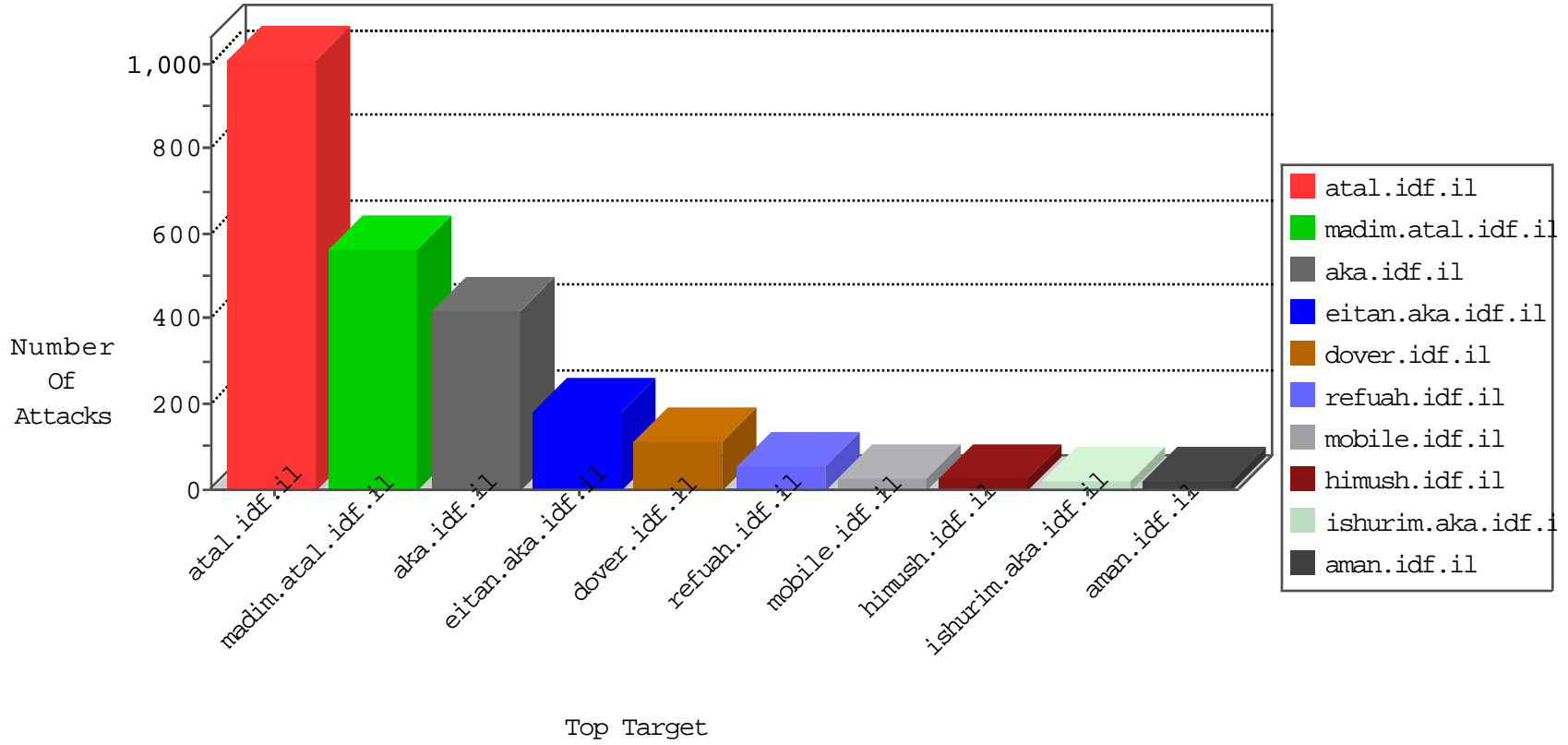


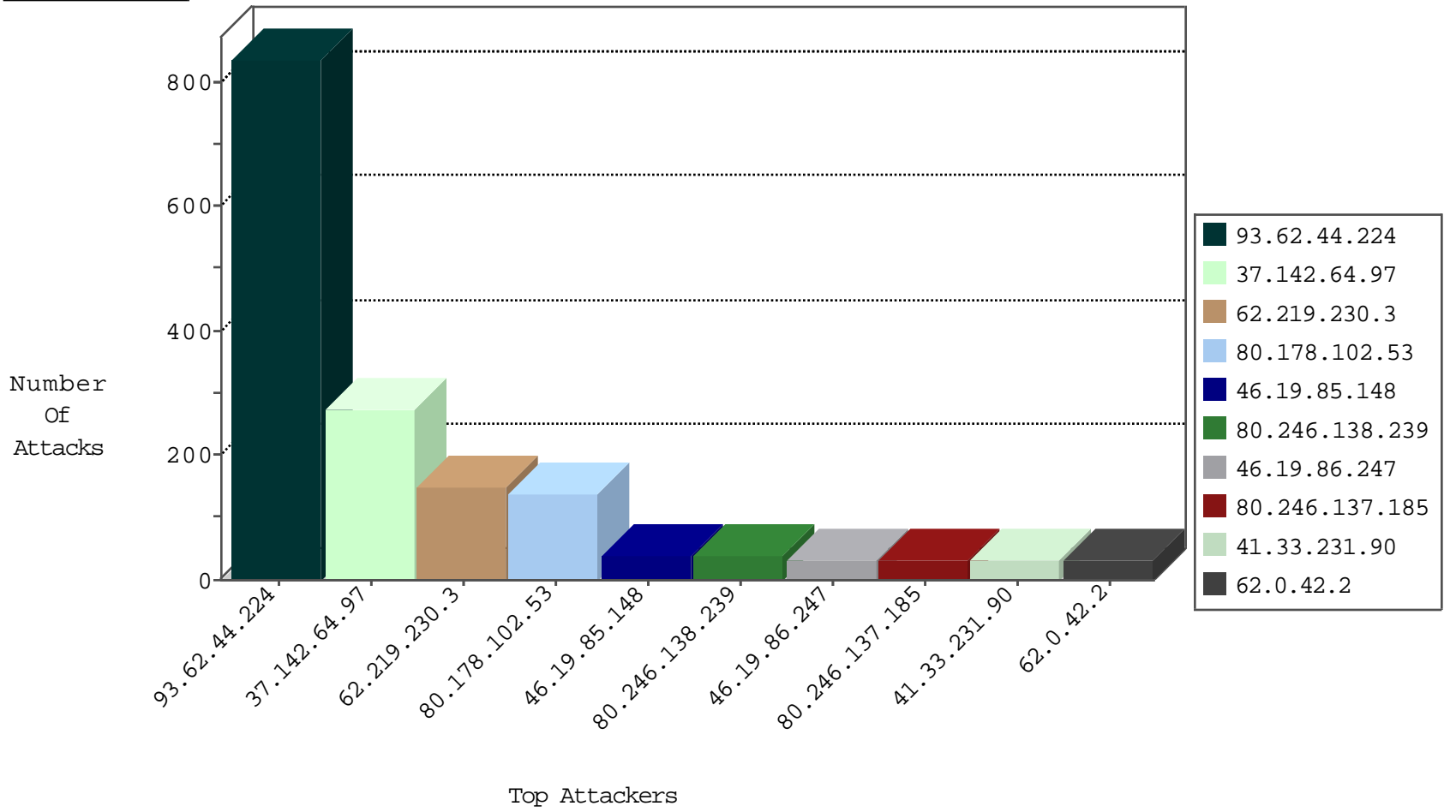
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
5.39.218.13	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
173.208.206.206	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-trafl	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
185.89.217.234	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.23.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.240.237	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.232.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.35.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.187.249.120	147.237.77.227	Europe	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
183.3.202.115	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
89.138.112.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.122.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.151.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.150.245.250	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
93.62.44.224	Italy	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	830
62.219.230.3	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	148
80.178.102.53	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	135
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
62.0.42.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.26.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
192.115.177.202	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
93.173.185.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
46.19.86.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.54.136.9	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
203.171.41.47	New Zealand	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
66.249.81.209	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.249	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.195	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.81.212	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
84.228.166.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.110.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.126.186.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.76.127.44	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.26.147.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.62.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.5.62	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	6
109.253.145.29	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
109.67.172.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.255.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.26.147.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
2.54.146.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.9.125	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.195	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.80.140.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
80.179.9.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.59.8	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
115.230.124.164	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
176.13.22.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.139.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.147.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.1.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.43		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
62.219.135.78	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
37.142.64.97	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.64.97	Block	156
37.142.64.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
46.19.85.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
80.246.138.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.86.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
80.246.137.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.54.2.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
2.52.4.52	Israel	147.237.76.30	himush.idf.il	Multiple Unauthorized URL Access from 2.52.4.52	Block	21
176.13.12.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
37.26.149.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
185.32.176.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
80.246.136.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
80.246.136.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
176.13.21.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.137.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.65.165.119	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.165.119	Block	5
37.142.64.97	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 37.142.64.97	Block	4
109.253.145.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.180.7.93	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	4
80.246.138.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.2.209	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.117.2.209	Block	3
2.54.163.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.4.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.7.93	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	3
213.57.73.109	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$85 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	3
157.55.39.94	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.5.48	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$61 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
109.226.60.36	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$96 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
2.54.157.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
37.26.149.128	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$67 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
5.29.192.6	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
80.246.136.64	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$4 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
109.253.215.111	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
84.109.231.10	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	2
46.116.169.165	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.117	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
46.19.85.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.146.233	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
93.62.44.224	Italy	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/usercontrols/headerupper/	Block	1
46.19.85.113	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$7 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
84.111.162.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$67 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.54.156.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$95 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
80.178.102.53	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/xžx?x™ x" x@x-xžx•xÿ.aspx	Block	1
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$42 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
217.132.128.28	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$14 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.54.30.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$60 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.177.173.4	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$3 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1