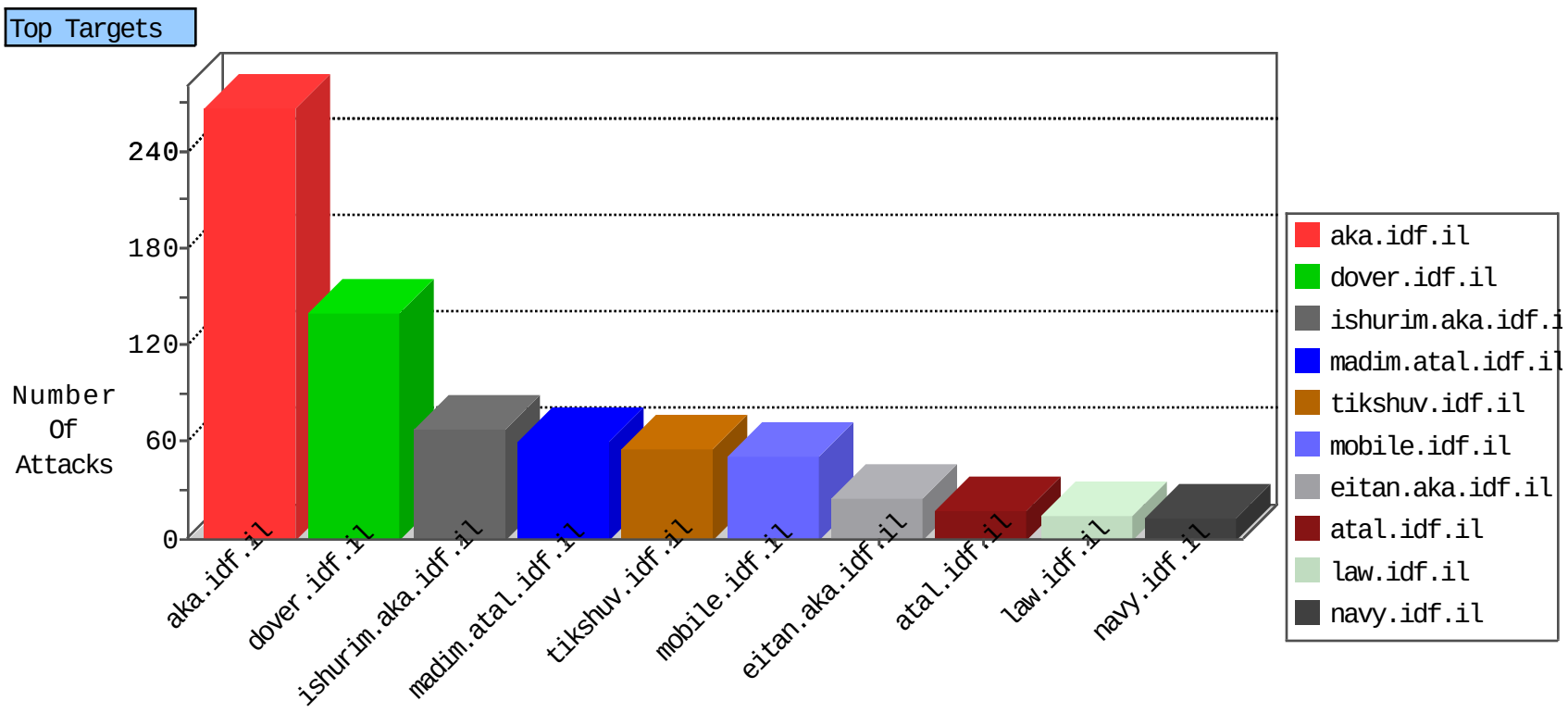
03-03-2016-14:04:05 to 03-03-2016-15:04:05

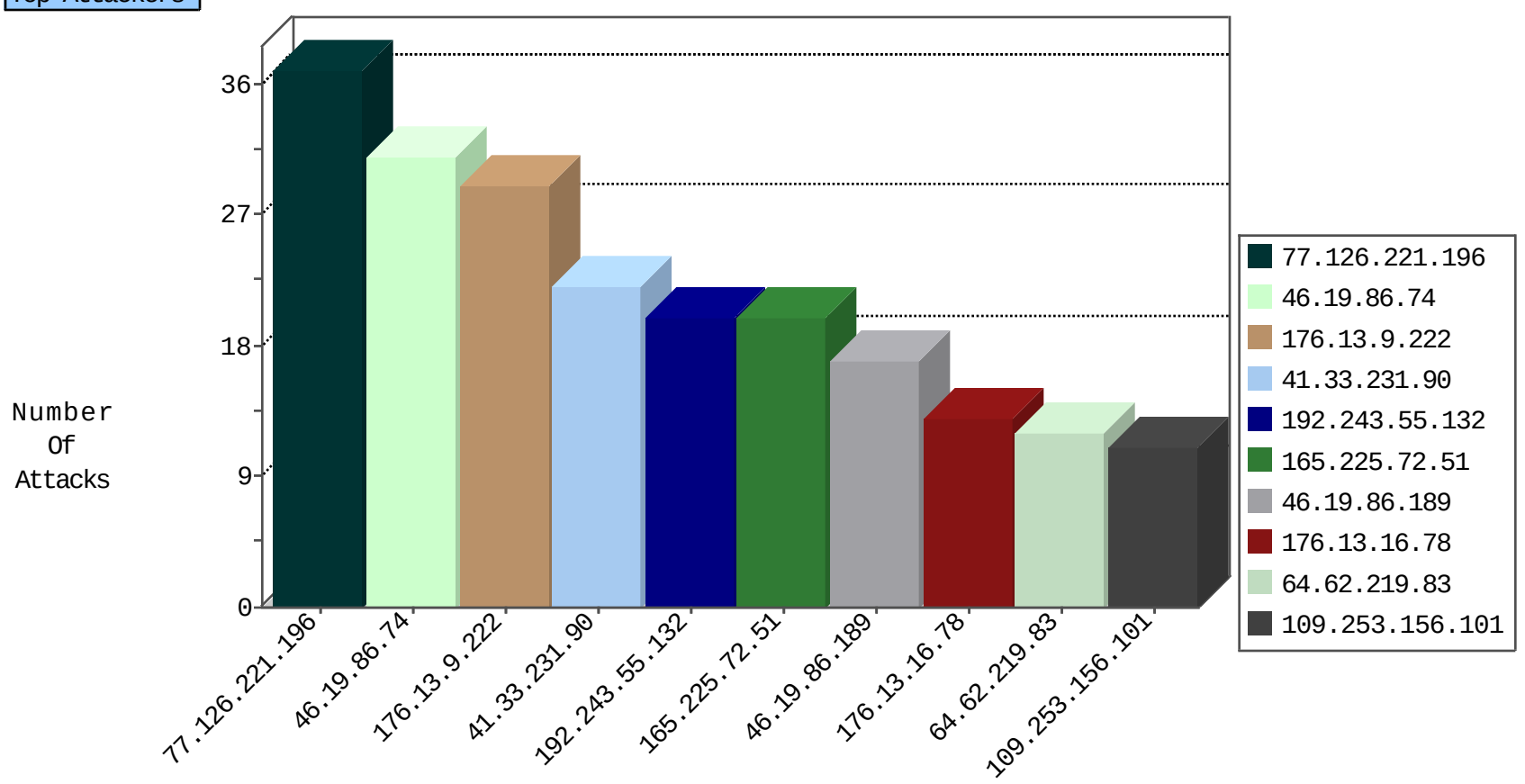
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-03-2016-14:04:05 to 03-03-2016-15:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.208.235	Europe	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	8
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
203.95.25.20	Japan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
66.151.55.113	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.144	United States	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
66.151.55.114	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1

03-03-2016-14:04:05 to 03-03-2016-15:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.44.93	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.64.5.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
80.246.130.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
46.19.86.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
157.55.39.210	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
93.172.176.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.142.68.4	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
131.253.25.161	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
149.78.14.21	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.177.162.254	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
207.46.13.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	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	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.132	Italy	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-03-2016-14:04:05 to 03-03-2016-15:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.247.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.254.206.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.68.4	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
185.120.126.31	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
5.22.130.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
172.87.221.214	147.237.0.15		kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
132.68.228.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.76.197		e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.139.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.188.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.76.38	Sweden	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
37.139.27.231	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.21.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.184.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
134.191.232.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.210.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.142.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.53.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-03-2016-14:04:05 to 03-03-2016-15:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
165.225.72.51	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
82.166.248.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.193.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.99.44	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.147.251	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.135.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.153.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.21.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
80.246.137.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.13.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.94	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
64.62.219.83	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.114.2.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.122.103	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
176.13.16.78	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
199.203.226.21	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
176.13.16.78	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.146.177	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.236	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.102.9.125	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
212.199.251.235	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
79.176.234.214	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.246.139.57	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.179.155.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.253.222.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.54.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.135.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
93.157.85.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
64.62.219.83	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
82.166.2.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.238.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
65.49.14.83	Anonymous Proxy	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.138.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.139.21.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.121.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-03-2016-14:04:05 to 03-03-2016-15:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.253.138.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.189	Israel	147.237.72.166	aka.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
176.13.9.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.253.156.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.253.209.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.126.221.196	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Malformed URL	Block	3
77.126.221.196	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Abnormally Long Request	Block	3
77.126.221.196	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	3
77.126.221.196	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Unknown HTTP Request Method	Block	3
109.253.194.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.13.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.147.86	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
62.219.165.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
81.218.66.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
176.13.13.171	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.126.221.196	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Abnormally Long Header Line from 77.126.221.196	Block	2
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	2
46.19.86.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
125.78.226.117	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 125.78.226.117	Block	2
77.126.221.196	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.64.25.86	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized Request Content Type from 109.64.25.86	Block	2
80.178.98.147	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.126.221.196	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 77.126.221.196	Block	2
46.19.85.115	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.54.42.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
54.240.197.225	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.147.247	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
125.78.226.117	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
77.126.221.196	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Illegal HTTP Version	Block	2
66.249.64.240	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-16581-en/dover.aspx	Block	1
212.235.56.185	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 212.235.56.185	Block	1
46.19.85.165	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
77.126.221.196	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Malformed HTTP Header Line from 77.126.221.196	Block	1
31.168.25.193	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
77.126.221.196	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
77.126.221.196	Israel	147.237.72.167	ishurim.aka.idf.il	Abnormally Long Header Line request header name	Block	1
2.54.145.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
87.71.14.5	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
62.219.122.103	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
195.138.85.250	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/sendtofriend.aspx?&amp	Block	1
77.126.221.196	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 77.126.221.196 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
77.126.221.196	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal URL Path Encoding ɿmŒ¡_žs[[#6]])¨·sv›q[[#3]]±wש¹-¸sj,ûד[[21#]]÷¸רס: מ-•u–תחn2›ג!q]]#16[[]]#11[[ס•b¯]]#19[[#012¦ ¸ ¨§]]#0[[]]#1[[·^{§%,!-§]]#1[[¸¨ ¦–c~[[#23]]ף¹[[™#15§k]]š"[[82#]]÷ם[[62#]].i"}ž]¨t[[#19]]cתmzi¸[[#17]]Ýך‹ ת^²z:§[n²'ˈ°f_°–Üו •]]w"[[#26]]¸ÞÛcû˜[[#18]]iv¶œe[[#24]]˙[[#26צŸפ·ת„•ץ +)9uא9נ·y–[¸–&גכ›1¸סת,[[32#]][[7#]]qu[[©א#22]]03#[[]]71#[[¸u.]]:c÷q	Block	1
37.26.148.188	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.78.218.28	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
5.254.97.99	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
80.246.137.191	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.76	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.235.56.185	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1796.jpg	Block	1
46.19.85.231	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1