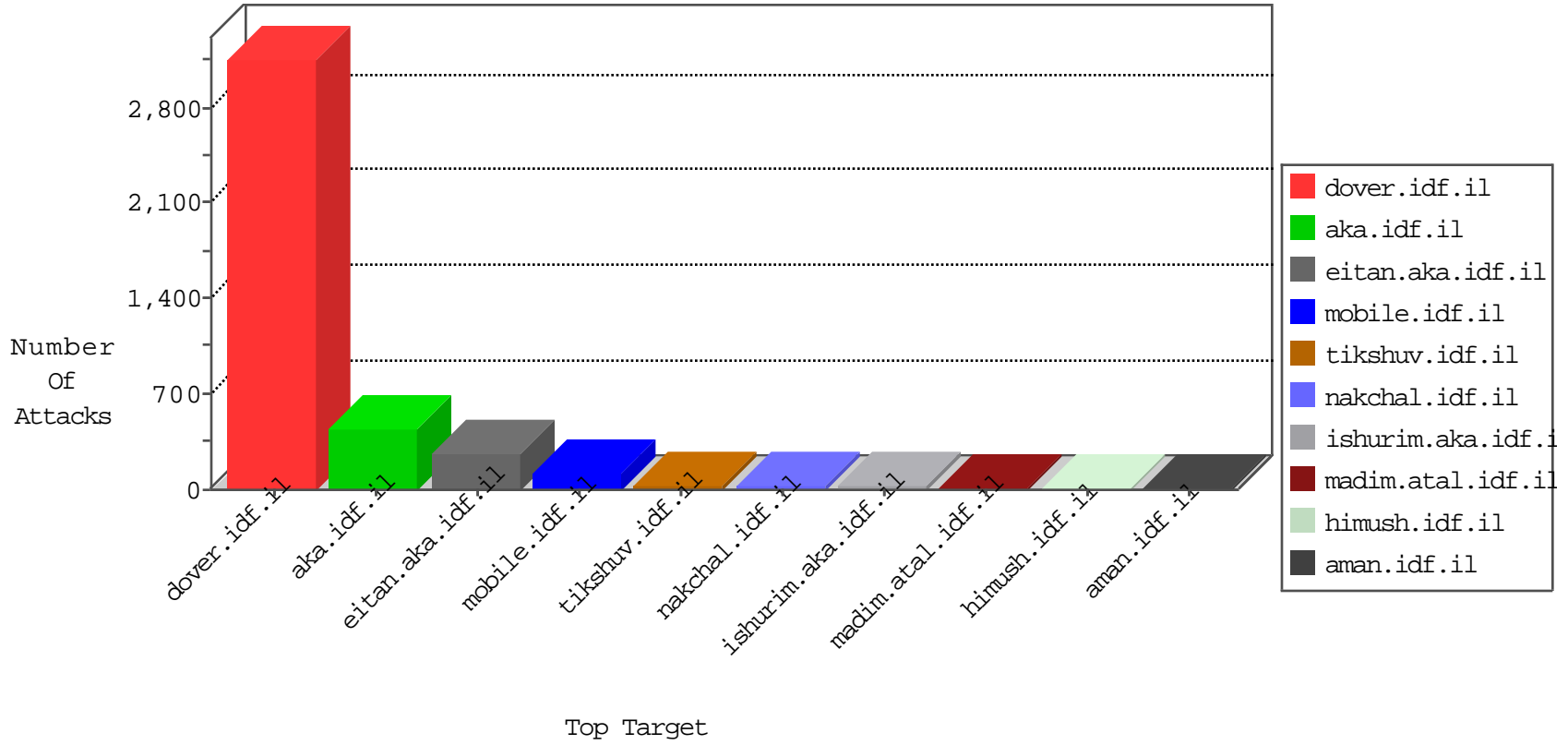


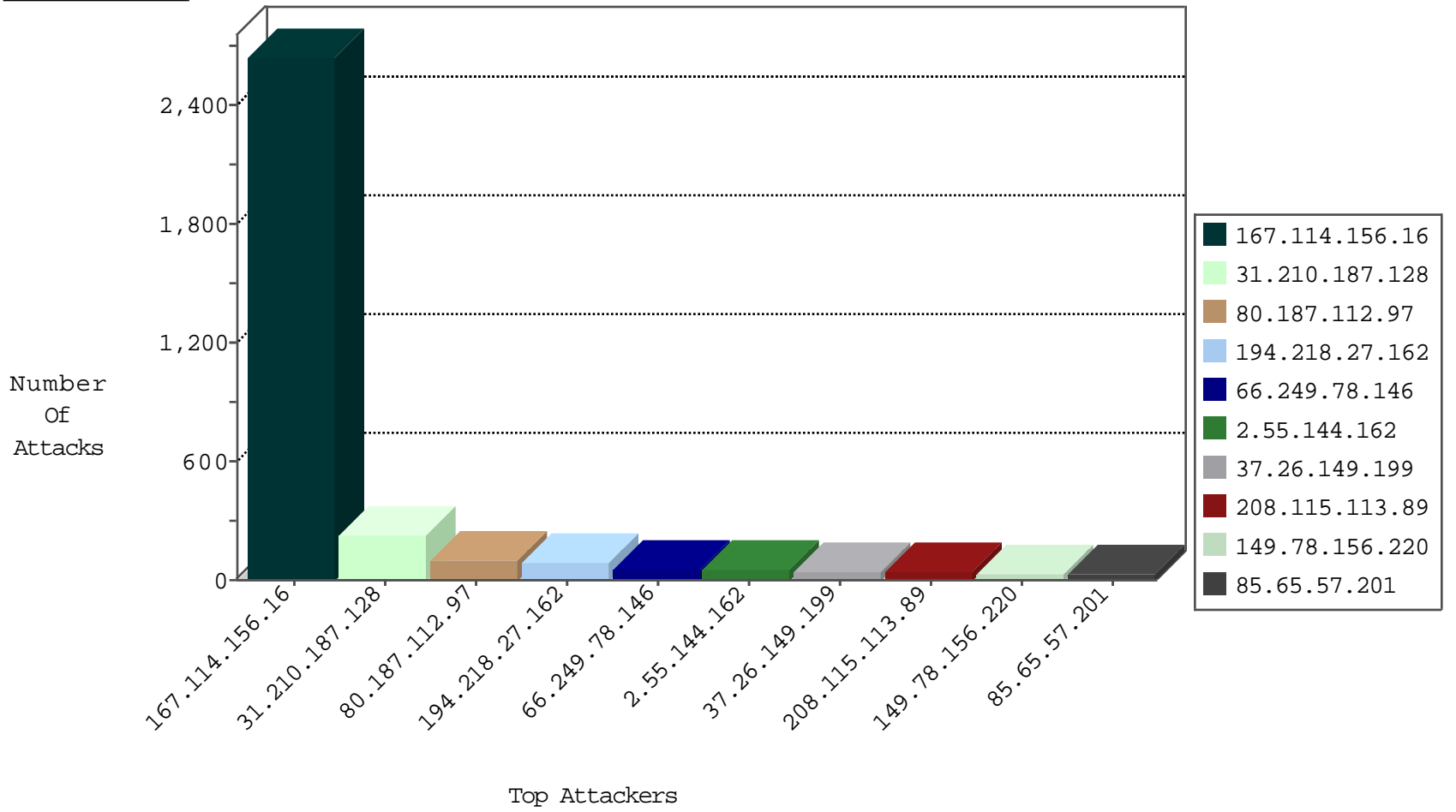
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3050
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3011
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1404
5.28.179.137	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	202
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
109.65.186.133	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1

05-01-2016-23:04:04 to 05-02-2016-00:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
177.12.174.145	Brazil	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.133.79	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
177.12.174.145	147.237.72.166	Brazil	aka.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
189.219.85.44	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
14.168.168.205	147.237.76.30	Vietnam	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.240.250.154	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.84.22	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
13.92.84.22	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
2.53.21.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.198	China	e.yochanan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2039
31.210.187.128	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	222
80.187.112.97	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
2.55.144.162	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	29
85.65.57.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.181.204.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
149.78.156.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.202	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.55.144.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.148.192	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
79.198.121.49	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.55.16.186	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.149.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	14
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.128	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.5.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.71.155.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.147.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.65.88.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.149.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
128.242.249.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.149.199	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
37.26.149.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	8
37.26.148.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.127.159.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.187.112.97	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
95.86.104.151	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.53.35.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.224.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.199.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.64.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.199	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.115	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.154.149.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.162.224.26	United States	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
79.183.193.155	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	12
149.78.156.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
2.55.16.186	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
80.246.136.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.5.194	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
37.26.147.153	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.4.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.183.193.155	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/sip_storage/files/8/	Block	3
46.19.85.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.207.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.182.2.20	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.246.139.130	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
176.13.1.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
46.19.86.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
91.68.168.94	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21905-he/	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
217.69.133.244	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
141.212.122.113	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /x	Block	1
54.244.135.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
79.182.4.113	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
217.69.133.247	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter doc.. in www.aka.idf.il/giyus/forum/	None	1
37.142.64.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.94.84.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
61.189.47.93	China	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.mag.idf.il/templates/getfile/getfile.aspx	Block	1
109.64.56.237	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/general/mobile	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	1
151.80.31.168	France	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
84.111.232.209	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
68.180.229.215	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakchal.idf.il/1073-he/nakhal.aspx	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
185.32.179.6	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.65.241.194	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/109552.pdf)-	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluiml/news/news.asp	Block	1
164.132.161.70	Italy	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
91.68.168.94	France	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/general.aspx	Block	1
213.57.70.130	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
37.26.146.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1