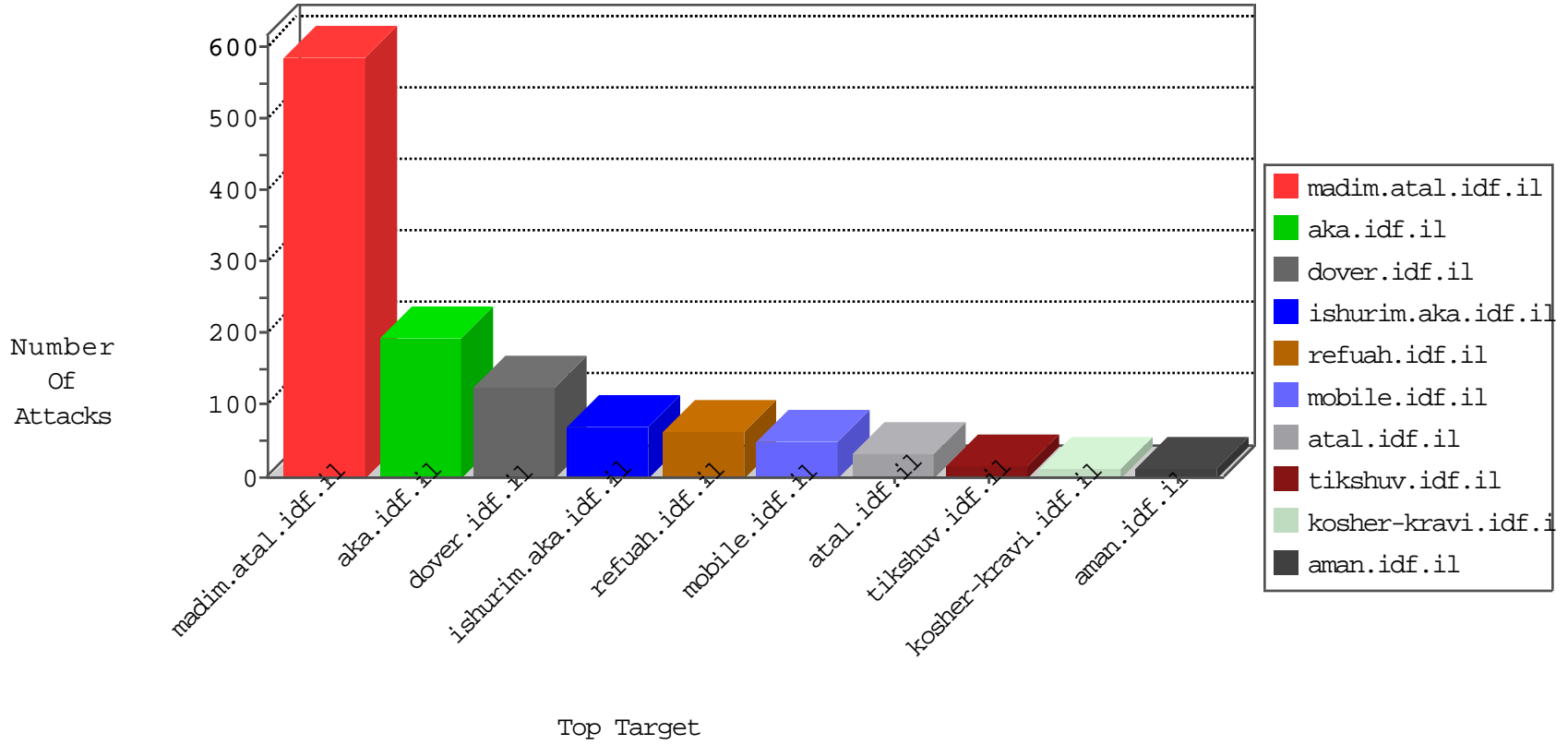


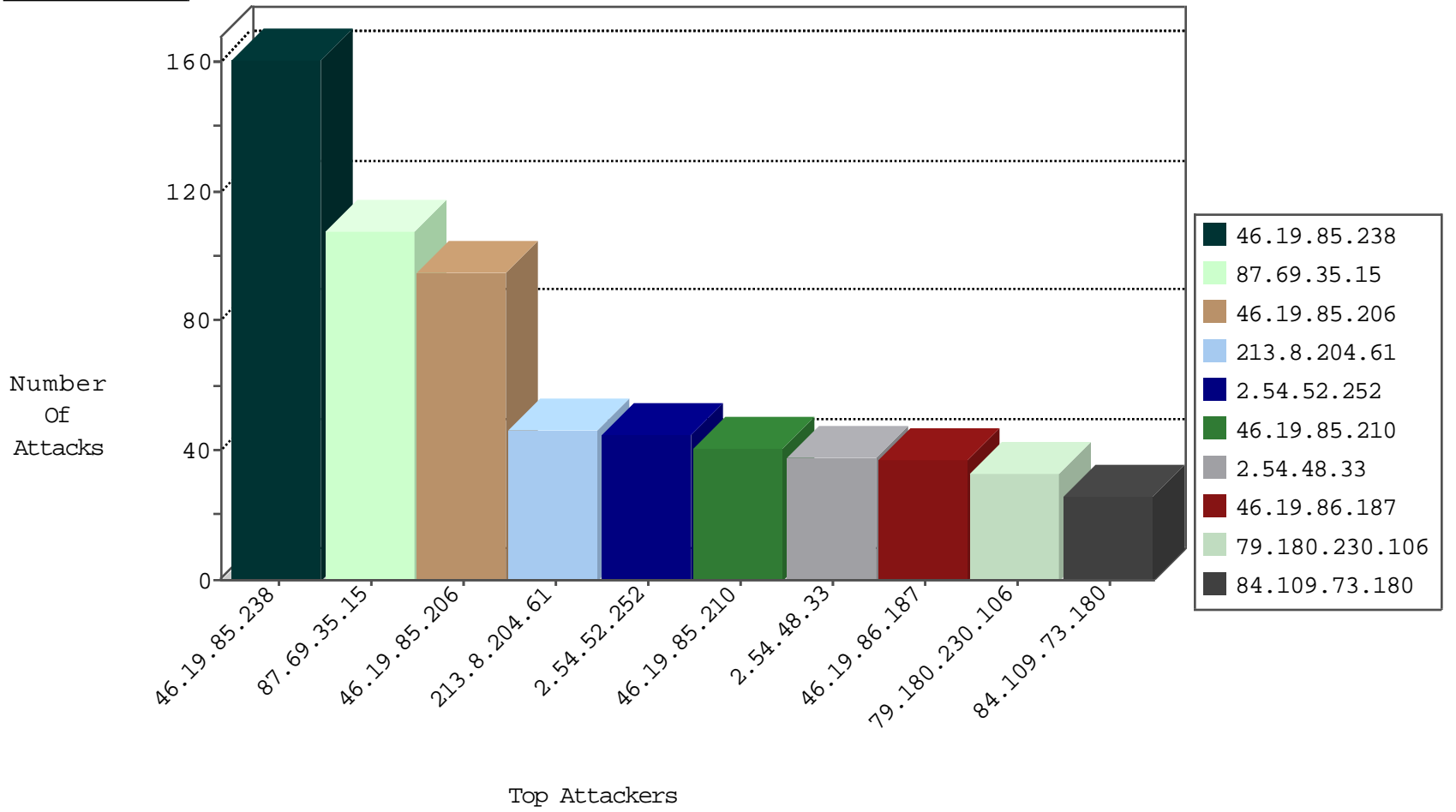
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
94.102.48.195	Netherlands	147.237.76.198	e.yochanan.idf.il	Block_Ntp_All_Net	drop	1
54.67.38.74	United States	147.237.76.147	chinuch.aka.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1
159.122.252.41	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
94.102.48.195	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
94.102.48.195	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
94.102.48.195	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
94.102.48.195	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
94.102.48.195	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
94.102.48.195	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
94.102.48.195	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

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

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	2
212.235.115.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.58.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.117.189.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.1	147.237.0.19		madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
185.72.179.1	147.237.0.19		madim.atal.idf.il	ET SCAN NMAP -f -sS	1
178.129.160.114	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 4096	1
83.130.101.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.221.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.129.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.116.239.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.1	147.237.0.19		madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
178.129.160.114	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
176.13.12.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.136.205	147.237.76.42	Israel	refuah.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
79.179.167.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.210	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
79.180.230.106	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
93.173.155.190	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
213.8.204.20	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
194.90.119.123	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
80.246.133.2	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
208.109.97.62	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
212.143.49.22	Israel	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	8
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.35.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.164.62	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.17.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.156.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.58.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.98.201	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.181.193.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.58.81	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.76	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.148.167	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.125	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
2.52.166.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.206	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
2.52.24.97	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.149.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
95.35.85.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.32.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.135.92	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.14.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.141.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.25.93.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.56.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.254	United States	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
80.178.99.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.46.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.219.132	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
212.143.49.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.3.146.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.236.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.26.148.165	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-04-2016-10:04:09 to 02-04-2016-11:04:09

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.6.189	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
46.19.85.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
87.69.35.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	77
213.8.204.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
2.54.52.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
2.54.48.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
46.19.86.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
84.109.73.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
2.54.149.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
87.69.35.15	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 87.69.35.15	Block	11
80.246.138.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
93.173.155.190	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
79.180.116.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	3
176.13.4.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.28.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.167.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.4.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.227	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	2
149.78.214.221	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct102\$ct103\$txtField in aka.idf.il/main/gyus/questionnaire.aspx	None	2
46.105.100.183	France	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 46.105.100.183	Block	2
87.69.35.15	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.94.161.80	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct102\$ct103\$txtField in aka.idf.il/main/gyus/questionnaire.aspx	None	2
176.13.17.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.180.20.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.86.104.188	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cb1Question\$67 in aka.idf.il/main/gyus/questionnaire.aspx	None	2
65.208.151.112	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/6/	Block	1
212.143.49.22	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/sip_storage/files/3/1773.jpg	Block	1
81.218.70.243	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/kkkkkkkk=748f35d0kkkkkkk_748f35d0	Block	1
113.76.90.95	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
37.26.147.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cb1Question\$88 in aka.idf.il/main/gyus/questionnaire.aspx	None	1
2.54.128.28	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cb1Question\$88 in aka.idf.il/main/gyus/questionnaire.aspx	None	1
91.199.69.254	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
212.34.23.95	Jordan	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
2.54.17.203	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl38\$ct101\$ct103\$cb1Question\$0 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
85.64.191.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.122.167.46	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-14178-en/shared/usercontrols/headerupper/	Block	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
79.179.146.142	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
31.168.21.80	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cb1Question\$15 in aka.idf.il/main/gyus/questionnaire.aspx	None	1
95.86.121.179	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
87.69.35.15	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.65.82	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in eitan.aka.idf.il/1149-en/eitan.aspx	None	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
2.54.56.111	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cb1Question\$71 in aka.idf.il/main/gyus/questionnaire.aspx	None	1
81.218.70.243	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	1