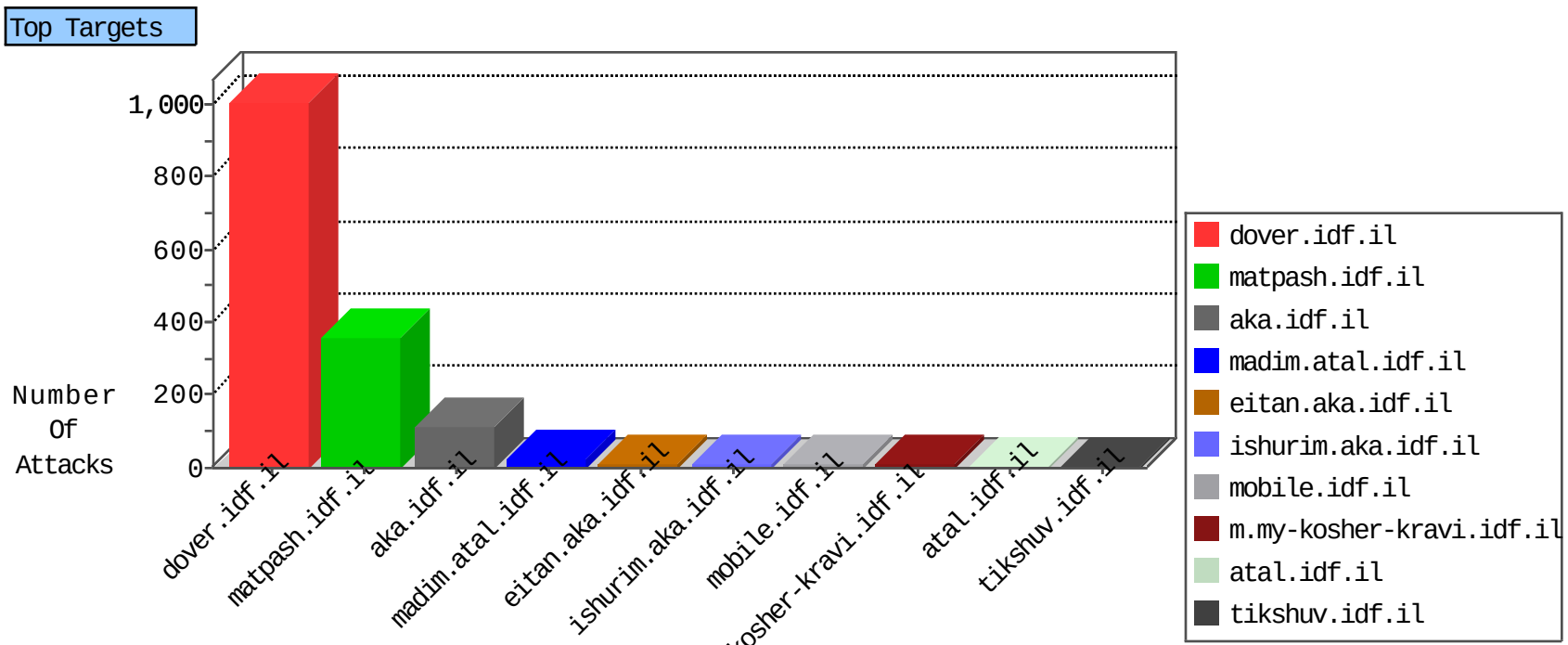
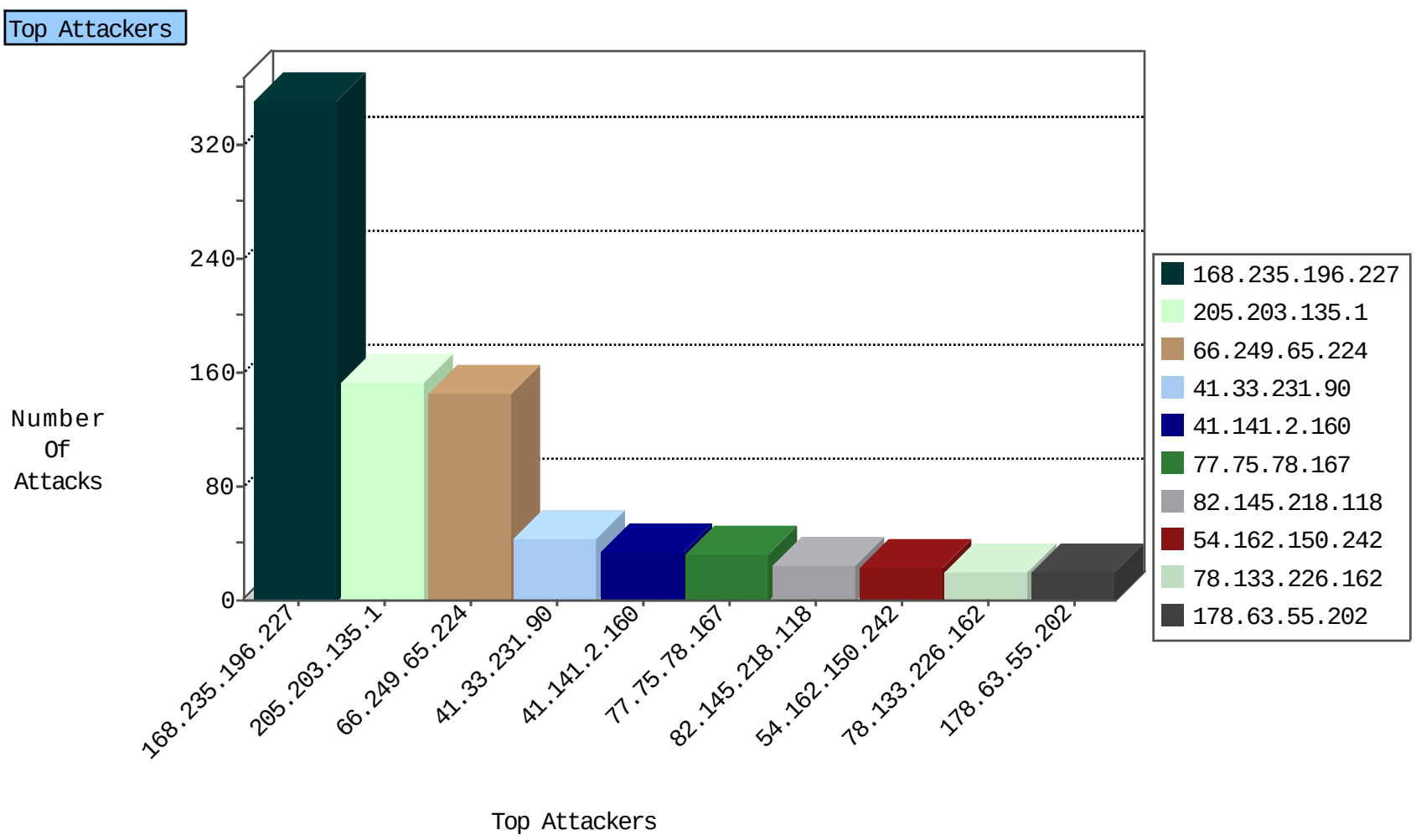
11-20-2015-23:04:06 to 11-21-2015-00:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-20-2015-23:04:06 to 11-21-2015-00:04:06

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	TCP handshake violation, first packet not syn	drop	132
79.180.31.37	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
41.141.2.160	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	11
109.65.139.167	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
222.186.56.39	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
141.212.121.193	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
108.161.253.41	United States	147.237.0.15	kosher-kravi.idf.il	L4 Source or Dest Port Zero	drop	1
176.123.29.54	Moldova, Republic of	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
108.161.253.41	United States	147.237.76.198	e.yohalan.idf.il	L4 Source or Dest Port Zero	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
108.161.253.41	United States	147.237.8.50	e.tikshuv.idf.il	L4 Source or Dest Port Zero	drop	1
108.161.253.41	United States	147.237.72.167	ishurim.aka.idf.il	L4 Source or Dest Port Zero	drop	1
115.239.228.8	China	147.237.0.17	m.my-kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1
176.123.29.54	Moldova, Republic of	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
108.161.253.41	United States	147.237.76.34	yohalan.idf.il	L4 Source or Dest Port Zero	drop	1

11-20-2015-23:04:06 to 11-21-2015-00:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.141.2.160	Morocco	147.237.77.216	dover.idf.il	10767: HTTP: Acunetix Security Scanner	Block	3
41.141.2.160	Morocco	147.237.77.216	dover.idf.il	13465: HTTP: Apache Roller OGNL Command Injection Vulnerability	Block	1
69.30.215.106	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
151.80.31.141	Italy	147.237.0.15	kosher-kravi.idf.i	C228: HTTP: AhrefBot crawler	Block	1

11-20-2015-23:04:06 to 11-21-2015-00:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.125	147.237.77.233	United States	atal.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
77.111.130.61	147.237.72.156	Hungary	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
68.168.137.2	147.237.76.200	Canada	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
68.168.137.2	147.237.76.177	Canada	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
68.168.137.2	147.237.76.30	Canada	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
68.168.137.2	147.237.0.19	Canada	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.56.39	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.6.71.154	147.237.76.34	Poland	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.39	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.49.102	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
68.168.137.2	147.237.76.202	Canada	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
68.168.137.2	147.237.76.197	Canada	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
68.168.137.2	147.237.76.39	Canada	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
68.168.137.2	147.237.0.34	Canada	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.67.224	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
31.6.71.154	147.237.76.177	Poland	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.39	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
23.99.54.247	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

11-20-2015-23:04:06 to 11-21-2015-00:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.196.227	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	351
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	134
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
77.75.78.167	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
82.145.218.118	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
54.162.150.242	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
37.201.169.254	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.35.18.192	Egypt	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
107.170.63.50	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
77.125.120.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
41.141.2.160	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
157.56.0.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	10
87.203.103.152	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.237.140.12	Egypt	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
95.108.132.166	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.65.224	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.142.64.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
70.210.19.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.176.187.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
130.193.50.36	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
95.108.158.173	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.235.80.111	Egypt	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
41.141.2.160	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.219.210.124	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
67.165.21.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
130.193.50.21	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.166.103.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
97.74.24.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.108.158.191	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.135.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.108.158.214	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
78.133.226.162	Poland	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
130.193.50.18	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.255.253.179	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.108.158.228	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
178.154.243.114	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.108.158.232	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.160.151.45	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	6
77.75.78.167	Czech Republic	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.75.78.167	Block	5
77.127.169.8	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
46.19.85.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.41.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.214.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.216.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/ ,mknj ,mkj mjnoikikjoojkmjn,kjj11114114	Block	2
109.160.142.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
79.178.148.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
37.26.147.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.202.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
111.206.116.217	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/login.action	Block	1
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.32.246.43	Italy	147.237.77.74	law.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
77.75.78.167	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.72	Block	1
188.138.1.218	Germany	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
46.120.21.75	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.109.71.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.2	United States	147.237.72.166	aka.idf.il	Unknown Parameter err in www.aka.idf.il/giyus/kiosk/default.asp	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.67.132	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
46.166.190.137	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
149.78.4.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.108.132.167	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar/	Block	1
2.54.46.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/memorial	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.120.79.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
41.141.2.160	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.141.2.160	Block	1
84.229.244.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.67.224	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
149.78.103.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
35.0.127.52	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
204.93.154.198	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 204.93.154.198 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/matak/pages/arbel.aspx	Block	1
109.201.154.225	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.120.216.120	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;utm_campaign in www.aka.idf.il/	None	1
41.143.136.199	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
85.65.17.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-9338-he/dover.aspx	Block	1
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding %K2mZ7Gw1V1 in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1