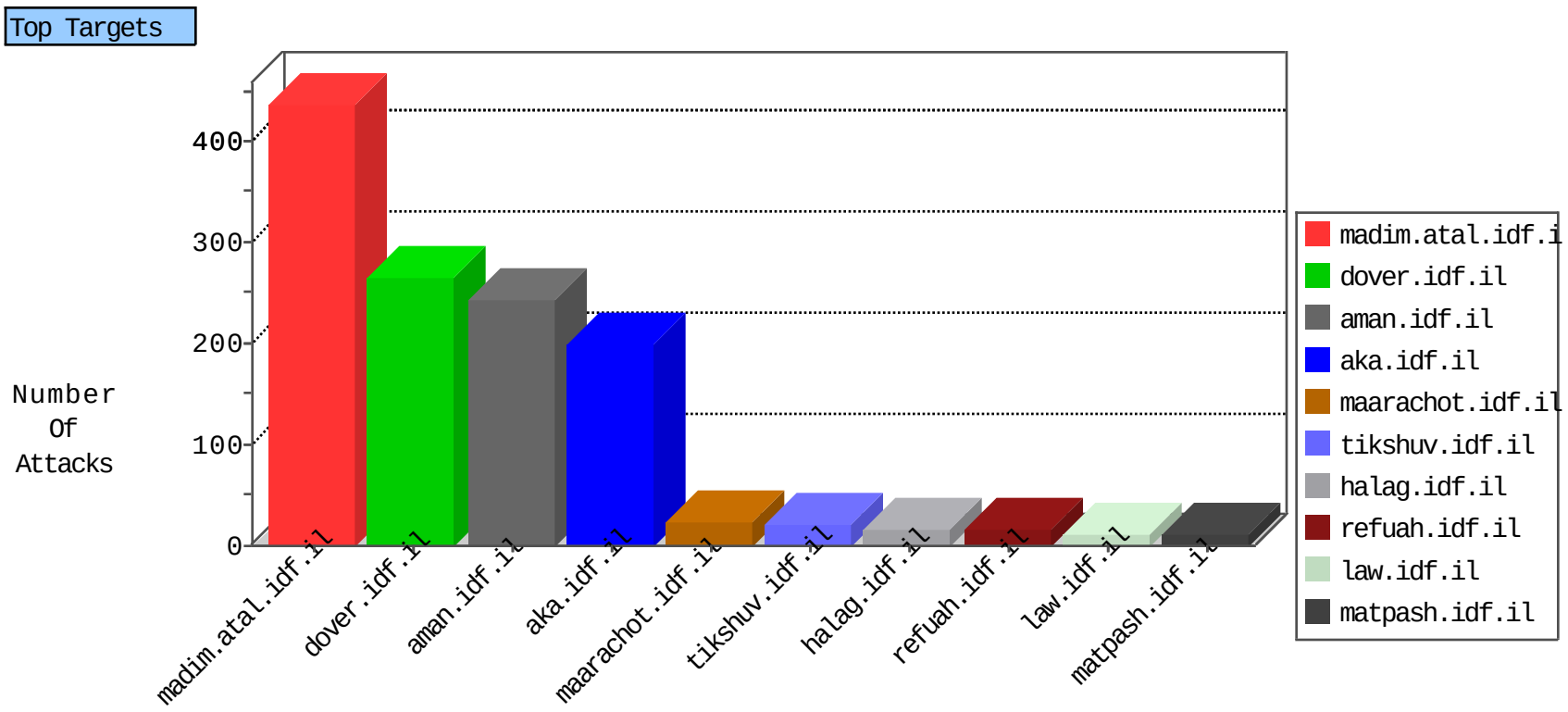
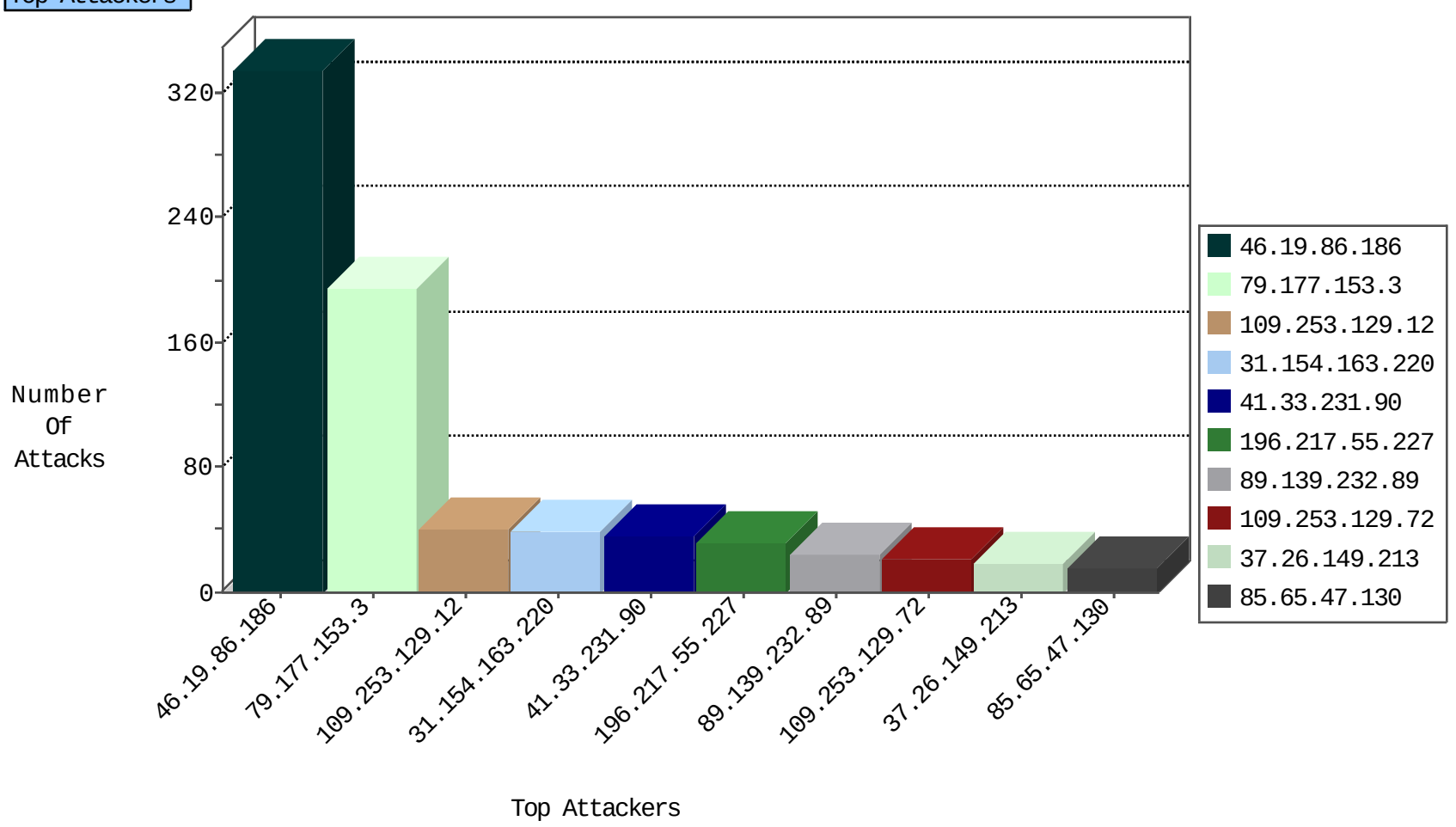
02-17-2016-17:04:06 to 02-17-2016-18:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-17-2016-17:04:06 to 02-17-2016-18:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.46.189	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
112.153.177.208	Korea, Republic of	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	2
185.94.111.1		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

02-17-2016-17:04:06 to 02-17-2016-18:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-17-2016-17:04:06 to 02-17-2016-18:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.26	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.140	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
149.78.1.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.130.185	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
97.74.236.44	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.154.17.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
97.74.236.44	147.237.72.217	United States	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
97.74.236.44	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.20.69.74	147.237.72.166	United States	aka.idf.il	ET DROP Dshield Block Listed Source	1
94.102.49.151	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.201.227.104	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.246.130.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.54.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
182.72.109.162	147.237.76.30	India	himush.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.63.156	147.237.77.176	Singapore	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.117.6.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.233.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.68.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
97.74.236.44	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.139.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
97.74.236.44	147.237.0.33	United States	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.179.155.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.49.151	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.95.49.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.240	147.237.77.205		prisha.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.127.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.82.106.200	147.237.76.86	India	navy.idf.il	ET SCAN NMAP -sS window 4096	1
79.176.104.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-17-2016-17:04:06 to 02-17-2016-18:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.154.163.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
196.217.55.227	Morocco	147.237.77.216	dover.idf.il	drop		drop	31
2.52.5.140	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.86.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.210.187.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.52.2.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.176.224.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.213	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence		monitor	6
109.64.39.60	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
172.56.35.73	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
149.88.151.144	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
172.56.35.73	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
149.88.151.144	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
5.28.130.228	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.149.213	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence		alert	5
192.116.158.98	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
89.108.155.34	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.213	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.64.39.60	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
89.108.155.34	Lebanon	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.158	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.37.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.34.114	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
176.13.4.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.222.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.236.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.5.83	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.179.177.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.211	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.142.68.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.235.55.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
199.203.63.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.199.34.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.28.130.228	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.176.102.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.34.251	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.22.131.103	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.34.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.134.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.209.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.130.228	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.66.12.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

02-17-2016-17:04:06 to 02-17-2016-18:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.153.3	Israel	147.237.72.156	aman.idf.il	Automated Vulnerability Scanning	Block	193
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	165
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	132
109.253.129.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	38
89.139.232.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
109.253.129.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
46.19.86.45	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.19.86.45	Block	13
85.65.47.130	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.47.130	Block	10
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
40.77.167.38	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
85.65.47.130	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	5
84.110.108.12	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.110.108.12	Block	4
2.54.160.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash/login/default.asp	Block	3
84.110.108.12	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
95.141.38.108	Italy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.171.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.144.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
95.141.38.110	Italy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.229.135.17	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
85.173.19.25	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
84.94.165.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$96 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
185.120.125.37		147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$76 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
89.139.232.217	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
37.142.219.76	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.219.76	Block	1
84.229.135.17	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
79.178.186.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$15 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
120.141.193.113	Malaysia	147.237.72.166	aka.idf.il	eMail Hoarding	Block	1
66.249.64.170	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
95.141.38.109	Italy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.71.11.157	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 87.71.11.157 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
193.169.70.108	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
89.139.232.217	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/ufi/reaction/	Block	1
37.142.219.76	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
85.64.156.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$71 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.179.4.80	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
132.74.211.123	Israel	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/107243.pdf	Block	1
87.71.11.157	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
31.210.187.82	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$23 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
197.38.197.170	Egypt	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
109.253.146.202	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1134-he/dover.aspx	Block	1
95.141.38.106	Italy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
213.151.44.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$105 in aka.idf.il/main/giyus/questionnaire.aspx	None	1

02-17-2016-17:04:06 to 02-17-2016-18:04:06