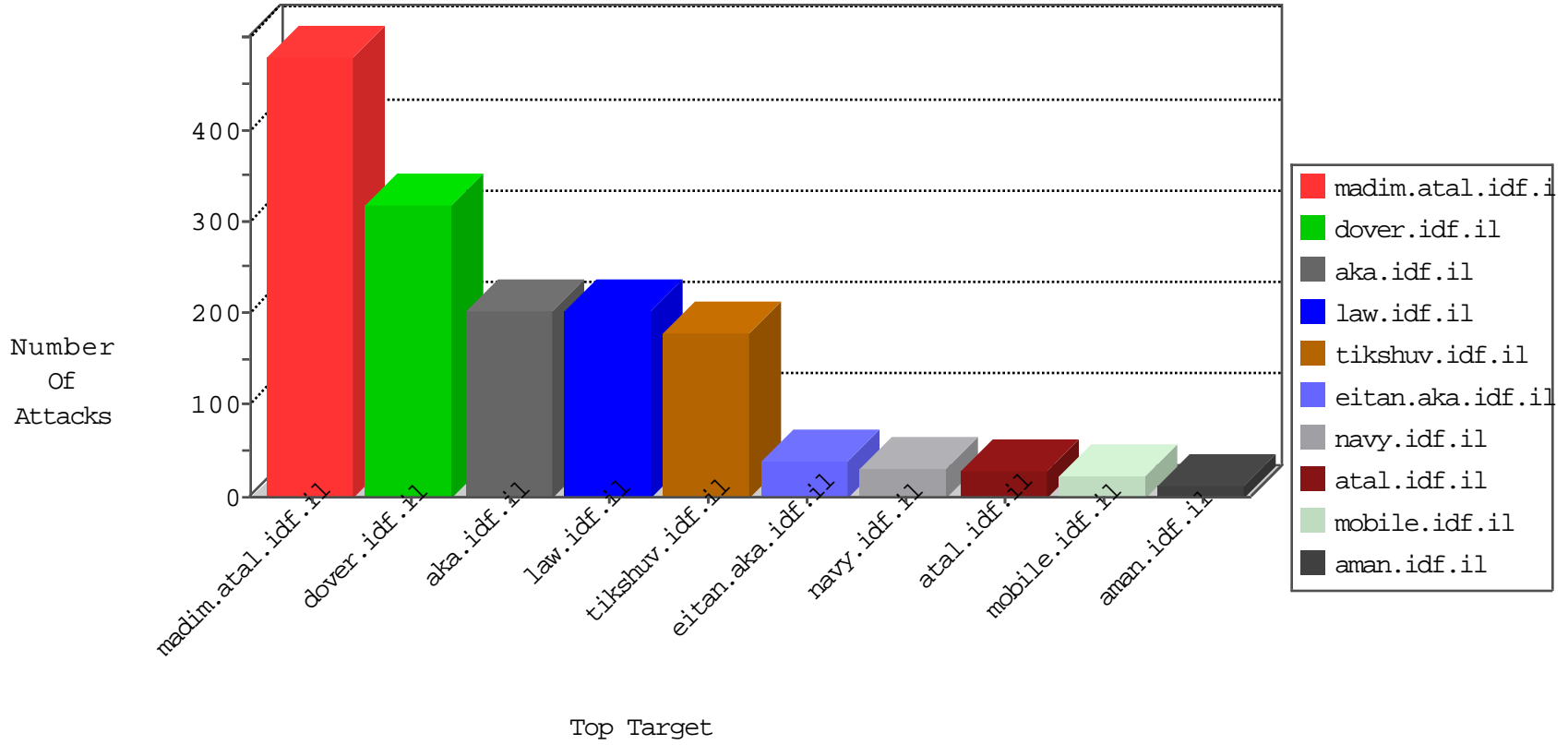


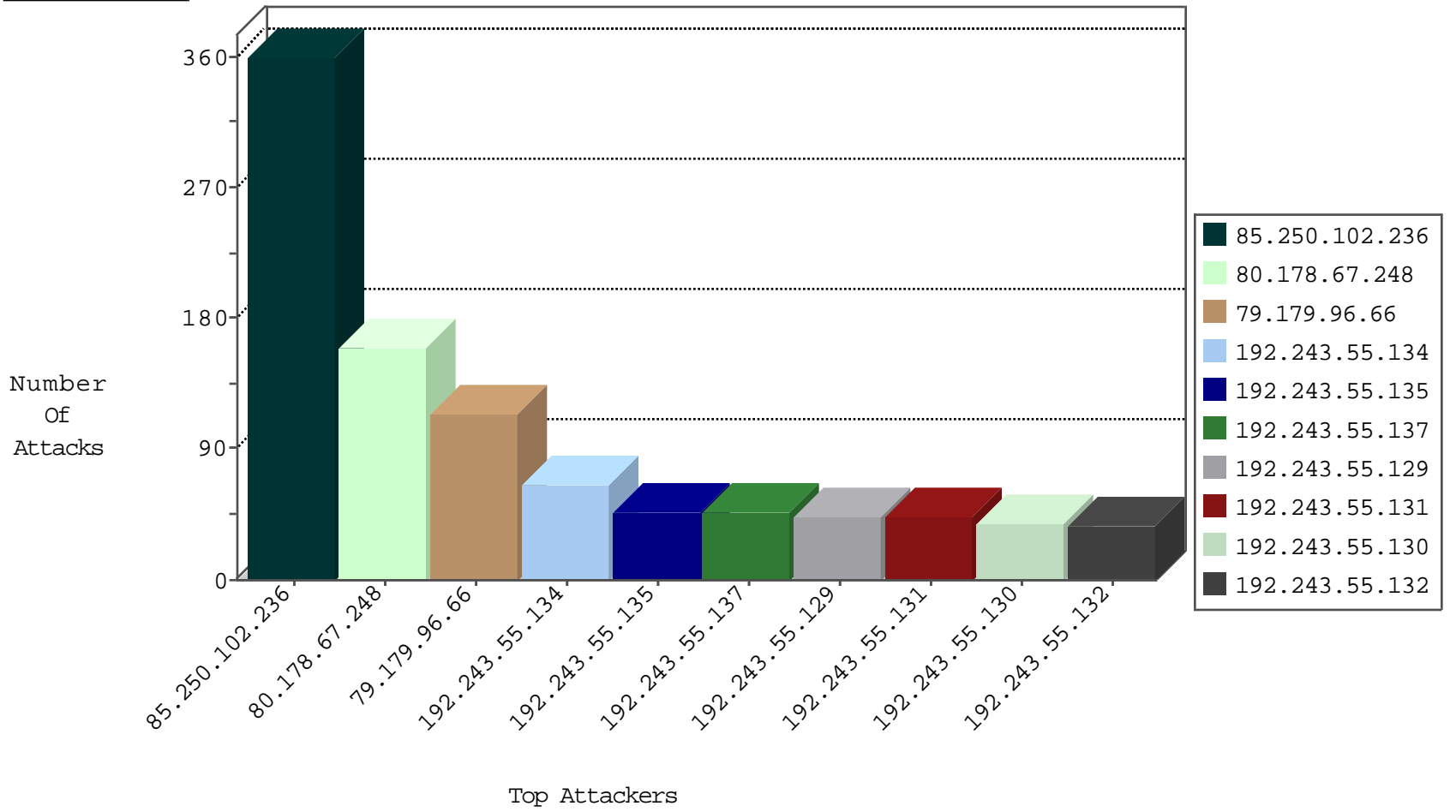
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.243.55.130	Dominica	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3098
72.9.148.10	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3068
192.243.55.137	Dominica	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	278
79.183.13.52	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	63
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
1.84.95.1	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
91.74.15.183	United Arab Emirates	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
117.62.180.162	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
91.74.15.183	United Arab Emirates	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.178.67.248	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	19
5.22.135.102	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	11
46.19.85.43	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
157.55.39.216	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
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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
109.253.205.234	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
98.119.105.221	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.11	147.237.72.14	Romania	dover.idf.il(old	ET SCAN NMAP -sS window 1024	1
80.246.133.103	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
27.106.40.185	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -sS window 2048	1
201.232.25.160	147.237.77.176	Colombia	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
179.43.141.234	147.237.0.34	Switzerland	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.113	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
27.106.40.185	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -sS window 4096	1
27.106.40.185	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.0.19	China	madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.178.67.248	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	140
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
89.139.152.192	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
77.12.38.224	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
77.12.38.224	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.176.22.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
109.253.205.234	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.182.56.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.22.130.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
109.253.205.234	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
85.64.59.244	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.132	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.129	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.176.137.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.253.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.129	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.141.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.177.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.135	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.135.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
85.250.102.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.129	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.134	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.102.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	186
85.250.102.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
79.179.96.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
85.250.102.236	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 85.250.102.236	Block	60
79.179.96.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	4
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
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.246.136.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.11.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.125	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	3
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	2
79.183.12.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
180.76.15.12	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
5.135.127.168	Portugal	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
149.78.171.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.78.171.41	Block	1
80.246.139.53	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl38\$ct101\$ct103\$cblQuestion\$1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
185.3.144.102	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy.	Block	1
17.138.56.26	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
149.78.253.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/	Block	1
84.94.74.41	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/history/stm	Block	1
85.250.102.236	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
149.88.54.76	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$36 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
84.109.101.163	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
79.177.177.172	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/band	Block	1
123.125.71.72	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.246.136.125	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 80.246.136.125	Block	1
207.46.13.193	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/327-he/patzar.aspx?pagenum=2	Block	1
5.22.129.101	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.212.122.160	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
46.116.31.145	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1