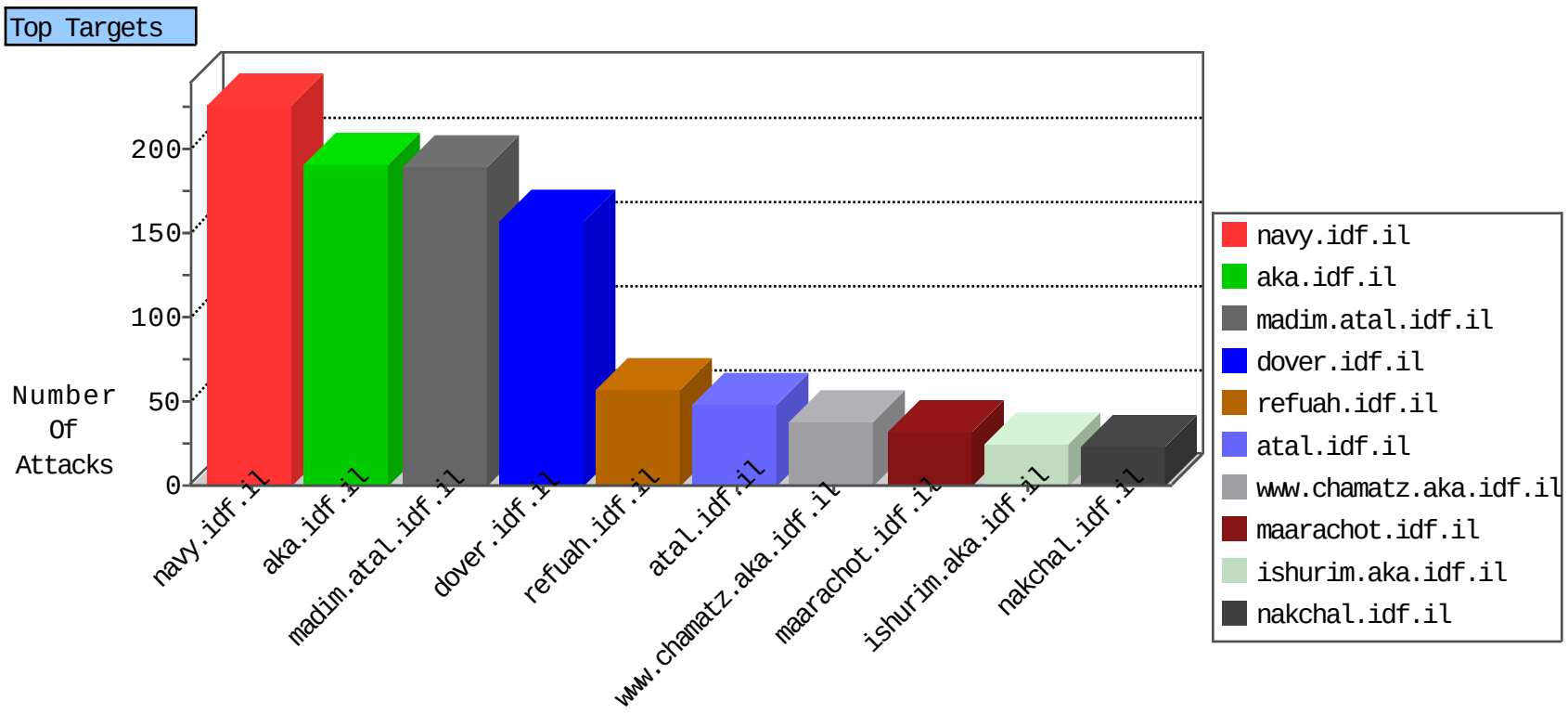
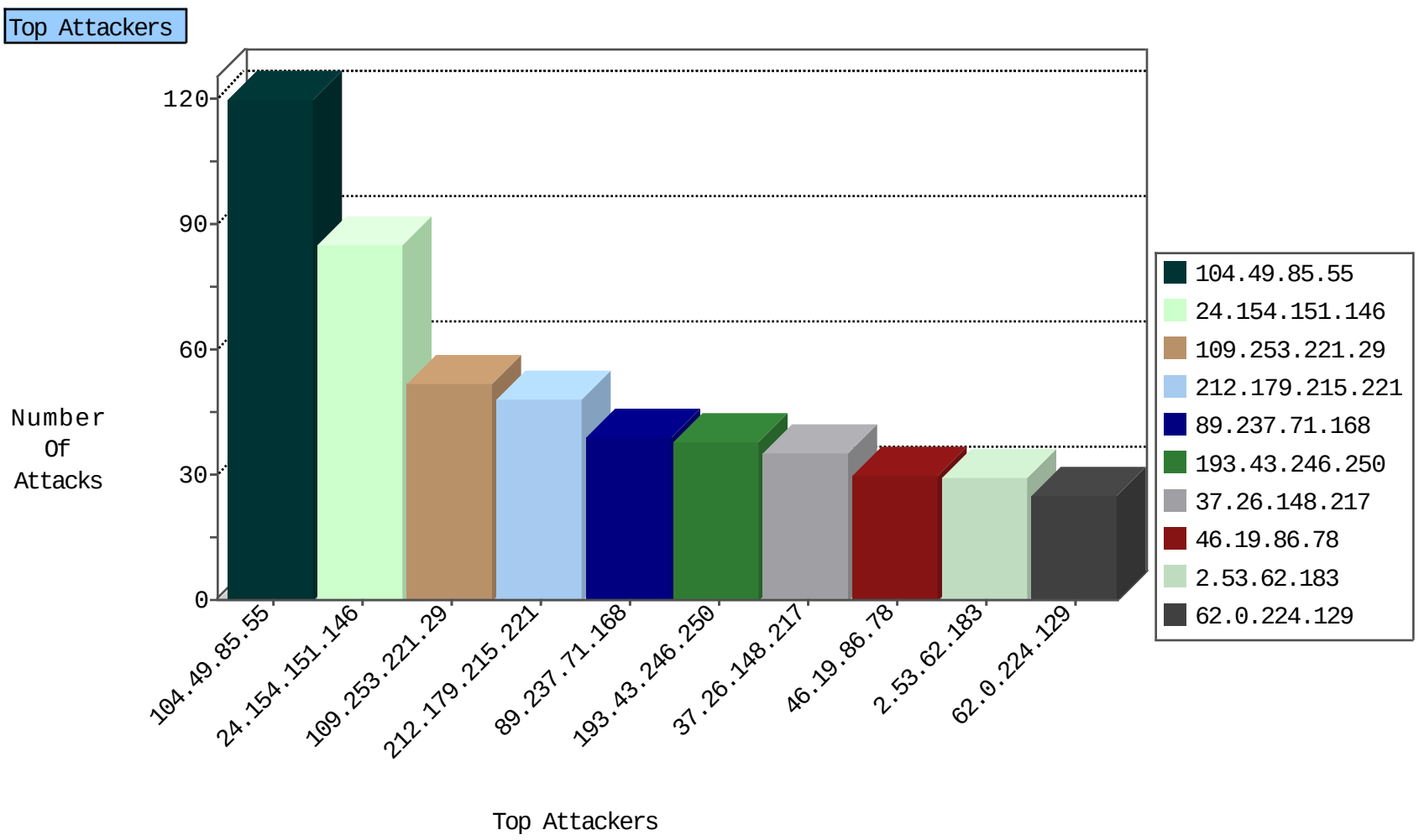
09-05-2016-09:04:04 to 09-05-2016-10:04:04

IDF Under Attack Daily Report





09-05-2016-09:04:04 to 09-05-2016-10:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.205.114.106	Iraq	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4

09-05-2016-09:04:04 to 09-05-2016-10:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.95.106	Netherlands	147.237.72.167	ishurim.aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
109.205.114.106	Iraq	147.237.77.216	dover.idf.il	10767: HTTP: Acunetix Security Scanner	Block	1

09-05-2016-09:04:04 to 09-05-2016-10:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.80.193.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
64.137.171.55	147.237.77.19	Canada	law-forum.idf.il	ET SCAN Potential SSH Scan	1
46.116.27.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
85.65.237.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.112.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.172.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.54.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.227.67.172	147.237.77.226	Sweden	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.166.131.142	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
87.68.10.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.88.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.95.193.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-05-2016-09:04:04 to 09-05-2016-10:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
104.49.85.55	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	116
24.154.151.146	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	85
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
89.237.71.168	France	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	27
62.0.224.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
50.245.216.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
80.246.133.92	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
62.0.227.9	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
2.55.152.96	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
82.163.70.201	United Kingdom	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
212.179.215.221	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
212.179.215.221	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
213.8.110.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
37.26.148.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	8
212.25.103.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
37.26.148.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
89.237.71.168	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.167	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
37.26.148.217	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.167	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.201	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.179.215.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.179.215.221	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
212.179.215.221	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.230	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.135.4	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.143	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.230	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.165.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
80.246.138.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.152.96	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
195.46.23.74	Greece	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.55.152.96	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
89.237.71.168	France	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
84.94.191.117	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.136.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
122.170.189.57	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.6.115	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
185.120.126.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
212.179.215.221	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.158	Europe	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.133.3	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.221	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
185.27.106.182	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
147.236.38.29	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
85.130.242.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

09-05-2016-09:04:04 to 09-05-2016-10:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.221.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
2.53.62.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.86.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
2.53.189.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
2.53.15.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
37.26.148.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
176.13.231.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
93.172.151.103	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	6
212.143.187.162	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	5
77.139.80.115	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.80.115	Block	4
2.55.154.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.173.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.50.10	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
46.19.86.78	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	3
109.253.145.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.143.187.162	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.143.187.162	Block	3
89.139.33.170	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.139.33.170	Block	3
46.19.86.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.130.139	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.55.188.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.55.0.62	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
212.117.140.170	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
80.246.139.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.80.115	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	2
2.53.132.51	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.205.114.106	Iraq	147.237.77.216	dover.idf.il	Malformed URL www.acunetix.wvs:443	Block	1
66.249.69.93	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/602-4730-he/patzar.aspx	Block	1
89.139.33.170	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	1
77.124.247.188	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
50.245.216.33	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/social/undefined	Block	1
203.127.96.198	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.205.114.106	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/j_security_check	Block	1
2.55.175.14	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
80.246.133.92	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.69.97	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/938-4500-he/patzar.aspx	Block	1
89.237.105.158	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
77.138.57.9	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
207.46.13.32	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
2.53.29.147	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
80.246.138.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.57.63.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
46.19.86.140	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
185.3.147.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/scroller/skin.css	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9269-he/dover.aspx	Block	1
190.102.56.100	Panama	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1

09-05-2016-09:04:04 to 09-05-2016-10:04:04