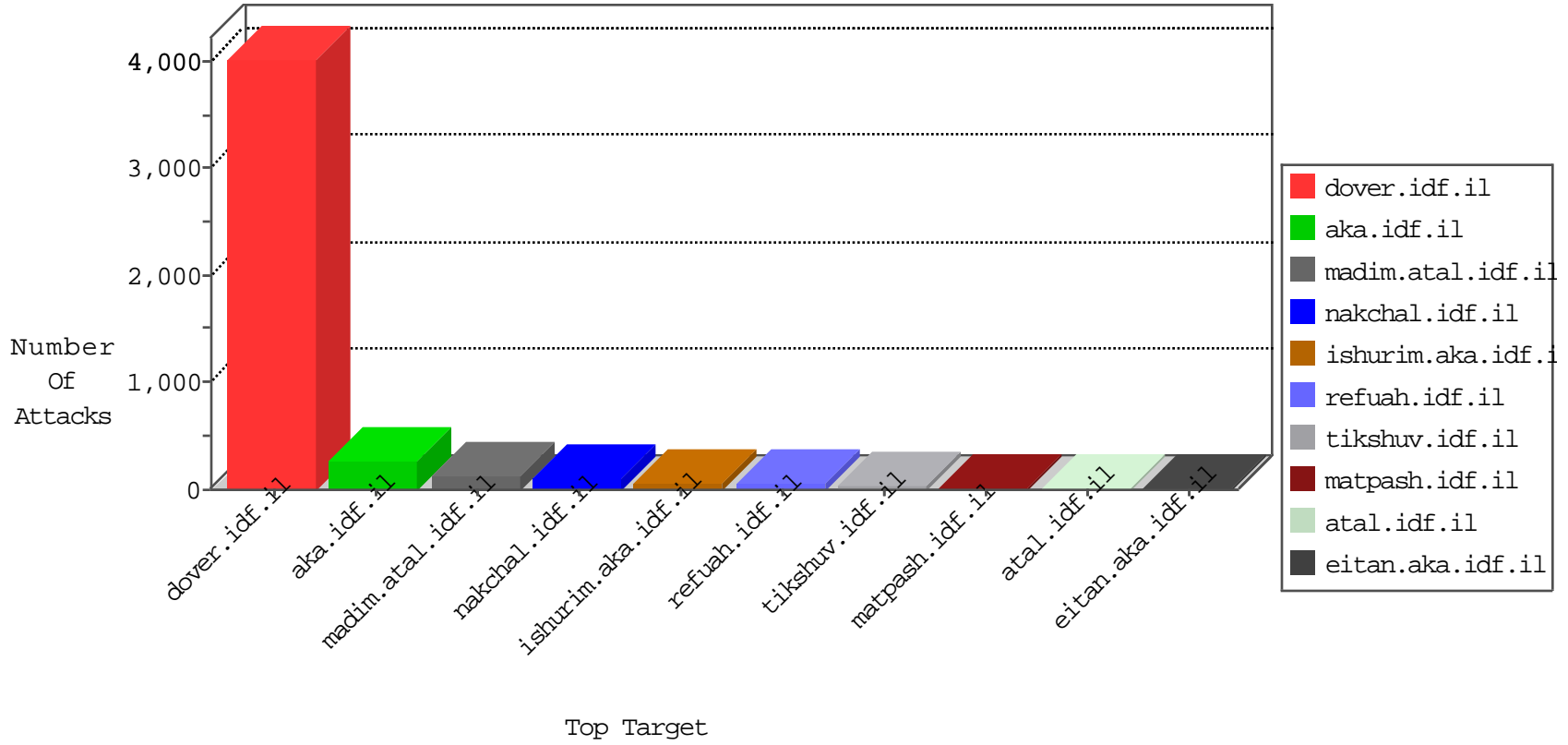


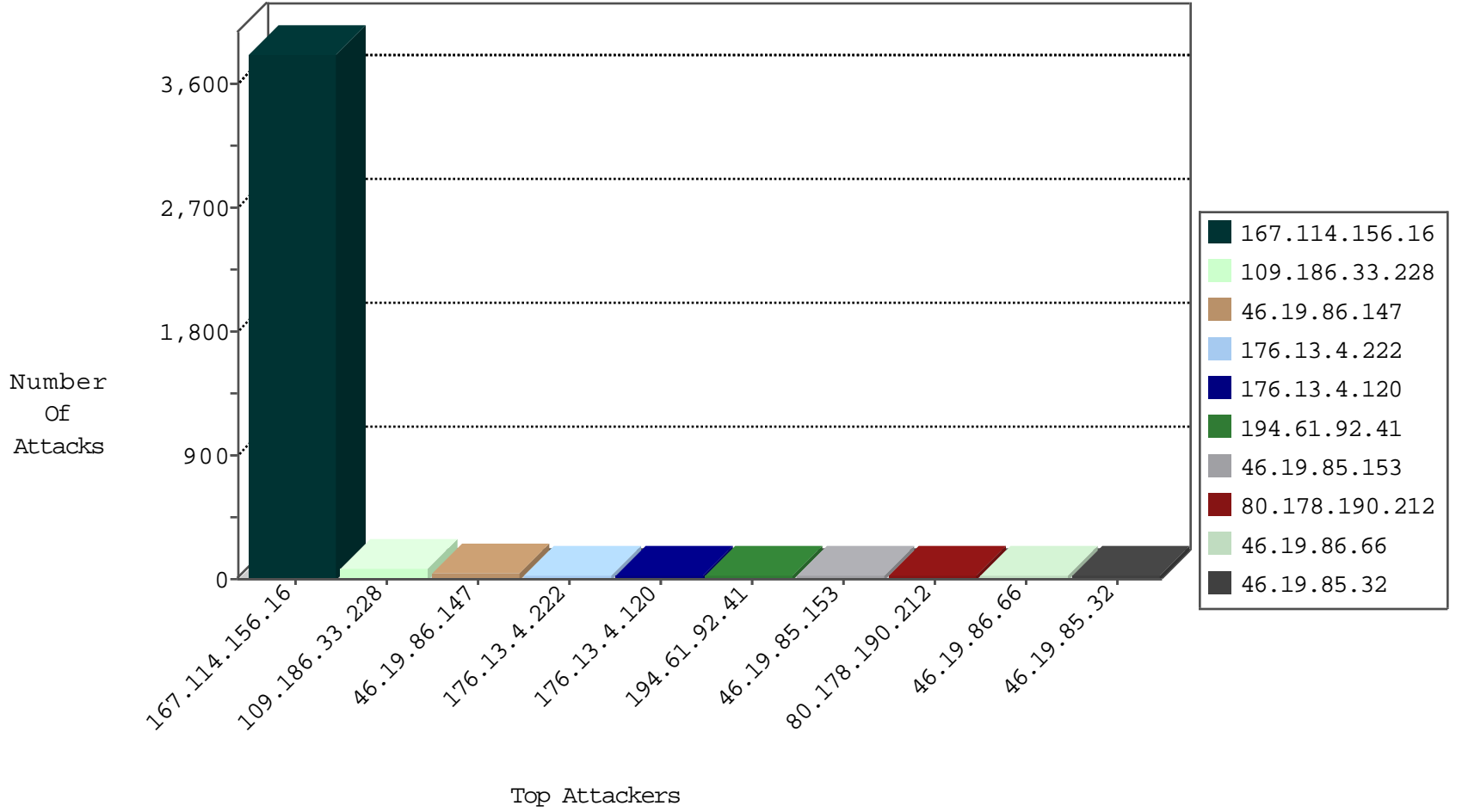
IDF Under Attack Daily Report



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	3816
77.218.243.222	Sweden	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	10
79.178.2.233	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
192.117.143.13	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
149.88.126.230	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
37.26.148.209	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
84.111.103.180	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
2.53.57.22	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
94.102.49.116	Netherlands	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
159.104.163.19	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
188.214.128.28	Lithuania	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
159.104.163.20	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.102.49.116	Netherlands	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
188.214.128.28	Lithuania	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
159.104.163.17	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.102.49.116	Netherlands	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
159.104.163.18	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.105.139.113	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.134	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
87.71.118.222	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.146.182	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
54.84.31.45	United States	147.237.77.216	dover.idf.il	3593: HTTP: SQL Injection (UNION)	Block	1
79.179.196.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
109.186.33.228	147.237.76.31	Israel	nakchal.idf.il	WEB-FRONTPAGE /_vti_bin/ access	2
194.90.25.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.158.255.194	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.252.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
76.181.249.213	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
37.26.149.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
1.39.115.7	147.237.72.166	India	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.136.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.158.255.194	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
86.122.136.30	147.237.77.216	Romania	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
76.181.249.213	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
37.26.149.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.140.144	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
46.19.85.153	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	22
80.178.190.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.87	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.86.77	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
82.166.84.159	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.66	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.86.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.85.86	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
194.61.92.41	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
88.209.84.67	Monaco	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
5.22.130.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.15.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.61.92.41	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
80.246.136.242	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.157	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.138.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.0	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.44	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.107	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.31	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.200.130.62	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.67	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
85.130.246.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.18.108	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.71	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
141.0.13.132	Norway	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
176.13.18.108	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.32	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.221	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
194.61.92.41	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.98	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
86.122.136.30	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.54	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.111.139.65	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.41	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.98	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.112	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
194.61.92.41	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.0	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
31.154.158.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.44	Israel	147.237.72.167	ishurim.aka.idf.i	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
109.186.33.228	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	45
46.19.86.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
176.13.4.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.13.4.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
109.186.33.228	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 109.186.33.228	Block	26
5.9.9.3	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.9.9.3	Block	16
80.246.137.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
80.246.136.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
109.186.33.228	Israel	147.237.76.31	nakchal.idf.il	Multiple signatures from 109.186.33.228	Block	8
80.246.137.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	3
109.253.129.60	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$cpMain\$cpMain\$cpMain\$ct135.x in www.aka.idf.il/main/sachar/payslips.aspx	None	2
82.80.181.180	Israel	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 82.80.181.180	Block	2
37.26.149.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.121.144.142	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyius/general.aspx	Block	2
5.9.9.3	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyius/	Block	2
80.246.138.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.224.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
2.55.33.175	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.235.31.216	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/modiin/default.aspx	Block	1
74.82.47.3	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in URL	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/gyius/general.aspx	Block	1
192.115.25.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
109.253.129.60	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$cpMain\$cpMain\$cpMain\$ct136.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
82.80.181.180	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
79.178.64.185	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.equalheights.js	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	NULL Character in URL	Block	1
41.227.169.108	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
207.46.13.29	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyius/general.aspx	Block	1
109.253.129.60	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$cpMain\$cpMain\$cpMain\$ct153.y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/gyius/general.aspx	Block	1
82.80.242.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
79.183.167.105	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$TochenPlaceHolder\$btnSave in www.aka.idf.il/main/gyius/faq.aspx	None	1
66.249.66.163	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method O'ÁÜB'k*.' in URL	Block	1
46.19.85.115	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
1.39.115.7	India	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyius	Block	1
212.199.112.144	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/gyius/general.aspx	Block	1
31.168.16.116	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
82.81.92.138	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
80.246.133.85	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.167	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
109.186.33.228	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/sip_storage/files/8/	Block	1