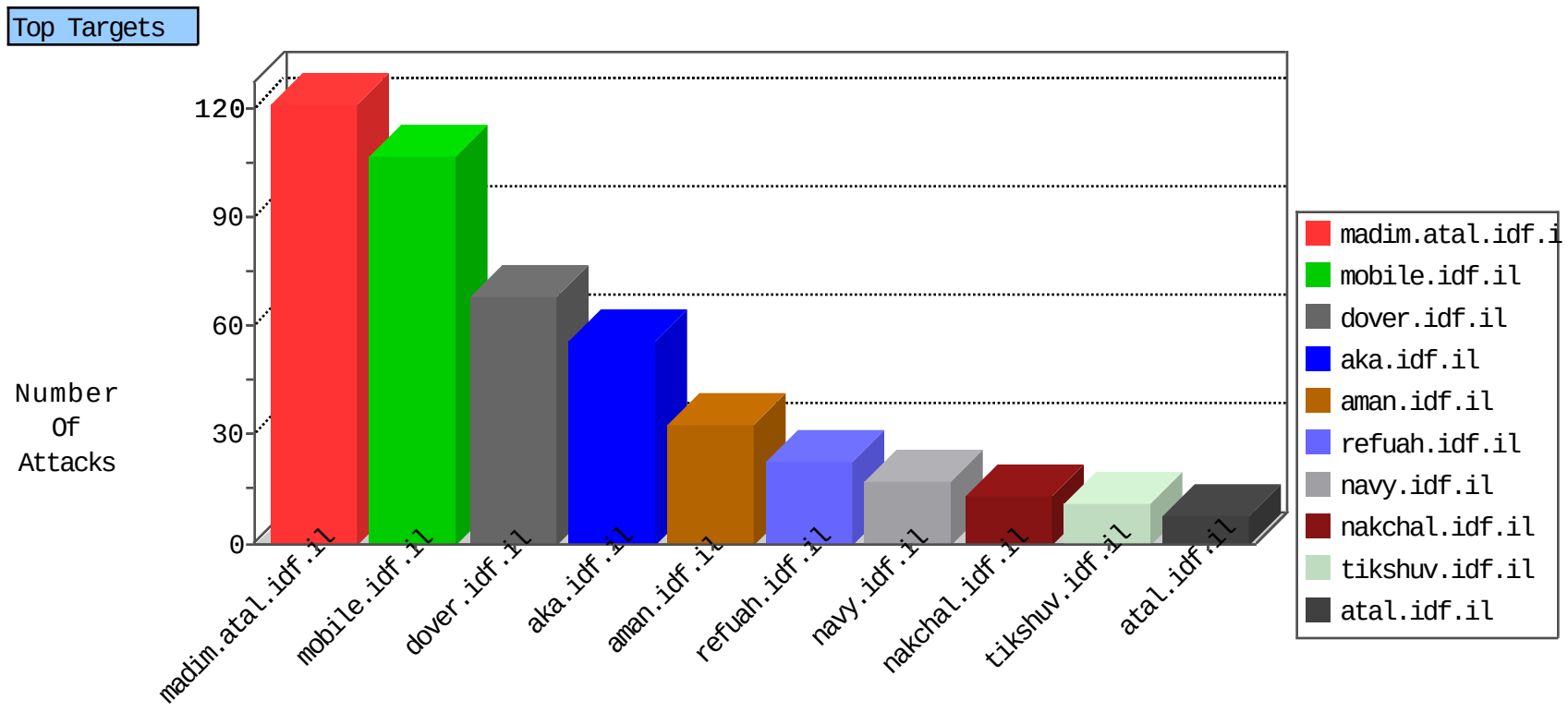
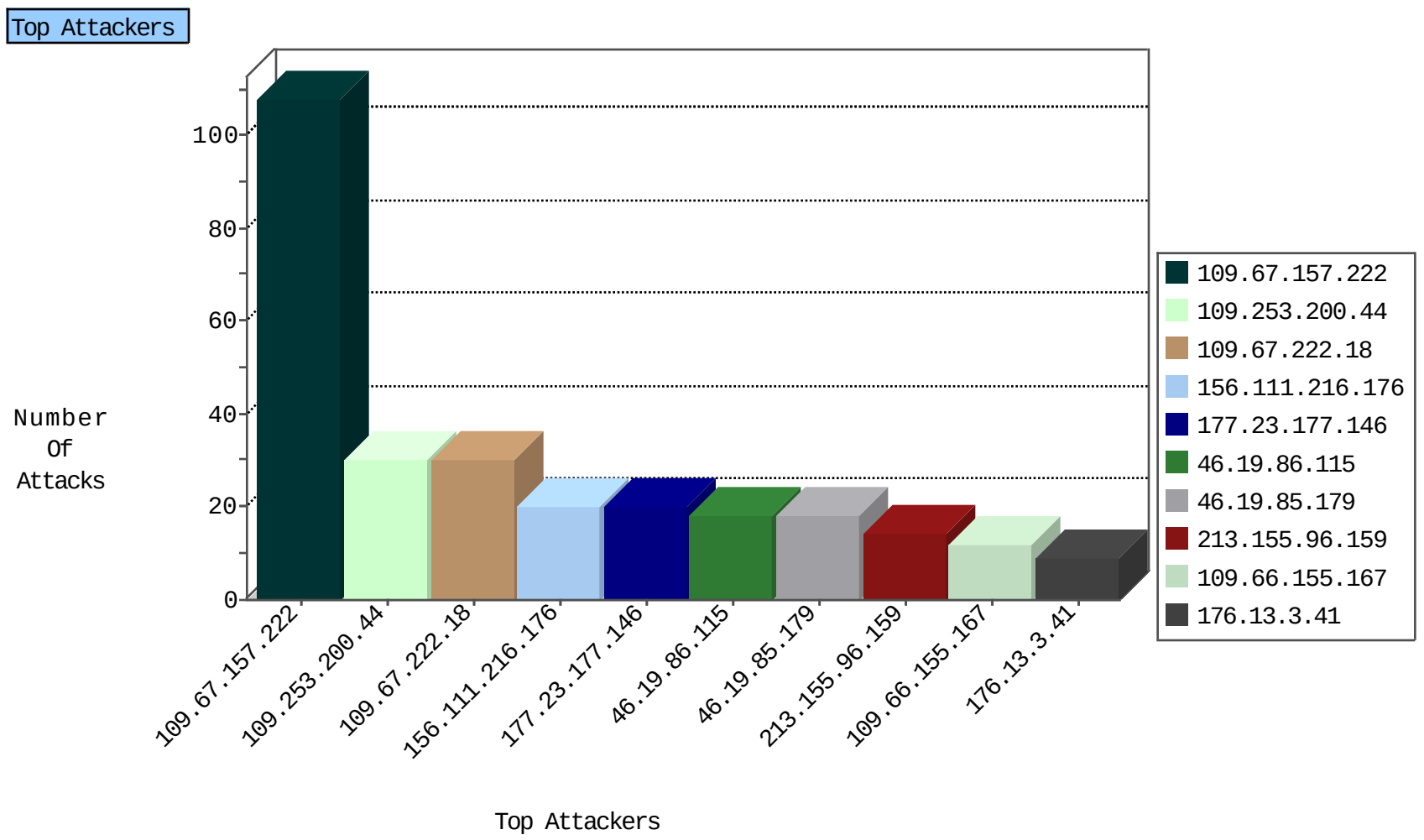
09-23-2016-18:04:06 to 09-23-2016-19:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-23-2016-18:04:06 to 09-23-2016-19:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
120.132.50.135	China	147.237.77.74	law.idf.il	block-sp-traf1	forward	2
69.30.193.254	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
142.54.174.82	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
198.204.224.237	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
173.244.198.5	United States	147.237.76.30	himush.idf.il	Black List	drop	1
63.141.231.198	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
209.126.136.2	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
123.59.59.52	China	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
173.244.198.5	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
198.55.103.48	United States	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	1
69.30.226.222	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
156.111.216.176	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-23-2016-18:04:06 to 09-23-2016-19:04:06

Top Attackers In IPS

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

09-23-2016-18:04:06 to 09-23-2016-19:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
104.167.6.84	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
210.212.207.80	147.237.77.233	India	atal.idf.il	ET SCAN Potential SSH Scan	1
139.162.187.89	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
213.155.96.159	147.237.72.156	Turkey	aman.idf.il	ET WEB_SERVER Poison Null Byte	1
180.213.5.205	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-23-2016-18:04:06 to 09-23-2016-19:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.67.222.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
177.23.177.146	Brazil	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	20
46.19.85.179	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.179	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.3.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
89.237.101.75	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.7.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.165.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.28.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.13.1.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.46.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
79.176.117.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.115	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.115	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
156.111.216.176	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
84.109.112.207	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
156.111.216.176	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.109.112.207	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
156.111.216.176	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
156.111.216.176	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.178.162.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.160.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.20.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.138.72.106	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
84.95.208.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.123.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.121.199.123	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
77.138.46.133	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.226.218.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.121.199.123	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
93.172.57.193	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	2
107.178.208.177	United States	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
89.138.72.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
93.172.57.193	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
5.102.242.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
77.138.9.204	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
109.65.86.219	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.124	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.138.167.152	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
37.142.217.144	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
77.139.84.44	France	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
139.162.37.147	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.243.31.2	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.172.57.193	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

09-23-2016-18:04:06 to 09-23-2016-19:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.157.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
109.66.155.167	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 109.66.155.167	Block	6
109.66.155.167	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	5
37.26.146.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.139.214.115	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
176.13.3.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.155.96.159	Turkey	147.237.72.156	aman.idf.il	Distributed Malformed URL	Block	2
5.102.221.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
109.65.94.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
156.111.216.176	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	2
84.109.6.4	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	2
213.155.96.159	Turkey	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Name [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2278.jpg	Block	1
213.155.96.159	Turkey	147.237.72.156	aman.idf.il	NULL Character in Header Name at [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
213.155.96.159	Turkey	147.237.72.156	aman.idf.il	Distributed Abnormally Long Request	Block	1
2.53.165.83	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.1	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
213.155.96.159	Turkey	147.237.72.156	aman.idf.il	Illegal Byte Code Character in URL ¸[[#20]]¸	Block	1
46.120.107.127	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
185.120.124.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.66.155.167	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/	Block	1
77.126.28.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.155.96.159	Turkey	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/changelog.txt	Block	1
213.155.96.159	Turkey	147.237.72.156	aman.idf.il	Distributed Illegal HTTP Version	Block	1
5.28.159.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/shakimquestionnaire.aspx	Block	1
109.64.89.65	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 109.64.89.65 (Open Mode)	None	1
66.249.64.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
213.155.96.159	Turkey	147.237.72.156	aman.idf.il	Malformed HTTP Header Line 1	Block	1
207.241.231.163	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
77.139.135.45	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
176.13.3.41	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3491.jpg	Block	1
213.155.96.159	Turkey	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 213.155.96.159	Block	1
209.249.5.246	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
80.246.130.202	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/null	Block	1
213.155.96.159	Turkey	147.237.72.156	aman.idf.il	Distributed Unknown HTTP Request Method	Block	1
176.13.7.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2293.jpg	Block	1
213.155.96.159	Turkey	147.237.72.156	aman.idf.il	Multiple NULL Character in Method from 213.155.96.159	Block	1
209.249.5.252	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
156.111.216.176	United States	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1

09-23-2016-18:04:06 to 09-23-2016-19:04:06