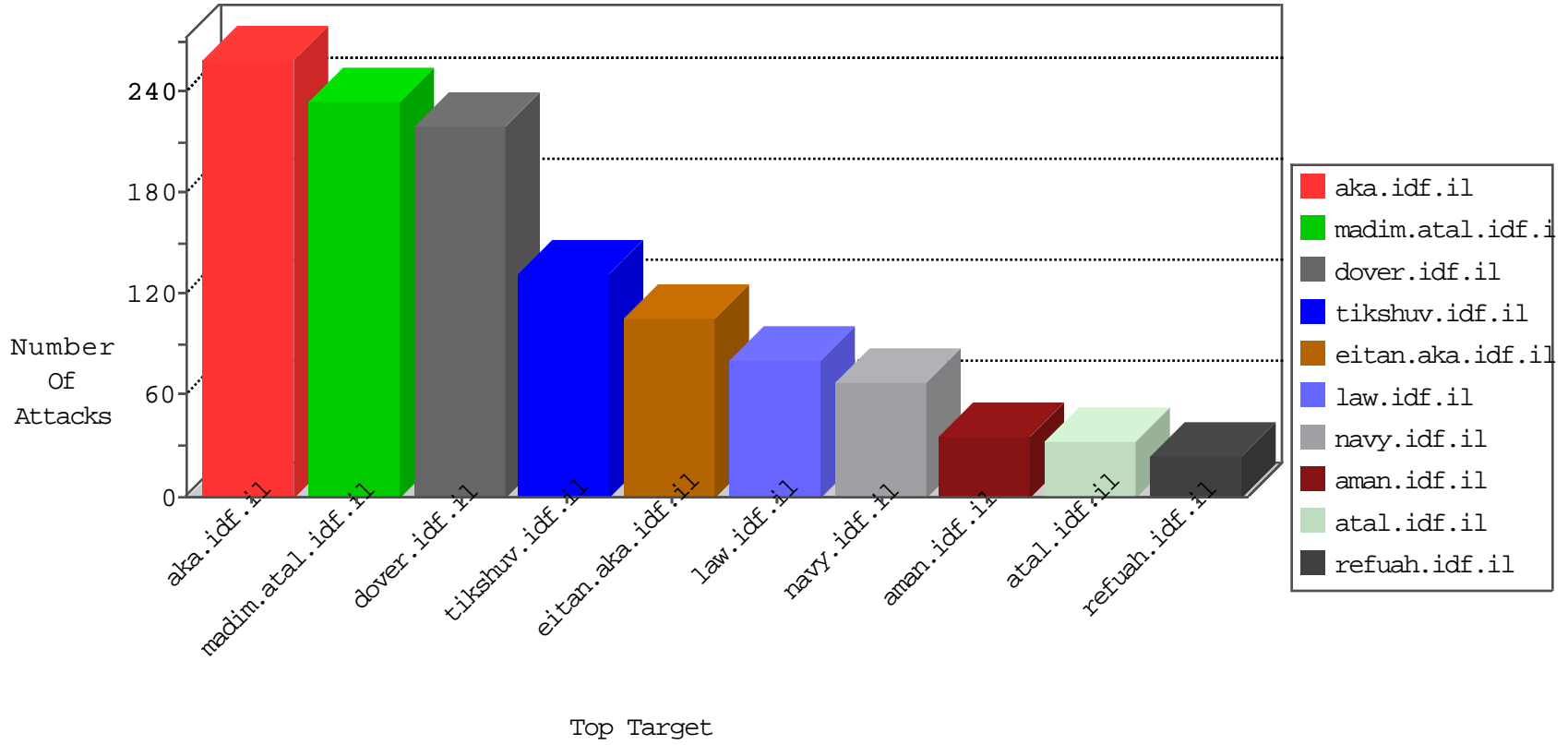


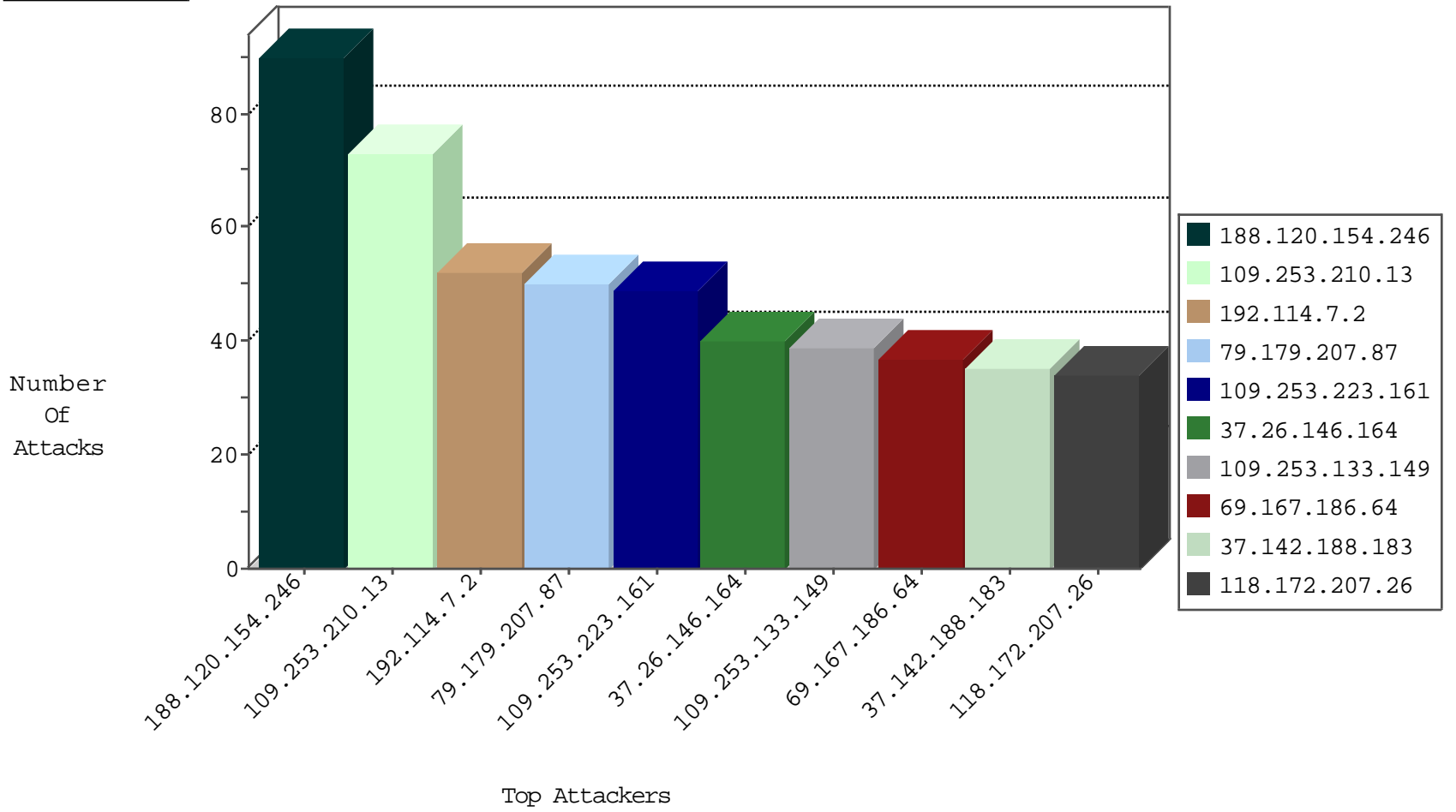
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.207.87	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	50
195.212.29.177	Europe	147.237.77.176	matpash.idf.il	Frk_Purple_Con_Limit_Http	drop	3
195.212.29.177	Europe	147.237.77.176	matpash.idf.il	Frk_Under_Attack_Con_Http	drop	2
217.172.189.11	Germany	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	2
119.131.76.12	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
5.39.218.13	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
60.246.118.41	Macau	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.233.201	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
69.167.186.64	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
84.111.138.219	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
195.154.185.20	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	6
108.168.219.174	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
195.234.228.90	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
69.167.186.64	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
46.117.62.87	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
85.64.249.42	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
69.167.186.64	United States	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
66.249.66.186	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
40.77.167.14	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
66.249.93.117	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
40.77.167.25	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
216.10.220.154	Jamaica	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	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
69.167.186.64	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	25
108.168.219.174	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	11
195.234.228.90	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.114.7.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
109.253.133.149	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
169.241.28.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.253.140.160	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.223.161	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
118.172.207.26	Thailand	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.249.66.95	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
79.183.235.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.179.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
77.125.78.89	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
62.0.84.78	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
95.30.43.206	Russian Federation	147.237.72.156	aman.idf.il	drop	SAM rule	drop	7
79.183.213.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.115.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
118.172.207.26	Thailand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
118.172.207.26	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.177.115.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	6
85.130.233.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.30.43.206	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
148.177.129.213	Europe	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	6
46.19.85.63	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.63	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.149	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
118.172.207.26	Thailand	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.149	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
194.127.8.12	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.102.254.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
118.172.207.26	Thailand	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.188.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.177.115.171	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	4
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.71.135.99	Denmark	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.177.115.171	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.210.187.240	Israel	147.237.77.216	dover.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
195.212.29.177	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.210.188.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
74.63.228.226	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
109.66.104.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.121.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.187.200	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
188.120.154.246	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	89
109.253.210.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
37.26.146.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
109.253.223.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
37.142.188.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
2.54.40.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
84.108.45.138	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
65.55.210.144	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
65.55.210.156	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
199.30.25.78	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.13.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.193.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.24.188	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
82.102.169.113	Israel	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.25.33	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.18.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.186.33	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
164.138.127.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 164.138.127.106	Block	2
84.108.186.33	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	2
109.73.242.14	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
80.179.9.115	Israel	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
62.219.210.200	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.150.1.90	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuesti on\$58 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
84.108.186.33	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
191.251.240.79	Brazil	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
74.63.228.226	United States	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
46.19.85.138	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuesti on\$81 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/7/1437.pdf/	Block	1
89.139.30.237	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
80.246.136.196	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuesti on\$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
207.232.21.105	Israel	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
37.142.189.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
84.108.186.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
195.154.226.90	France	147.237.77.216	doover.idf.il	Illegal HTTP Version HTTP/	Block	1
74.63.228.226	United States	147.237.72.166	aka.idf.il	Multiple signatures from 74.63.228.226	Block	1
46.19.85.148	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuesti on\$7 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
148.251.21.227	Germany	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/228-he/faq.aspx	Block	1
2.54.42.37	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
109.64.112.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Å	Block	1
80.246.136.196	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuesti on\$96 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
207.232.21.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/admin	Block	1
177.52.102.123	Brazil	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
40.77.167.29	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.125.78.89	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
46.19.86.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuesti on\$56 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.64.112.66	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
31.168.87.189	Israel	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
208.115.111.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.111.72	Block	1
66.249.66.36	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1