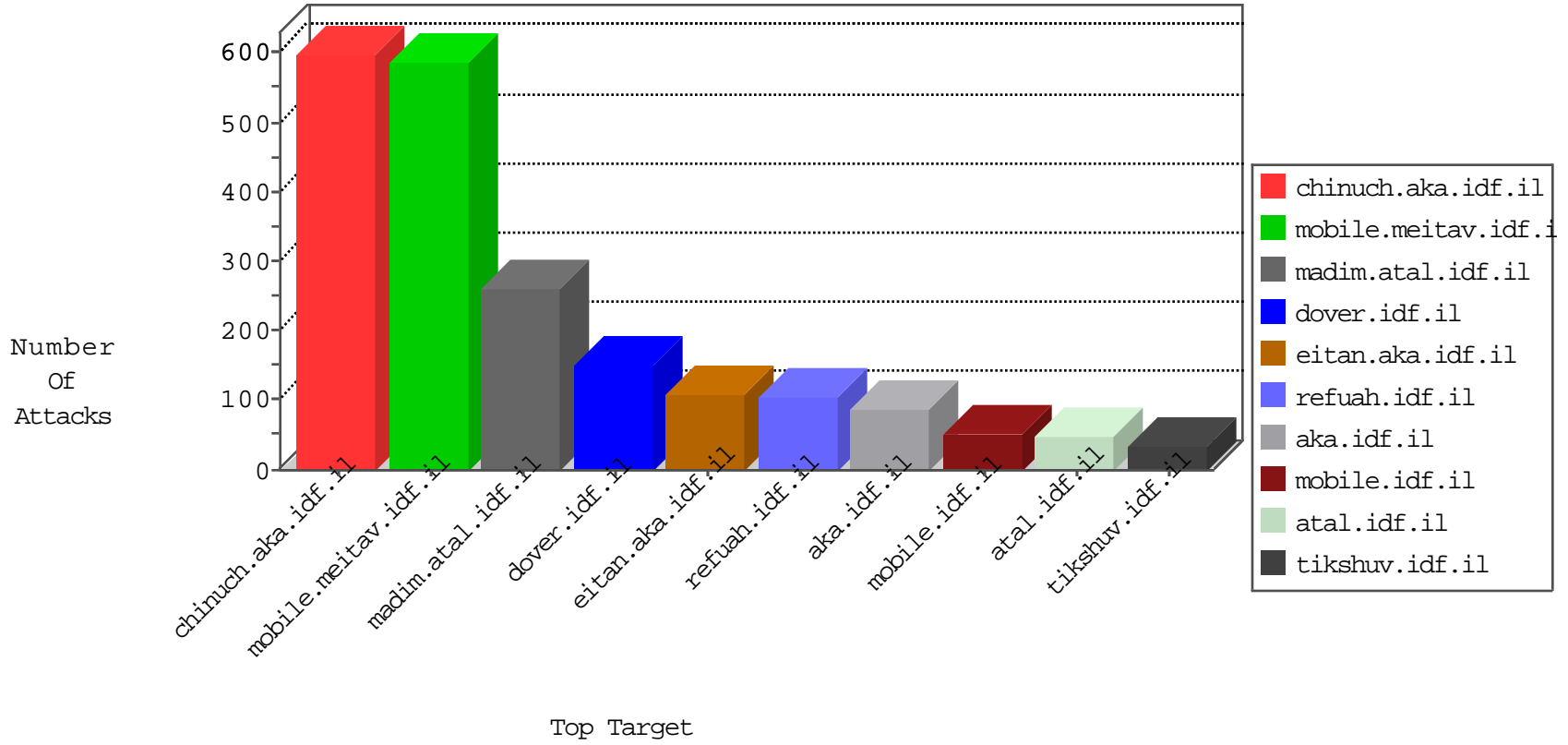


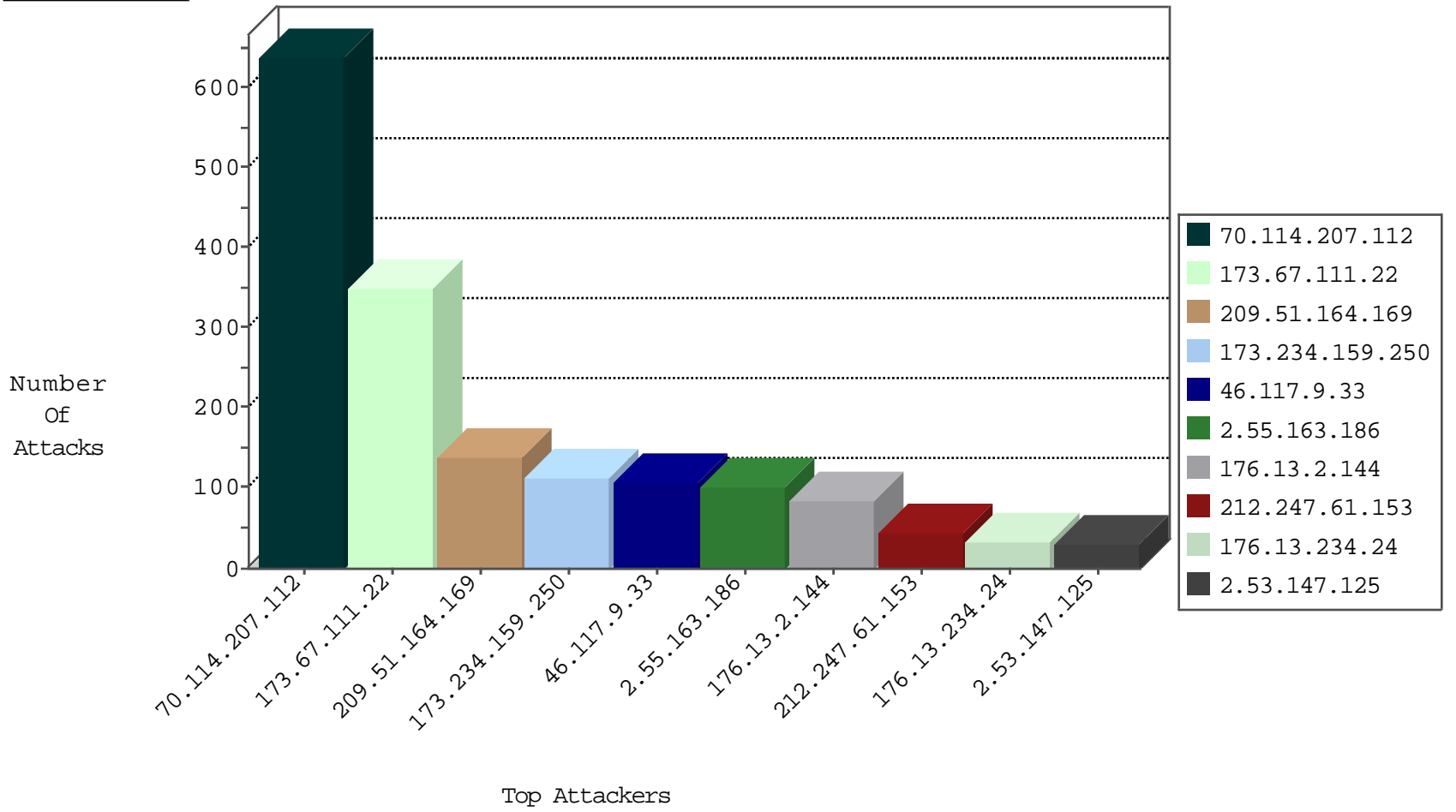
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.106.54.37	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
213.114.163.207	Sweden	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
185.128.40.162	Switzerland	147.237.76.31	nakchal.idf.il	Black List	drop	1
71.6.146.186	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
191.96.249.34	Chile	147.237.76.196	e.sviva.idf.il	Black List	drop	1
96.8.70.110	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
185.128.40.162	Switzerland	147.237.76.30	himush.idf.il	Black List	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.234.159.250	United States	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	106
212.247.61.153	Sweden	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
212.247.61.153	Sweden	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
212.247.61.153	Sweden	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
91.121.101.78	France	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.247.61.153	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	25
94.101.186.42	147.237.8.24	Iran, Islamic Republic of	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.29.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.220.2.5	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.148.16.179	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.148.16.179	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
193.169.70.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.192.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.32.30.116	147.237.72.217	China	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.101.186.42	147.237.8.46	Iran, Islamic Republic of	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.107.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.115.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.200.137	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
46.148.16.179	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
46.148.16.179	147.237.76.30	Ukraine	himush.idf.il	ET SCAN Potential SSH Scan	1
212.179.243.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.148.16.179	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
193.47.165.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
106.187.45.144	147.237.8.45	Japan	e.eitan.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
70.114.207.112	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	330
70.114.207.112	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	308
173.67.111.22	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	181
173.67.111.22	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	167
46.117.9.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	81
2.53.147.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.117.9.33	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
209.51.164.169	United States	147.237.76.39	mobile.meitav.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
209.51.164.169	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
209.51.164.169	United States	147.237.76.39	mobile.meitav.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	19
209.51.164.169	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	18
209.51.164.169	United States	147.237.76.39	mobile.meitav.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	18
209.51.164.169	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	15
192.241.170.19	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
193.106.54.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
209.51.164.169	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
77.127.53.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.241.170.19	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
209.51.164.169	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
97.87.138.222	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
81.218.97.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.55.148.204	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
62.0.251.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
81.218.97.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
100.92.76.26		147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
199.193.78.77	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
213.8.115.122	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
193.106.54.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.27.153.35	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.244.93.169	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
193.106.54.37	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
109.253.209.104	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.53.22.200	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
97.87.138.222	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.4.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
77.127.53.215	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
192.115.215.60	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
209.51.164.169	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.46	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.127.53.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.69.22	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.148.204	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.240	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.55.150.91	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.10.15	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.32.179.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.53.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
173.234.159.250	United States	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.163.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
176.13.2.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
176.13.234.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
46.19.86.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
85.250.140.190	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	20
46.120.124.96	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.120.124.96	Block	9
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	4
85.64.146.246	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/	Block	3
2.53.177.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.138.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.250.140.190	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/sip_storage/files/2/	Block	3
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
46.19.86.27	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
212.235.98.139	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	2
80.246.140.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.2.144	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ***** ***** *****, Observed ***** ***** *****	None	2
85.64.146.246	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	2
80.246.140.233	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
85.64.146.246	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
77.139.157.84	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
207.46.13.178	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
86.152.194.49	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2341.jpg	Block	1
176.13.232.0	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.182.33.218	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1442-he/refuah.aspx	Block	1
66.102.9.30	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
89.139.184.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/back.png	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2363.jpg	Block	1
46.117.9.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.166	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json	Block	1
213.133.110.35	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
157.55.39.186	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
188.244.34.136	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
46.120.124.96	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
85.250.140.190	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 85.250.140.190	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1
37.26.146.139	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
77.139.56.173	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
194.90.99.193	Israel	147.237.72.166	aka.idf.il	Cookie Tampering on cookie wb48617274: Expected F95E7DB4, Observed 01A368BA	None	1