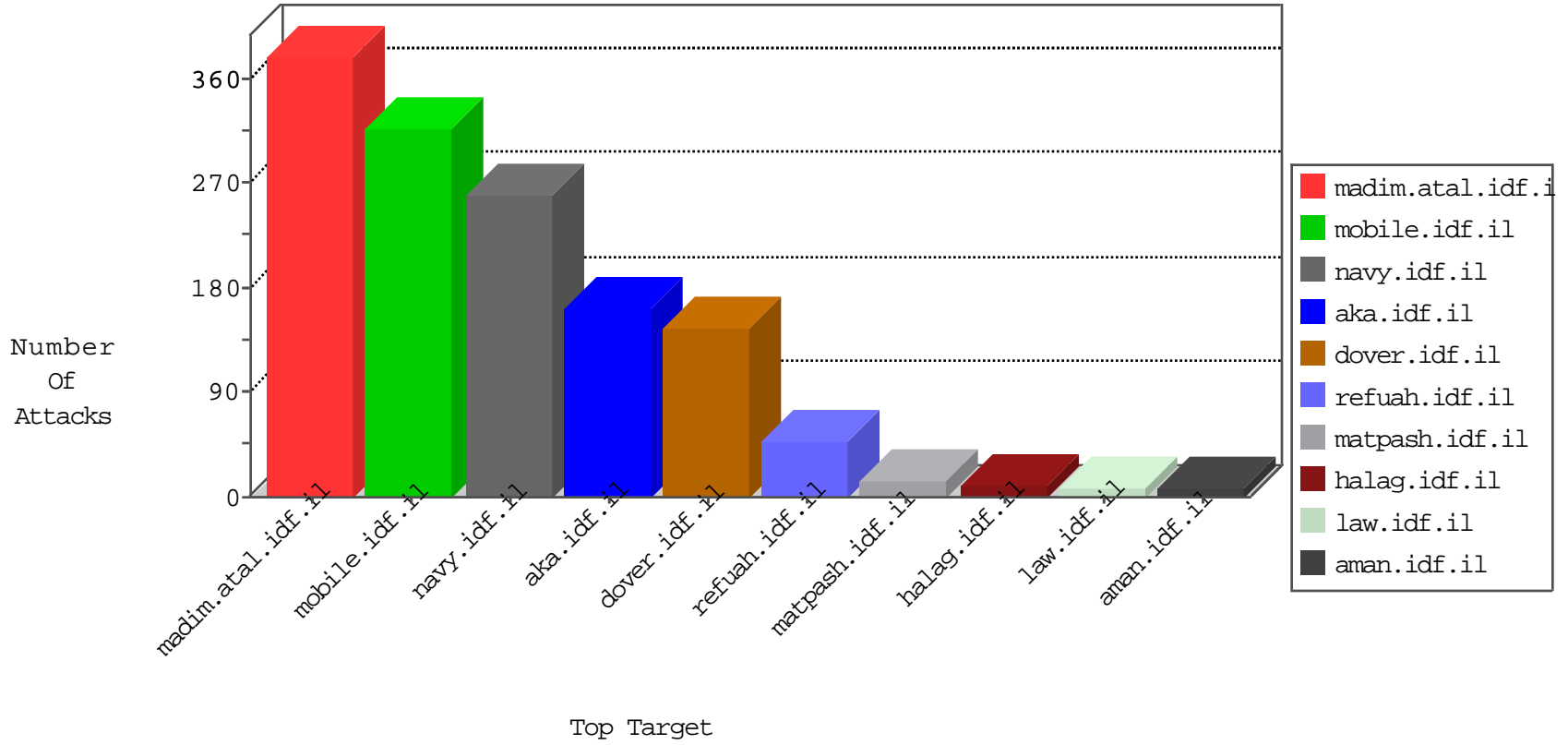


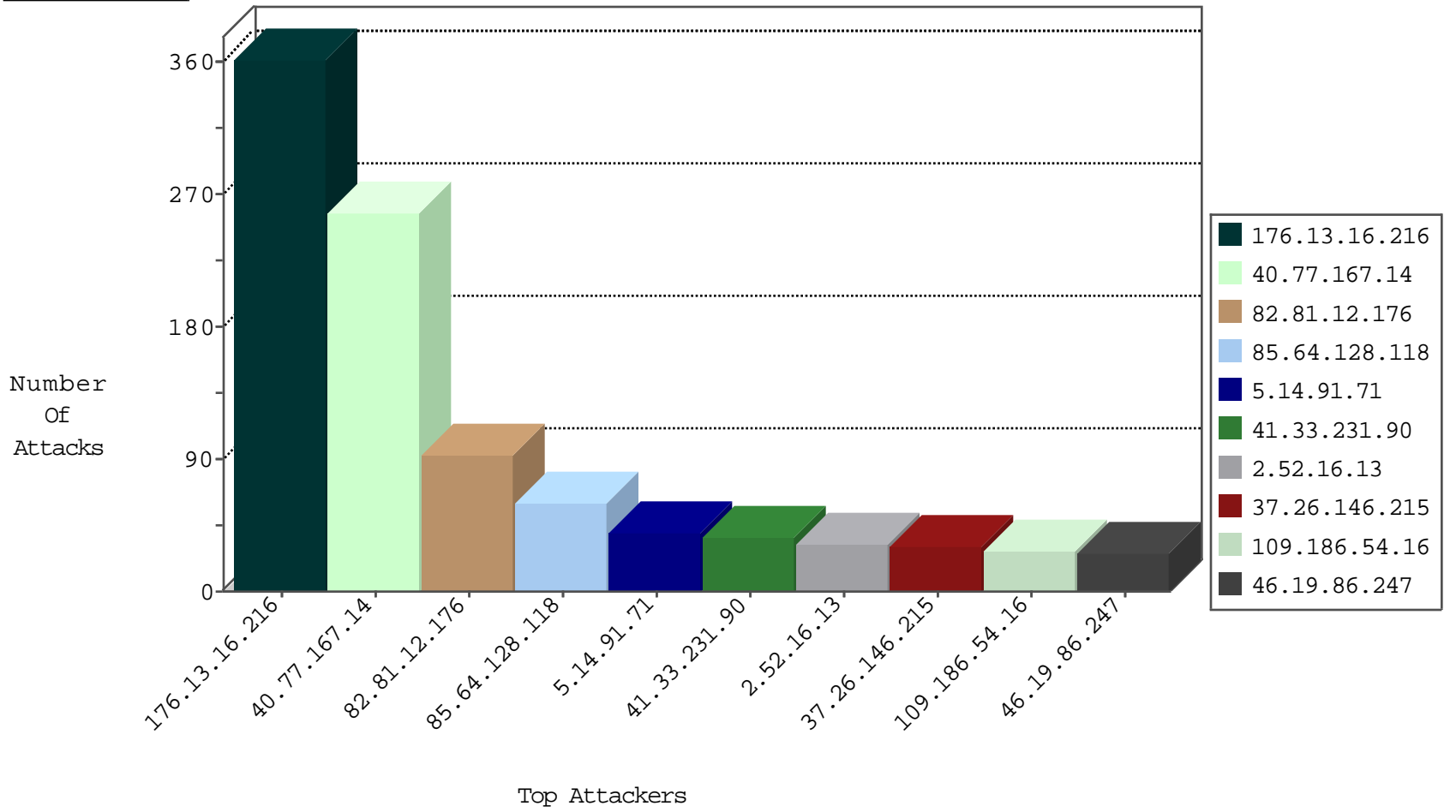
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	92
82.145.219.101	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	11
79.177.197.49	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
162.248.100.195	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
162.248.100.195	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
76.76.200.45	Puerto Rico	147.237.77.233	atal.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	3
52.26.202.58	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.84	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
114.112.90.54	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
54.179.135.126	147.237.72.14	Singapore	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
125.208.25.216	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.208.25.216	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
114.112.90.54	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.49.79	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
54.179.135.126	147.237.72.14	Singapore	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
45.55.236.147	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
193.201.227.71	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
125.208.25.216	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
40.77.167.14	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	258
85.64.128.118	Israel	147.237.77.243	mobile.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
5.14.91.71	Romania	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	32
2.52.16.13	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.26.146.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
109.186.54.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
2.52.181.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.181.21.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
85.250.28.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.129.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.65.18	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
185.120.126.12		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.14.91.71	Romania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
45.79.168.168		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
176.13.19.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.209.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.193.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.108.193.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.108.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.84.120	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
81.218.106.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
94.230.86.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.214.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.210.186.234	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
85.130.214.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
199.30.25.38	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.130.214.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.22.131.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.64.108.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.38.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.96.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
191.232.136.76	United States	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.42.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
208.52.154.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
78.229.100.85	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
108.30.243.88	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.180.2.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.4.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-31-2016-01:04:01 to 01-31-2016-02:04:01

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
87.231.124.73	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.16.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	181
176.13.16.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	179
85.64.128.118	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
2.52.16.13	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
37.26.146.215	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
109.186.54.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
2.52.181.191	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
79.181.21.21	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.247	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
109.253.216.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.101.220	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
46.121.194.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.97.216	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	2
46.19.86.1	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.16.216	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ***** ***** *****, Observed ***** ***** *****	None	2
37.142.209.148	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
185.120.126.12		147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.254.183.189	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
2.54.129.39	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.120.18.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.97.216	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
85.250.28.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.254.183.189	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.254.183.189	Block	1
94.159.210.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.94.85.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
72.167.190.172	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
50.62.208.40	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
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	1
85.250.28.2	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.178.191.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.216.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1
94.199.151.22	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
46.19.86.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.45.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.52.154.243	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /phpmyadmin2/scripts/setup.php	Block	1
84.108.101.220	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
77.125.84.120	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 77.125.84.120	Block	1
66.249.65.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
85.250.28.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.167.9	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
191.232.136.132	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
151.252.97.244	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.254.183.189	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
99.41.173.29	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
77.125.84.120	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/size338x0/1564.jpg	Block	1