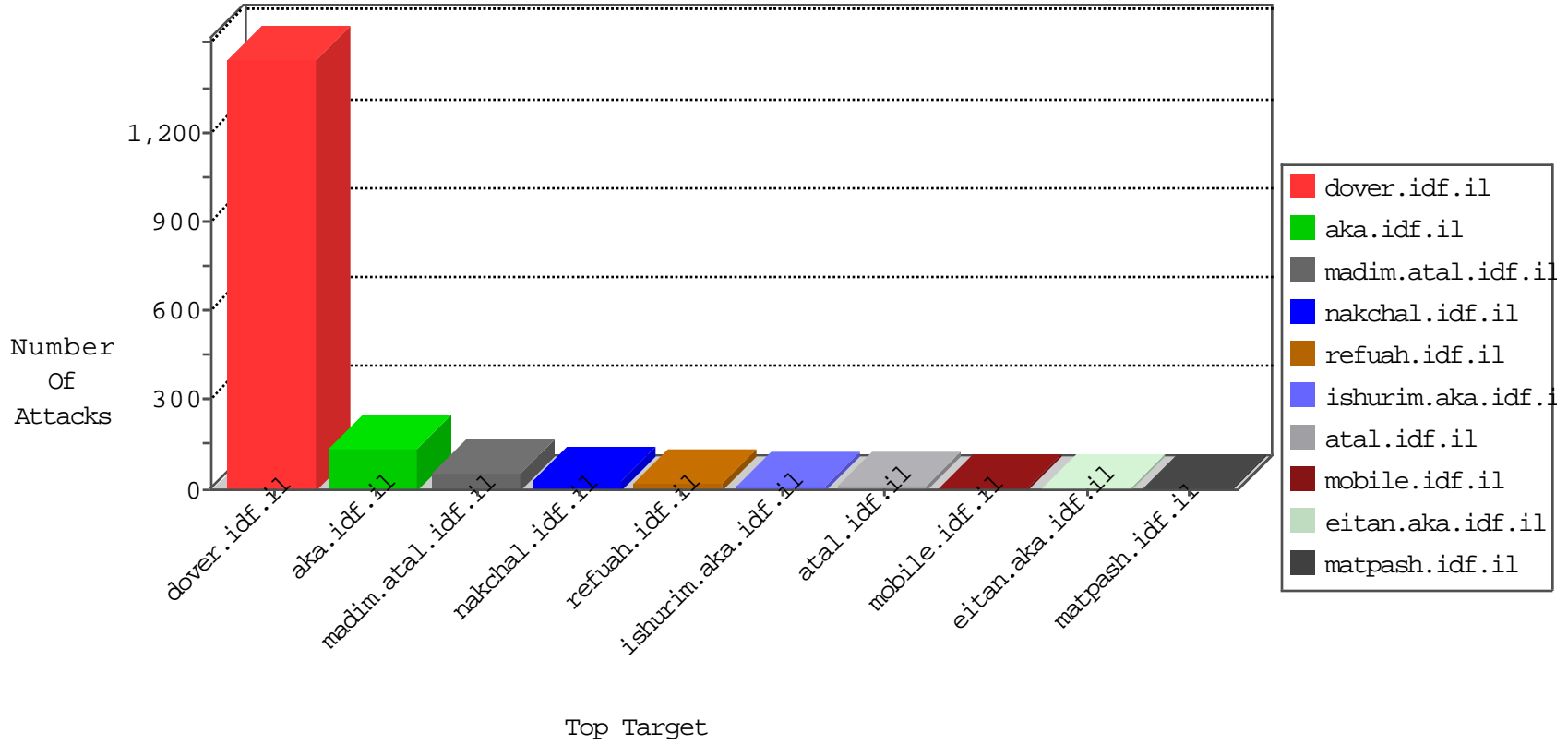


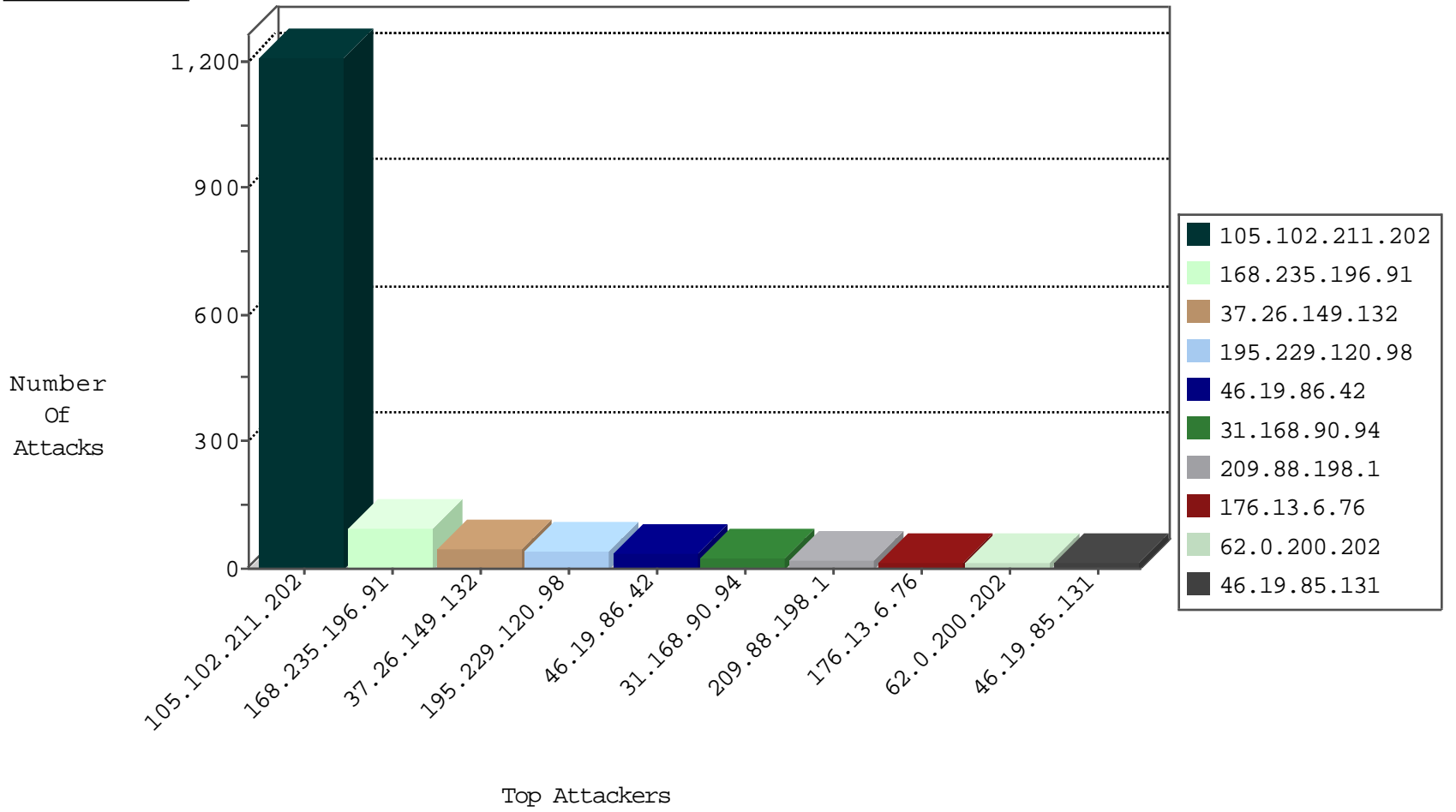
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.2.99	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	27
168.235.196.91	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
212.25.74.130	Israel	147.237.77.216	dover.idf.il	Black List	drop	3
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.112	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.14	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.226	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.62.53.168	Russian Federation	147.237.77.176	matpash.idf.il	block-sp-trafl	forward	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.131.246	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.254.131.246	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.162.105.152	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.93.66	147.237.76.42	Europe	refuah.idf.il	ET SCAN NMAP -sA (2)	1
58.220.2.5	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.4.85.112	147.237.76.198	Germany	e.yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
195.70.44.28	147.237.77.61	Hungary	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
164.52.227.101	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.160.155	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
74.63.246.42	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.173	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.76.34	Netherlands	yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
164.52.227.101	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
105.102.211.202	147.237.77.216	Algeria	dover.idf.il	portscan: TCP Distributed Portscan	1
78.46.36.168	147.237.76.42	Germany	refuah.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
105.102.211.202	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1210
168.235.196.91	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	78
195.229.120.98	United Arab Emirates	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
37.26.149.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
37.26.149.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
31.168.90.94	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
62.0.200.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
37.26.149.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
168.235.196.91	United States	147.237.77.216	dover.idf.il	SYN Attack		monitor	10
31.168.90.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.131	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
213.57.109.136	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
84.111.120.9	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.111.120.9	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.143.99	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
157.55.39.87	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.143	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.67.31.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.177.165.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.46.38.61	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.21	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.110	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
89.139.207.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
109.253.147.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.139.207.93	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
173.252.74.99	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.26.149.132	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
203.83.20.138	Papua New Guinea	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.22.134.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.152	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.85.18	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.182.21.84	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.138.52.97	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.4.120.149	Germany	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
78.46.36.168	Germany	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.50	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
70.45.206.227	Puerto Rico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-20-2016-07:04:00 to 09-20-2016-08:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.13.6.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	9
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 209.88.198.1	Block	4
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/sip_storage/files/4/	Block	3
80.246.139.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.196	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/login.aspx?moduleto goto=0	Block	1
84.229.59.201	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation asperrorpath in www.idf.il/error.htm	Block	1
185.89.217.230	Netherlands	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
2.53.3.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.226.217.71	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.62.53.168	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
157.55.39.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
84.109.18.232	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/3/2823.pdf	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/searchback.png	Block	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
84.110.178.91	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
31.168.90.94	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
180.76.15.153	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1

09-20-2016-07:04:00 to 09-20-2016-08:04:00