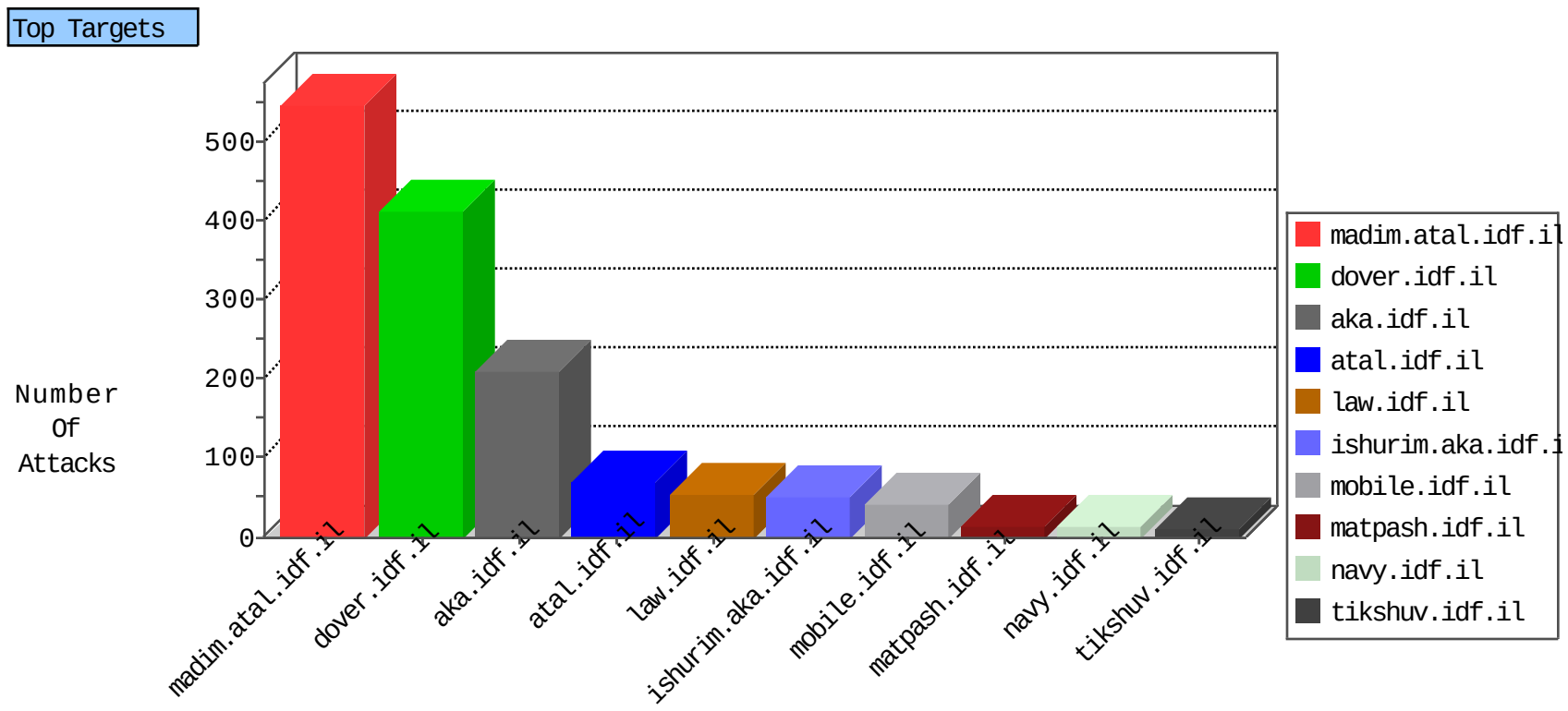
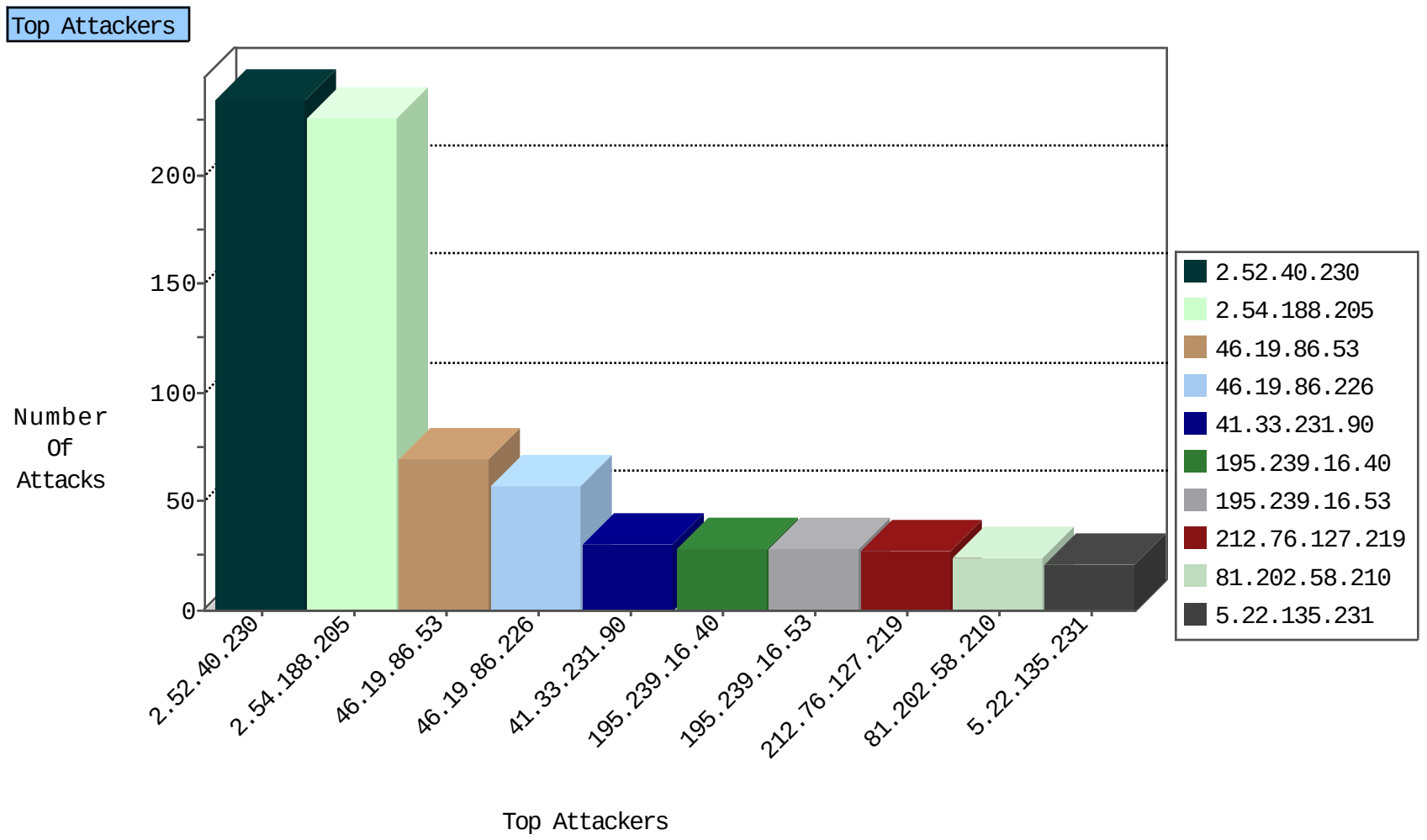
01-26-2016-23:04:07 to 01-27-2016-00:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-26-2016-23:04:07 to 01-27-2016-00:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.204.65	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
185.130.5.231		147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1

01-26-2016-23:04:07 to 01-27-2016-00:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-26-2016-23:04:07 to 01-27-2016-00:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
31.44.135.165	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
81.202.58.210	147.237.8.28	Spain	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
5.22.131.72	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
81.202.58.210	147.237.77.234	Spain	halag.idf.il	ET SCAN Potential SSH Scan	2
5.22.131.72	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
168.62.238.153	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
81.202.58.210	147.237.8.50	Spain	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.76.197	Ukraine	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
81.202.58.210	147.237.77.243	Spain	mobile.idf.il	ET SCAN Potential SSH Scan	1
81.202.58.210	147.237.0.200	Spain	m4u.idf.il	ET SCAN Potential SSH Scan	1
81.202.58.210	147.237.77.212	Spain	e.dover.idf.il	ET SCAN Potential SSH Scan	1
81.202.58.210	147.237.0.19	Spain	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
81.202.58.210	147.237.77.176	Spain	matpash.idf.il	ET SCAN Potential SSH Scan	1
81.202.58.210	147.237.0.15	Spain	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
81.202.58.210	147.237.76.202	Spain	e.halag.idf.il	ET SCAN Potential SSH Scan	1
222.186.31.57	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
81.202.58.210	147.237.76.196	Spain	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.77.176	United States	matpash.idf.il	ET DROP Dshield Block Listed Source	1
81.202.58.210	147.237.76.34	Spain	yohalan.idf.il	ET SCAN Potential SSH Scan	1
81.202.58.210	147.237.72.166	Spain	aka.idf.il	ET SCAN Potential SSH Scan	1
164.39.11.198	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
81.202.58.210	147.237.8.45	Spain	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.76.197	Ukraine	e.himush.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
81.202.58.210	147.237.8.14	Spain	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
81.202.58.210	147.237.0.34	Spain	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
81.202.58.210	147.237.77.179	Spain	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
81.202.58.210	147.237.0.17	Spain	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
81.202.58.210	147.237.77.19	Spain	law-forum.idf.il	ET SCAN Potential SSH Scan	1
81.202.58.210	147.237.76.200	Spain	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.31.57	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
81.202.58.210	147.237.76.177	Spain	ncore.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.76.31	Latvia	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
81.202.58.210	147.237.72.167	Spain	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1

01-26-2016-23:04:07 to 01-27-2016-00:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.53	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	27
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
5.22.135.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
46.117.130.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
85.250.224.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
79.182.169.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.176.19.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.254	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
149.78.203.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.54.54.196	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
81.218.27.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.54.182.237	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.149.130	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.197.199	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.160.238.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.126.18.106	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.152.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.53	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.208	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.102.197.199	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	6
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.53	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.160.238.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.250.224.216	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
64.61.21.78	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
151.80.37.228	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.236	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
2.52.40.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	145
2.54.188.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
2.54.188.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	93
2.52.40.230	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.52.40.230	Block	83
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
213.57.57.135	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 213.57.57.135	Block	11
2.54.188.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	10
2.52.40.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
185.120.126.12		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.228.177.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.211.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.169.118	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.3.144.55	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
85.65.168.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.181.115.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.104.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.140.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
89.138.253.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
71.178.94.44	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
176.13.6.40	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	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
109.226.21.167	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
85.25.103.12	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.236	Block	1
79.177.36.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.163.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17225-he/dover.asp	Block	1
93.115.241.2	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
37.142.185.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149-he/dover	Block	1
213.57.57.135	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many 404: Response Code per Session	Block	1
82.80.141.203	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
176.13.19.62	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$5 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.236	Block	1
79.177.52.83	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
149.88.82.120	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	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
46.117.181.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
41.199.130.230	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
83.130.100.199	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
73.205.105.211	United States	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
2.52.40.230	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
178.152.156.97	Qatar	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1065-en/dover.aspx	Block	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	1
66.249.65.188	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1245-he/atal.aspx	Block	1
85.250.194.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1