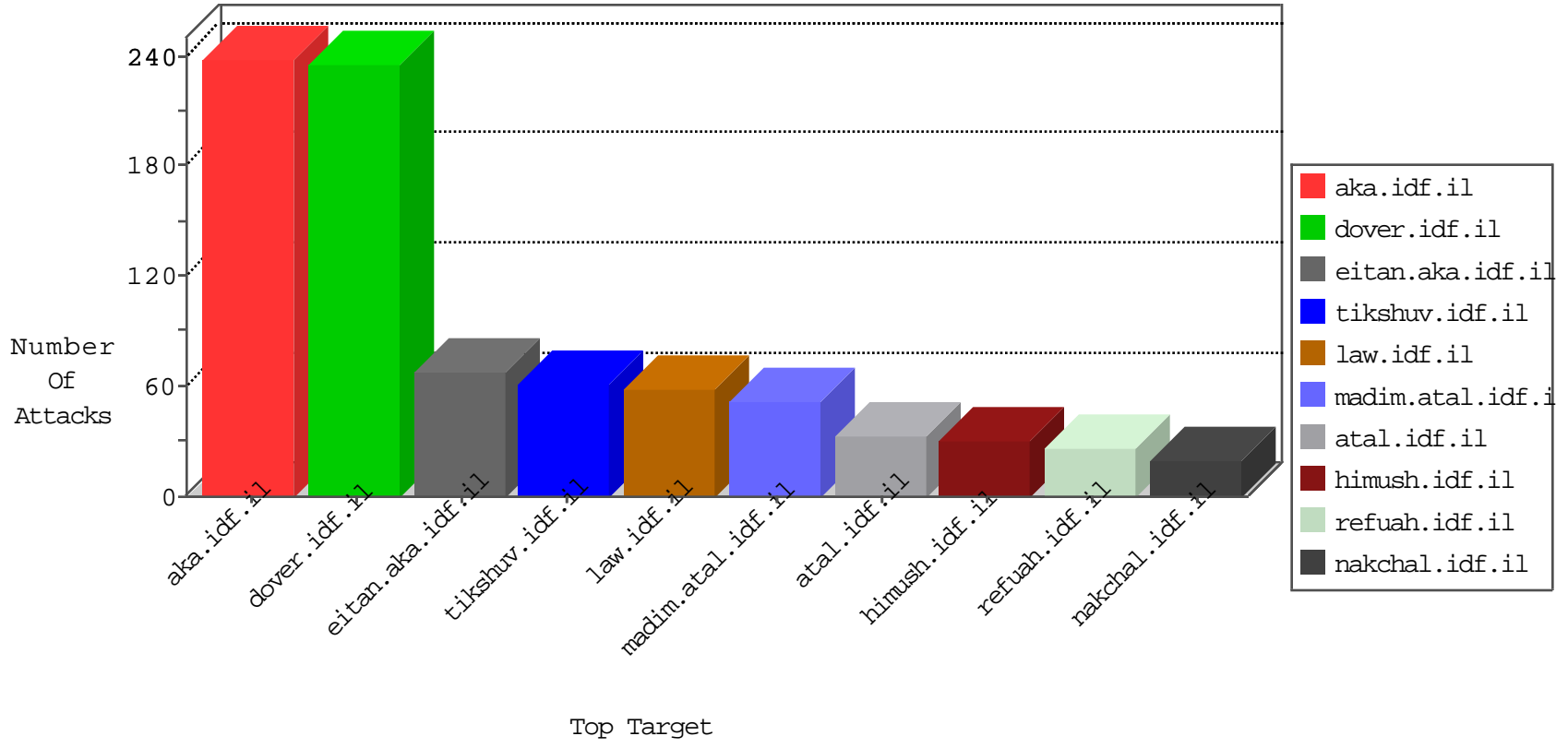


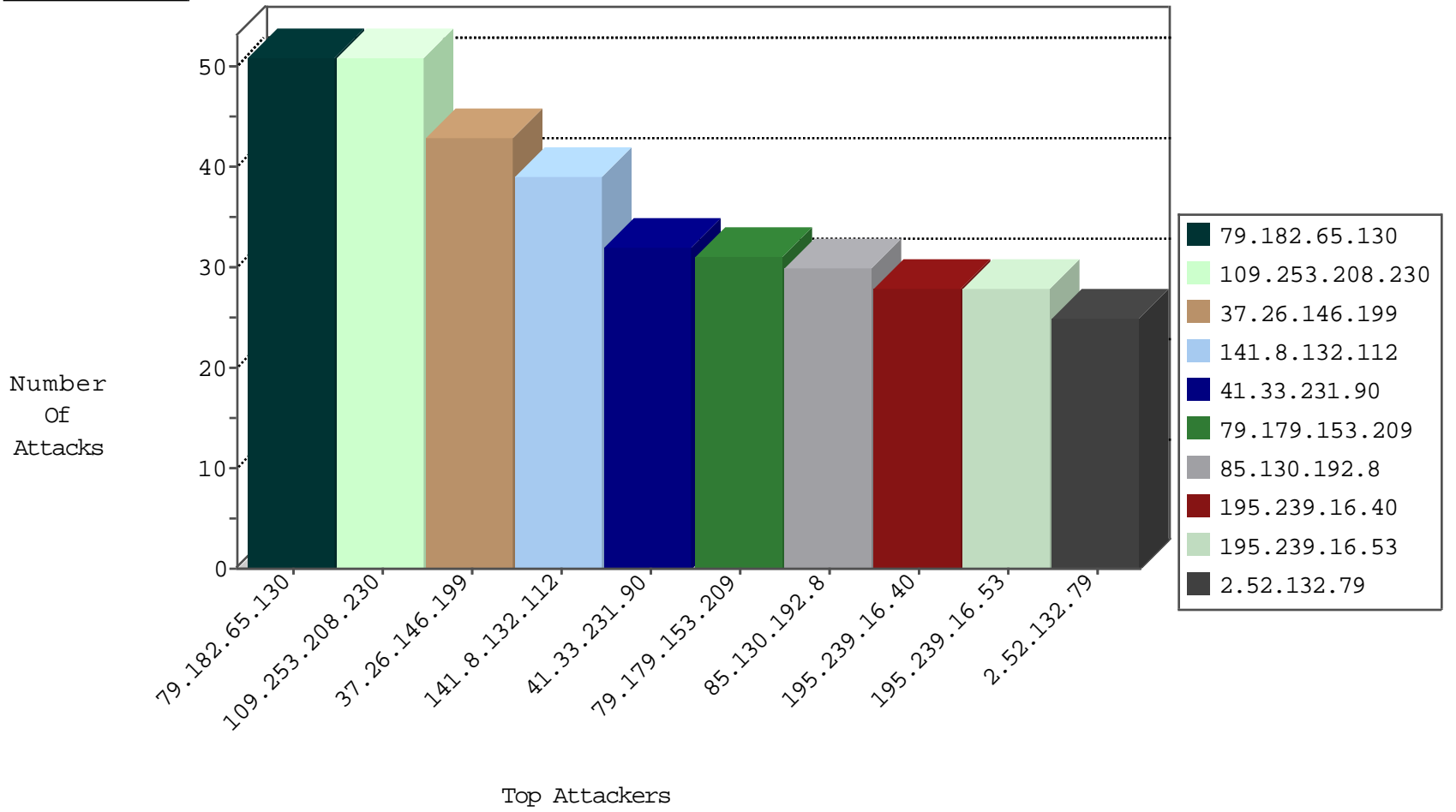
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.148.100.2	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
159.122.252.41	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
37.59.28.127	France	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
75.112.11.74	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.185.192.77	147.237.72.166	Brazil	aka.idf.il	SQL Injection - Select From	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
59.46.193.114	147.237.76.176	China	test.ncoore.idf.il	GPL SCAN nmap TCP	2
66.249.66.15	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
218.24.171.223	147.237.76.176	China	test.ncoore.idf.il	GPL SCAN nmap TCP	2
218.246.0.97	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.240	147.237.72.14		dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
185.130.5.240	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.208.230	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
79.179.153.209	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
77.125.151.45	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
95.86.77.89	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.86.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.86.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.19.85.47	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
85.130.192.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
85.130.192.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
85.130.192.8	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.52.132.79	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
31.210.186.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.172	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.64.39.60	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
66.249.79.12	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.114.34	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
31.168.114.34	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.172	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.76.127.219	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.86.85	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.168.123.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.79.9	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.64.39.60	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.132.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.52.132.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
31.210.187.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.187.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.131.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.121.136.131	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.52.132.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.120.153.130	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
212.76.127.111	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
176.13.21.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.186.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
141.8.132.70	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.188	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
79.182.65.130	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
37.26.146.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
46.19.86.34	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 46.19.86.34	Block	14
138.162.128.52	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
2.52.28.187	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.52.28.187	Block	4
95.86.109.96	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	3
84.108.174.136	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.174.136	Block	3
37.26.146.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.208.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.109.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/d	Block	2
199.30.24.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.52.28.187	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	2
185.32.179.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.174.136	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
80.246.130.42	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.9.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$23 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
117.78.13.54	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.66.39	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
46.19.85.180	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$60 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
84.108.172.211	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.108.172.211	Block	1
149.78.90.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$83 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.178.188.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$76 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.116.140.238	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$96 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.253.206.196	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$7 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
84.228.218.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.136.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
180.76.15.14	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
95.86.109.96	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 95.86.109.96	Block	1
207.46.13.25	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
84.108.172.211	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ajax/updatestatus.php	Block	1
79.179.153.209	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
149.78.90.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$96 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.121.113.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$78 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.253.206.196	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$71 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
85.65.233.233	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$100 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.52.38.230	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$83 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
82.166.20.236	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$117 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
180.76.15.29	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1073-he/nakhal.aspx	Block	1
138.162.128.53	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
46.19.86.34	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/1115-he/nakhal.asp	Block	1
212.179.243.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$75 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.180.63.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.172	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
62.210.181.15	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13885-en	Block	1
109.253.206.196	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$74 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
89.100.153.204	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1

02-16-2016-23:04:07 to 02-17-2016-00:04:07

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.126.3	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$85 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
144.76.71.83	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/newsite/english/main.asp	Block	1

02-16-2016-23:04:07 to 02-17-2016-00:04:07