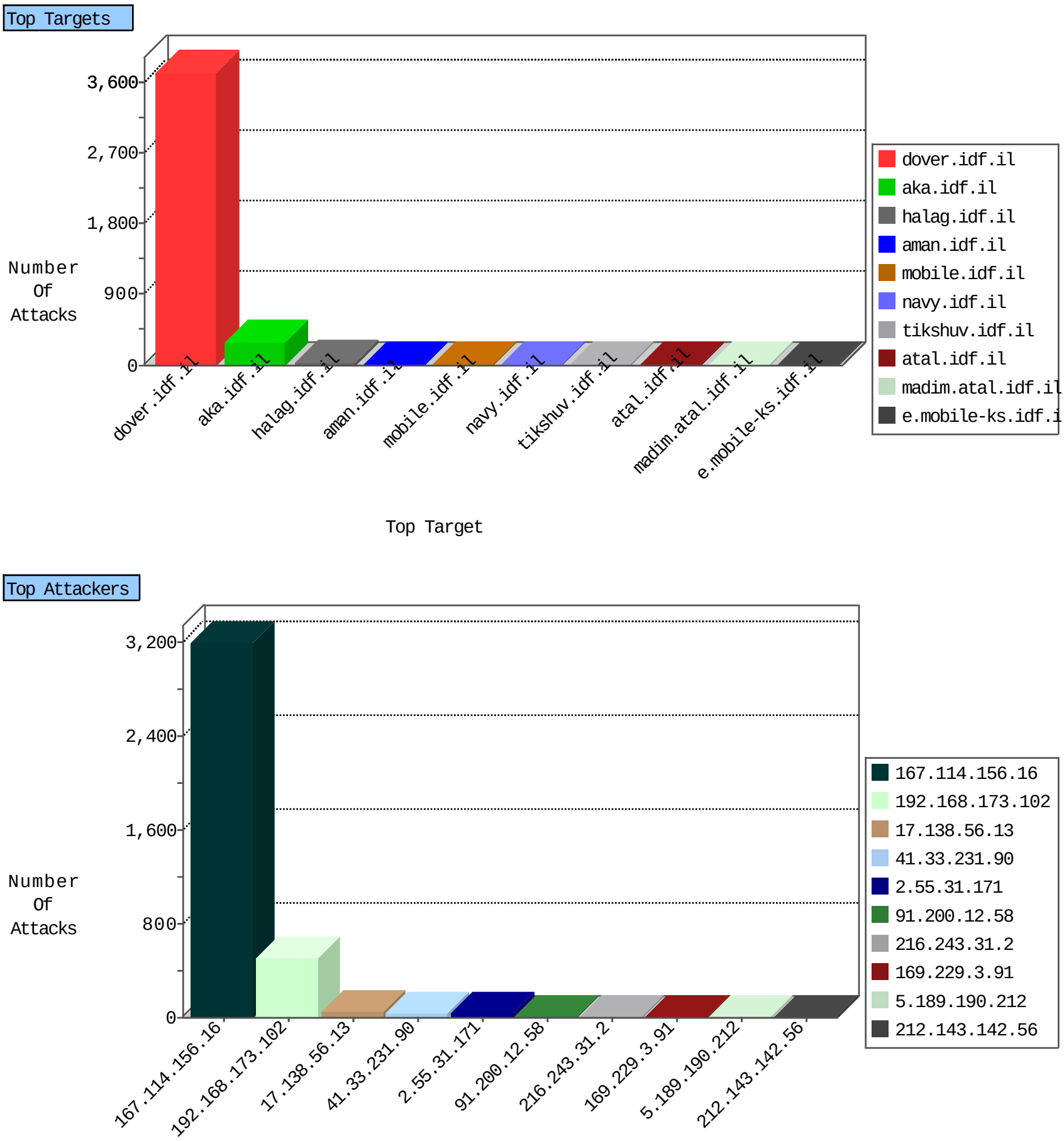
04-09-2016-13:04:01 to 04-09-2016-14:04:01

IDF Under Attack Daily Report



04-09-2016-13:04:01 to 04-09-2016-14:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3187
79.180.113.119	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
118.236.120.102	Japan	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	2
208.67.1.19	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.19	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
168.235.196.227	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
93.201.71.212	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
208.67.1.19	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

04-09-2016-13:04:01 to 04-09-2016-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.39.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
87.71.54.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
151.80.31.158	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.172	France	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.177	France	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
151.80.31.101	France	147.237.77.176	matpash.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.179	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
85.187.236.218	Bulgaria	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
151.80.31.107	France	147.237.77.216	dover.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

04-09-2016-13:04:01 to 04-09-2016-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
106.81.44.255	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.20.69.98	147.237.76.197	United States	e.himush.idf.il	ET DROP Dshield Block Listed Source	1
124.105.63.208	147.237.76.34	Philippines	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

04-09-2016-13:04:01 to 04-09-2016-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	335
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	175
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.55.31.171	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	14
2.55.31.171	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
5.189.190.212	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
91.200.12.58	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.148.194	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
157.55.39.108	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.83.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.193.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.173.53.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.197.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
105.102.4.21	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.180.187.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.200.12.58	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
79.181.118.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.12.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.66.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
118.173.140.248	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
176.13.13.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.141.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.171.215	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.129.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
213.8.129.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.105.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.135.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.144.24.129	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
149.88.255.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
213.8.204.19	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
82.166.237.150	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
149.50.26.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
195.154.173.103	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
5.102.254.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.153.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.7	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
85.65.57.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
193.43.245.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
5.102.195.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.187.114.171	France	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
195.62.53.168	Russian Federation	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.102.242.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.180.39.138	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.77.91.113	Turkey	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-09-2016-13:04:01 to 04-09-2016-14:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
96.125.181.175	Canada	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 96.125.181.175	Block	3
109.65.83.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.83.112	Block	2
46.19.86.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.111.1.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
41.109.167.94	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/	Block	1
157.55.39.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
96.125.181.175	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.30.90.132	Azerbaijan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
109.67.3.239	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
79.183.105.135	Israel	147.237.72.166	aka.idf.il	Unknown Parameter _ in www.aka.idf.il/main/giyus/terms.aspx	None	1
157.55.39.226	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/drushim/misrot.aspx	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
2.55.31.171	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
188.161.113.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
109.241.135.1	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
82.166.118.226	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
176.13.13.192	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.65.83.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
207.46.13.118	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
114.97.56.215	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11435-he/cogat.aspx/trackback/	Block	1
46.120.116.210	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
182.33.49.129	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
109.65.85.55	Israel	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
68.180.230.155	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/1103-he/eitan.aspx	None	1
41.109.167.94	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.109.167.94	Block	1
157.55.39.177	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/departmentslobby/	Block	1
65.55.210.33	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.30.90.132	Azerbaijan	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
109.65.194.107	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1

04-09-2016-13:04:01 to 04-09-2016-14:04:01