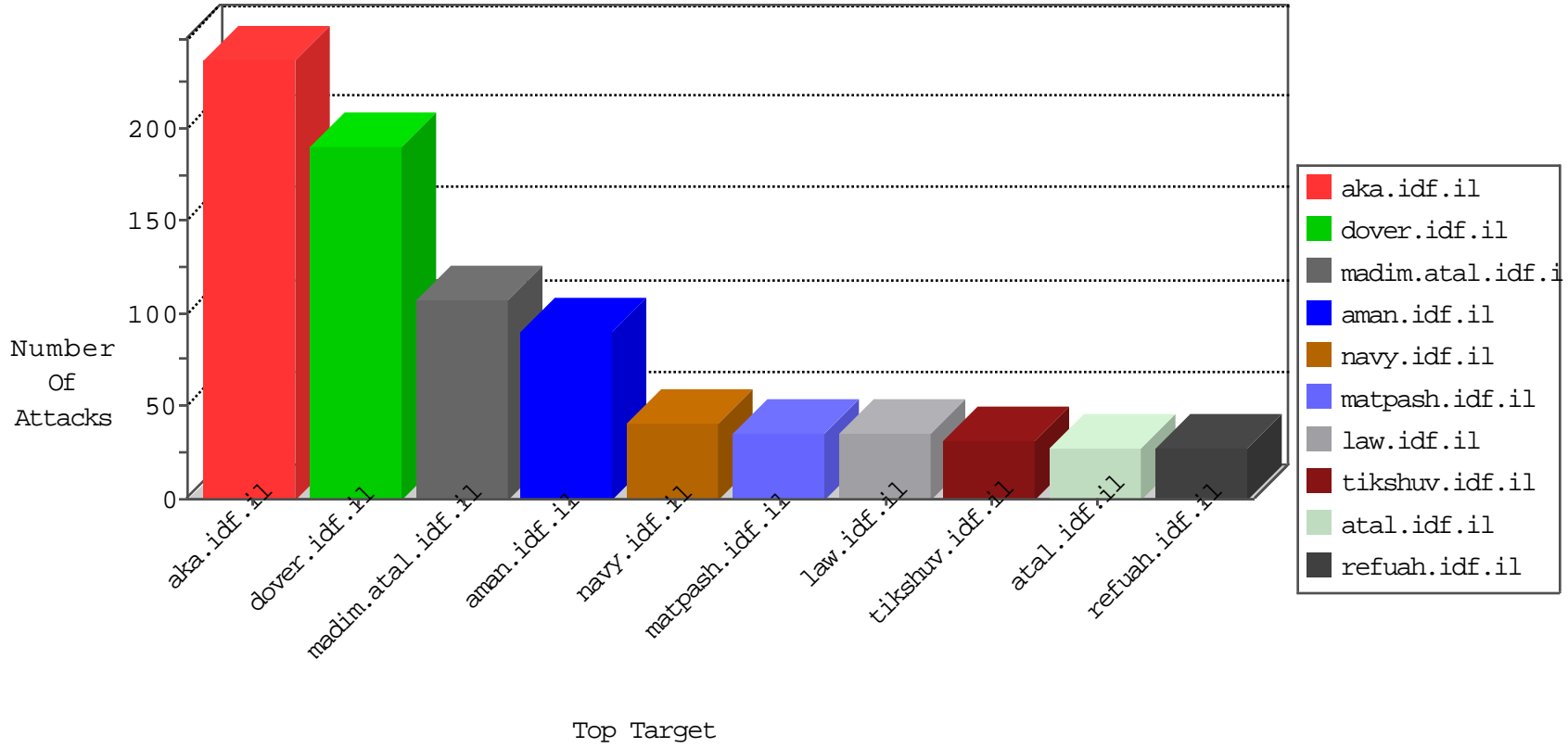


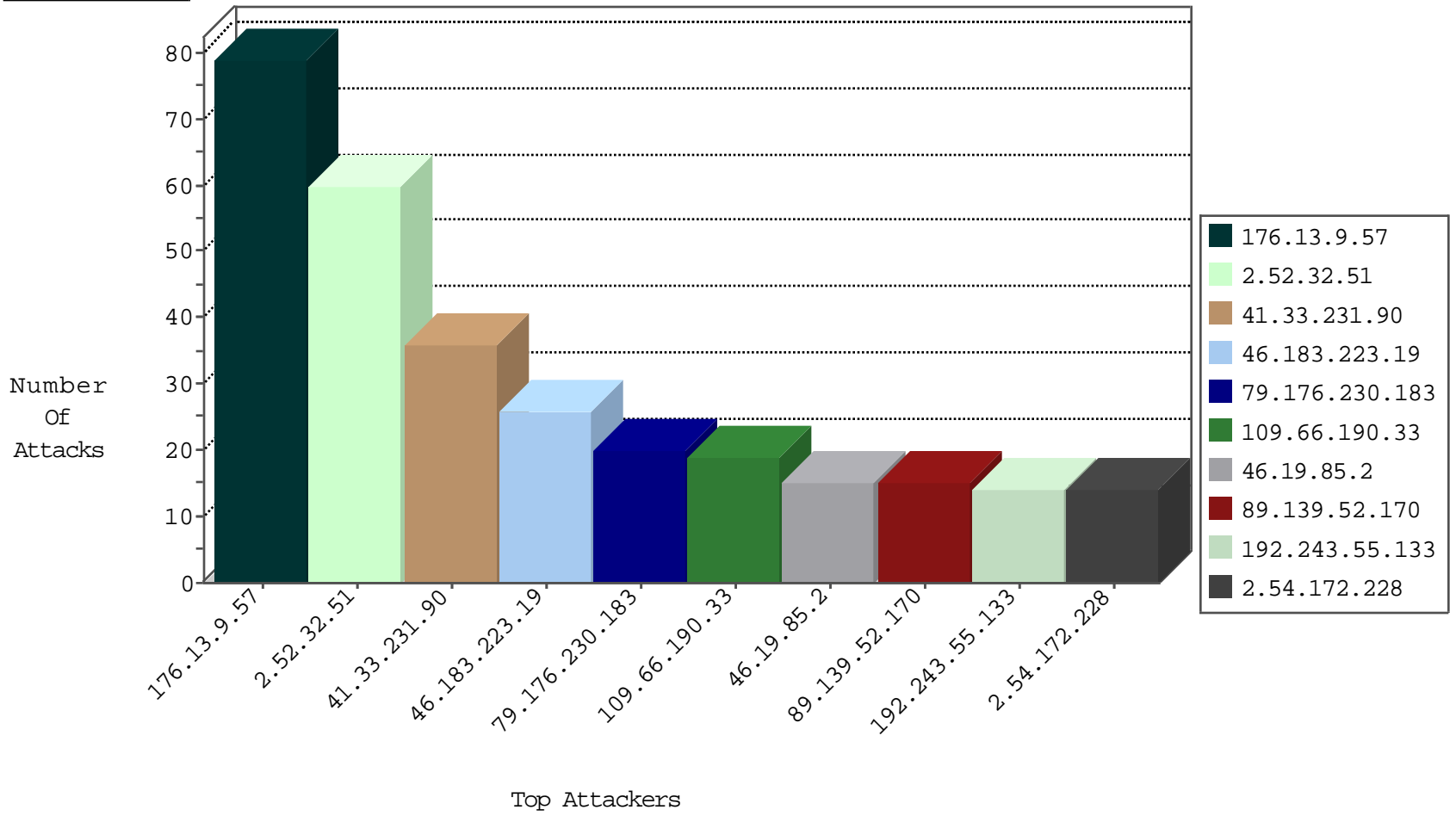
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.222.38	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
45.32.161.174		147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.77.234	halag.idf.il	block-sp-trafl	drop	1
45.32.161.174		147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
45.32.161.174		147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.33.59	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
82.81.4.54	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
79.182.180.44	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
109.87.138.56	Ukraine	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	3
46.4.32.75	Germany	147.237.77.176	matpash.idf.il	C1000106: HTTP: majestic bot	Block	2
46.4.32.75	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	2
49.246.230.40	China	147.237.77.74	law.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
------------------	----------------	------------------	------	-----------	-------

## 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
2.52.32.51	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
79.176.230.183	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
109.66.190.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
89.139.52.170	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
46.183.223.19	Latvia	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
2.52.178.32	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
2.52.149.251	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.102.195.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.52.32.51	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.189.129.74	Portugal	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	9
2.52.32.51	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
79.177.209.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
77.126.10.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.168.90.170	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
109.160.169.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.32.51	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.132.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.32.51	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
45.79.168.168		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.54.172.228	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
213.8.95.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.134.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.205.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.83.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.32.51	Israel	147.237.72.156	aman.idf.il	SYN Attack		reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.3.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.195.159	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.117.26.56	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.135.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.200.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.193.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.126.212.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.130.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.199.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.118.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.12.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.10	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.81.22.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.38.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.143.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.9.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
46.19.85.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
46.183.223.19	Latvia	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.183.223.19	Block	11
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
79.180.24.251	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	5
79.180.24.251	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	5
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
46.19.85.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
199.30.16.172	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
176.13.17.38	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	3
176.13.17.58	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.17.58	Block	3
80.246.136.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.154.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.68.191	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 37.142.68.191	Block	2
84.108.248.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
77.125.140.97	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
217.156.218.158	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.191.155.58	Denmark	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
4.79.123.2	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.182.206.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/aman	Block	1
207.46.13.90	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
149.78.117.17	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$98 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
85.93.91.84	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/artillery	Block	1
217.156.218.159	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.191.155.58	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/magmi/web/magmi.php	Block	1
31.44.141.162	Israel	147.237.0.15	kosher-kravi.idf.il	Parameter Type Violation searchText in kosher-kravi.idf.il/1115-he/orchot.aspx	Block	1
79.183.218.61	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
209.58.128.167	United States	147.237.77.74	law.idf.il	Parameter Type Violation Master\$Header1\$ucHeaderSearch\$txtSearch in www.law.idf.il/320-en/patzar.aspx	Block	1
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.142.68.191	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/	Block	1
149.78.216.111	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/gyus/atuda/asmachta.aspx	None	1
89.139.235.217	Israel	147.237.72.166	aka.idf.il	Unknown Parameter moduleToGoTo in www.aka.idf.il/main/gyus/main/gyus/resources/images/master/favicon.gif	None	1
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-5176-he/patzar.aspxborn-vagabond-where-have-you-been-all-myl-of-these-hitdreamsarticle&r=2&tmpl=blog	Block	1
46.183.223.19	Latvia	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
95.86.77.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/&sa=u&ved=0ahukewin3szdvohlahxfw4khvllcczeqfggnmai&usg=afqjcneeywysowwococycbntx0qxav91bkw	Block	1
31.168.243.6	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
212.179.21.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
66.249.66.36	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
37.142.134.249	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$7 in aka.idf.il/main/gyus/questionnaire.aspx	None	1
176.13.3.206	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	1
93.113.125.11	Romania	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	1
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct167 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
62.219.228.23	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct138\$ct101\$ct103\$cblQuestion\$3 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
109.66.190.33	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
31.168.243.6	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 31.168.243.6	Block	1
82.81.195.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/login	Block	1
217.156.218.156	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.113.125.11	Romania	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct171 in www.aka.idf.il/main/sachar/payslips.aspx	None	1