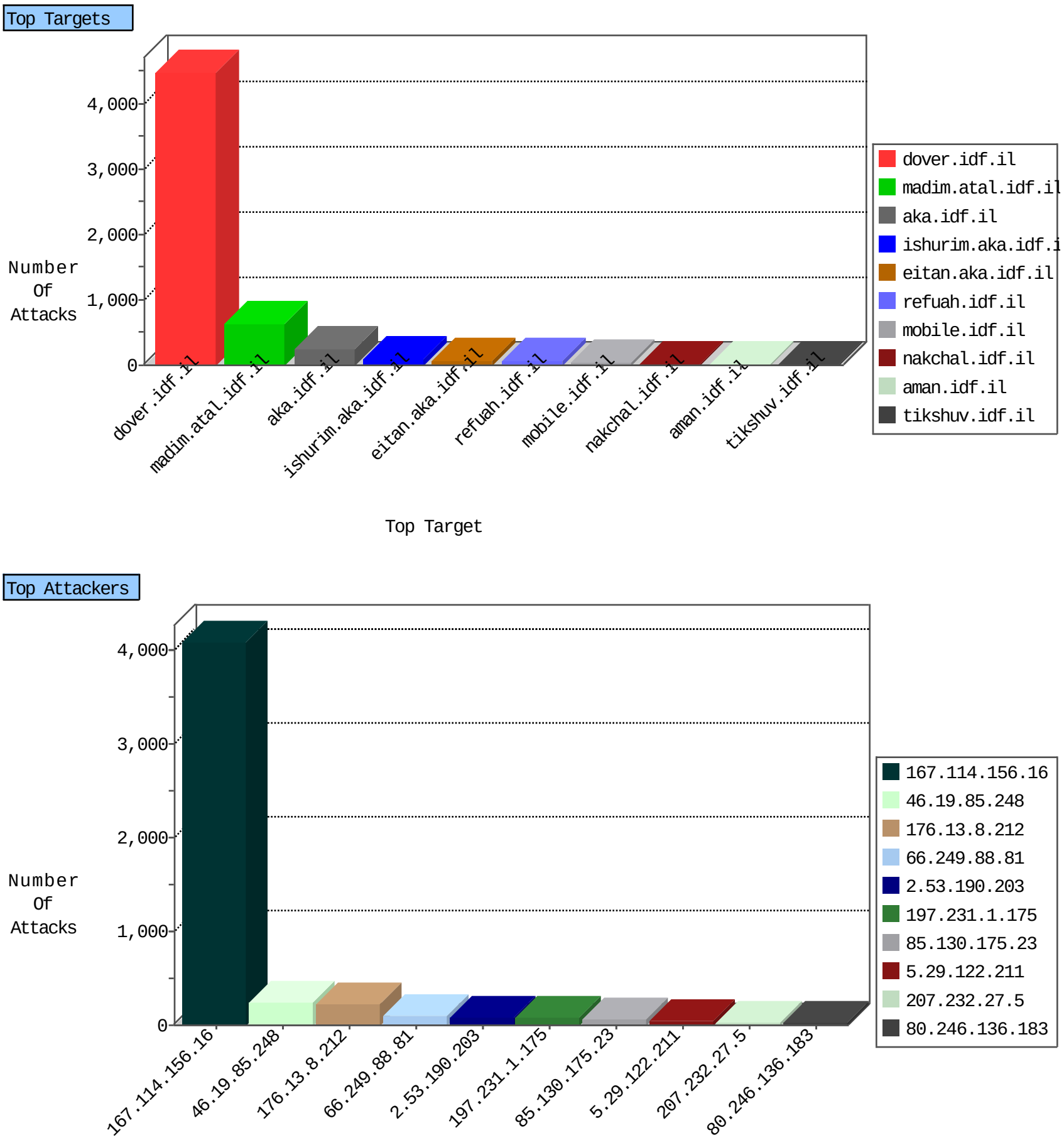
04-18-2016-15:04:05 to 04-18-2016-16:04:05

IDF Under Attack Daily Report



04-18-2016-15:04:05 to 04-18-2016-16:04:05

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	4086
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
173.208.197.250	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	2
107.150.32.61	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	2
74.91.17.181	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	forward	2
173.208.197.251	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
107.150.46.35	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	2
74.91.23.108	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	2
82.145.218.0	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	2
69.197.185.20	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	forward	2
185.5.30.59	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
204.12.196.236	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
159.122.220.135	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
159.122.220.135	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
151.80.96.8	France	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
76.171.193.23	United States	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
85.130.175.23	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
74.91.17.178	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	1
159.122.220.135	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
76.171.193.23	United States	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1

04-18-2016-15:04:05 to 04-18-2016-16:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-18-2016-15:04:05 to 04-18-2016-16:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.88.81	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	104
84.94.197.13	147.237.76.202	Israel	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
221.226.31.210	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
80.82.78.38	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.164.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.157.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.240.250.154	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.240.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
112.218.60.60	147.237.76.86	Korea, Republic of	navy.idf.il	ET SCAN NMAP -sS window 3072	1
109.65.224.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.71.44.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.227.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.94.197.13	147.237.76.202	Israel	e.halag.idf.il	ET SCAN NMAP -f -sS	1
221.226.31.210	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -f -sS	1
80.74.103.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
73.70.123.193	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
123.159.204.173	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.121.125.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.240.250.154	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
109.253.142.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.219.238.10	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.173.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-18-2016-15:04:05 to 04-18-2016-16:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.231.1.175	Mauritania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
5.29.122.211	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
207.232.27.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
85.130.175.23	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.8.212	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
2.53.142.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.8.212	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.55.149.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
217.132.14.81	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.57.251.198	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
85.130.175.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
82.166.140.117	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
85.130.175.23	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.55.165.4	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.65.218.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.76.112.189	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
87.70.66.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.9.77	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
46.19.85.217	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.139.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.53.142.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.8.112.233	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.8.63.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.175.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.219.231.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.76.112.189	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	alert	6
81.255.154.162	France	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
192.114.105.254	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
140.242.217.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.217	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.148.213	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
94.230.86.209	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.0.238.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.29.120.208	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
197.2.42.201	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
217.132.14.81	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
89.138.218.181	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.179.222.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.63.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.64.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.102.9.10	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.63.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.246.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.178.201.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-18-2016-15:04:05 to 04-18-2016-16:04:05

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

04-18-2016-15:04:05 to 04-18-2016-16:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	244
176.13.8.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	181
2.53.190.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
80.246.136.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
176.13.12.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.85.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
213.8.63.16	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	11
31.171.244.115	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
157.55.39.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
2.53.169.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
212.199.93.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 212.199.93.122	Block	4
82.166.190.11	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1620.jpg	Block	4
199.30.24.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.55.131.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.219	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.182.12.171	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
132.74.212.75	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 132.74.212.75	Block	2
2.53.142.185	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
93.173.168.84	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/contactus/mobile	Block	2
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	2
2.53.154.214	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	2
106.186.113.132	Japan	147.237.77.226	www.chamatz.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
157.55.39.1	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
173.208.197.251	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
2.53.169.218	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
82.166.98.221	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/mobile	Block	1
195.182.75.6	Lithuania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1520-en/	Block	1
46.117.8.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
180.253.250.102	Indonesia	147.237.77.74	law.idf.il	PHP Attempt	Block	1
157.55.39.111	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/901-8504/tikshuv.aspx	Block	1
23.81.248.96	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/shared/usercontrols/headerupper/	Block	1
87.70.67.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 195.160.242.40	Block	1
40.77.167.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.166.140.117	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
180.253.250.102	Indonesia	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
31.13.102.123	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/ https:/twitter.com/	Block	1
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sip_storage/files/7	Block	1
80.86.94.7	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 80.86.94.7	Block	1
176.13.9.219	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
132.74.212.75	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/3/113003.pdf	Block	1
204.12.196.236	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
185.103.252.5	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.73.227	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8/4538.pdf	Block	1
165.225.72.80	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	1
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	1
80.246.133.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-18-2016-15:04:05 to 04-18-2016-16:04:05