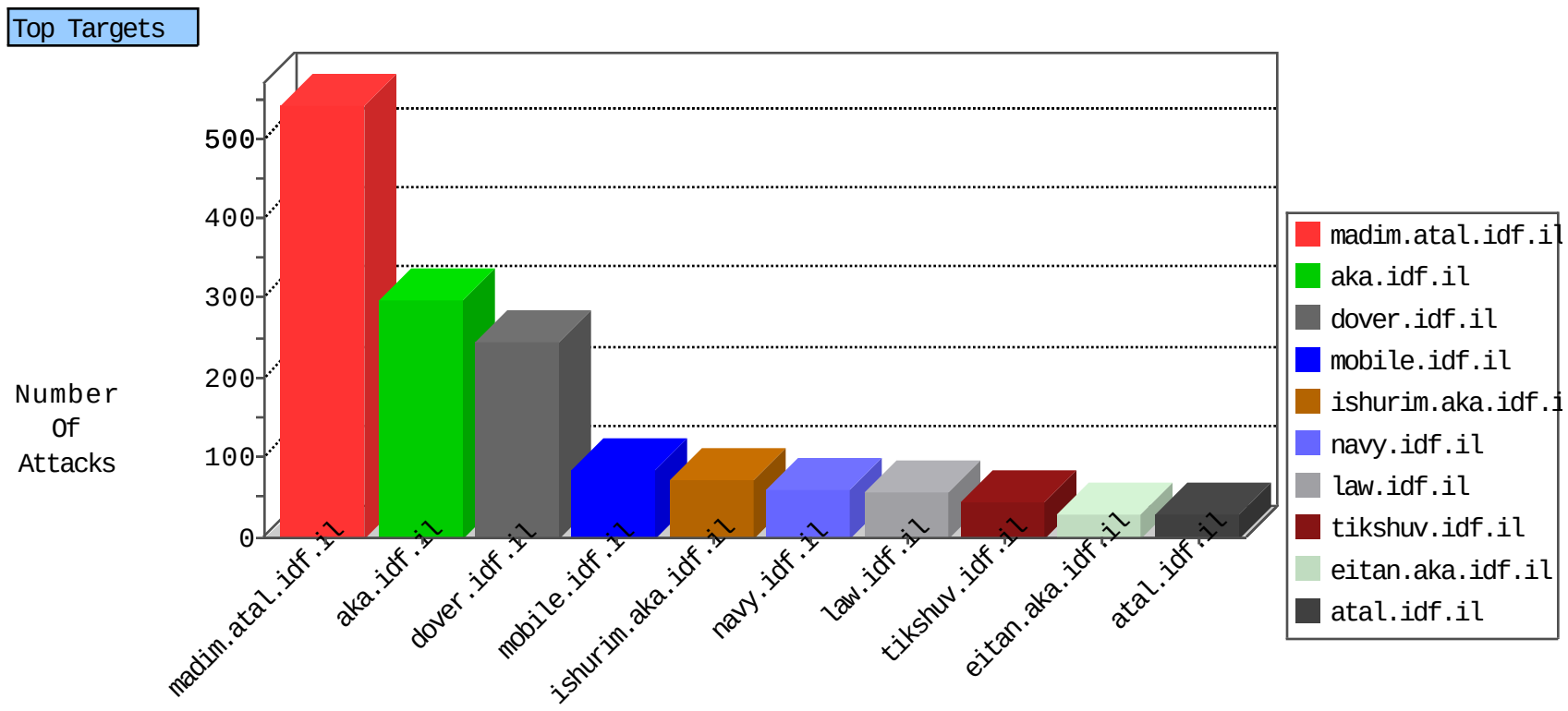
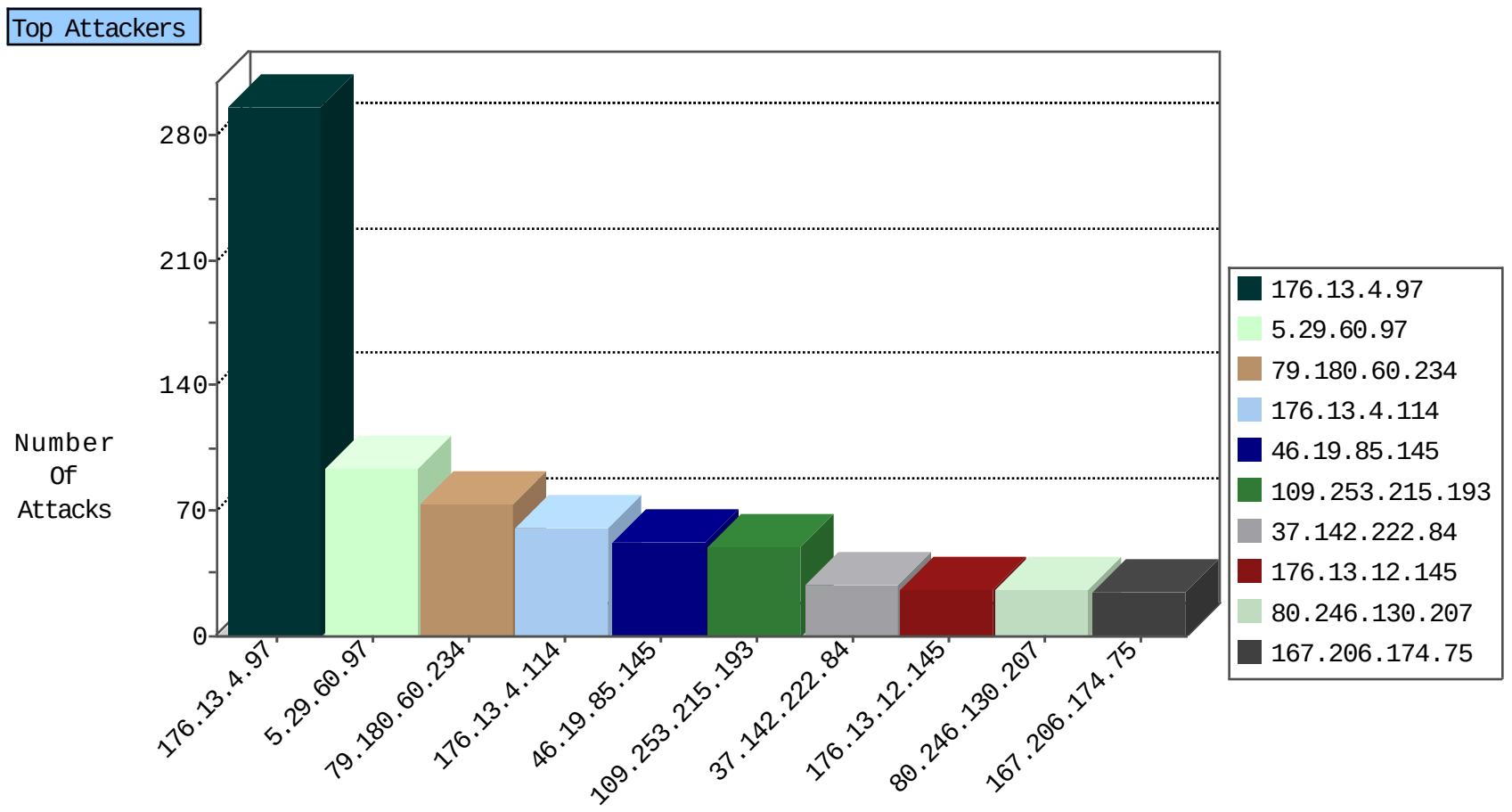
03-08-2016-20:04:10 to 03-08-2016-21:04:10

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-08-2016-20:04:10 to 03-08-2016-21:04:10

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.182.150	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
79.182.162.137	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.143.254.66	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
222.186.52.140	China	147.237.0.17	m.my-kosher-kravi.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
223.197.242.78	Hong Kong	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
104.156.246.165	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
104.156.246.165	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
180.17.42.114	Japan	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
104.156.246.165	United States	147.237.72.217	e.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

03-08-2016-20:04:10 to 03-08-2016-21:04:10

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.233.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	17
83.130.108.116	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
5.29.32.142	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
149.78.89.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
61.135.189.69	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
10.0.0.7		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.64.94.55	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
84.94.187.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.209	United States	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Block	2
188.165.15.41	France	147.237.72.167	ishurim.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.97	France	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
188.165.15.212	France	147.237.77.226	www.chamatz.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
54.186.138.241	United States	147.237.77.74	law.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
212.235.40.29	Israel	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-08-2016-20:04:10 to 03-08-2016-21:04:10

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.207	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.93.117	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.32	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
176.13.4.97	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
79.181.117.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
14.161.5.248	147.237.76.199	Vietnam	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
192.243.55.137	147.237.77.216	Dominica	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.240.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.45.210.69	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
93.189.26.18	147.237.77.176	Austria	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.136.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.11.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
68.180.229.239	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.187.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
112.124.10.141	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.77.205	Austria	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.76.42	Austria	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

03-08-2016-20:04:10 to 03-08-2016-21:04:10

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.4.97	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	90
79.180.60.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
176.13.4.114	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
176.13.4.97	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	45
167.206.174.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
109.65.197.155	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
176.13.12.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
85.65.153.239	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
84.94.194.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.130.207	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
188.29.165.152	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
66.249.64.169	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.66.16.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.140.114	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.130.207	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
79.180.60.234	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.26.149.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
109.253.143.169	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.190.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.178.19.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.12.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.144.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.201	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.64.16.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.104.125	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.177.190.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.102.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.130.221.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
37.26.149.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
211.23.251.92	Taiwan	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
94.230.86.72	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.129	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
89.139.186.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.219.122.4	Poland	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.70.44.165	Sweden	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
37.26.147.248	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.120.126.62		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.39.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.4.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
5.29.60.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
46.19.85.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
109.253.215.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
37.142.222.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
185.3.144.76	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	10
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	6
96.56.9.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
2.54.20.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.142.64.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.150.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
183.206.160.57	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 183.206.160.57	Block	2
46.19.85.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
101.226.168.200	China	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
220.255.97.58	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
207.46.13.37	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
85.250.138.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl67 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17060-en/dover.aspx>.	Block	1
183.206.160.57	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/includes/fckeditor/editor/	Block	1
105.157.254.150	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
79.180.60.234	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sip_storage/files/	Block	1
207.46.13.99	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/1132-8613-he/navy.aspx.aspx	Block	1
5.29.203.30	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
149.78.194.94	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
86.31.127.203	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	1
213.57.37.251	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.65.51.190	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.246.130.116	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1437-he/atal.aspx	Block	1
207.46.13.100	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
156.199.76.2		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
93.173.32.63	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/armored/barak.stm<p>	Block	1
213.151.47.162	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/&sa=u&ved=0ahukewinopll4rhlahxdwhqkhqg7dlmqfggumae&usg=afqjcnexum5xtap6fajrxy3kwnzuhyjgig	Block	1
183.206.160.57	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/includes/fckeditor/editor/	Block	1
109.160.170.210	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
84.94.194.236	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
156.199.76.2		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
217.132.106.88	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
84.229.133.22	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/yoman.asp	Block	1

03-08-2016-20:04:10 to 03-08-2016-21:04:10