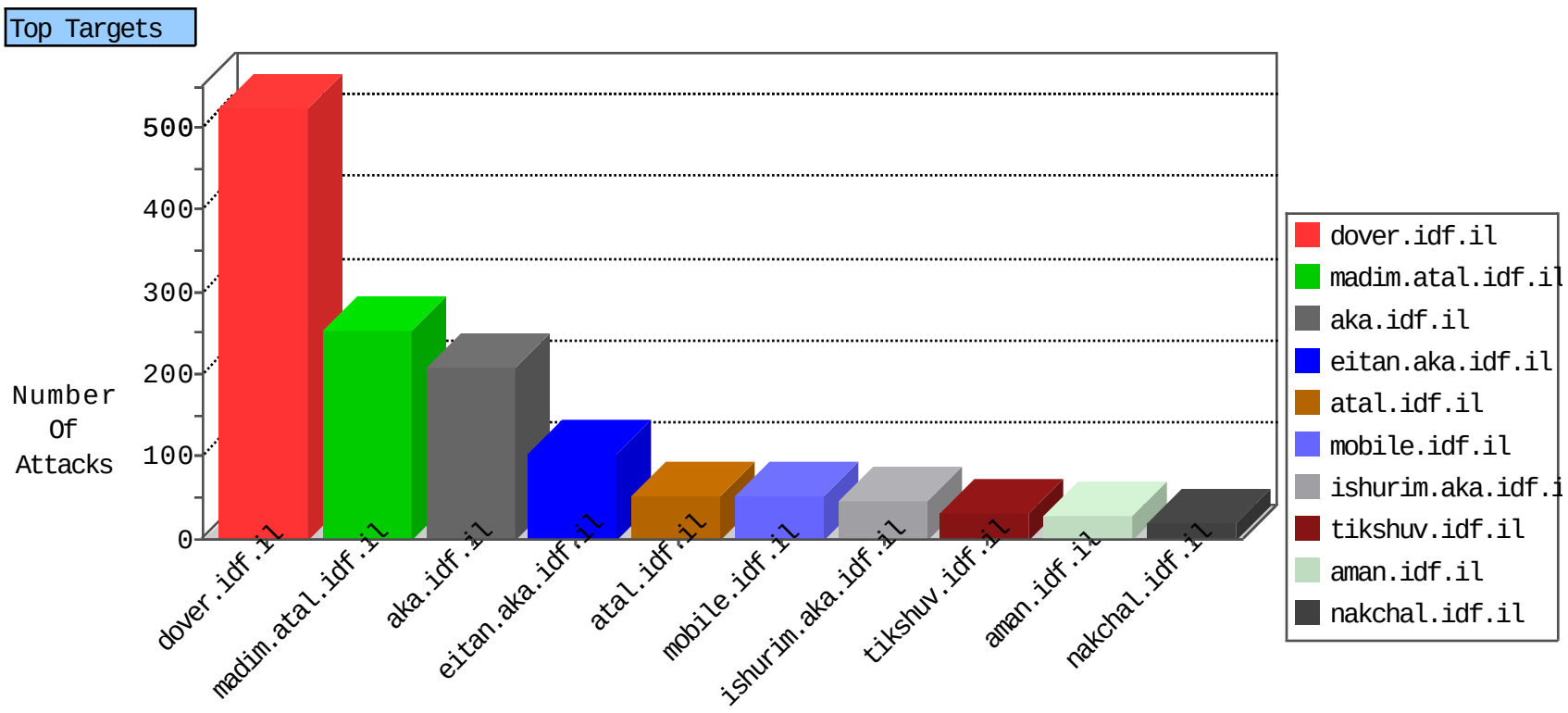
03-06-2016-08:04:02 to 03-06-2016-09:04:02

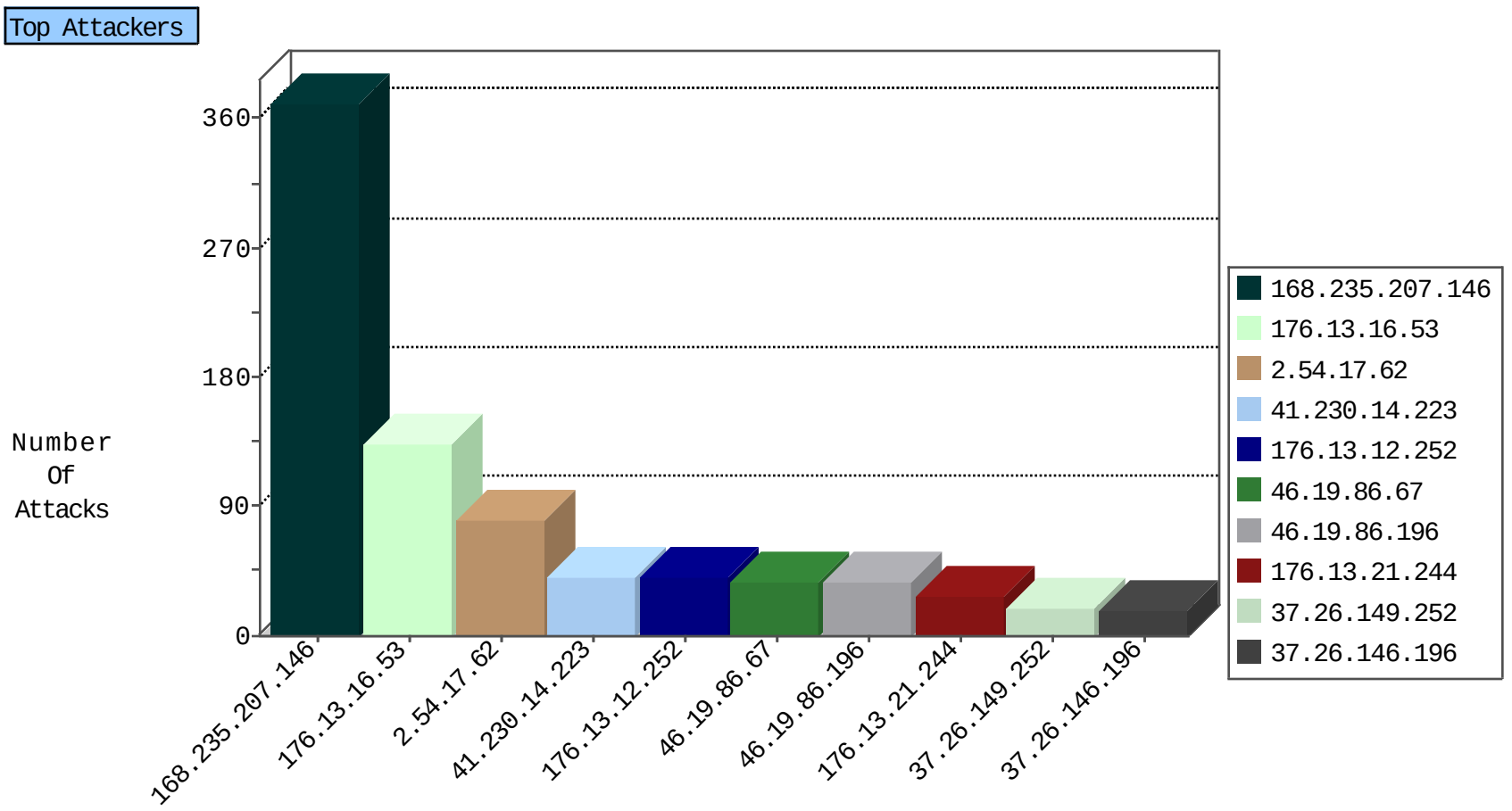
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-06-2016-08:04:02 to 03-06-2016-09:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.146.58	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
2.54.143.43	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
46.19.85.72	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
168.235.207.146	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
168.235.207.146	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	2
46.174.52.5	Russian Federation	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
50.30.37.59	United States	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
50.30.37.59	United States	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
218.57.11.7	China	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
71.6.135.131	United States	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1
46.174.52.5	Russian Federation	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	1
50.30.37.59	United States	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1

03-06-2016-08:04:02 to 03-06-2016-09:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.130.34	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
37.26.147.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
212.235.56.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
207.46.13.98	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-06-2016-08:04:02 to 03-06-2016-09:04:02

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	2
82.200.142.180	147.237.77.19	Kazakstan	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
79.181.181.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.131.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.50.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.213.219.175	147.237.77.234	Romania	halag.idf.il	ET SCAN Potential SSH Scan	1
188.213.219.175	147.237.72.167	Romania	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
188.213.219.175	147.237.0.200	Romania	m4u.idf.il	ET SCAN Potential SSH Scan	1
82.200.142.180	147.237.77.19	Kazakstan	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.181.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.15.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.72.40.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.193.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.213.219.175	147.237.76.200	Romania	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
188.213.219.175	147.237.72.156	Romania	aman.idf.il	ET SCAN Potential SSH Scan	1

03-06-2016-08:04:02 to 03-06-2016-09:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.207.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	365
2.54.17.62	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
46.19.86.67	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	35
176.13.21.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
176.13.12.252	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
176.13.12.252	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
37.142.64.17	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
176.13.17.119	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.52	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.26.149.252	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.185.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.252	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
82.80.179.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.138.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.9.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
37.26.149.252	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.179	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.199.250.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.42.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.55	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.65.109.210	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.64.78.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.69.107.189	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.93.248	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
138.134.192.10	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.39.147	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.178.198.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.17.42.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.200.205.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.16	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.2.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.188.106	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.188.106	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack		reject	3
2.54.21.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.117.105.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.17.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.55	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
80.179.9.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.33.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.158.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.23.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-06-2016-08:04:02 to 03-06-2016-09:04:02

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.64.84.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.105	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

03-06-2016-08:04:02 to 03-06-2016-09:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.16.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	132
46.19.86.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
37.26.146.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
109.253.137.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
46.19.86.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
109.253.131.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	8
176.13.21.244	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.54.188.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
81.218.190.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
37.26.148.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	3
2.54.42.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
80.246.130.94	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
95.86.81.232	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/&sa=u&ved=0ahukewia0pdgtkvlahxmqzokhv7javiqfggtmai&usg=afqjcnhsjqzgxohl-8ga1aemjbw8wkvaxw	Block	2
108.181.188.110	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
84.109.107.72	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
5.141.226.90	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter amp;pagenum in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
80.246.133.235	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
203.133.170.162	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.208.7.104	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/1381.pdf&quot	Block	1
40.77.167.14	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
96.37.251.35	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
84.109.107.72	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/contactus/contactus.aspx	Block	1
198.20.69.74	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
46.19.86.235	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
84.109.107.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
212.76.107.57	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 212.76.107.57	Block	1
66.249.64.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
40.77.167.92	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
96.37.251.35	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
217.194.199.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.109.107.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
203.127.58.234	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
49.205.20.125	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
94.76.47.87	Bahrain	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
37.26.146.238	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.76.107.57	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1256-he/refuah.aspx&sa=u&ved=0ahukewj3kcknvkvlahwknpokhwaideeqfggimaa&usg=afqjcnednnsd4ekw3ac366wui0wxpegsow	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=f1d1ae64kkkkkkk_f1d1ae64	Block	1
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	1
98.130.2.59	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/old/wp-admin/	Block	1
84.109.107.72	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
2.54.185.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
219.74.37.98	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.178.201.104	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 80.178.201.104	Block	1
203.127.96.212	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

03-06-2016-08:04:02 to 03-06-2016-09:04:02