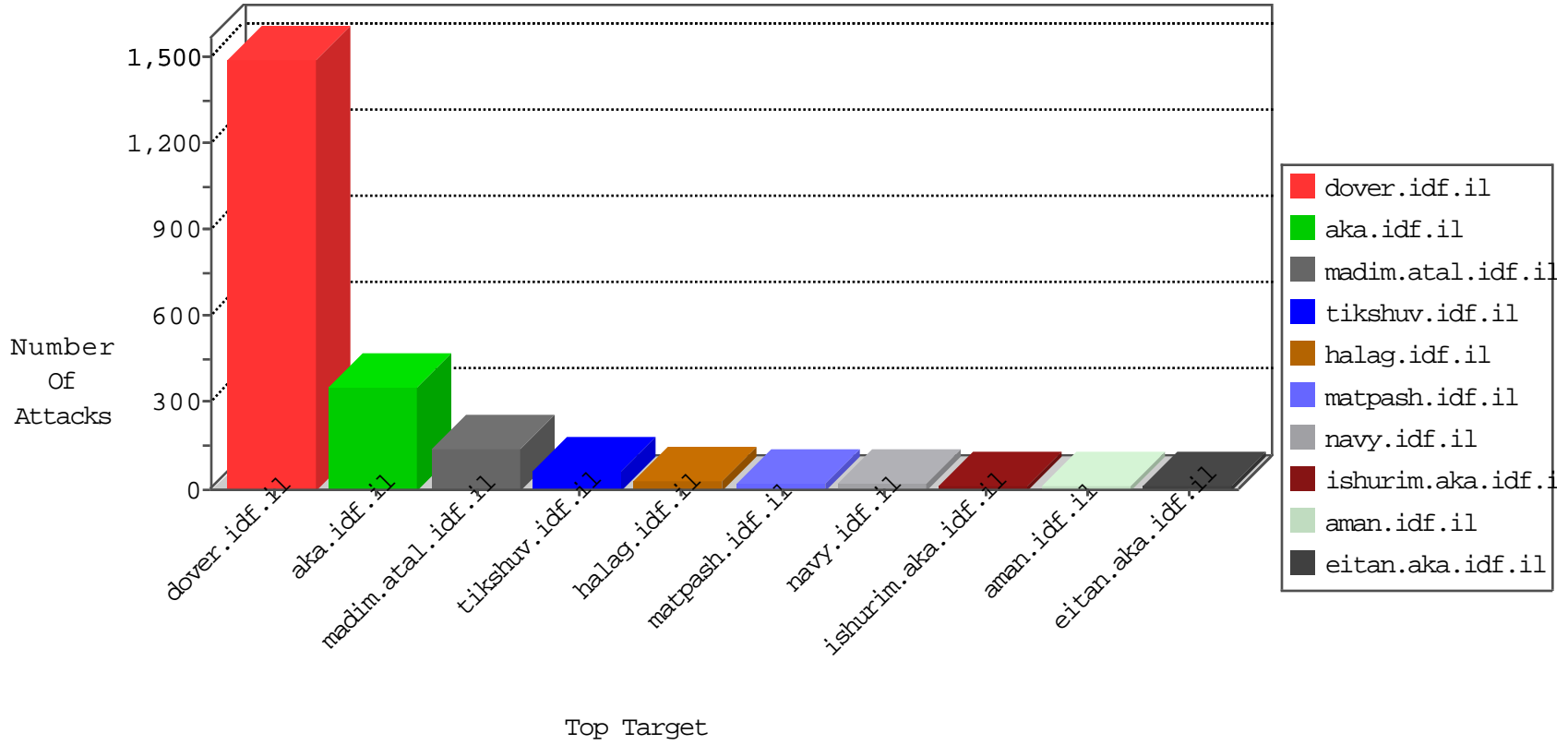


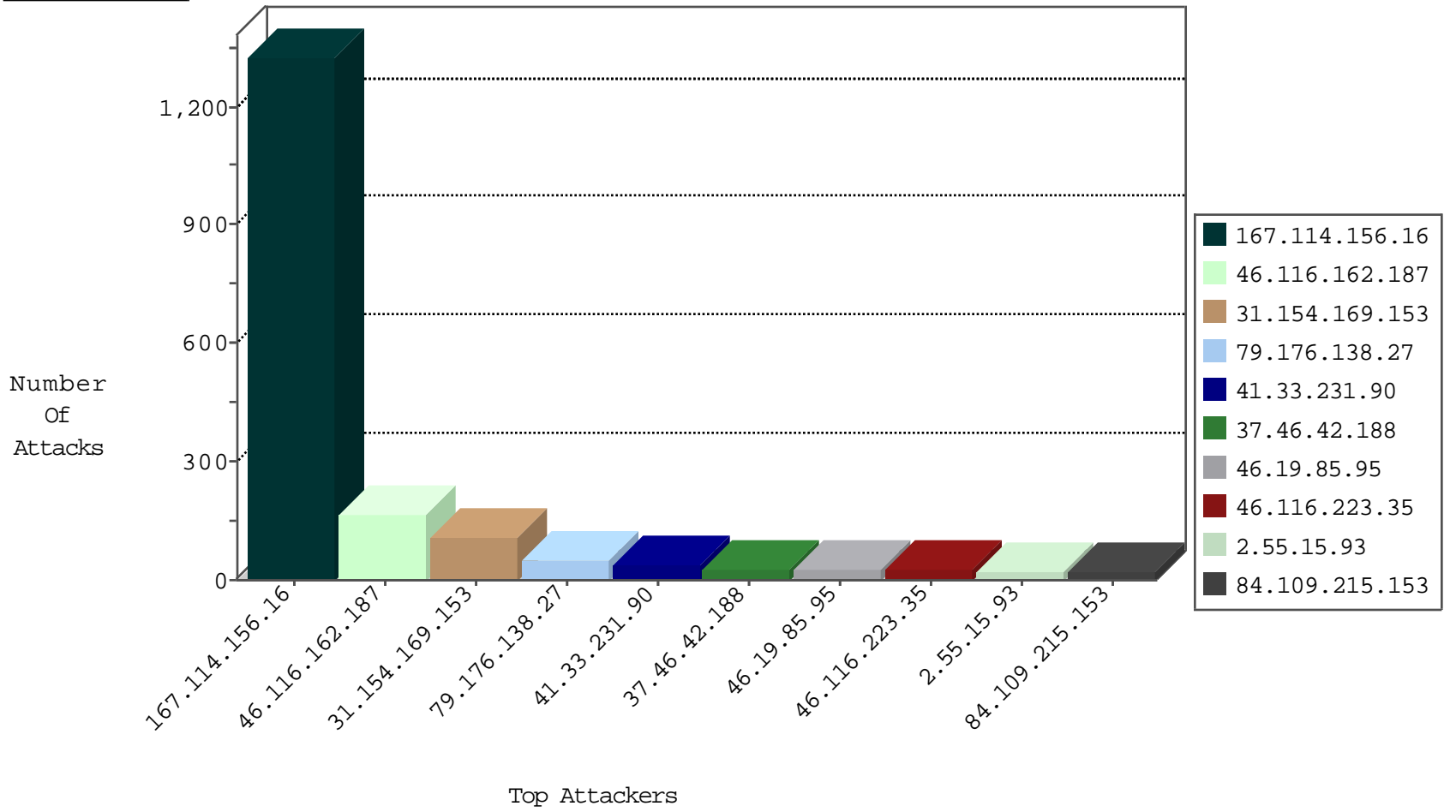
# IDF Under Attack Daily Report



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	Block_Ip_Web_In	drop	1314
109.65.71.4	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
80.82.78.38	Netherlands	147.237.76.42	refuah.idf.il	block-sp-trafl	forward	2
66.240.236.119	United States	147.237.76.196	e.sviva.idf.i	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.254.26	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
158.69.200.203	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
5.28.169.13	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
207.241.237.222	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
158.69.200.203	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
158.69.200.203	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
79.176.138.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.206	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
158.69.200.203	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.165.229.190	France	147.237.77.176	matpash.idf.il	C1000016: HTTP: administrator in URI	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.46.42.188	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
82.166.247.138	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
76.181.249.213	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.100.128	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.100.128	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
180.97.106.162	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.8.27	China	e.medim.atal.idf.il	ET SCAN Potential SSH Scan	1
113.199.28.253	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
88.204.187.90	147.237.0.35	Kazakstan	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
80.82.78.38	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.100.128	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.100.128	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -f -sS	1
180.97.106.162	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
115.29.138.97	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.113.132	147.237.77.216	Japan	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.116.162.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	57
46.116.162.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	50
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.116.162.187	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
46.116.162.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	14
79.176.138.27	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
79.176.138.27	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	13
2.53.128.71	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.116.223.35	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	12
46.116.223.35	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
73.38.58.206	United States	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.253.157.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.116.162.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
79.176.138.27	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
79.176.138.27	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
79.178.58.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.28.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.180.196.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.176.138.27	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
123.126.113.101	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
185.3.147.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.71.4	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.108.65.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.47	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.116.162.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.95	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.116.162.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.230.86.161	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.28.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.24.118	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.95	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.23.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.68.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.54.220.79	Greece	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.54.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.224.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.169.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
2.55.15.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
84.109.215.153	Israel	147.237.0.34	tikshuv.idf.il	Automated Vulnerability Scanning V1	Block	18
207.46.13.72	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.53.134.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.218.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.230.86.161	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/916-he/refuah.aspx	Block	2
2.53.182.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.204.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/images/aka-logo.jpg	Block	1
188.165.229.190	France	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
46.120.165.39	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112745.pdf	Block	1
106.186.113.132	Japan	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation pageNum in www.idf.il/1815-he/dover.aspx	Block	1
66.249.64.189	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
217.69.136.204	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ israel defence force site	Block	1
157.55.39.54	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
87.71.136.171	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
188.165.229.190	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
54.163.24.48	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp/catId in www.aka.idf.il/rights/asp/info.asp	None	1
109.64.94.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
68.180.231.46	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
217.132.43.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
157.55.39.83	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/sip_storage/files/5/68625	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
198.71.230.46	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/old/wp-admin/	Block	1
54.210.18.124	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
79.182.142.149	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/headers/tfasim.gif	Block	1
184.168.193.33	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp/wp-admin/	Block	1
46.19.86.133	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.98	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
149.78.154.98	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
80.82.78.38	Netherlands	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.baidu.com/cache/global/img/gs.gif	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/images/miluum.jpg	Block	1
185.27.105.123	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https://www.aman.idf.il/	Block	1
46.116.223.35	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
94.242.222.23	Luxembourg	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.89.120	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/images/inservice.jpg	Block	1