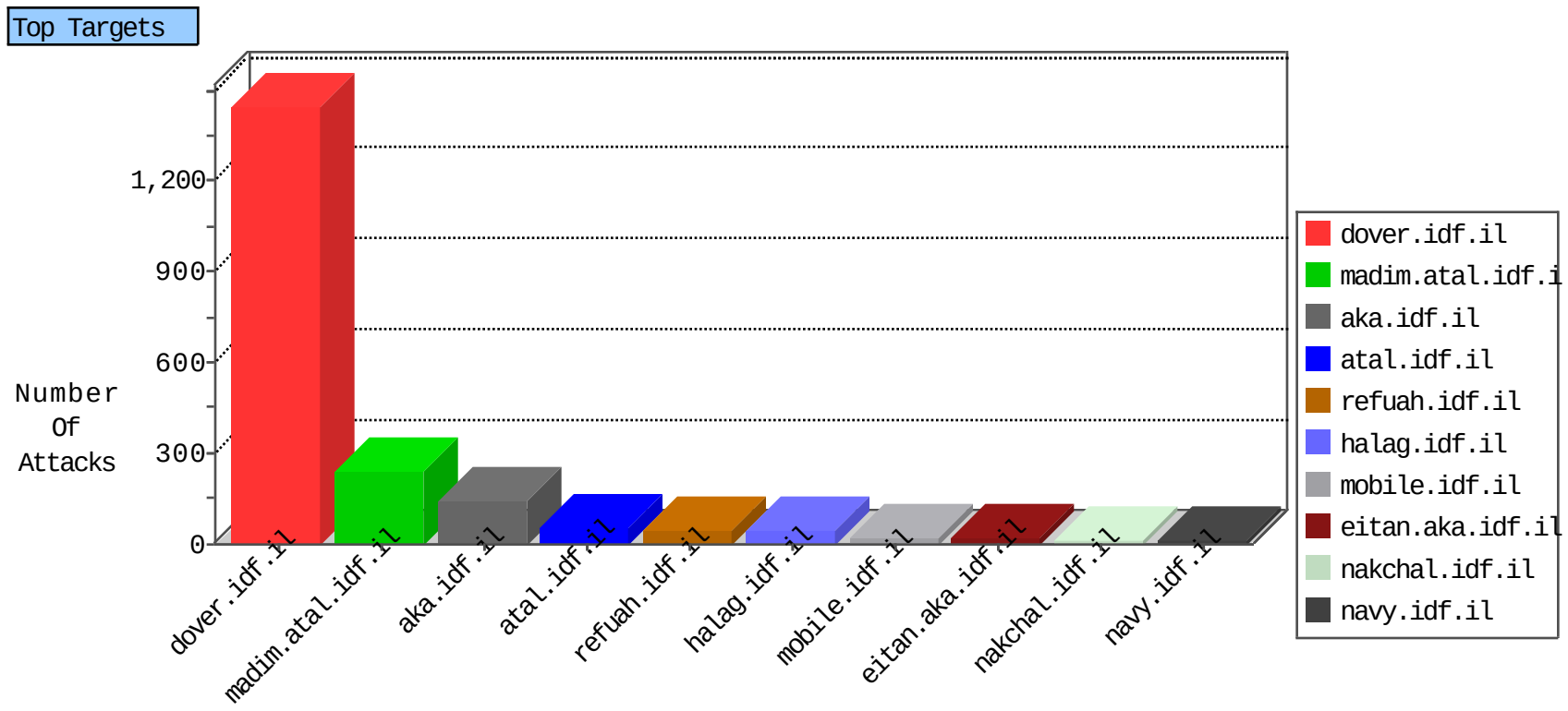
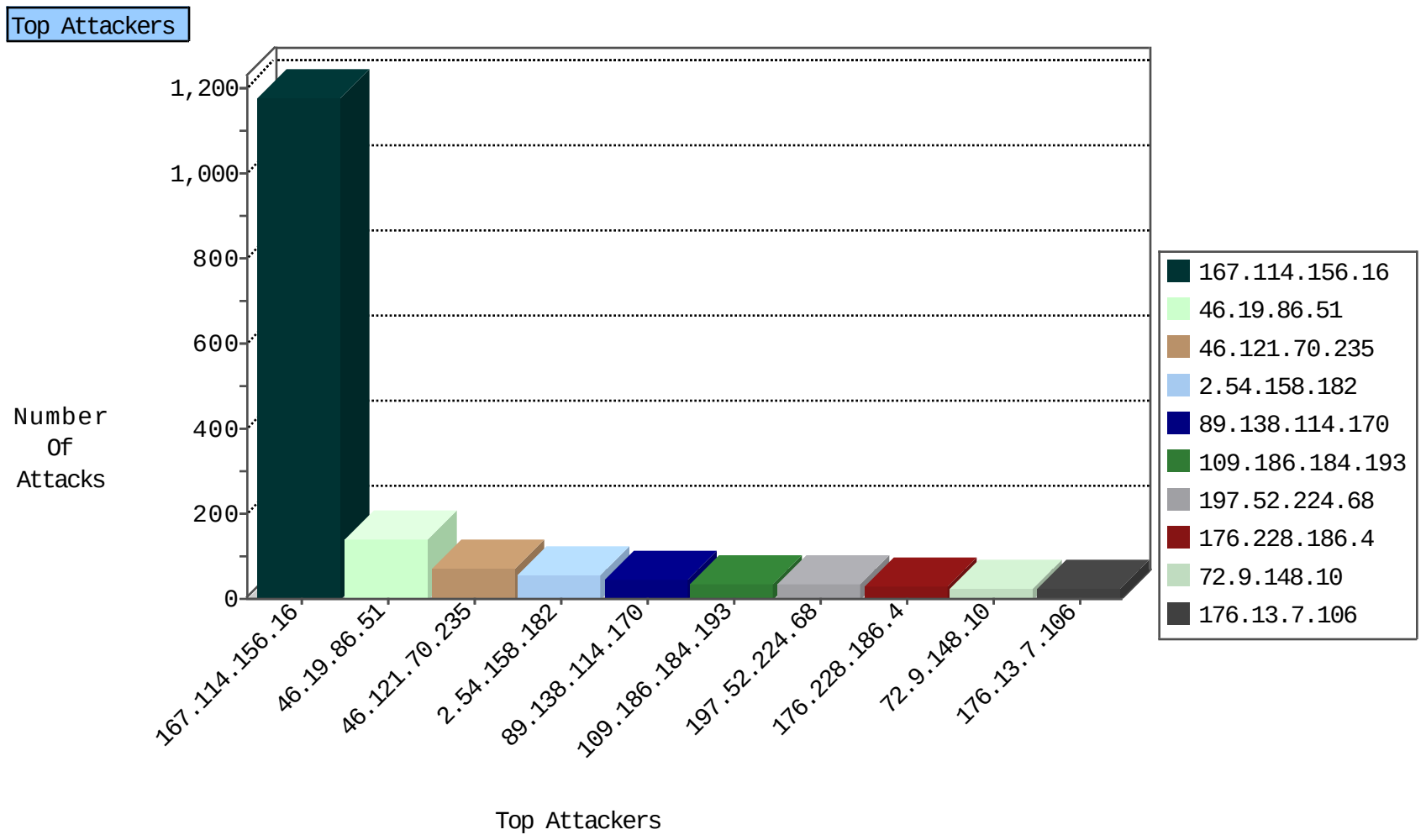
03-12-2016-17:04:05 to 03-12-2016-18:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-12-2016-17:04:05 to 03-12-2016-18:04:05

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	DOS-Tool-SwitchbladG	dest-reset	3196
134.147.203.115	Germany	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	4
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
134.147.203.115	Germany	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	2
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
170.161.102.40	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
37.187.158.138	France	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1

03-12-2016-17:04:05 to 03-12-2016-18:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.85.4	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
5.9.85.4	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
80.229.107.21	United Kingdom	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
197.52.128.201	Egypt	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1
197.52.198.220	Egypt	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1

03-12-2016-17:04:05 to 03-12-2016-18:04:05

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
176.13.7.106	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
197.52.224.68	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP adminlogin access	2
197.52.198.220	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP login.htm access	2
185.72.179.221	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.77.227	Turkey	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
104.45.210.69	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
197.52.198.220	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP admin.php access	1
197.52.189.168	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP adminlogin access	1
109.235.254.181	147.237.77.227	Turkey	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
98.119.105.221	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
218.246.0.97	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.76.31	Austria	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
197.52.224.68	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP admin.php access	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
197.52.198.220	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP adminlogin access	1
197.52.189.168	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP login.htm access	1
197.52.160.36	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP login.htm access	1

03-12-2016-17:04:05 to 03-12-2016-18:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	41
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
89.138.114.170	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	21
89.138.114.170	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
176.228.186.4	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
46.19.86.46	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.12.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.121.70.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	12
2.52.134.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
89.31.57.5	Italy	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
176.13.7.106	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.121.70.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.121.70.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
176.13.7.106	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.121.70.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.64.164.92	Israel	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	7
46.121.70.235	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.212	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.121.70.235	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.121.70.235	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
87.68.146.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.59.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.121.70.235	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.121.70.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.76	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.76	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
149.78.27.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
37.46.39.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.106	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
46.19.85.156	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.32.179.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.85.156	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
149.88.111.143	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.29.224.178	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.78.27.58	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
185.32.179.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.7.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.164.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.178.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.110.32.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.16.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.22.125	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
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	139
2.54.158.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
109.186.184.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
197.52.224.68	Egypt	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	12
197.52.224.68	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.52.224.68	Block	11
68.180.228.158	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/tmuna	Block	8
197.52.224.68	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	7
197.52.198.220	Egypt	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	7
197.52.189.168	Egypt	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	6
197.52.128.201	Egypt	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	6
197.52.198.220	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.52.198.220	Block	6
197.52.189.168	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.52.189.168	Block	6
197.52.160.36	Egypt	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	5
197.52.128.201	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.52.128.201	Block	4
197.52.160.36	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.52.160.36	Block	4
37.26.147.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.57.241.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.188.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
197.52.160.36	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
197.52.189.168	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
197.52.198.220	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
197.52.160.36	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
148.251.178.213	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
197.52.189.168	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/login/	Block	1
79.180.162.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in URL	Block	1
89.139.230.96	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
68.180.228.151	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
46.117.80.182	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/miyun/miyunderugotzmotfortafkidim.aspx	None	1
157.55.39.11	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.217.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1240-he/atal.aspx	Block	1
176.228.186.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.220.145.244	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
197.52.128.201	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
1.39.36.67	India	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Abnormally Long Request method	Block	1
87.71.53.175	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3394.jpg	Block	1
185.25.148.240	Poland	147.237.76.86	navy.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
40.77.167.18	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/contactus.aspx	Block	1
213.57.207.33	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
130.193.240.39	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
197.52.189.168	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
78.55.223.97	Germany	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.220.145.245	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.52.59.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Unknown HTTP Request Method	Block	1
87.71.104.102	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1

03-12-2016-17:04:05 to 03-12-2016-18:04:05