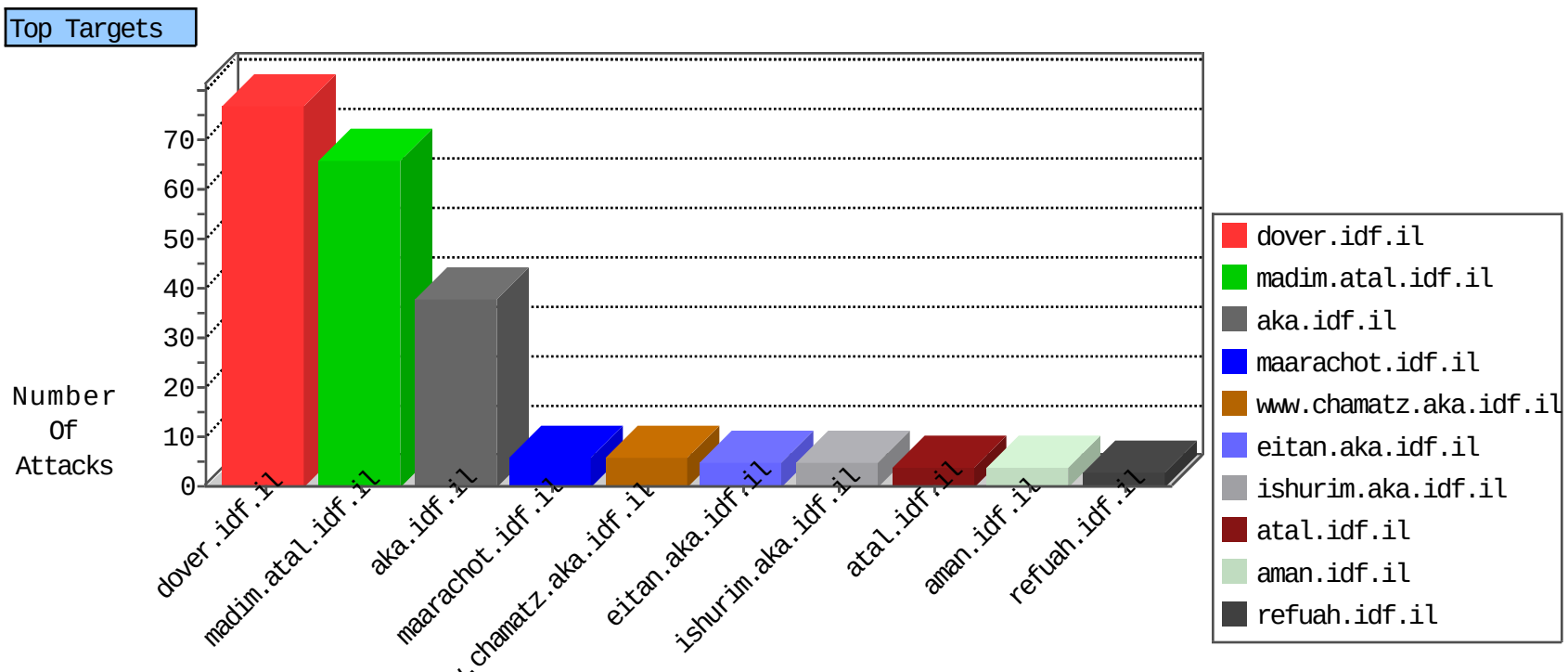
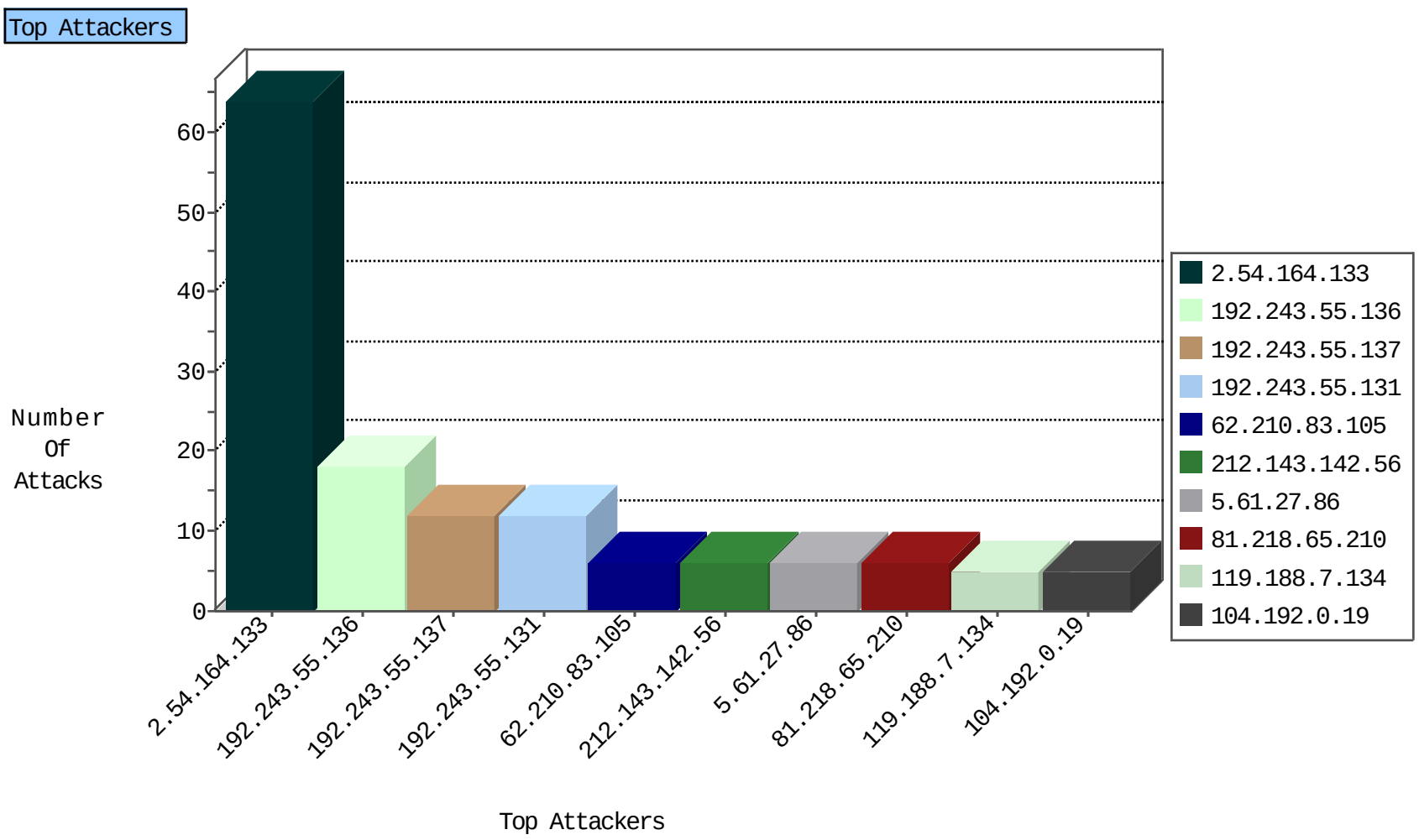
03-05-2016-07:04:05 to 03-05-2016-08:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-05-2016-07:04:05 to 03-05-2016-08:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
185.94.111.1		147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.67	United States	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
162.216.114.158	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.119	United States	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.67	United States	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.67	United States	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
209.126.122.102	United States	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1

03-05-2016-07:04:05 to 03-05-2016-08:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.104.37.122	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
188.165.214.26	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
192.168.1.159		147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
175.9.139.65	China	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

03-05-2016-07:04:05 to 03-05-2016-08:04:05

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
66.102.9.17	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
96.45.10.173	147.237.0.19	Canada	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
189.202.241.84	147.237.77.226	Mexico	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.114	147.237.77.212	Ukraine	e.dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
119.188.7.134	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
119.188.7.134	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
45.32.182.189	147.237.0.33		idf.il	ET SCAN Potential SSH Scan	1
119.188.7.134	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.20	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.192.0.19	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.192.0.19	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.19	147.237.72.156	United States	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.201.227.63	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
189.202.241.84	147.237.77.226	Mexico	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
119.188.7.134	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
45.32.182.189	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
119.188.7.134	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
45.32.182.189	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.20	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.192.0.20	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.192.0.19	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.192.0.19	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

03-05-2016-07:04:05 to 03-05-2016-08:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.164.133	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.136	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	6
62.210.83.105	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
131.253.25.206	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.253.140.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
82.81.75.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.102.6.243	United States	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	3
207.46.13.111	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
37.142.68.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.133.169.17	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
76.167.195.171	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.121.136.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.116	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.8.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
94.230.86.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.20	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.32.179.106	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.102.242.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.71	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.237.138.202	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
46.121.136.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.139.116	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.55	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.71	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.239.102	Russian Federation	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
213.57.161.22	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.116	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.63.105.85	Germany	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
74.208.69.220	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.100	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.239.102	Russian Federation	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
220.181.108.184	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.64.88.197	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.231	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

03-05-2016-07:04:05 to 03-05-2016-08:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.164.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
5.61.27.86	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.61.27.86	Block	5
207.241.229.33	United States	147.237.72.166	aka.idf.il	Unknown Parameter moduletogo in aka.idf.il/main/miluim/login.aspx	None	1
77.237.138.202	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
203.133.168.70	Korea, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
66.249.64.56	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/scroller/jquery.jcarousel.js	Block	1
207.241.229.215	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.61.27.86	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
207.46.13.70	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
66.249.69.81	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1273-he/atal.aspx	Block	1
207.241.237.227	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
178.33.39.74	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
40.77.167.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/events/events.aspx	Block	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.69.97	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1
213.57.39.74	Israel	147.237.76.39	mobile.meitav.idf.il	SSL Untraceable Connection - Open Mode	None	1
185.89.101.191		147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
46.117.196.79	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl23 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
207.46.13.111	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/gen...px	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18863-en/dover.aspx.	Block	1
66.249.64.51	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/expand.js	Block	1

03-05-2016-07:04:05 to 03-05-2016-08:04:05