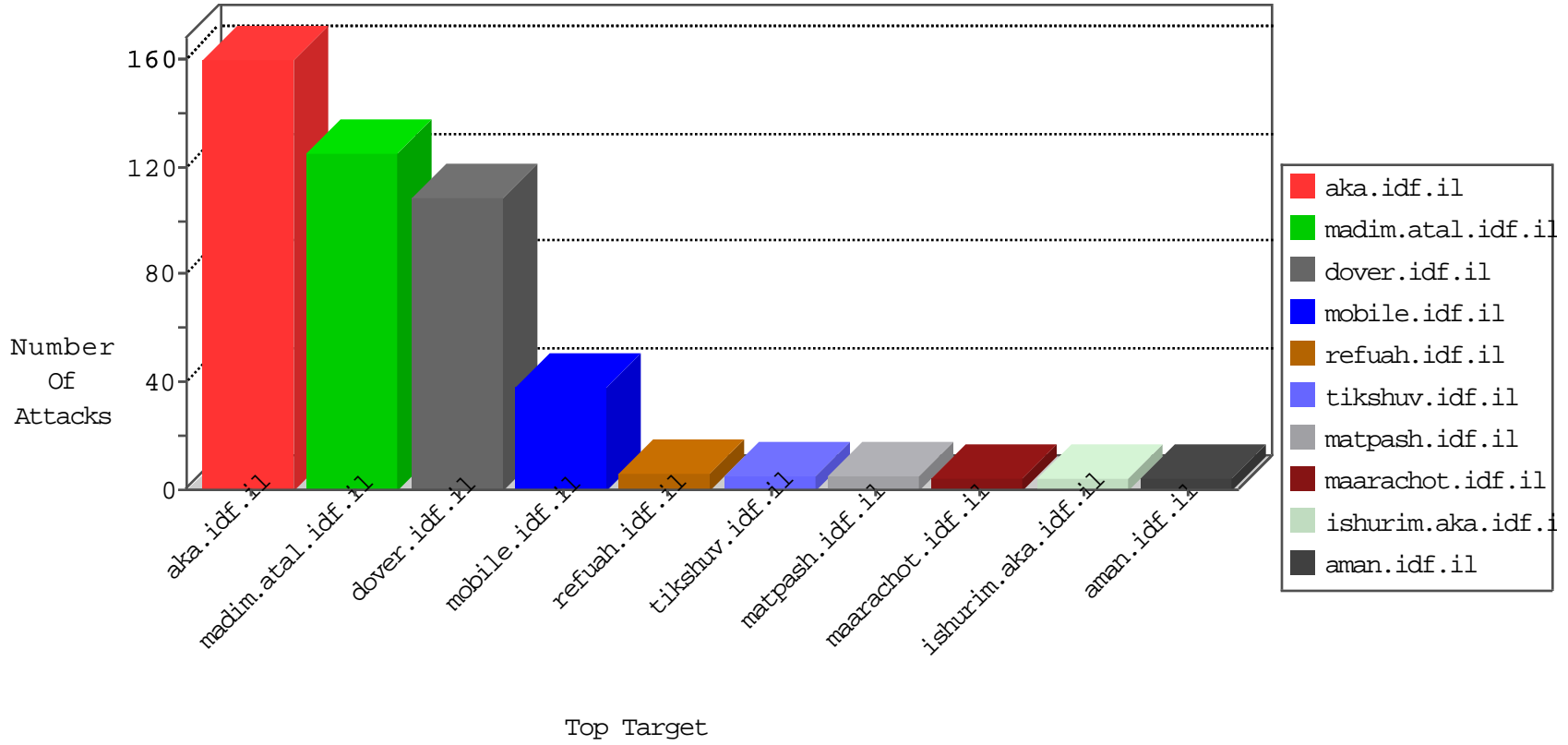


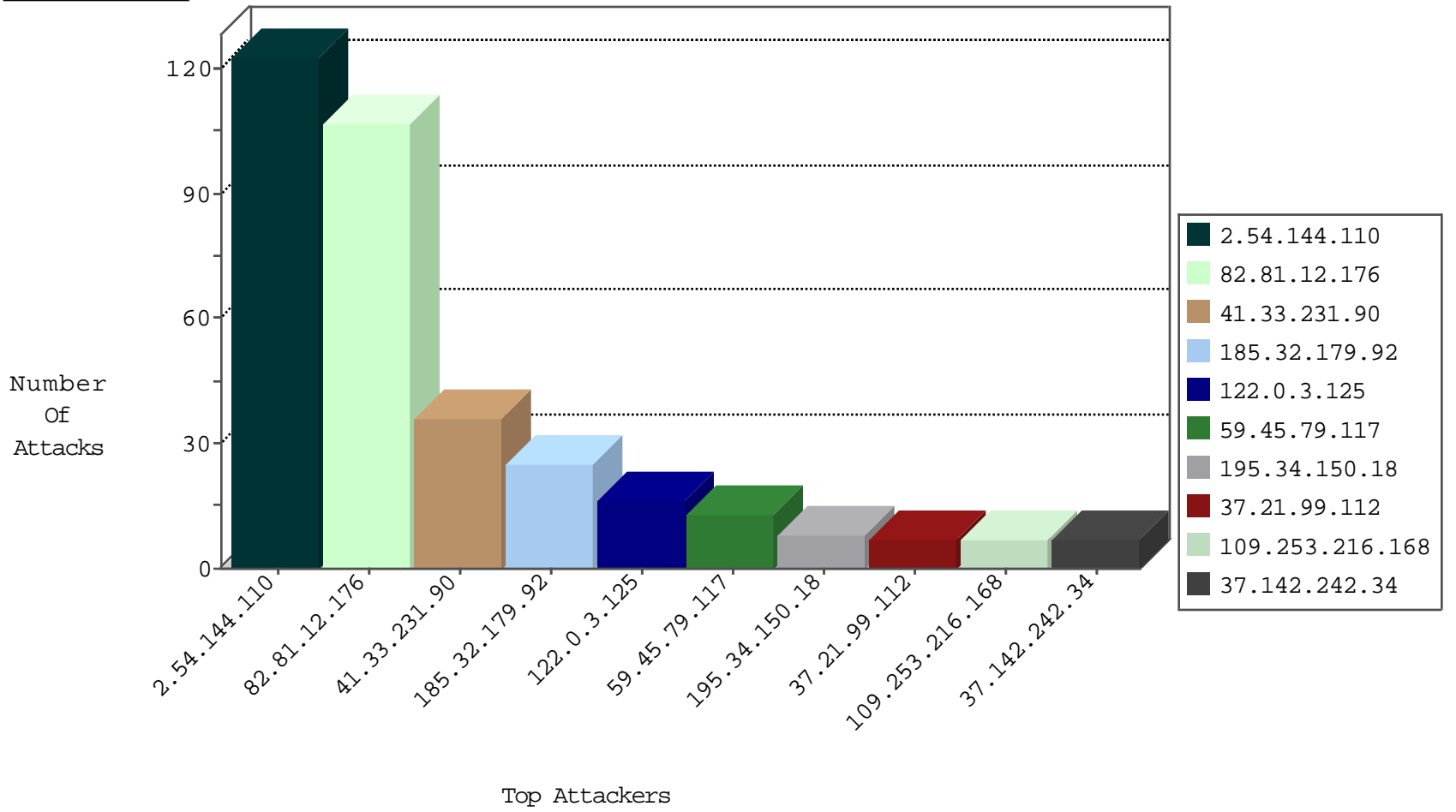
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	107
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.125	Italy	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.202	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
94.76.11.255	147.237.72.14	Bahrain	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
23.96.118.28	147.237.77.233	United States	atal.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.78.9	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
180.150.177.188	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
37.21.99.112	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Potential SSH Scan	1
64.107.14.40	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
37.21.99.112	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
37.21.99.112	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.34	China	yochalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.71	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
94.76.11.255	147.237.72.166	Bahrain	aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.21.99.112	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN Potential SSH Scan	1
37.21.99.112	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
37.21.99.112	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
37.21.99.112	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.32.179.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
122.0.3.125	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.253.216.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
201.205.49.48	Costa Rica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.142.242.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
109.66.114.123	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.180.201.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.227.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.242.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.228.122.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.195.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.138	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.143.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.200.12.7	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	2
77.127.53.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
207.241.229.36	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.78.153	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
91.200.12.136	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	2
118.161.99.133	Taiwan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
199.30.24.129	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.230	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
216.218.206.82	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.20	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.102	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.210.186.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.66.114.123	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.7.17.171	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.83	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.24	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.37	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
72.198.222.160	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.118	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.87	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.38	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.77.121	e.navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.89	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.228.71.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.71	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
72.198.222.160	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.123	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.229.32.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.99	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.144.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
2.54.144.110	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.144.110	Block	41
185.32.179.92	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
5.102.236.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.57.98.204	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
81.200.91.15	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1514-en/dover.aspx.	Block	1
157.55.39.197	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/searchresults/searchresults.aspx	Block	1
94.159.209.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
74.82.47.4	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
109.186.156.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.200.91.15	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.247	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/modiin/default.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
77.127.227.135	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
109.253.147.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.200.91.15	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.86.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.2.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.181.147.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
216.218.206.68	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
109.253.216.168	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.109.178.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1384-he/dover.aspx	Block	1
46.120.164.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.186.156.81	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
81.200.91.15	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.law.idf.il/163-en/patzar.aspx	Block	1
217.132.13.145	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born	Block	1
2.54.144.110	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
149.88.241.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.103.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
74.82.47.2	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.102.9.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
109.186.156.81	Israel	147.237.72.166	aka.idf.il	Unknown Parameter POST /Main/Giyus/UserDetails/UpdateUserDetails.aspx HTTP/1.1 Host: www.aka.idf.il Referer: https://www.aka.idf.il/Main/Giyus/UserDetails/UpdateUserDetails.aspx Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	1