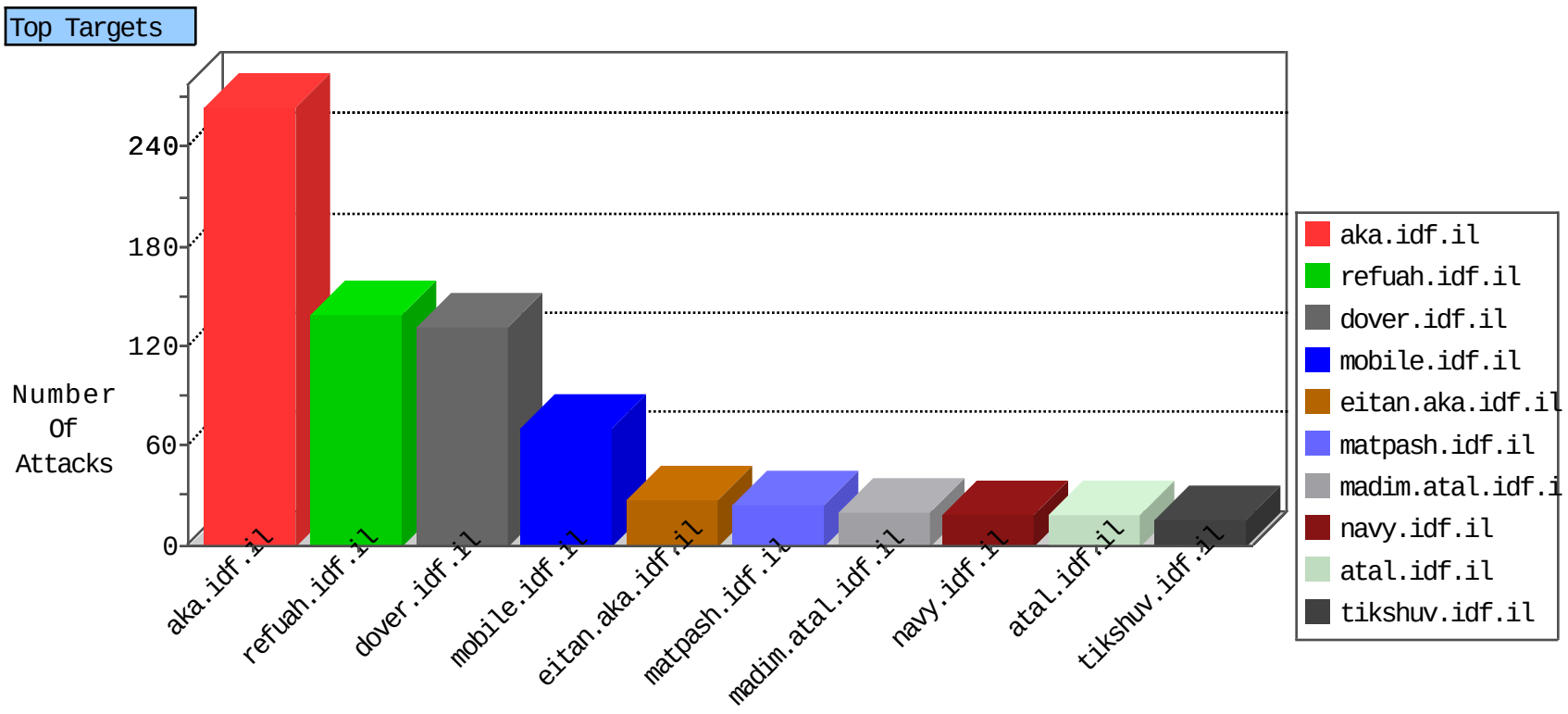
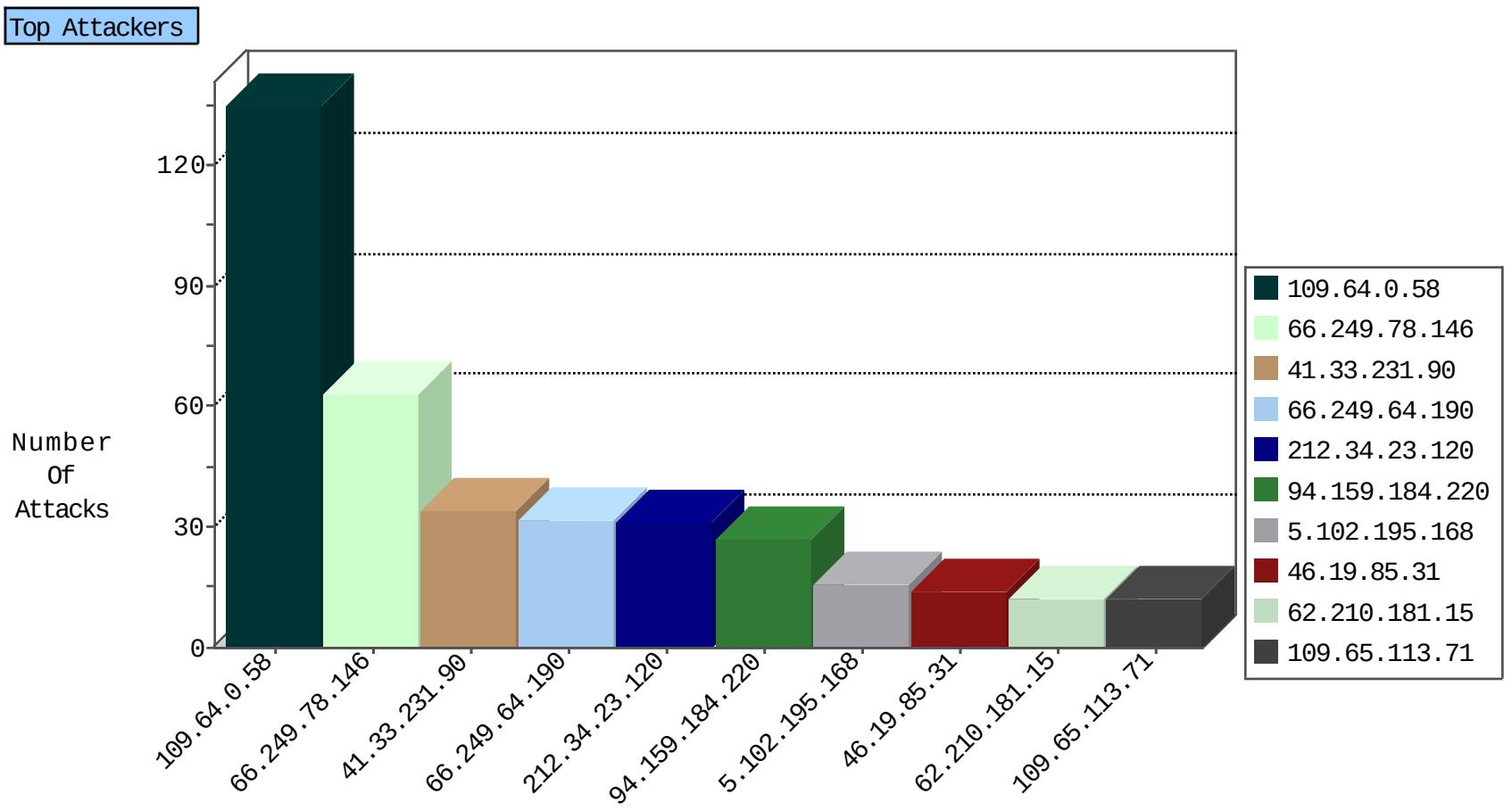
02-28-2016-00:04:07 to 02-28-2016-01:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-28-2016-00:04:07 to 02-28-2016-01:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.151.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
77.81.191.126	Romania	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
77.81.191.126	Romania	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
205.209.185.11	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
157.208.240.5	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
77.81.191.126	Romania	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
216.220.226.51	United States	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
82.81.19.8	Israel	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	1
168.235.207.43	United States	147.237.77.233	atal.idf.il	JLM_Under_Attack_Con_Http	drop	1
77.81.191.126	Romania	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
205.209.185.11	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1

02-28-2016-00:04:07 to 02-28-2016-01:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.132.13.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
82.81.19.8	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
61.135.189.121	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
185.106.92.164		147.237.76.31	nakchal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	3
95.86.87.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.59	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
185.106.92.164		147.237.76.31	nakchal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
51.255.65.71	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.72	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.29	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-28-2016-00:04:07 to 02-28-2016-01:04:07

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	4
118.165.7.106	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN Potential SSH Scan	1
89.248.162.167	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1
202.71.25.29	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -sS window 2048	1
202.71.25.29	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -f -sS	1
198.180.198.235	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
195.216.176.244	147.237.8.50	Latvia	e.tikshuv.idf.i	ET SCAN NMAP -sS window 1024	1
190.255.254.128	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
118.165.7.106	147.237.76.197	Taiwan	e.himush.idf.il	ET SCAN Potential SSH Scan	1
109.253.214.242	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
89.248.162.167	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
202.71.25.29	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -sS window 1024	1
198.180.198.235	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
198.180.198.235	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
185.106.92.164	147.237.76.31		nakchal.idf.il	ET WEB_SERVER Muieblackcat scanner	1

02-28-2016-00:04:07 to 02-28-2016-01:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.0.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	134
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
94.159.184.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
5.102.195.168	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
149.88.77.185	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.113.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.210.181.15	France	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.212	Israel	147.237.0.15	kosher-kravi.idf.i	drop	First packet isn't SYN	drop	7
109.65.59.204	Israel	147.237.72.166	aka.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
185.32.179.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.69.121.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
109.253.214.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.253.214.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
70.199.106.89	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.180.192.82	Israel	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
185.32.179.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.242.220	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.28.145.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.64.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.207.190	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.141.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.65.180.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.99.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.81.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.227.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.253.137.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.179.87	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.65.193.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.18.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.150.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
85.130.227.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.158.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.200.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.177	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.5.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.219.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.24.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.190.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-28-2016-00:04:07 to 02-28-2016-01:04:07

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

02-28-2016-00:04:07 to 02-28-2016-01:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	23
79.180.123.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
212.34.23.120	Jordan	147.237.77.176	matpash.idf.il	Multiple Unknown HTTP Request Method from 212.34.23.120	Block	7
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	7
212.34.23.120	Jordan	147.237.77.176	matpash.idf.il	Multiple Malformed URL from 212.34.23.120	Block	7
46.19.85.189	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	6
79.179.233.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	3
2.54.61.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.5.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.60.96	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
212.34.23.120	Jordan	147.237.77.176	matpash.idf.il	Multiple Illegal HTTP Version from 212.34.23.120	Block	3
212.34.23.120	Jordan	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 212.34.23.120	Block	2
82.132.215.202	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	2
212.34.23.120	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.23.120	Block	2
79.178.12.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
212.34.23.120	Jordan	147.237.77.176	matpash.idf.il	Multiple Abnormally Long Request from 212.34.23.120	Block	2
40.77.167.3	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.34.23.120	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.23.120	Block	2
149.88.156.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	2
176.13.8.82	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
2.54.25.181	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
157.55.39.154	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.64.160	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/2/1682.doc	Block	1
89.139.232.161	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 38.111.147.88	Block	1
79.177.152.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
185.7.123.134	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter Ca in www.aka.idf.il/giyus/general/default.asp	None	1
46.19.86.229	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.64.0.58	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.81.218	United States	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
212.34.23.120	Jordan	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
173.252.90.124	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.170	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21744-ar/idfgdover.aspx	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter Do in www.aka.idf.il/giyus/general/default.asp	None	1
46.117.134.101	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
109.253.209.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
82.166.240.205	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.179.87	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	1
212.34.23.120	Jordan	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
94.230.86.177	Israel	147.237.77.243	mobile.idf.il	Multiple Untraceable SSL Sessions from 94.230.86.177 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/giyus/kadatz/	None	1
62.210.181.15	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/2/2772	Block	1
86.164.46.15	United Kingdom	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.29.39.233	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
212.34.23.120	Jordan	147.237.77.216	dover.idf.il	Malformed URL http/1.1	Block	1

02-28-2016-00:04:07 to 02-28-2016-01:04:07