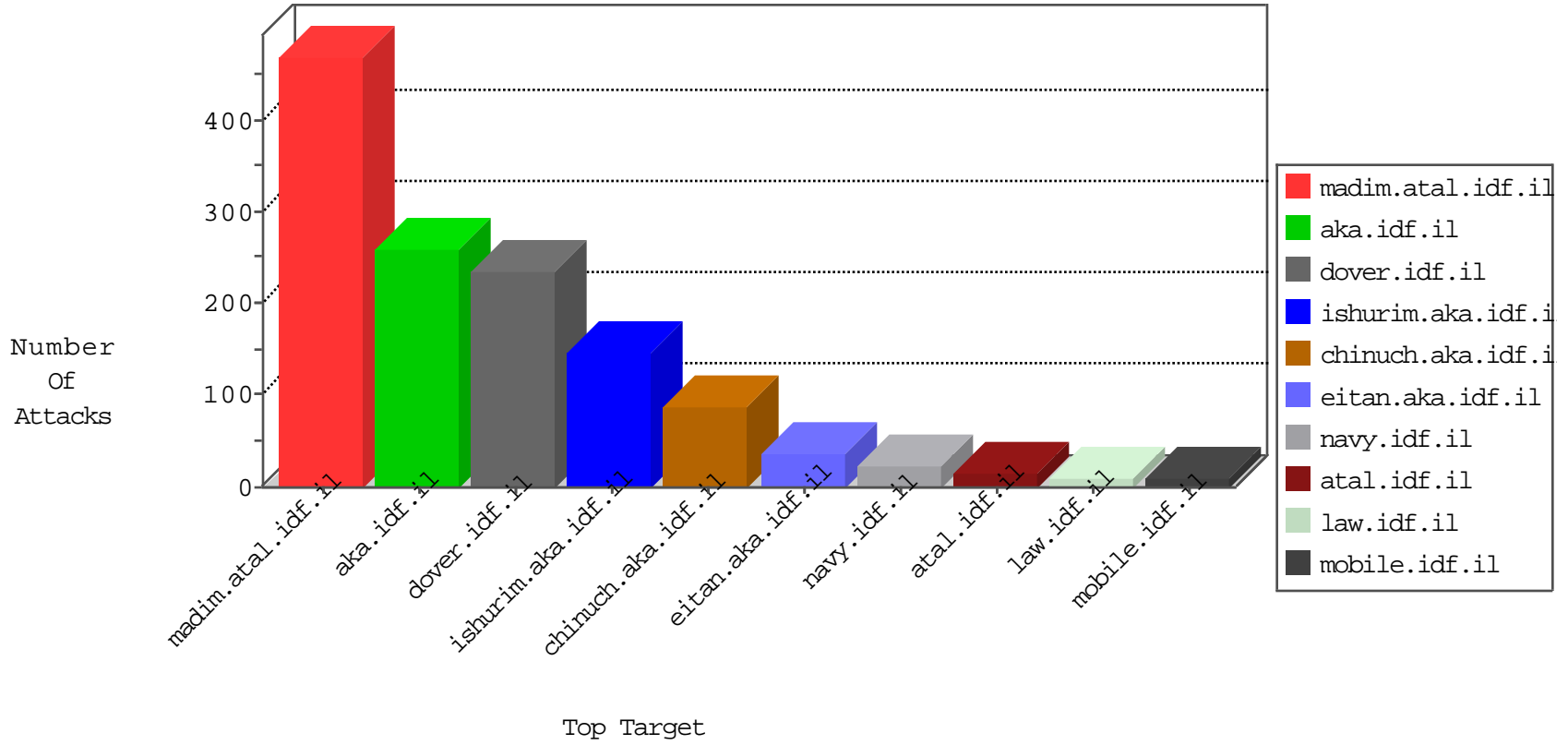


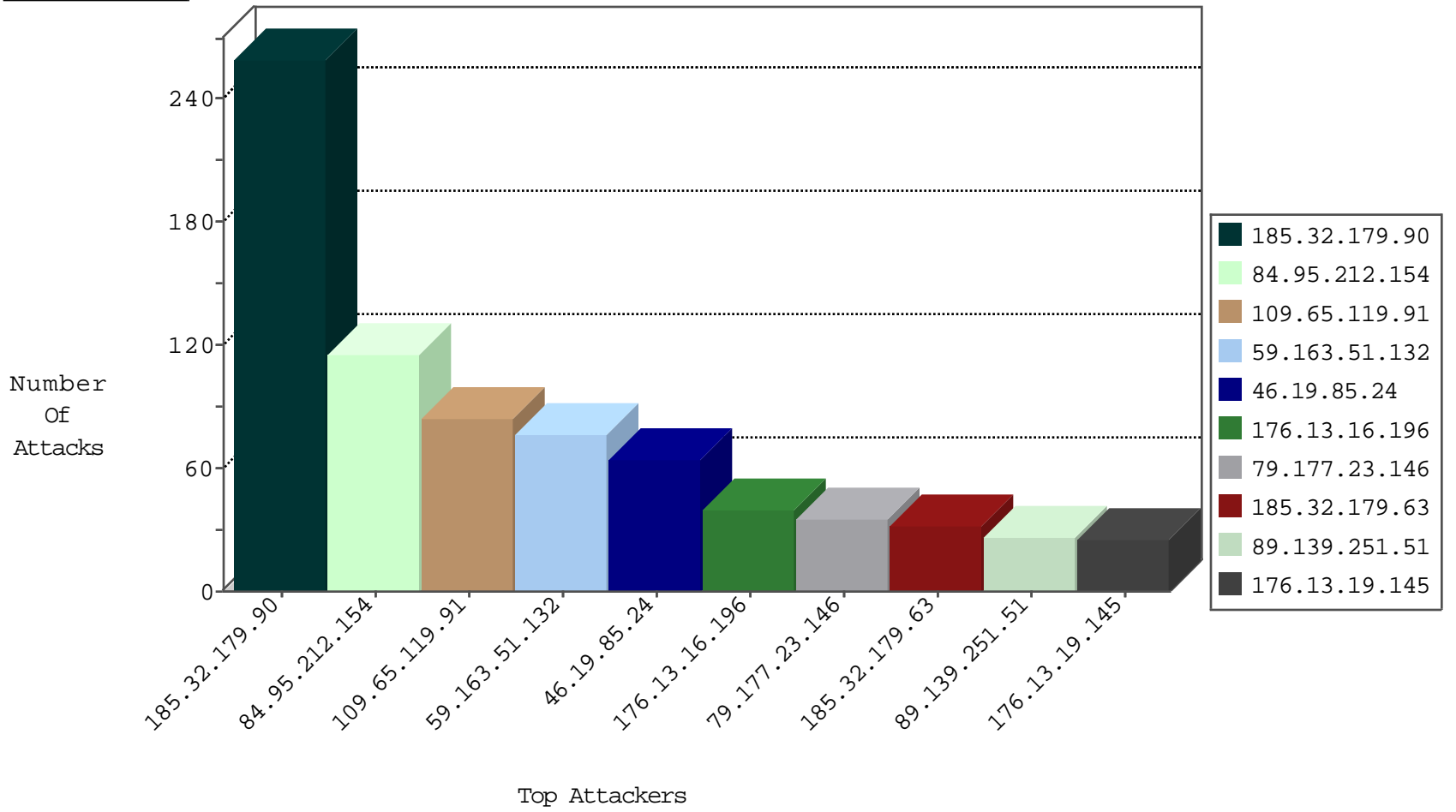
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.23.146	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
109.64.223.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
204.42.253.130	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.130	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.10	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Http	drop	2
61.182.170.38	China	147.237.76.44	e.refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
173.208.206.205	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	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
46.19.86.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.138.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.232.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.13.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.54.96	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.5.14	147.237.77.74	Israel	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.82.79.104	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.37.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
223.4.174.30	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.3.169.108	147.237.0.17	Philippines	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.65.61.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.119.91	Israel	147.237.76.147	chimuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
59.163.51.132	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
89.139.251.51	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
59.163.51.132	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
46.19.85.243	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.86.38	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
59.163.51.132	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
37.26.149.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
59.163.51.132	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
84.94.199.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.251.252	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.239	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.24	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.147.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.168	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
78.41.196.34	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.168	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.28.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.159.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.178.17.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.116.62.151	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.23.146	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.177.23.146	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
79.177.23.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.64.223.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.64.223.69	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
192.114.23.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.24	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.210.165.94	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
37.46.38.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.228.128.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
82.81.40.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.65.3.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.34.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.41.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.168.200.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.34.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.1.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.159.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.26.147.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
171.48.48.250	India	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	3
5.28.151.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.58.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.17.146.185	United Kingdom	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.168.36	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
185.32.179.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	166
84.95.212.154	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 84.95.212.154	Block	114
185.32.179.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
176.13.16.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.85.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
185.32.179.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
176.13.19.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
185.32.179.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	24
185.32.179.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
37.26.148.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
80.246.140.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.146.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.193.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.219.234.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.178.227.165	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
65.55.210.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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
46.19.85.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
17.138.60.14	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	2
176.28.78.48	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation pageNum in www.idf.il/1362-he/dover.aspx	Block	1
46.19.85.69	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$7 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
149.78.231.142	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$116 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
109.66.205.78	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
213.8.204.30	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$35 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
2.54.8.3	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$78 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
85.250.76.45	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$88 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
61.135.190.71	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/shared/clientscripts/sa_swfobject.js	Block	1
46.120.199.19	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$23 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
176.13.6.17	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$47 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
79.182.18.166	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$96 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
66.249.66.126	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
46.19.85.4	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$42 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
5.29.228.250	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$14 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
93.173.248.24	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$58 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
54.198.69.245	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
176.28.78.47	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.94	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.67.188.37	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct138\$ct101\$ct103\$cb1Question\$0 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/	Block	1
213.8.204.30	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$42 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
2.54.26.9	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 2.54.26.9 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
85.250.87.137	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
61.135.190.72	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/reset.css	Block	1
46.121.214.156	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$102 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
46.19.85.4	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$82 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
109.253.199.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$1 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1