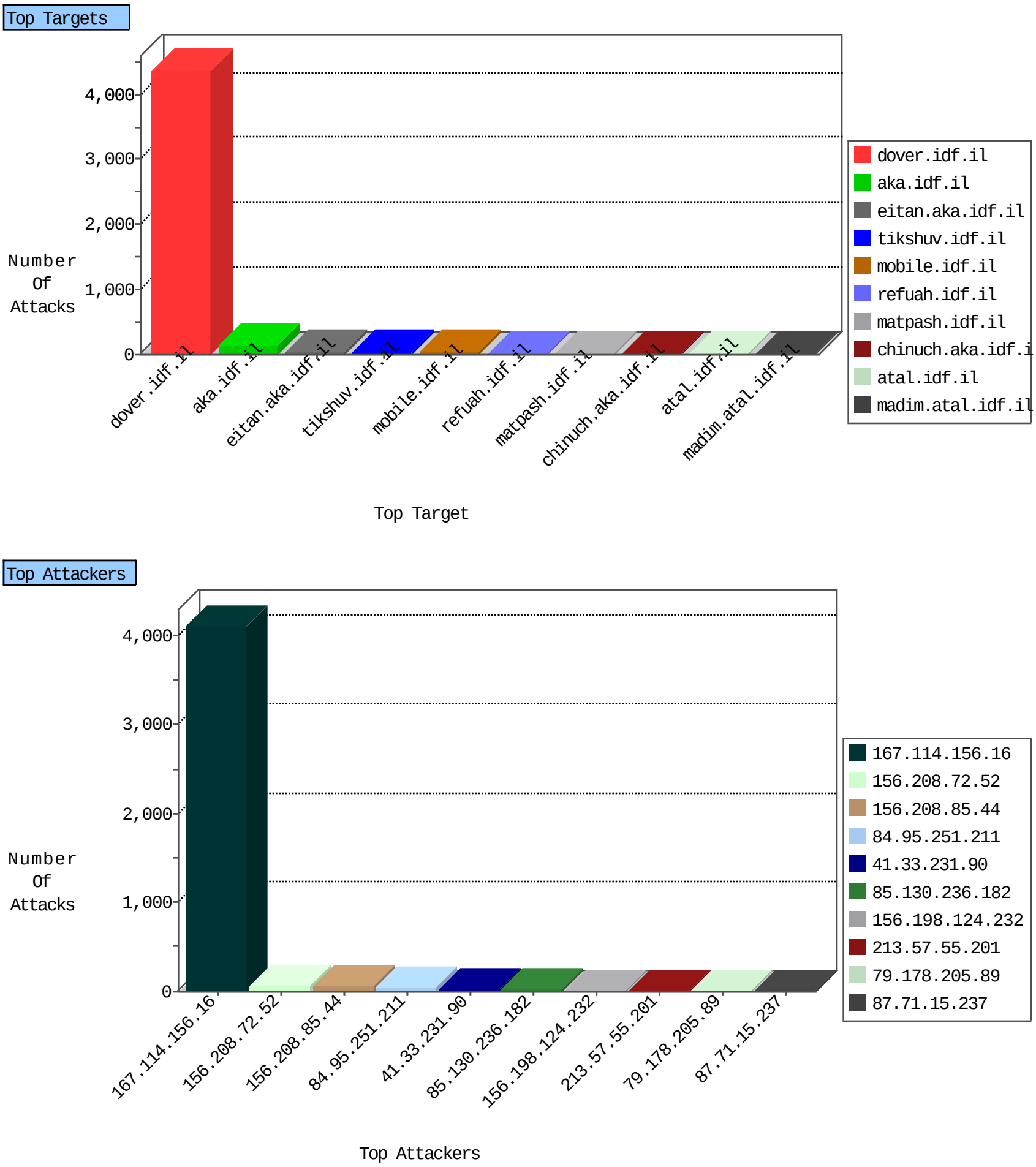
04-16-2016-14:04:02 to 04-16-2016-15:04:02

IDF Under Attack
Daily Report



04-16-2016-14:04:02 to 04-16-2016-15:04:02

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	4118
82.80.230.228	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
93.201.93.17	Germany	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
45.32.95.13	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
180.153.235.242	China	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
45.32.95.13	Netherlands	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
82.145.211.95	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1
218.250.245.181	Hong Kong	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
45.32.95.13	Netherlands	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
93.201.85.174	Germany	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
45.32.95.13	Netherlands	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1

04-16-2016-14:04:02 to 04-16-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.102.17	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.88.112.235	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
2.53.159.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-16-2016-14:04:02 to 04-16-2016-15:04:02

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	3
5.29.22.140	147.237.77.243	Israel	mobile.idf.il	ET SCAN NMAP -sA (2)	2
107.158.255.194	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
107.158.255.194	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 3072	1
103.225.96.43	147.237.0.35	Australia	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.103.76.109	147.237.8.45	Pakistan	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
40.84.148.3	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
107.158.255.194	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
107.158.255.194	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 4096	1
104.219.234.2	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
46.4.79.76	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
40.84.148.3	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
107.158.255.194	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
40.84.148.3	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -f -sS	1

04-16-2016-14:04:02 to 04-16-2016-15:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
84.95.251.211	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
156.198.124.232	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
79.178.205.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.236.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
85.64.98.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.55.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
207.46.13.144	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.236.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.106.46.74	Palestinian Territory Occupied	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
66.249.66.19	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.32	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.179	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	5
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.46.39.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.149.179	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
87.71.15.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	5
37.26.148.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.70.81.222	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.57.55.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.187.165.74	France	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
5.43.210.11	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
79.182.206.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.22	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.84.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.69.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.55.201	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
176.13.1.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.14.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.151.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.33.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.16	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.35.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.173.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.130.236.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.69.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.188.60	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.55.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
87.71.15.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
188.120.148.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
85.65.112.169	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

04-16-2016-14:04:02 to 04-16-2016-15:04:02

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
80.246.136.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-16-2016-14:04:02 to 04-16-2016-15:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.8.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
131.253.25.144	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
213.8.204.5	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
79.177.84.45	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/	Block	2
5.29.22.140	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sip_storage/files/3	Block	2
46.19.86.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.78.236.241	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.66.179	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/5/1555.jpg	Block	1
213.8.204.5	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 213.8.204.5	Block	1
37.187.114.171	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to /irj/portal	Block	1
157.55.39.26	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/page.asp	Block	1
85.65.55.102	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1
62.210.152.87	France	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
176.13.14.49	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1
149.78.236.241	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
78.178.5.34	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
157.55.39.32	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/..aspx	Block	1
85.65.73.174	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
62.210.152.87	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
207.46.13.102	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list2.htm	Block	1
156.198.124.232	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
213.8.204.5	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/	Block	1
157.55.39.163	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
87.71.15.237	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/smalim/&sa=u&ei=zqsutjfxmn-fopdm-pkb&ved=0cauqfjaa&usg=afqjcnf2apehywz9apusaqdzaz5_jkfq7g	Block	1
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
79.177.84.45	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
46.19.85.163	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
157.55.39.163	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/cometous/	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2359.jpg	Block	1
208.90.57.196	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/www.youtube.com/embed/02xlfsfhjyk	Block	1
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
80.246.136.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.236	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/klali/null	Block	1

04-16-2016-14:04:02 to 04-16-2016-15:04:02