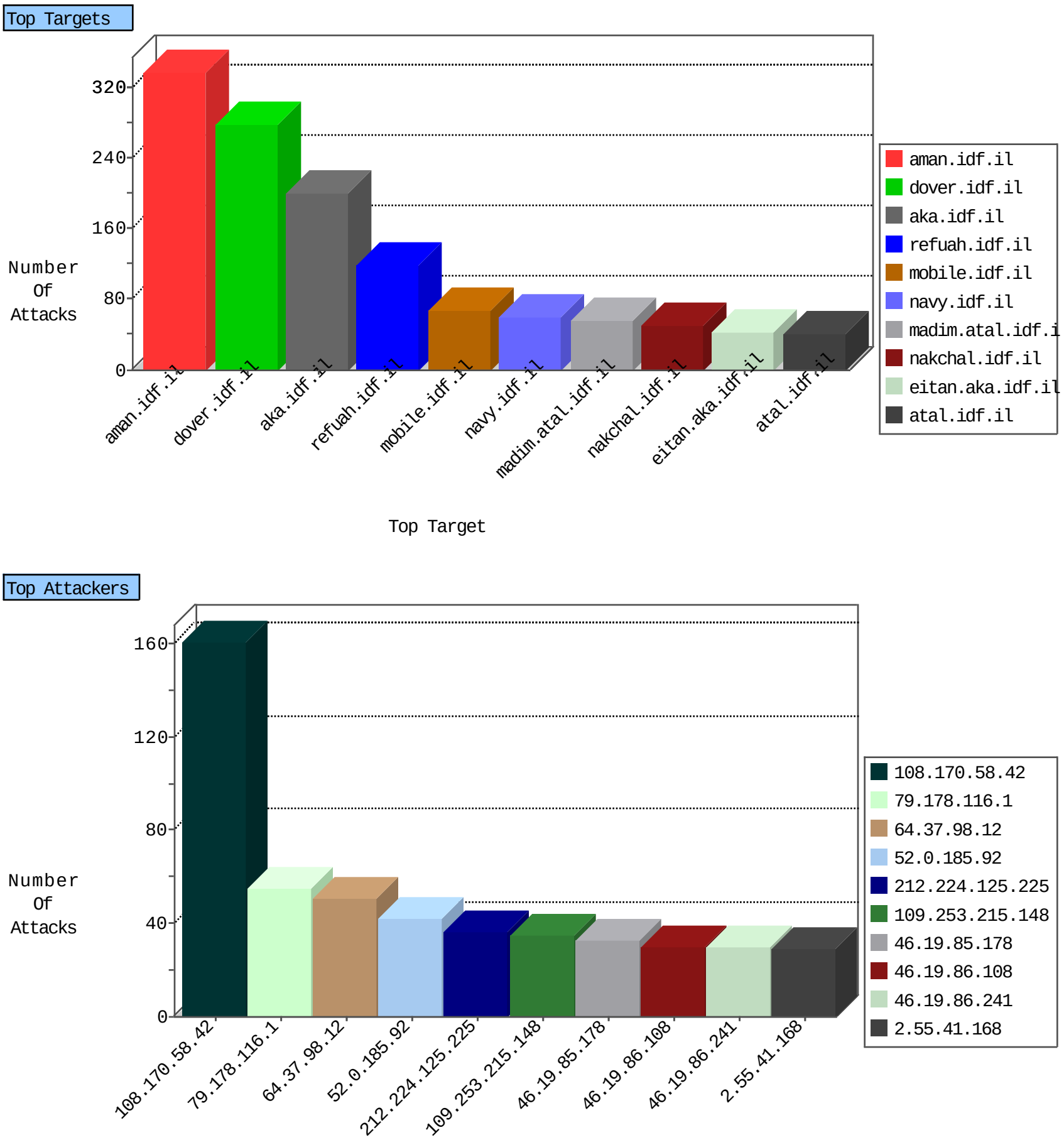
09-07-2016-17:04:07 to 09-07-2016-18:04:07

IDF Under Attack Daily Report



09-07-2016-17:04:07 to 09-07-2016-18:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.68.48.181	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.66.178.52	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3

09-07-2016-17:04:07 to 09-07-2016-18:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-07-2016-17:04:07 to 09-07-2016-18:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.88.208.193	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.198.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.110.54.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.227.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
64.137.171.55	147.237.76.34	Canada	yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.120.212.154	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
84.111.66.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.229.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.96.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-07-2016-17:04:07 to 09-07-2016-18:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.116.1	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
79.178.116.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
79.179.99.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
46.19.86.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
37.46.41.45	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
213.8.90.143	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
109.253.207.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.86.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
62.0.197.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.178	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.178	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
87.69.36.223	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
46.210.164.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
77.239.224.35	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
46.19.86.68	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
94.82.107.18	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.179.128.11	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
194.67.211.187	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
79.178.254.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.53.27.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
108.170.58.42	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
108.170.58.42	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
108.170.58.42	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
108.170.58.42	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
108.170.58.42	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
108.170.58.42	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
79.178.254.24	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
108.170.58.42	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
108.170.58.42	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.253.212.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
64.37.98.12	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
108.170.58.42	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
108.170.58.42	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
79.179.128.11	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	7
108.170.58.42	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
108.170.58.42	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
108.170.58.42	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
64.37.98.12	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
108.170.58.42	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
79.178.254.24	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
108.170.58.42	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
64.37.98.12	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
108.170.58.42	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
108.170.58.42	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
79.176.60.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.120.12.155	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6

09-07-2016-17:04:07 to 09-07-2016-18:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.215.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
84.111.41.50	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	22
77.127.90.61	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	16
85.64.115.128	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	15
87.69.81.177	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	13
46.19.86.165	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	9
46.116.14.218	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	6
109.253.207.255	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
79.178.39.183	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
80.246.139.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.120.38.133	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.147	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	3
46.19.86.170	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.121	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
212.76.120.127	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
46.120.246.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
46.19.85.168	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
176.13.17.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.248.230	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniot.aspx	Block	2
109.67.33.235	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
87.71.47.106	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
40.77.167.19	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
80.246.136.233	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.74	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.74	Block	1
77.138.161.15	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	1
66.249.64.228	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/2/302.pdf	Block	1
94.230.86.155	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
46.19.86.150	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
2.55.150.1	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.116.53.240	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.124.43.165	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.139.158.207	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
212.179.40.171	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/1/71751.pdf	Block	1
157.55.39.74	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
77.138.252.22	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
66.249.65.24	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
95.79.45.114	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan/main/main.asp	Block	1
85.64.245.112	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
79.178.116.1	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
31.168.68.202	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
194.242.168.227	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
77.127.36.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
91.199.69.254	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	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
213.57.168.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.80.138.31	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
77.139.56.173	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
2.53.147.222	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	1

09-07-2016-17:04:07 to 09-07-2016-18:04:07