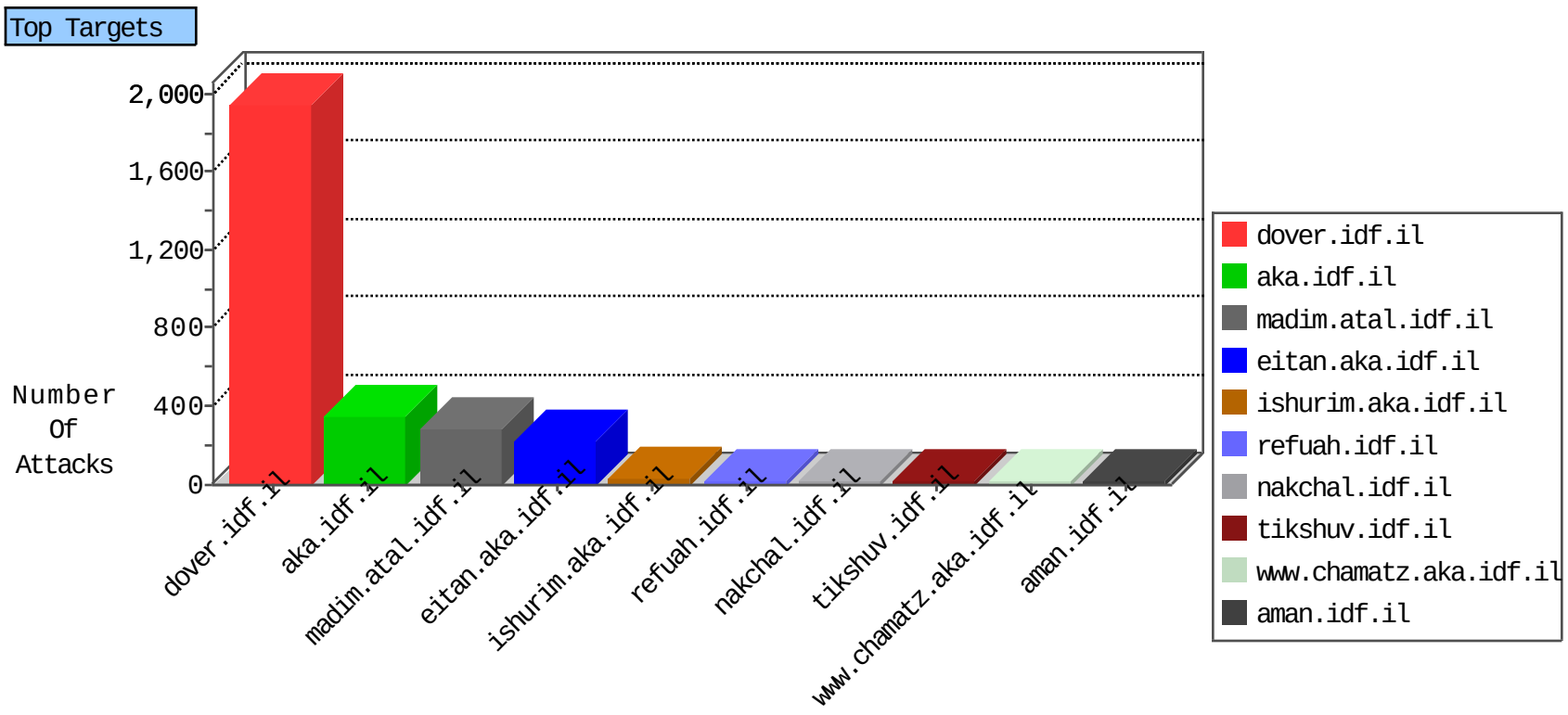
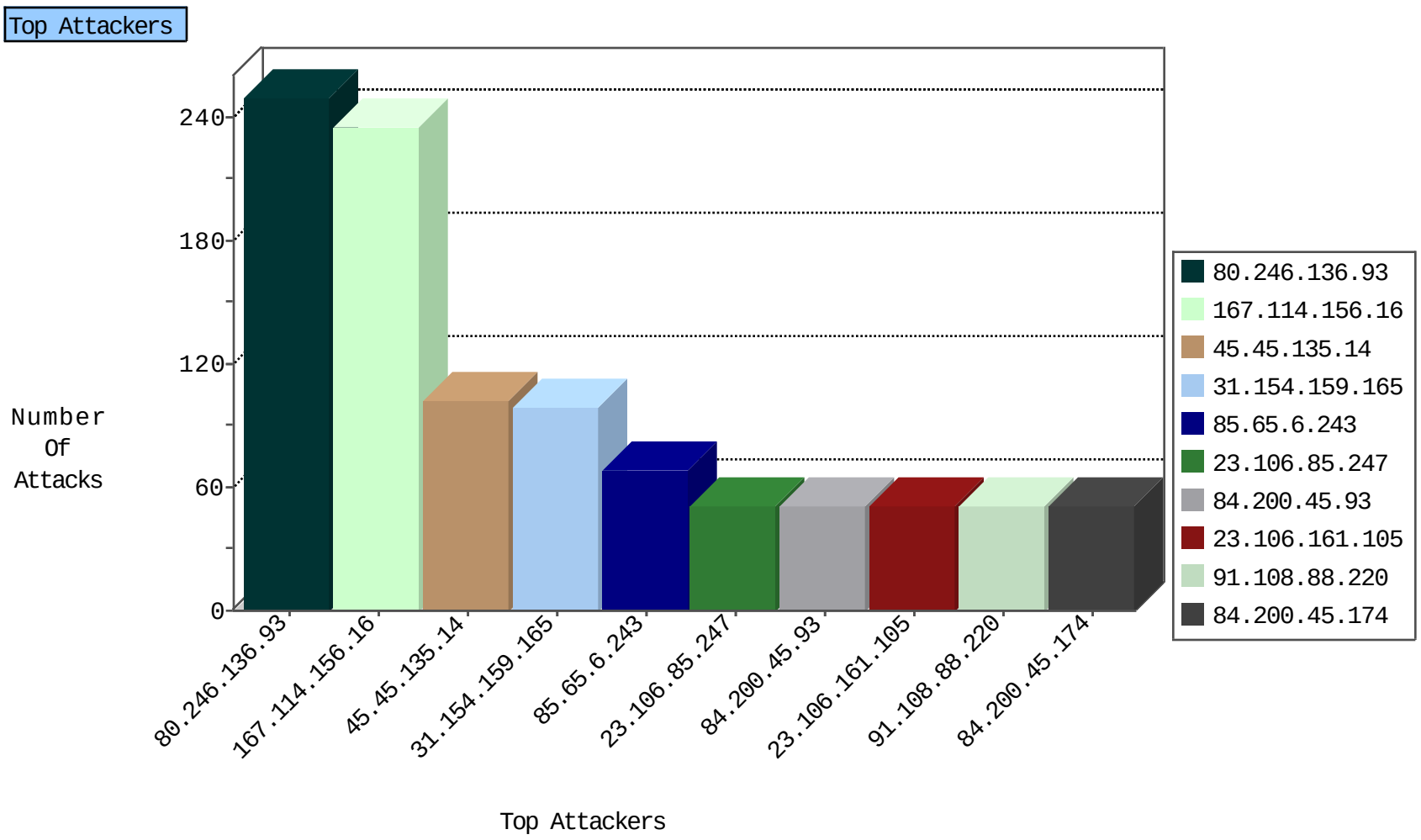
05-04-2016-21:04:05 to 05-04-2016-22:04:05

IDF Under Attack
Daily Report

Top Targets



Top Attackers



05-04-2016-21:04:05 to 05-04-2016-22:04:05

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	HTTP-POST-Segmented-DoS	dest-reset	8721
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1017
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	522
212.143.254.66	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
82.81.10.8	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	2
191.96.249.50	Chile	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
175.141.16.109	Malaysia	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
66.240.236.119	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
201.75.114.166	Brazil	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
176.13.23.72	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
71.6.146.185	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
183.60.48.25	China	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

05-04-2016-21:04:05 to 05-04-2016-22:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-04-2016-21:04:05 to 05-04-2016-22:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.136.93	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
188.214.249.152	147.237.72.166	Romania	aka.idf.il	Xenu Link Sleuth User Agent	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
91.197.232.25	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.25	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
201.166.198.92	147.237.77.176	Mexico	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.111.203.235	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
74.118.239.21	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
177.225.207.141	147.237.76.177	Mexico	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.64.71.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.219.234.3	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
91.197.232.25	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.25	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.25	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
200.153.130.132	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.177.139.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
74.118.239.21	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
177.225.207.141	147.237.76.198	Mexico	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
118.68.248.120	147.237.76.31	Vietnam	nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.219.234.3	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.197.232.25	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN Potential SSH Scan	1

05-04-2016-21:04:05 to 05-04-2016-22:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
45.45.135.14	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
31.154.159.165	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	99
85.65.6.243	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	68
84.200.45.93	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
23.106.166.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
91.108.88.147	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
84.200.45.174	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
91.108.88.220	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
23.106.166.175	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
23.106.85.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
91.108.88.238	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
84.200.45.21	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
23.106.161.105	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
84.200.45.43	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
23.106.161.126	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
91.108.88.146	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
104.251.85.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
23.106.85.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
23.80.147.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
23.80.147.210	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
23.80.148.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
84.228.248.43	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
23.80.148.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
23.80.148.202	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
104.251.90.150	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
23.106.211.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
82.83.70.152	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
73.4.150.47	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
176.58.70.110	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
5.22.129.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
104.251.90.87	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
23.106.211.176	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
176.13.2.20	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
23.81.235.248	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
23.81.248.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
23.81.205.124	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
65.222.205.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
77.124.43.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
23.81.235.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
8.18.120.105	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	242
149.78.245.141	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.78.245.141	Block	17
37.142.64.66	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 37.142.64.66	Block	8
37.142.64.66	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	7
2.53.32.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
5.22.130.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.22.130.235	Block	6
79.182.39.228	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	5
149.88.182.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.216.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.132.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.136.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.21.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.46.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.73.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.35.148	Israel	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/657-en/patzar.aspx	Block	2
79.181.166.223	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
109.253.144.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.21.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.139.253.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.117.35.160	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.117.35.160	Block	1
149.78.245.141	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus	Block	1
94.230.86.105	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
5.22.129.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general	Block	1
79.183.225.158	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
173.71.197.93	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/mo	Block	1
109.253.156.76	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
91.108.88.224	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/kiosk/general.aspx	Block	1
190.7.136.147	Colombia	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/admin/config.php	Block	1
79.177.249.168	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
46.117.35.160	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
108.231.20.133	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/general/mobile	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2977.jpg	Block	1
134.0.11.15	Spain	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
93.103.66.246	Slovenia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
203.127.96.212	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
164.132.161.26	Italy	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/rights/hebrew/html	Block	1
5.29.6.130	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
84.108.87.44	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
185.120.126.33	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile	Block	1
66.249.93.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
37.142.64.66	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
142.54.167.98	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
2.53.35.148	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-7420-he	Block	1
93.173.28.200	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gen204	Block	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.120.210.164	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
31.154.5.181	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1