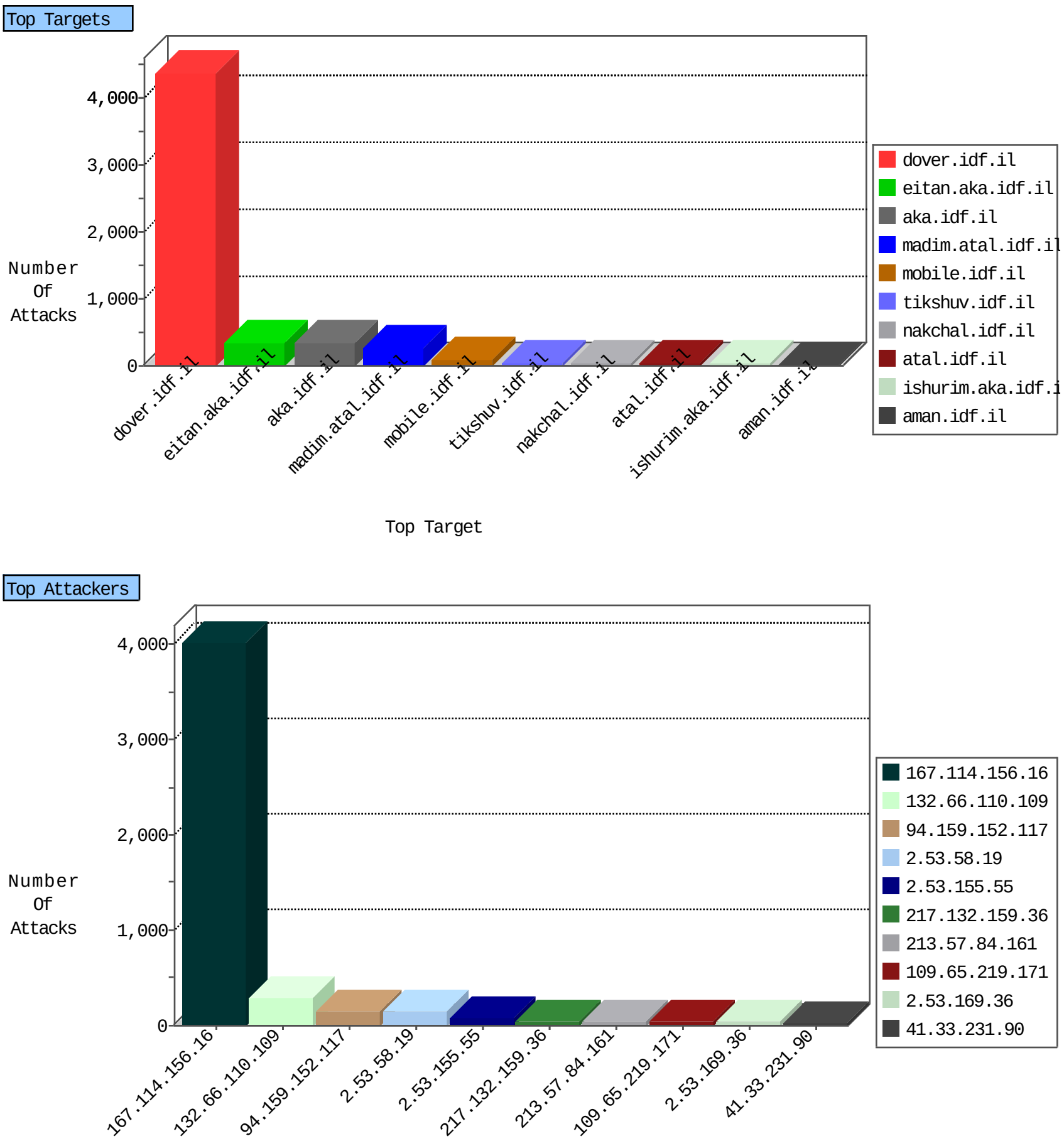
04-18-2016-12:04:09 to 04-18-2016-13:04:09

IDF Under Attack
Daily Report



04-18-2016-12:04:09 to 04-18-2016-13:04:09

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	4018
94.159.152.117	Israel	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	16
109.65.172.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	11
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
82.145.211.4	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
66.249.79.10	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
120.24.4.61	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
159.122.220.135	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.97	United States	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
159.122.220.135	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
159.122.220.135	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

04-18-2016-12:04:09 to 04-18-2016-13:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.187.101.234	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
192.187.101.234	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-18-2016-12:04:09 to 04-18-2016-13:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.131	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
80.82.78.38	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.42.13	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.5.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.63.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
172.87.221.214	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -f -sS	1
106.186.113.67	147.237.77.205	Japan	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.225.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.0.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.170.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
172.87.221.214	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
109.64.149.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.238.82.190	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1

04-18-2016-12:04:09 to 04-18-2016-13:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
132.66.110.109	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	297
2.53.169.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
109.65.219.171	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
2.53.175.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
37.26.148.153	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
80.246.137.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
213.57.84.161	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
213.57.84.161	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	13
2.53.170.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.177.178.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
31.168.13.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.177.178.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
2.55.62.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.114.177.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
77.127.157.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.114.177.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
213.57.84.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.191	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	7
79.177.208.170	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.177.208.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
176.13.13.94	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.147.16	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.9.80	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
80.178.208.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.38	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.181.164.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.173.174.28	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
84.228.38.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.79.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.13.94	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.54.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.249	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.55.62.40	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
213.244.88.21	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.106.44.104	Palestinian Territory, Occupied	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.3.147.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.93.24	Europe	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
195.191.52.10	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.160.158.165	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.48.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.18.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.92	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.126.237.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.119.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.24.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.200.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-18-2016-12:04:09 to 04-18-2016-13:04:09

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.64.149.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.22.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.58.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	145
2.53.155.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
94.159.152.117	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	72
94.159.152.117	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.159.152.117	Block	68
217.132.159.36	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 217.132.159.36	Block	48
109.253.211.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
109.253.196.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	6
31.129.170.42	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
31.129.170.42	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.129.170.42	Block	5
192.187.101.234	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.187.101.234	Block	5
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
79.177.79.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	4
80.246.130.210	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.253.227.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
94.159.152.117	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19604-he/	Block	3
82.196.42.196	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
212.179.132.204	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	3
37.26.149.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.81.218	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.179.81.218	Block	3
84.109.193.84	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	3
31.168.13.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.121.123.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.123.29	Block	2
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.226.44.156	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.108.170.63	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.108.170.63	Block	2
2.53.18.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.200.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.55.10.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.179.132.204	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 212.179.132.204	Block	2
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
213.57.192.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
131.114.197.117	Italy	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 131.114.197.117	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.109.193.84	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
31.168.13.78	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	1
157.55.39.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1806-he/dover.aspx	Block	1
123.59.59.52	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.mafengwo.cn/894-he/orchot.aspx	Block	1
46.121.123.29	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 106.38.241.106	Block	1
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
2.53.15.24	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
131.114.197.117	Italy	147.237.77.74	law.idf.il	PHP Attempt	Block	1
212.179.132.204	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/	Block	1
93.173.174.28	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
2.53.155.55	Israel	147.237.77.233	atal.idf.il	Distributed Parameter Type Violation on atal.idf.il/1440-he/atal.aspx parameter search	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/home.png	Block	1

04-18-2016-12:04:09 to 04-18-2016-13:04:09