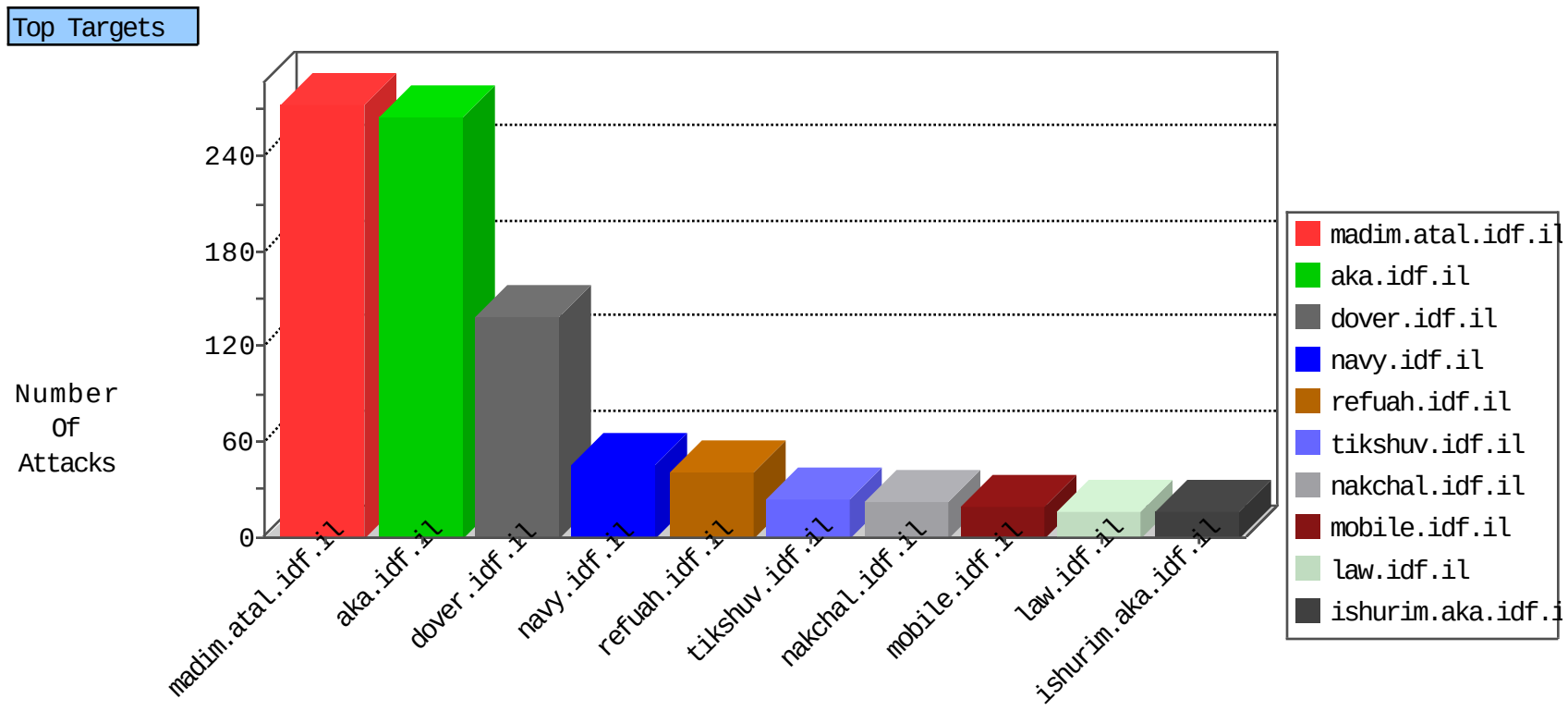
02-23-2016-13:04:00 to 02-23-2016-14:04:00

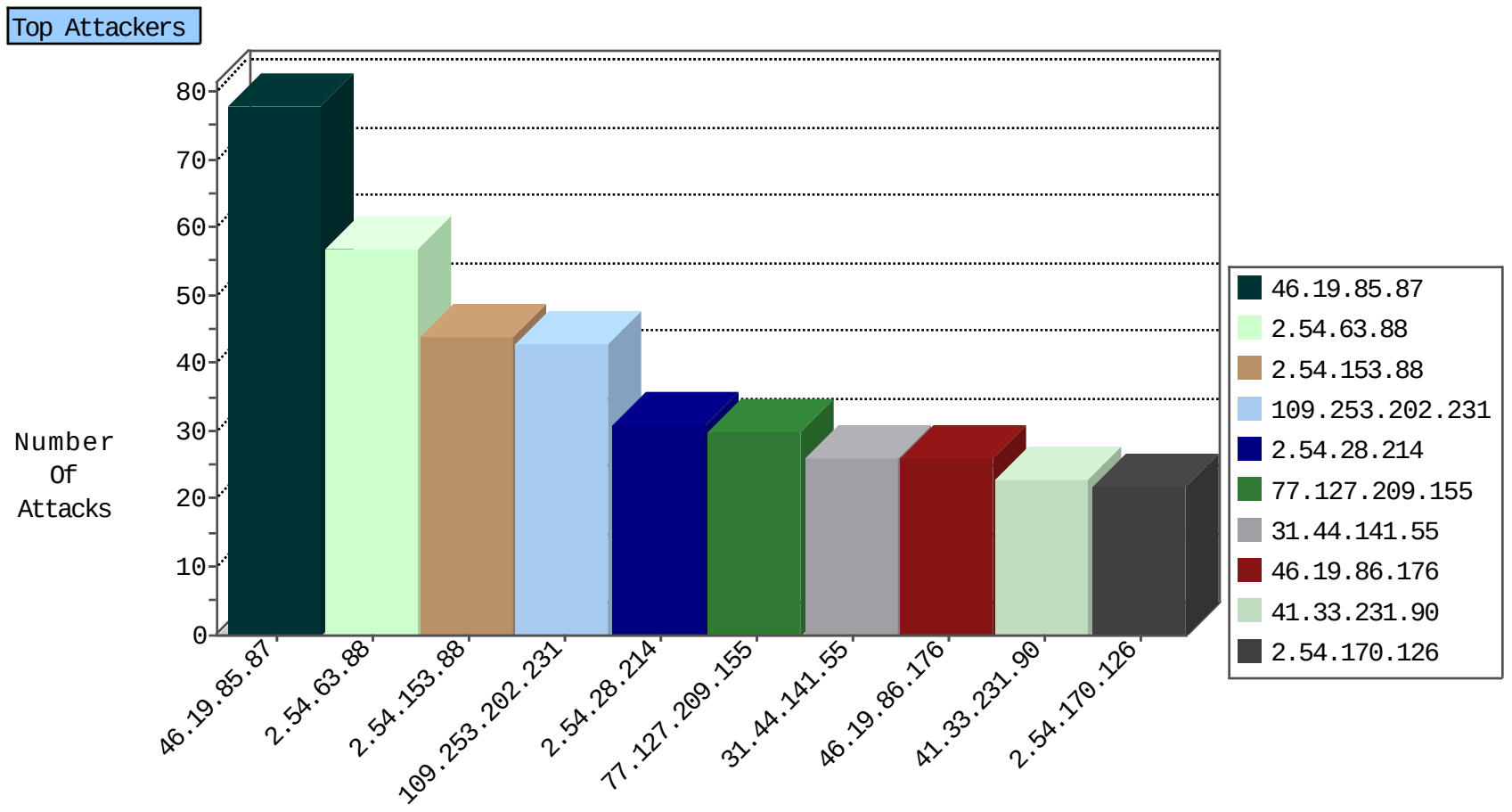
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-23-2016-13:04:00 to 02-23-2016-14:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.44.141.55	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
31.44.141.55	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
221.215.123.74	China	147.237.77.212	e.dover.idf.il	Invalid TCP Flags	drop	1
62.219.229.81	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

02-23-2016-13:04:00 to 02-23-2016-14:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.28.132.173	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
109.253.198.15	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
62.210.225.135	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
82.69.125.19	United Kingdom	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

02-23-2016-13:04:00 to 02-23-2016-14:04:00

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	5
79.177.27.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.225.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.198.151.44	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1
37.73.209.133	147.237.77.216	Ukraine	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.5.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.59.33.61	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
109.64.21.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.113.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.162.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
46.151.52.210	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
37.142.68.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.89.216.239	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.18.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.162.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.186.11.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.113.125.11	147.237.8.14	Romania	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.133.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-23-2016-13:04:00 to 02-23-2016-14:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.153.88	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	44
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
88.198.48.46	Germany	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.117.124.164	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
59.40.23.208	China	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
31.44.141.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.54.174.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.68.251.218	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	11
79.182.200.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.59.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
62.0.207.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.166.23.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.59.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.194.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.66.15	Israel	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	5
80.178.195.117	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.4.223	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
62.0.207.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.59.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.59.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
79.181.212.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.88.0.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
37.26.149.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.204.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.226.48.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.196.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.63.88	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.233.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
84.110.38.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.18.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.6.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.44.141.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
77.125.96.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.10	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.63.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.39.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.169.70.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.57.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.19.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-23-2016-13:04:00 to 02-23-2016-14:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.114.2.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.79.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.200.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-23-2016-13:04:00 to 02-23-2016-14:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
2.54.63.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
109.253.202.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
2.54.28.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
2.54.170.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
132.74.28.190	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 132.74.28.190	Block	9
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	6
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.160.242.40	Block	6
79.177.236.245	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.177.236.245	Block	5
185.89.216.227		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.66.53.245	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 109.66.53.245	Block	4
191.252.48.220	Brazil	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 191.252.48.220	Block	4
213.8.204.77	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/1137-he/patzar.aspx	Block	4
46.19.86.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.4.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
80.178.195.117	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	3
79.177.236.245	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
88.198.48.46	Germany	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 88.198.48.46	Block	3
109.253.131.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.13.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.181.173.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.194.153	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.6.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.66.53.245	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	2
176.13.0.39	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	2
134.249.54.139	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	2
185.89.216.236		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
131.253.25.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
217.194.197.154	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
88.198.48.46	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/usercontrols/headerupper/	Block	1
84.95.251.241	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/print.css	Block	1
189.219.197.194	Mexico	147.237.77.74	law.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
146.90.96.63	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.66.188	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
84.111.6.52	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
59.40.23.208	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/homepage/homepage.aspx	Block	1
31.168.23.60	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.60	Block	1
217.194.197.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.251.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/1740.png	Block	1
157.55.39.188	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
46.19.85.252	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
207.46.13.19	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.65.87.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$7 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
80.230.56.45	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.89.216.228		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
62.219.47.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
132.74.28.190	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1796.jpg	Block	1

02-23-2016-13:04:00 to 02-23-2016-14:04:00