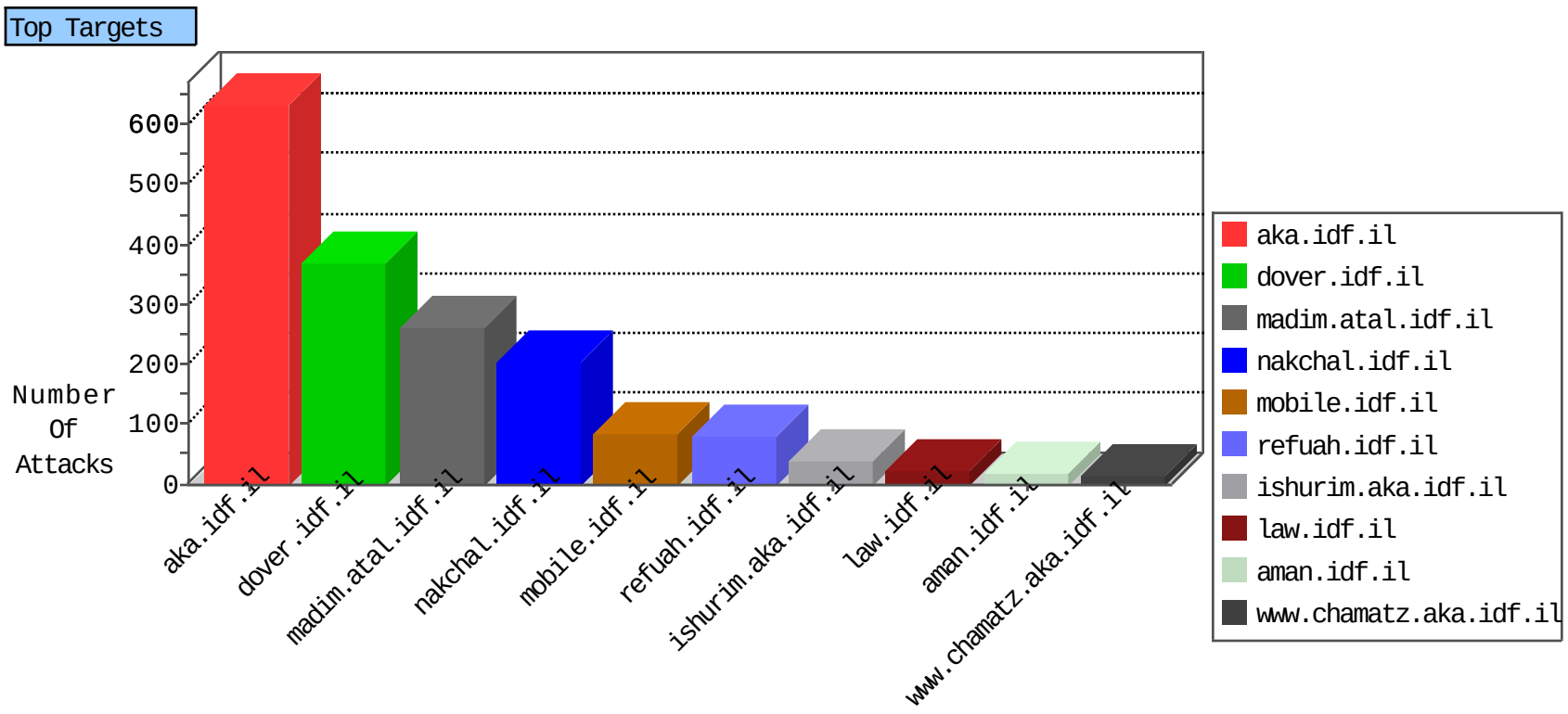
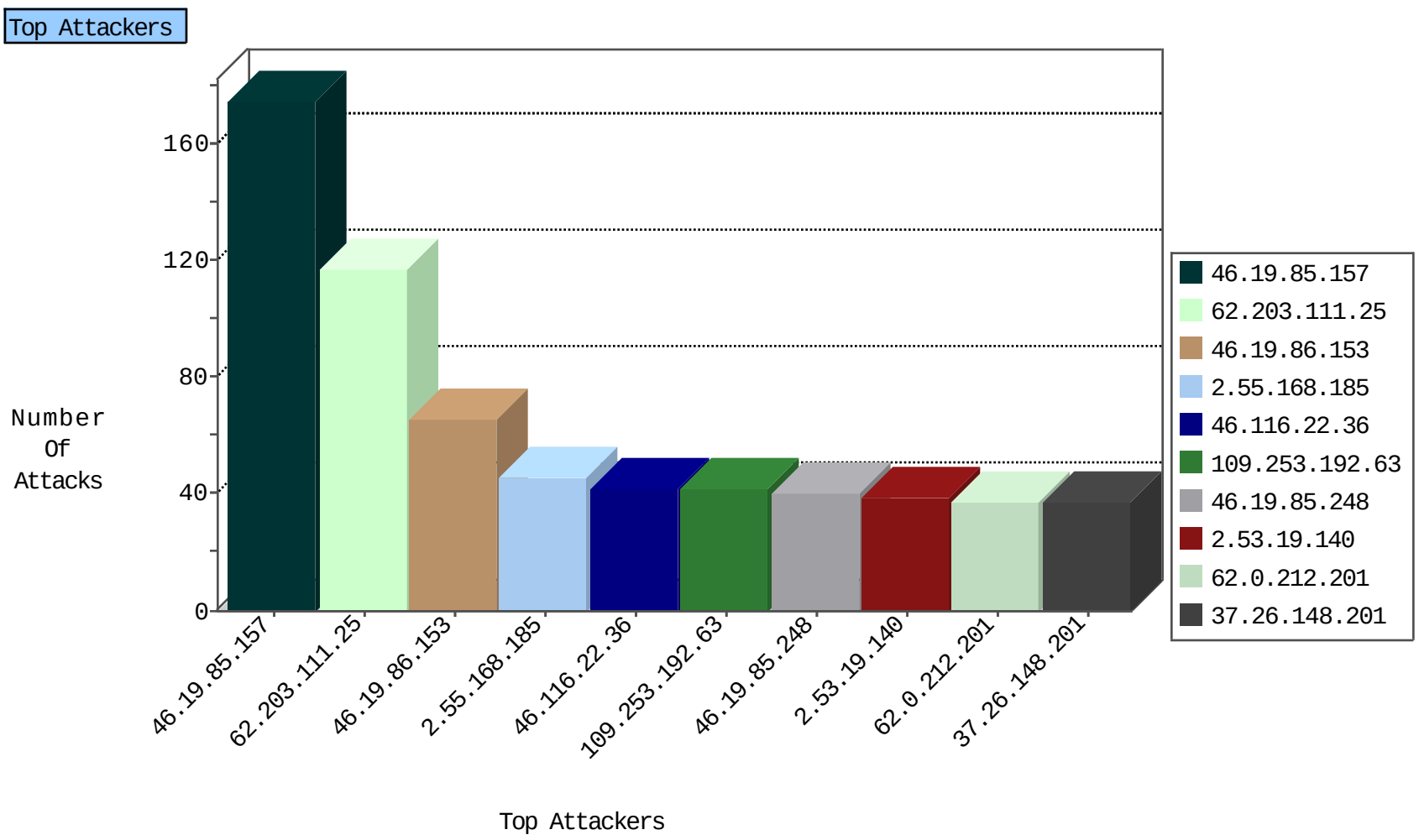
09-28-2016-18:04:01 to 09-28-2016-19:04:01

IDF Under Attack
Daily Report





09-28-2016-18:04:01 to 09-28-2016-19:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.48.249	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	122

09-28-2016-18:04:01 to 09-28-2016-19:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.97.22	France	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	1

09-28-2016-18:04:01 to 09-28-2016-19:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.180.23.224	147.237.0.34	Israel	tikshuv.idf.i	ET SCAN NMAP -sA (2)	6
217.132.155.5	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
103.234.209.93	147.237.76.34	Indonesia	yohalan.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
71.15.85.176	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
46.120.132.241	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	1
23.91.75.231	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.77.212	United Kingdom	e.dover.idf.i	ET SCAN NMAP -sS window 1024	1
80.246.133.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.17.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.76.106	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
46.19.86.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.157.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-28-2016-18:04:01 to 09-28-2016-19:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.19.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
100.92.64.37		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	26
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
46.19.86.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	25
213.57.48.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
62.0.212.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	22
46.116.22.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
46.116.22.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	21
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	18
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
46.19.86.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.83	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.86.162	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
2.55.144.102	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.86.179	Israel	147.237.76.31	nakchal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
62.0.212.201	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
176.13.249.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.83	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
109.253.213.212	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.178.17.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.178.17.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.86.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
109.253.192.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
217.132.58.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
85.64.160.172	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
185.86.201.55	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.192.63	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.59.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.253.147.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.179	Israel	147.237.76.31	nakchal.idf.i	Bad TCP sequence	Invalid ACK number	alert	6
31.168.97.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.192.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.162	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.26.148.238	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.53.187.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.192.63	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	6
79.178.226.56	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
112.124.124.227	China	147.237.76.31	nakchal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
77.125.1.0	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
213.8.204.40	Israel	147.237.0.34	tikshuv.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5

09-28-2016-18:04:01 to 09-28-2016-19:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	175
2.55.168.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
79.181.230.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
84.108.65.217	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.65.217	Block	16
2.53.164.33	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	15
109.67.185.36	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.67.185.36	Block	8
46.117.47.249	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.117.47.249	Block	5
93.172.152.94	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/2/71772.pdf	Block	4
79.178.76.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	4
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	4
109.65.138.229	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.65.138.229	Block	3
176.13.14.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.213.212	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
31.168.104.92	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
109.253.136.168	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/2/71772.pdf	Block	2
46.19.86.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.143.112	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	2
109.65.194.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.202.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.211.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/2/71772.pdf	Block	2
99.31.227.98	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	2
46.120.55.85	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.55.85	Block	2
213.151.35.221	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/faq.aspx	Block	2
77.138.104.132	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
2.53.9.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.216.32	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
84.108.89.161	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.120.55.85	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus/general.aspx	Block	1
213.151.38.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/site/templates/controller.asp	Block	1
176.13.12.156	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
77.139.78.242	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/megurim/	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/70123.doc	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
185.120.126.16	Israel	147.237.72.166	aka.idf.il	Unknown Parameter asm in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
80.178.191.251	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 80.178.191.251	Block	1
141.0.15.142	Norway	147.237.72.166	aka.idf.il	Unknown Parameter utm_source in www.aka.idf.il/main/giyus/	None	1
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
84.229.79.133	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
46.210.169.217	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl58.y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
37.26.146.229	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
68.132.133.66	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 66.102.9.8	Block	1
93.172.216.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/2/71772.pdf	Block	1
80.178.191.251	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
77.138.197.196	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/booklets.aspx	Block	1
141.226.217.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip	Block	1
109.67.185.36	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storag	Block	1
66.249.69.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9628-he/refuah.aspx	Block	1
85.64.111.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-28-2016-18:04:01 to 09-28-2016-19:04:01