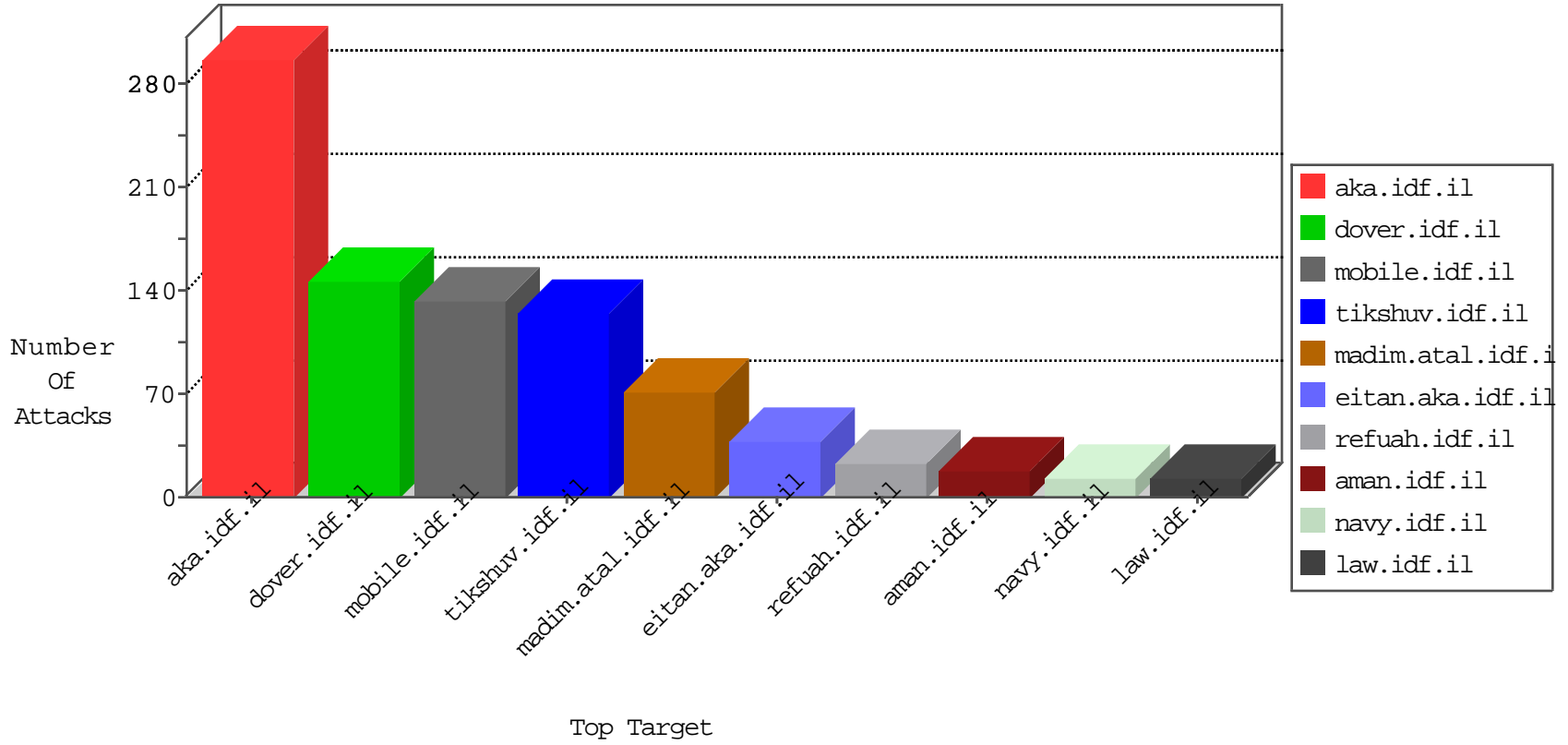


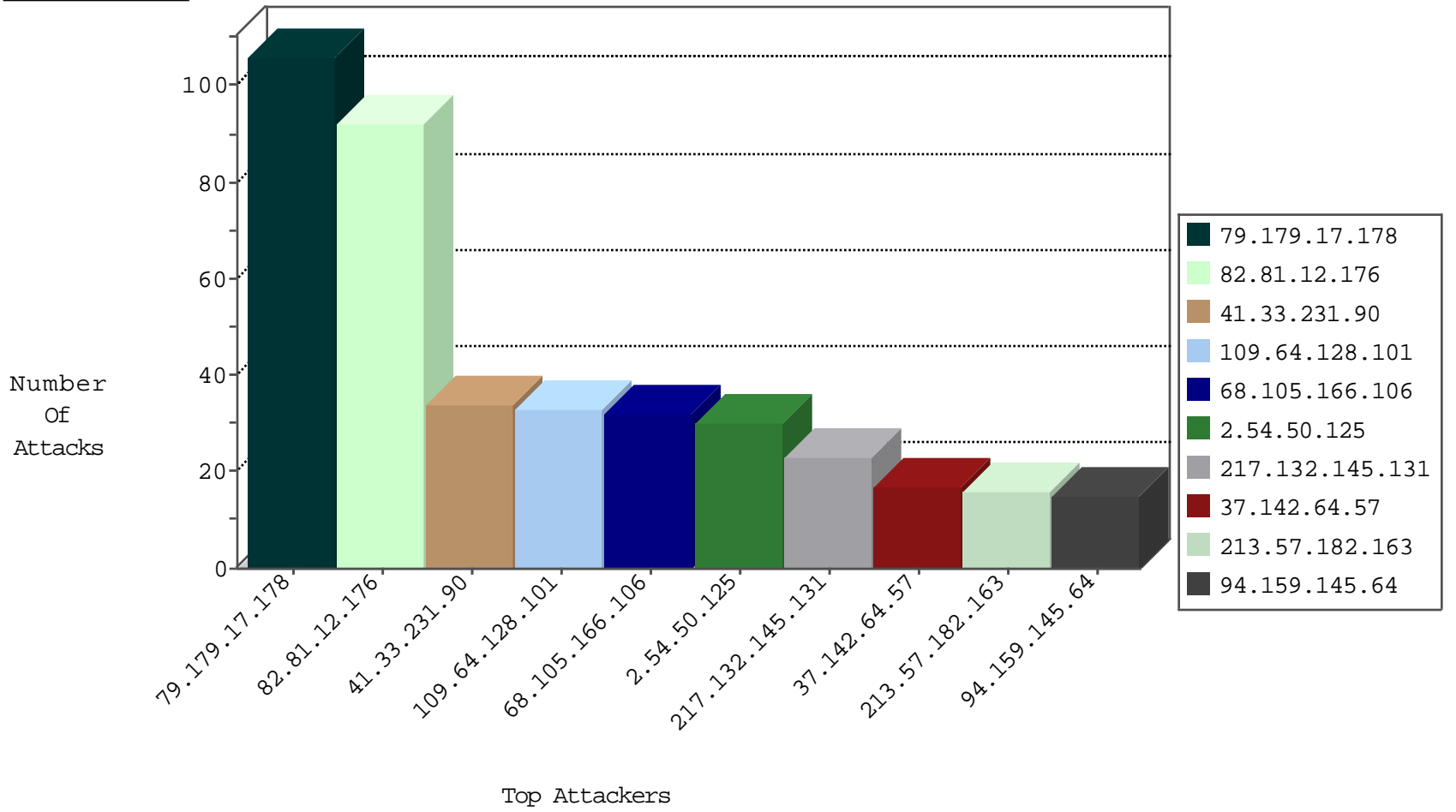
# IDF Under Attack Daily Report



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
185.56.28.67	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
198.56.164.154	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
198.56.164.154	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
198.56.164.154	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
198.56.164.154	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
198.56.164.154	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
115.239.228.10	China	147.237.0.17	m.ny-kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1
198.56.164.154	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.9.205	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2
188.165.15.87	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
66.176.172.168	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
79.181.9.205	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
79.181.9.205	Israel	147.237.76.86	navy.idf.il	C008: HTTP: Xenu UserAgent	Block	1

## Top Attackers In IDF

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
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
201.164.246.190	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.7	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
175.6.228.149	147.237.0.35	China	akaws.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
125.89.70.205	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.168.218	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential SSH Scan	1
46.148.18.162	147.237.77.243	Lithuania	mobile.idf.il	ET SCAN Potential SSH Scan	1
89.248.168.218	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
41.140.253.9	147.237.0.19	Morocco	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
89.248.168.218	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
89.248.168.218	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
212.199.57.193	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
188.0.236.123	147.237.8.28	Moldova, Republic of	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.237	147.237.0.33		idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
116.115.56.212	147.237.76.44	China	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
89.248.168.218	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
41.140.253.9	147.237.0.19	Morocco	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
89.248.168.218	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
41.140.253.9	147.237.0.19	Morocco	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
89.248.168.218	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
68.105.166.106	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
217.132.145.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
94.159.145.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.67.69.245	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.183.127.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.10.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.166.102.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.166.244.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	8
31.210.187.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.150.252.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.166.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.12	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
109.65.18.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.144.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.250	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.234.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.142.195.167	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
92.40.249.59	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
91.200.12.106	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	4
84.111.0.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
94.159.147.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.111.0.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.120.249.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.106	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
31.210.188.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.45.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.165.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.150.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.111.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.2.0	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.139.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.58.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.62.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-29-2016-17:04:00 to 01-29-2016-18:04:00

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.74.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.6.32	Israel	147.237.77.243	mobile.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
79.179.17.178	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	106
109.64.128.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
2.54.50.125	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.50.125	Block	23
37.142.64.57	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.64.57	Block	14
217.132.145.131	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
2.54.50.125	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1557	Block	4
46.19.86.84	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	4
185.32.179.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.241.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.121.27.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.50.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.166.244.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.65.104.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.150.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.10.160	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
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
46.19.86.36	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
149.88.151.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.182.0.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.6.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.150.70	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
31.154.94.10	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
109.253.144.254	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
5.29.128.19	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.94.45.169	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
46.19.86.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.150.70	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	1
31.154.94.10	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
149.78.163.225	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
5.29.128.19	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
109.66.172.96	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
79.179.9.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.102.9.101	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	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
89.138.72.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
40.77.167.73	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
157.55.39.123	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
79.183.150.70	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.183.150.70	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	1
31.154.94.10	Israel	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	1
116.75.156.74	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.78.199	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
5.29.128.19	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 5.29.128.19	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
2.54.18.169	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$TochenPlaceHolder\$ct138\$ct101\$ct103\$cb1Question\$1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
84.108.60.100	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatgauntity.aspx	Block	1