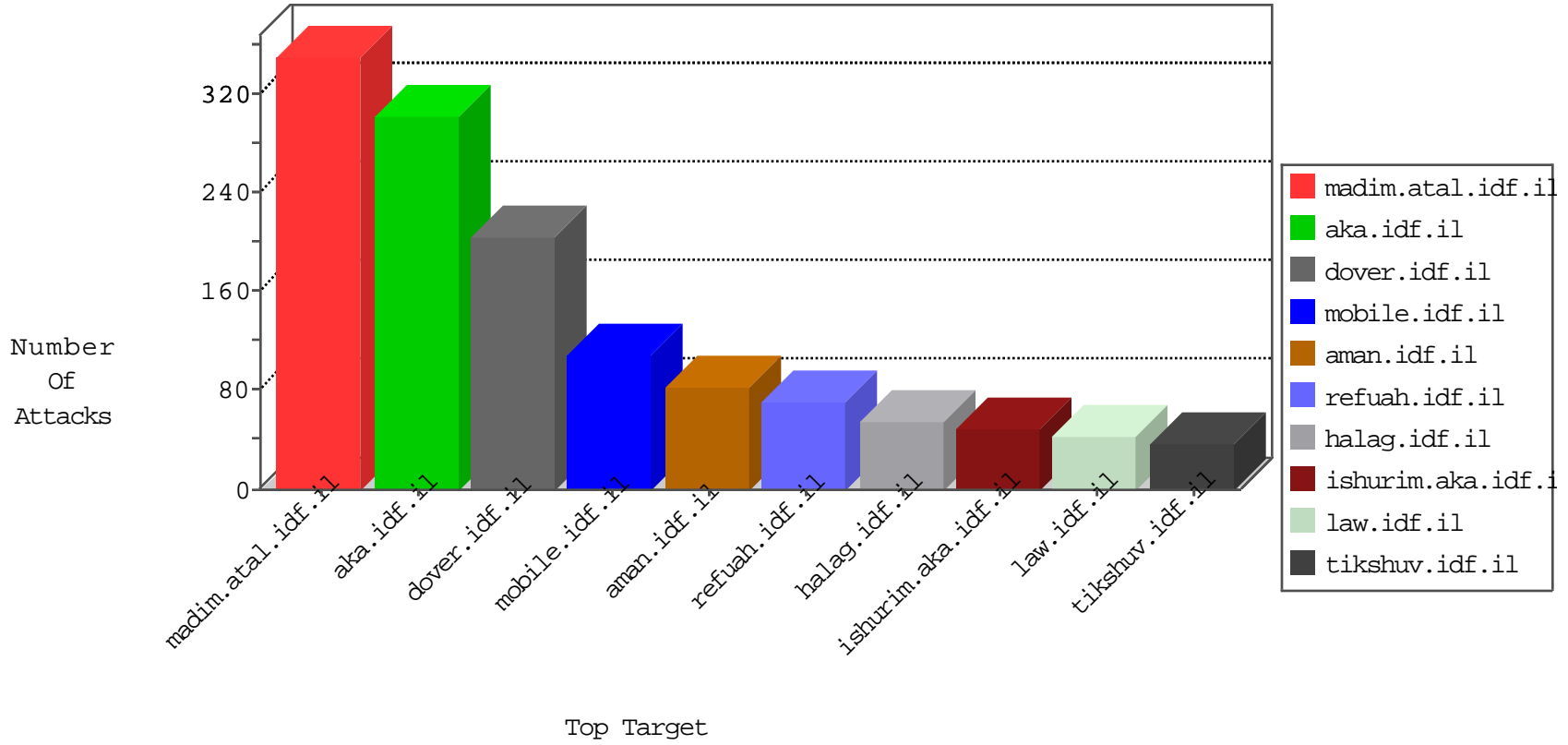


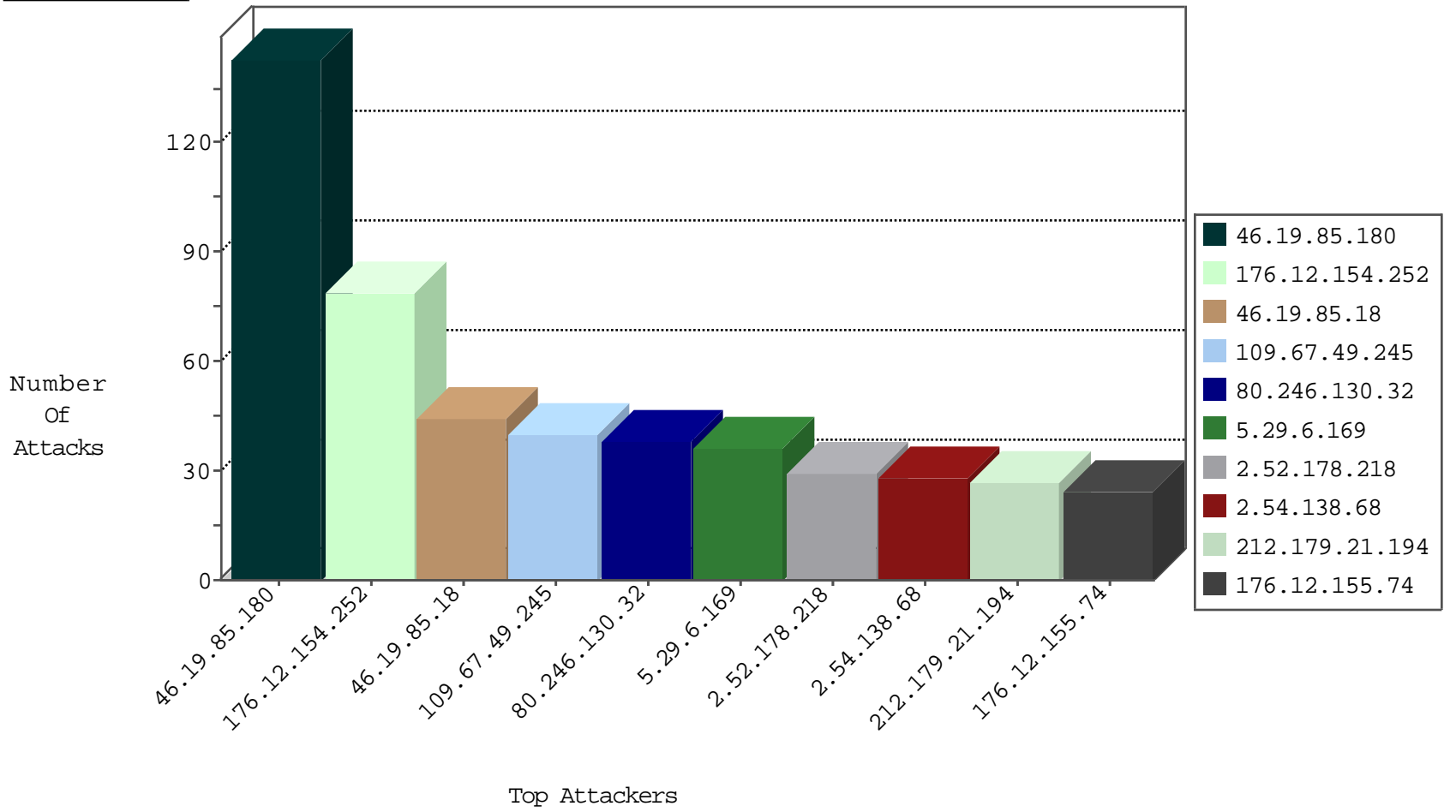
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
91.202.171.11	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
84.109.112.43	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
192.118.132.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
115.239.228.10	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Http	drop	1
185.130.5.224		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
52.28.32.164	United States	147.237.76.196	e.sviva.idf.il	JLM_Purple_Con_Limit_Https	drop	1
94.102.48.195	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.31	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1

02-02-2016-14:04:00 to 02-02-2016-15:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
118.238.227.101	Japan	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	21
5.29.147.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.244	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
134.191.232.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.220.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
183.61.109.189	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.32	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
5.29.6.169	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
176.12.155.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.67.49.245	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
93.172.163.128	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
2.52.178.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
158.85.253.245	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
109.66.196.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.67.248.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.67.49.245	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
185.32.179.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.81	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	11
109.67.110.35	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.61.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
195.160.242.40	Israel	147.237.77.74	law.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
62.0.227.93	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.110.35	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
46.19.85.171	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.199.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.227.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
94.230.86.70	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	6
2.54.44.198	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.205.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.34.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.226.34.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.190	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.102.254.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.120.217.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
188.120.148.128	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
132.72.71.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.22.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.254.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.136.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.12.154.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
40.77.167.58	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.216.191.117	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.16.192	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.230.86.70	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
213.8.96.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
176.12.154.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
176.12.154.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	48
46.19.85.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
2.54.138.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
2.52.47.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
2.54.148.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
85.250.108.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
185.32.179.175	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.55	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
185.32.179.175	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
176.12.154.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.154.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.196.245	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.10.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.154.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.195.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	2
109.160.140.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.179.61.123	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/589-he/patzar.aspx=	Block	2
176.12.154.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.12.154.138	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
46.19.85.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/gyius/main/gyius/resources/images/master/favicon.gif	None	1
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sip_storage/files/7	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
37.26.148.130	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 37.26.148.130 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
176.12.155.55	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
109.67.49.245	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.81.250	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
2.54.38.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
46.19.86.222	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/gyius/main/gyius/resources/images/master/favicon.gif	None	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
158.85.253.245	United States	147.237.72.156	aman.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	1
46.19.85.15	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 46.19.85.15 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
5.29.6.169	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
84.109.116.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/gyius/atuda/asmachta.aspx	None	1
2.52.22.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
176.102.51.132	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyius/general.aspx	Block	1
73.3.77.56	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
2.54.61.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	1
66.102.9.101	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
158.85.253.245	United States	147.237.72.156	aman.idf.il	Multiple signatures from 158.85.253.245	Block	1
46.19.85.15	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1