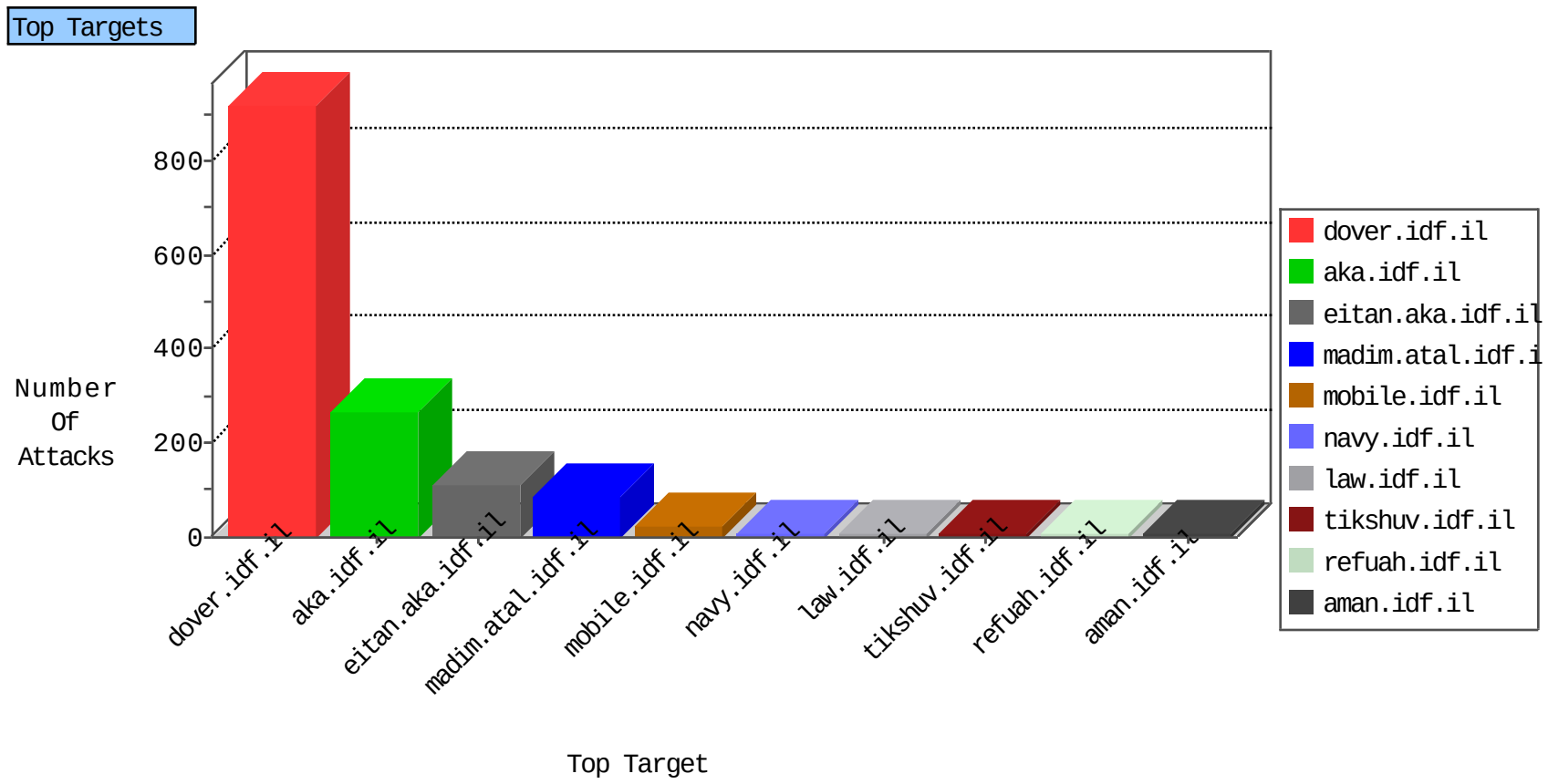
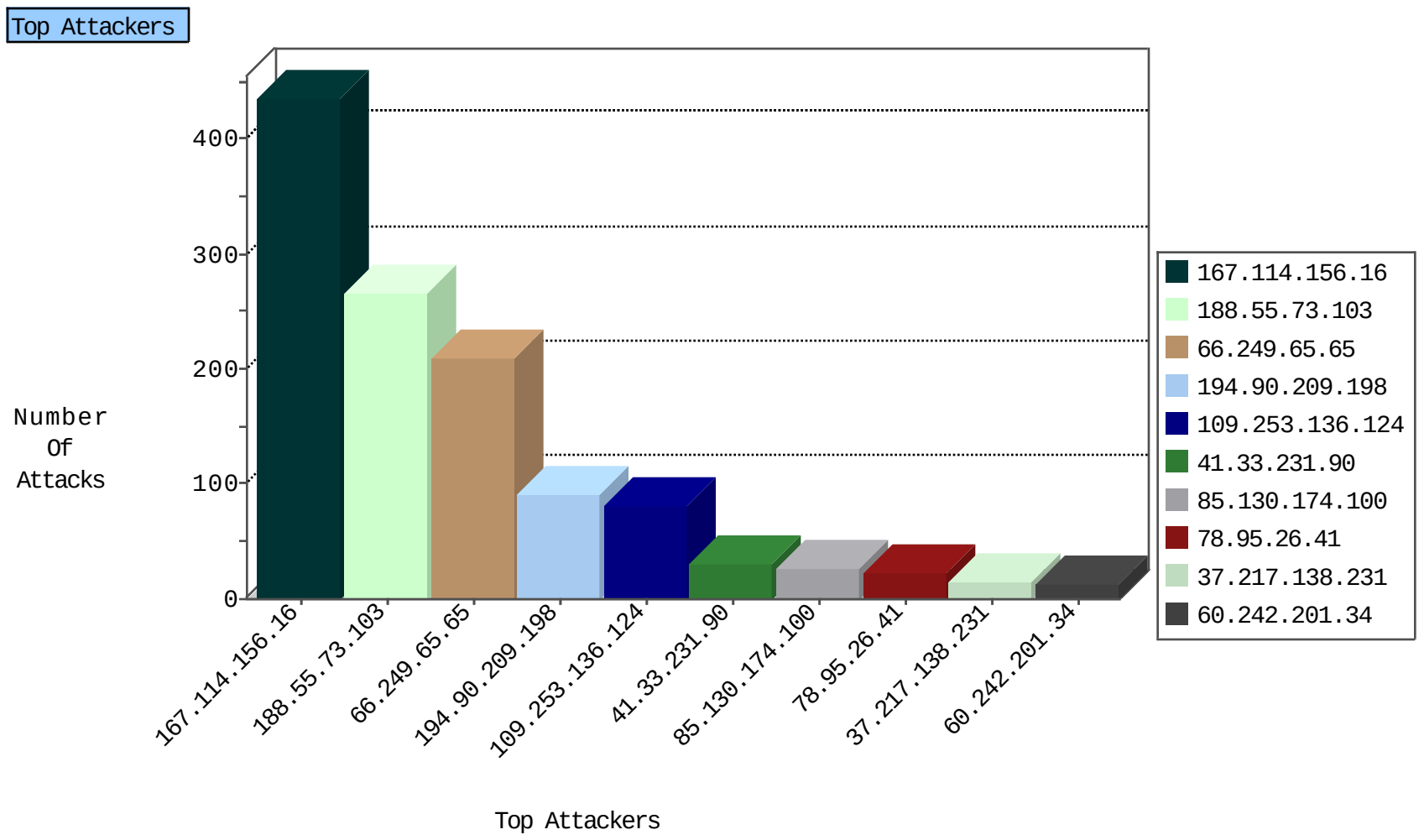
04-22-2016-00:04:00 to 04-22-2016-01:04:00

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-22-2016-00:04:00 to 04-22-2016-01:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	20177
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3508
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2302
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	21
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
94.102.52.10	Netherlands	147.237.76.176	test.ncore.idf.i	Block_Ntp_All_Net	drop	1

04-22-2016-00:04:00 to 04-22-2016-01:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-22-2016-00:04:00 to 04-22-2016-01:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
188.55.73.103	147.237.77.216	Saudi Arabia	dover.idf.il	SERVER-WEBAPP admin.php access	10
188.55.73.103	147.237.77.216	Saudi Arabia	dover.idf.il	SERVER-WEBAPP login.htm access	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
188.55.73.103	147.237.77.216	Saudi Arabia	dover.idf.il	SERVER-WEBAPP adminlogin access	3
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
91.201.236.155	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.173.27.62	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.139.150.224	147.237.77.216	Israel	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
82.117.208.243	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.99	147.237.76.86	Lithuania	navy.idf.il	ET SCAN Potential SSH Scan	1
13.92.196.2	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
185.130.5.99	147.237.72.166	Lithuania	aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.8.27	Lithuania	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.0.19	Lithuania	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.155	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
82.117.208.243	147.237.72.14		dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.99	147.237.77.205	Lithuania	prisha.idf.il	ET SCAN Potential SSH Scan	1
61.135.189.113	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
185.130.5.99	147.237.76.30	Lithuania	himush.idf.il	ET SCAN Potential SSH Scan	1
13.92.196.2	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -f -sS	1
185.130.5.99	147.237.72.14	Lithuania	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.0.200	Lithuania	m4u.idf.il	ET SCAN Potential SSH Scan	1
104.214.73.227	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1

04-22-2016-00:04:00 to 04-22-2016-01:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	203
194.90.209.198	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
188.55.73.103	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
37.217.138.231	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
60.242.201.34	Australia	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.174.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.65.136.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.174.100	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
85.130.174.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
78.95.26.41	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
78.95.26.41	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
78.95.26.41	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.178.123.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.175.142.142	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.14.176.28	Spain	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.76.107.108	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
12.13.100.90	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
100.127.150.249		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
149.88.186.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.26.146.177	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
87.70.79.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.177	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
188.55.73.103	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
118.173.135.239	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
52.90.224.157	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
195.239.16.53	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.142.64.2	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
78.164.105.211	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
131.253.25.240	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.177.84.176	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
5.254.65.18	Turkey	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
94.230.86.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.55.73.103	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.55.73.103	Block	83
109.253.136.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
188.55.73.103	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 188.55.73.103	Block	79
188.55.73.103	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	57
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.65.65	Block	4
181.30.30.166	Argentina	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 181.30.30.166	Block	3
62.0.71.3	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/2/	Block	2
88.198.48.46	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/shared/usercontrols/headerupper/	Block	2
17.138.55.96	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.55.96	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
81.218.202.150	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 81.218.202.150	Block	2
62.0.71.3	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	2
2.53.134.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.27.25	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
212.179.60.30	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
181.30.30.166	Argentina	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.181.27.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/xmlrpc.php	Block	1
181.30.30.166	Argentina	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8944-he/refuah.aspx	Block	1
54.189.238.182	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
188.55.73.103	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/admin/	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
188.55.73.103	Saudi Arabia	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
157.55.39.32	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.193.247	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/faq/mobile	Block	1
199.30.24.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
61.135.189.113	China	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
173.252.88.189	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
85.64.67.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl79 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
157.55.39.32	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily_statistics/english	Block	1
79.179.231.173	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl79 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
208.115.111.74	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
85.65.109.18	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/shalishut/site/general.aspx	None	1
157.55.39.189	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1