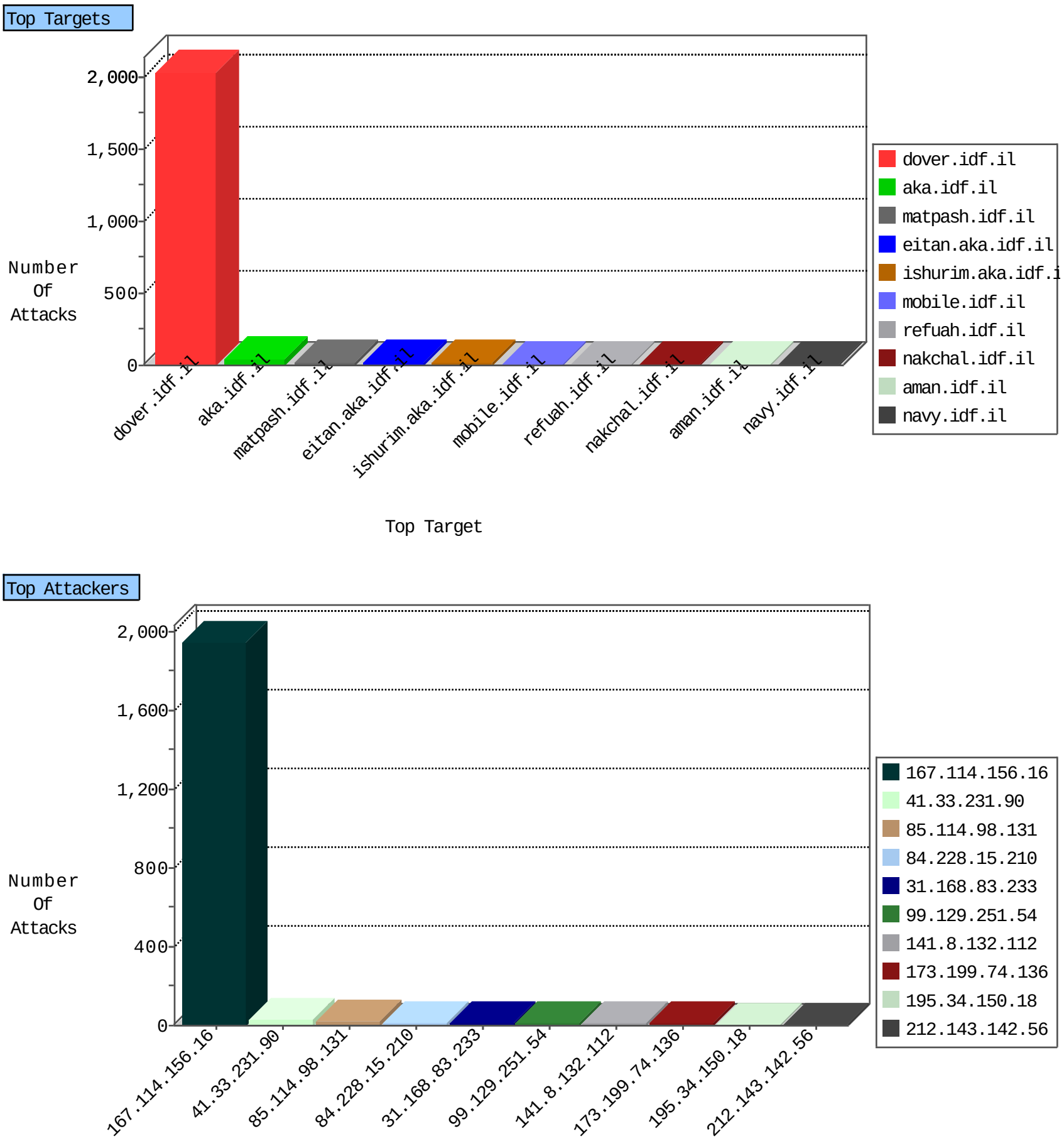
01-08-2016-05:04:00 to 01-08-2016-06:04:00

IDF Under Attack Daily Report



01-08-2016-05:04:00 to 01-08-2016-06:04:00

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	DOS-Tool-SwitchbladG	dest-reset	3506
180.97.106.36	China	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
107.150.60.242	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
116.8.53.200	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

01-08-2016-05:04:00 to 01-08-2016-06:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.94.153.178	United States	147.237.76.200	eitan.aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
23.94.153.178	United States	147.237.76.200	eitan.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
51.255.48.155	United Kingdom	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
136.243.5.215	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

01-08-2016-05:04:00 to 01-08-2016-06:04:00

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
209.126.116.147	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
99.129.251.54	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.7	147.237.77.74	Ukraine	law.idf.il	ET SCAN NMAP -sS window 1024	1
99.129.251.54	147.237.77.233	United States	atal.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
99.129.251.54	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
99.129.251.54	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
99.129.251.54	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.0.33	United Kingdom	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
99.129.251.54	147.237.77.121	United States	e.navy.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.53.196	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
128.127.0.45	147.237.0.19	Italy	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
99.129.251.54	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential SSH Scan	1
99.129.251.54	147.237.77.234	United States	halag.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
99.129.251.54	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
99.129.251.54	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
99.129.251.54	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
99.129.251.54	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.117.208.243	147.237.76.197		e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
128.127.0.45	147.237.0.19	Italy	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
23.94.153.178	147.237.76.200	United States	eitan.aka.idf.il	ET WEB_SERVER Muieblackcat scanner	1
128.127.0.45	147.237.0.19	Italy	madim.atal.idf.il	ET SCAN NMAP -f -sS	1

01-08-2016-05:04:00 to 01-08-2016-06:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
84.228.15.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
31.168.83.233	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.114.98.131	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
85.114.98.131	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
131.253.25.164	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
85.114.98.131	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.114.98.131	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.114.98.131	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.78.160	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
31.168.83.233	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.114.98.131	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
199.30.24.92	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
89.139.32.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
184.105.247.216	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.161	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
141.212.122.106	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.81	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
206.253.224.14	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
99.231.47.161	Canada	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.97.106.162	China	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
84.111.123.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.36	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
141.212.122.101	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.162	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
69.146.195.140	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.107	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.82	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.49	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
99.231.47.161	Canada	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.92	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.36	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
141.212.122.102	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.65	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.162	China	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
71.229.99.193	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.210.158.71	Netherlands	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.83	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
115.230.124.164	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.92	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.37	China	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
141.212.122.102	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

01-08-2016-05:04:00 to 01-08-2016-06:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
141.212.122.64	United States	147.237.76.31	nakchal.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.207.74	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 5.29.207.74 (sigalgs DoS Attack)	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
157.55.39.75	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/62532.pdfg2=whvq9jgvov3igm-oflegda	Block	1
65.55.210.34	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.152	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
89.139.32.183	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 89.139.32.183	Block	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
206.253.224.14	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
172.56.19.234	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.139.32.183	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1513	Block	1
66.249.69.46	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1762	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1512-he/refuah.aspx	Block	1
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1

01-08-2016-05:04:00 to 01-08-2016-06:04:00