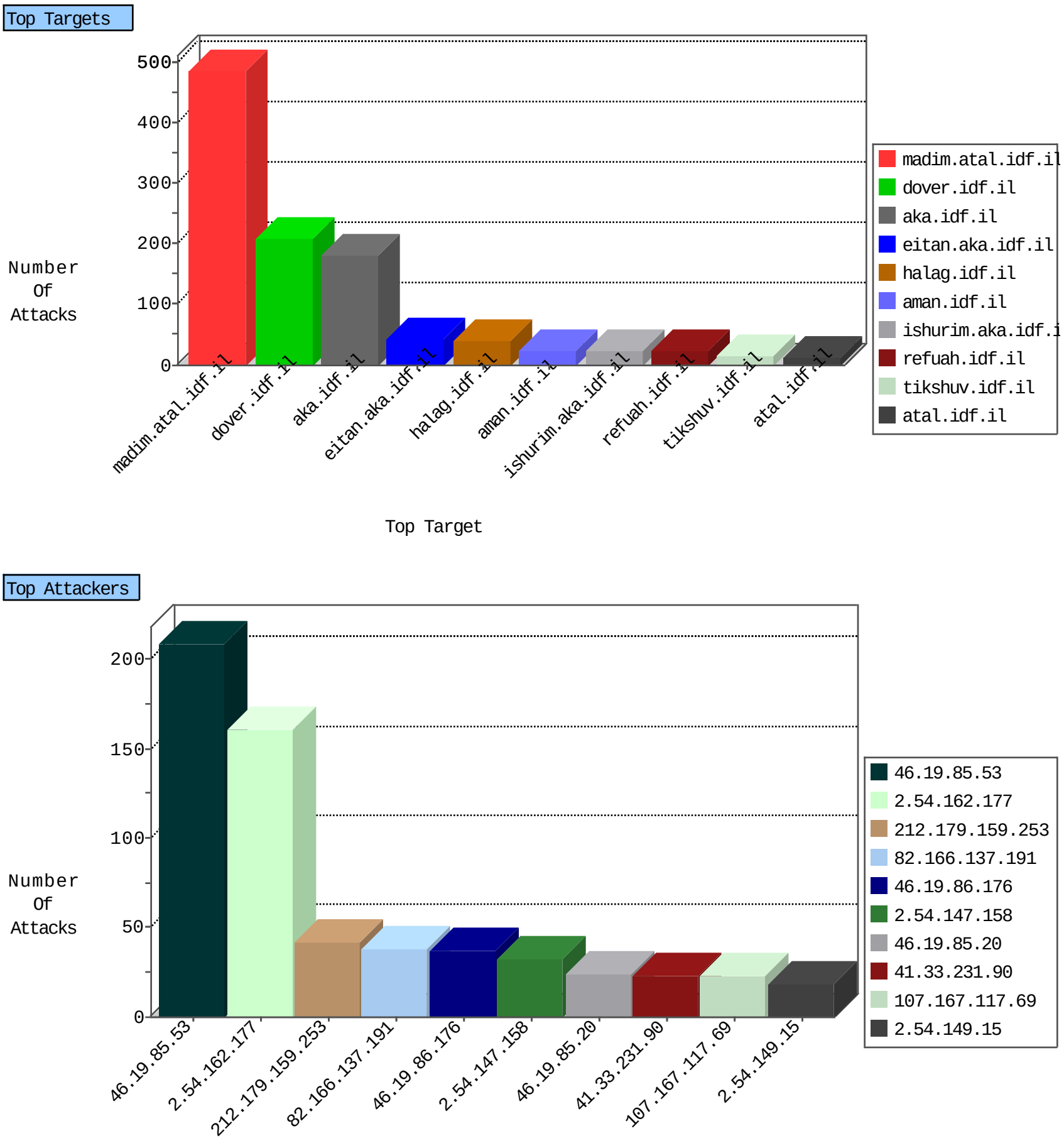
02-23-2016-12:04:09 to 02-23-2016-13:04:09

IDF Under Attack Daily Report



02-23-2016-12:04:09 to 02-23-2016-13:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.136.93	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
46.19.85.221	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
176.13.21.212	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
115.239.228.10	China	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Http	drop	1
115.239.228.10	China	147.237.76.176	test.ncore.idf.il	JLM_Purple_Con_Limit_Http	drop	1

02-23-2016-12:04:09 to 02-23-2016-13:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.178.219	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
197.48.101.171	Egypt	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	4
80.178.143.82	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.149.207	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
83.149.126.98	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
188.165.15.75	France	147.237.77.216	dover.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
37.142.152.103	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
62.210.225.135	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

02-23-2016-12:04:09 to 02-23-2016-13:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.210.225.135	147.237.77.74	France	law.idf.il	SQL Injection - Select From	3
197.48.101.171	147.237.77.216	Egypt	dover.idf.il	GPL WEB_SERVER /etc/passwd	3
197.48.101.171	147.237.77.216	Egypt	dover.idf.il	SQL Injection - Select From	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
80.246.139.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.55.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
69.64.46.86	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.121.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.185.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.92.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.234.39.13	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
109.186.38.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.16.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
69.64.46.86	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
217.194.203.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.143.35.213	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.137.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.234.39.13	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
109.234.39.13	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN NMAP -sS window 1024	1

02-23-2016-12:04:09 to 02-23-2016-13:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.159.253	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
82.166.137.191	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
107.167.117.69	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.0.42.2	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	8
62.0.42.2	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
36.85.215.140	Indonesia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.86.161	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
81.218.195.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.86.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.20	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.117.167.66	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.127	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.20	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.214.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
109.253.195.105	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.149.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.149.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.253.195.105	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.246.137.45	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
157.55.39.188	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
77.125.156.31	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	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
176.13.2.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.96.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.40.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.69.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.153.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.215.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.35.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.3.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.150.71.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.57.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
176.13.22.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.45.117	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
83.130.113.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.178.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
81.218.139.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.149.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3

02-23-2016-12:04:09 to 02-23-2016-13:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	208
2.54.162.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	161
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
2.54.147.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
109.253.199.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
109.253.159.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.85.11	Israel	147.237.76.39	mobile.meitav.idf.il	Distributed Suspicious Response Code	Block	7
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
197.48.101.171	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.48.101.171	Block	4
109.253.142.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.13.147	Israel	147.237.72.166	aka.idf.il	Distributed Double URL Encoding	Block	3
136.243.172.46	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/index.php	Block	3
185.32.179.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.57.144	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	3
212.235.56.185	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 212.235.56.185	Block	3
136.243.172.46	Germany	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
176.13.13.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
194.90.66.15	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 194.90.66.15	Block	2
176.13.3.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.134.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
70.39.157.195	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.53	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
191.252.48.220	Brazil	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 191.252.48.220	Block	1
8.37.70.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-en/dover.aspx&usg=alkjrhirko5qltnhvv0joop6mdpncaup6w	Block	1
82.166.137.191	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.165	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/510-he/patzar.asph	Block	1
37.26.147.217	Israel	147.237.72.166	aka.idf.il	Distributed Double URL Encoding	Block	1
2.54.13.147	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
77.127.44.133	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH_RESUMED_SESSION)	None	1
191.252.48.220	Brazil	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
8.37.70.237	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1400-en/dover.aspx&usg=alkjrhjuiyav5zpixvkwmh36_9ob_jxvda	Block	1
141.212.122.209	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/	Block	1
93.172.136.177	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
197.48.101.171	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/abc123/	Block	1
66.249.78.159	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
212.143.214.185	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.181.52.70	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.117.167.66	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
157.55.39.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	1
109.66.158.79	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/valtam	Block	1
207.46.13.19	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
188.165.15.75	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
128.232.110.28	United Kingdom	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
79.181.215.251	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1

02-23-2016-12:04:09 to 02-23-2016-13:04:09