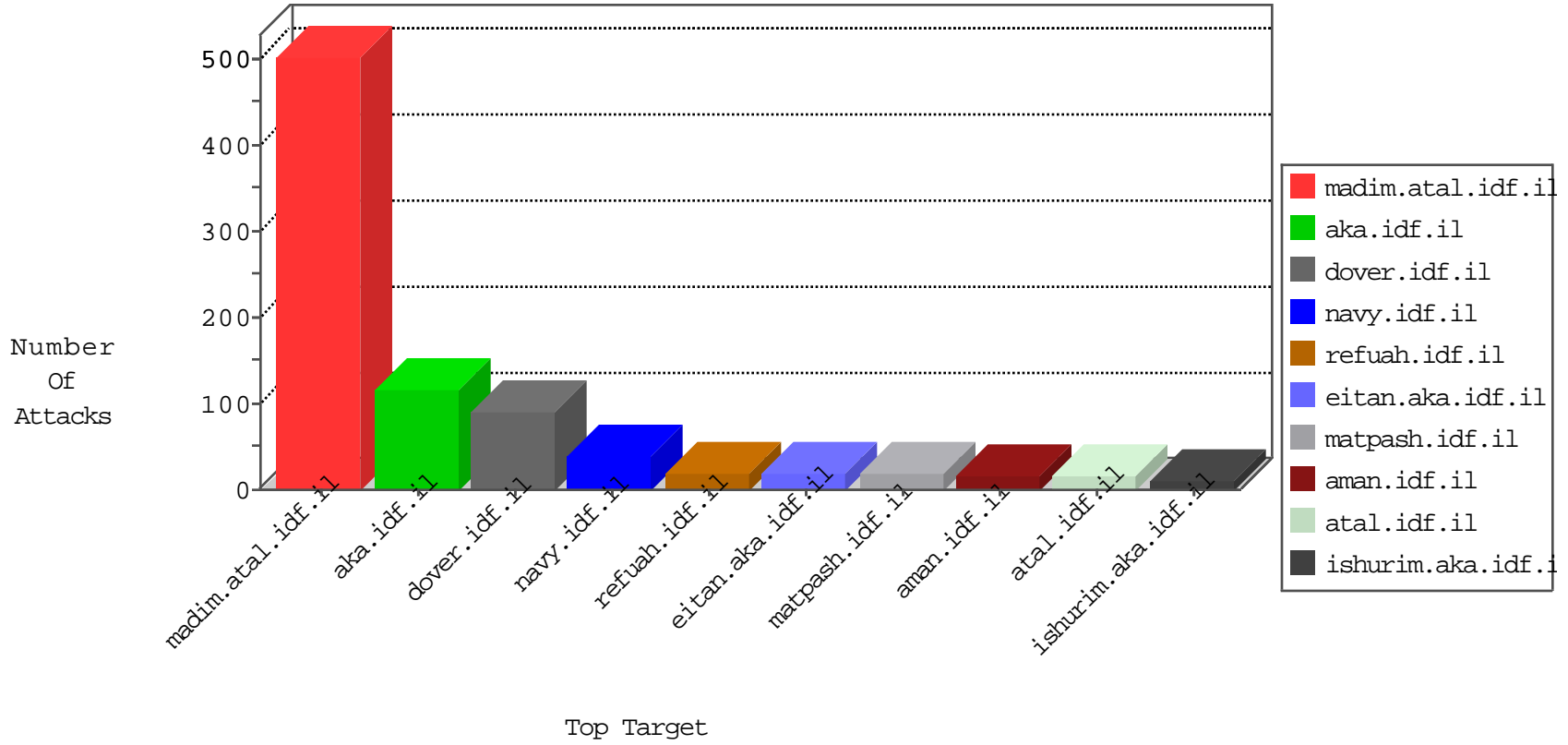


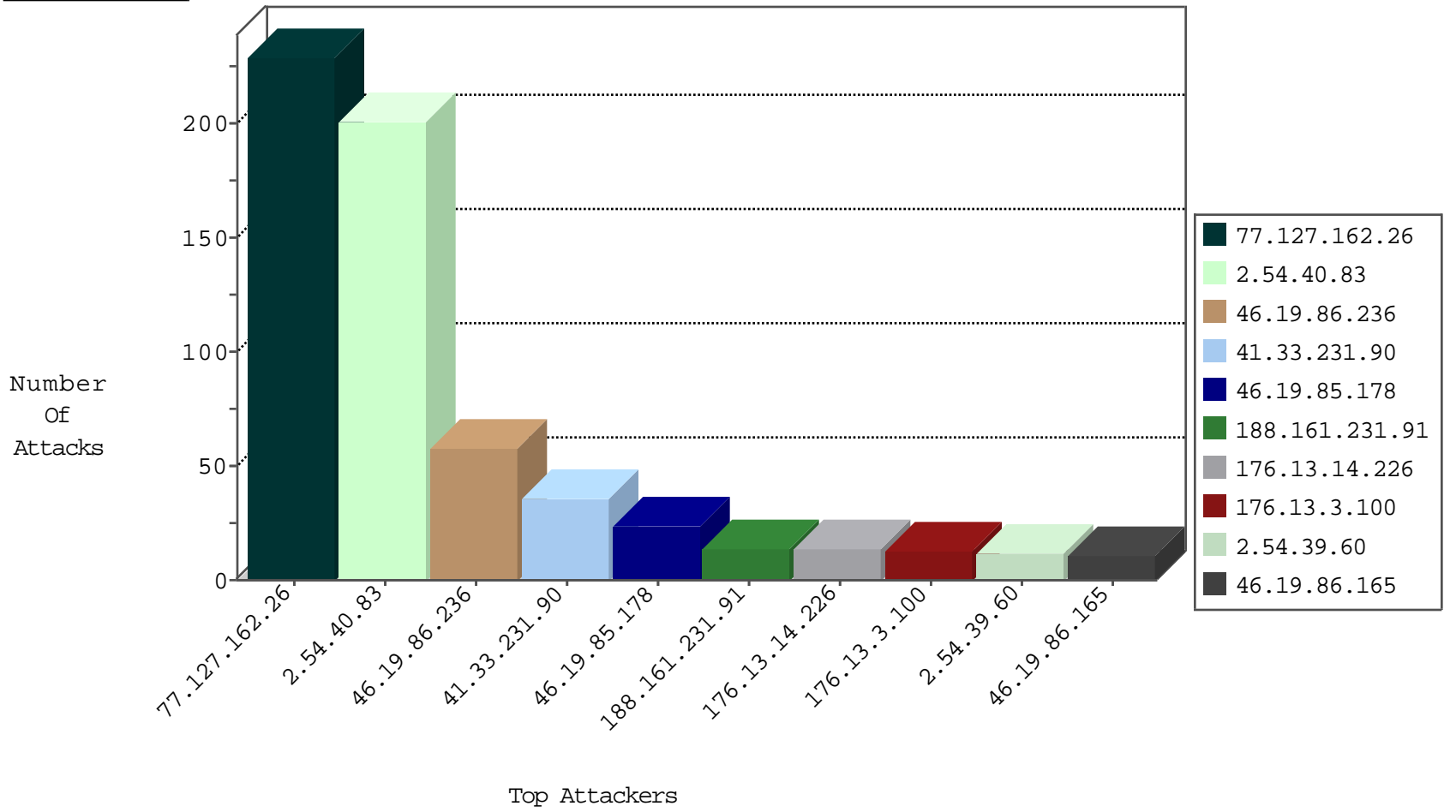
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.91.28.62	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
142.54.169.164	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
123.151.42.61	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
142.54.160.210	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
142.54.160.214	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
116.119.128.46	India	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
206.180.246.167	Canada	147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	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	3
66.249.66.77	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
185.130.5.165	147.237.0.33		idf.il	ET SCAN Potential SSH Scan	1
139.196.57.234	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
121.201.27.61	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
115.85.192.40	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.72.166	United States	aka.idf.il	ET DROP Dshield Block Listed Source	1
115.85.192.40	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
186.62.129.254	147.237.0.33	Argentina	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.183.193.194	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
185.130.5.165	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.165	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.165	147.237.8.28		e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
176.13.3.100	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
121.201.27.61	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
121.201.27.61	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
115.85.192.40	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.165	147.237.77.176		matpash.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.165	147.237.77.19		law-forum.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.165	147.237.8.50		e.tikshuv.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
176.13.14.226	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
188.161.231.91	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
2.54.39.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.231	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.165	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.3.100	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.3.100	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.178	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.178	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.120.148.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.165	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.109.86.79	Israel	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
217.132.116.40	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
66.249.78.233	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.22.130.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.135.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.153.129.226	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.1.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.19.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.196.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.147.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.123.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.19.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.225	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.81.62.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.63.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.199		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.128.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
5.22.130.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.212.85.185	Jordan	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.140.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.4.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.75.129	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
66.249.65.2	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
165.91.13.142	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
128.232.110.28	United Kingdom	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
66.249.65.125	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

02-10-2016-00:04:02 to 02-10-2016-01:04:02

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
165.91.13.142	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
66.249.78.245	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.109.102.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.127.162.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
77.127.162.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	103
2.54.40.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	101
2.54.40.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
46.19.86.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
77.127.162.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	22
82.81.15.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
165.91.13.142	United States	147.237.72.166	aka.idf.il	Distributed NULL Character in Method	Block	4
176.13.15.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.24.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.68.15.7	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.68.15.7	Block	2
37.239.185.151	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
188.120.148.143	Israel	147.237.72.166	aka.idf.il	Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
142.54.160.210	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.1916wh.com/	Block	1
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.88	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/894-he	Block	1
85.250.118.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$79 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.94	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding j.e[8l2tEjLR>S>2vSL;*\$zzuM(&4WRz in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
213.8.204.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/geneal.aspx	Block	1
157.55.39.103	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
66.249.65.122	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter PageNum in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
109.64.100.200	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.78.170	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/916-en/eitan.aspx	None	1
165.91.4.53	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
66.249.65.122	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter tab in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
109.253.221.51	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct102\$ct103\$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.177	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/894-en	Block	1
165.91.13.142	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.78.4	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
188.68.15.7	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
136.243.67.234	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
66.249.78.177	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SortDir in www.eitan.aka.idf.il/938-en/eitan.aspx	None	1
66.249.78.54	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1