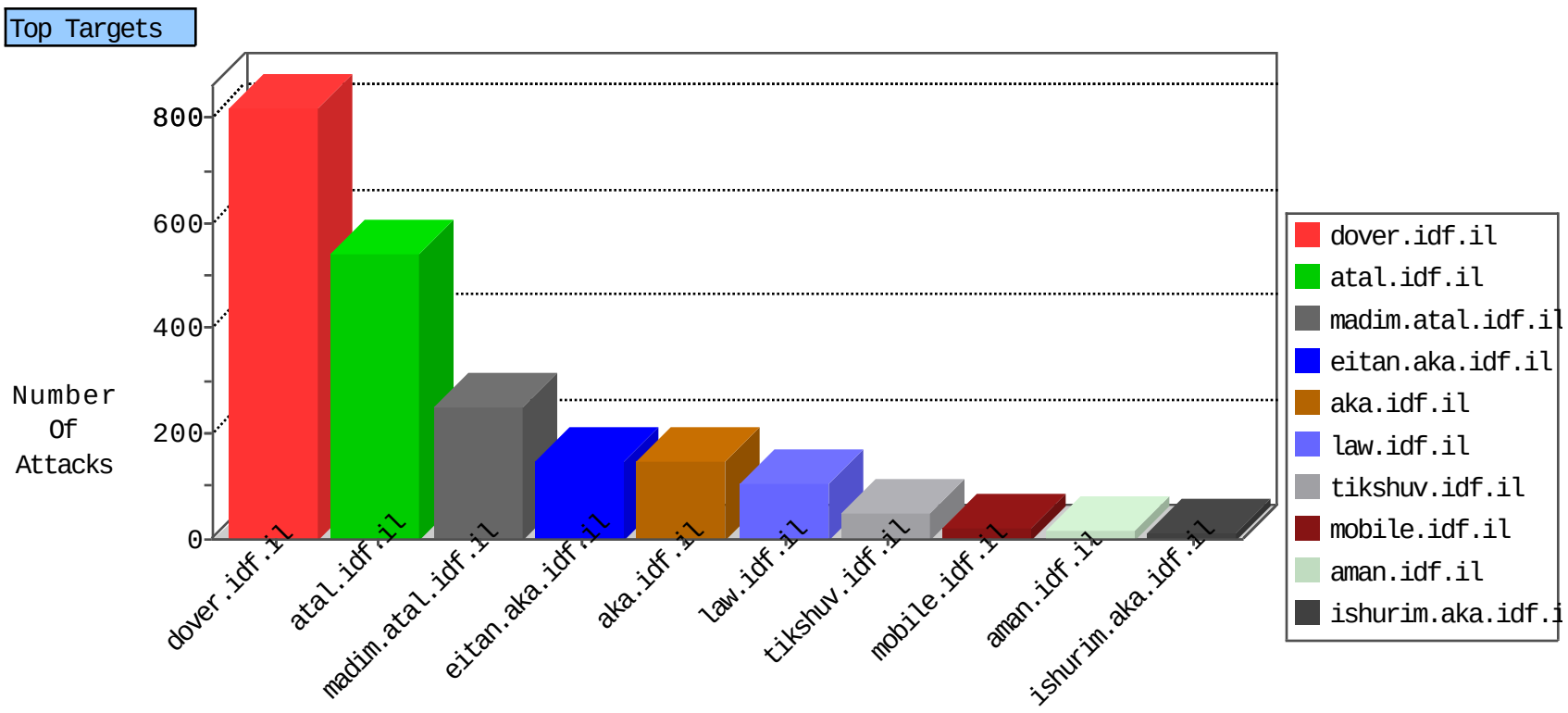
04-22-2016-17:04:05 to 04-22-2016-18:04:05

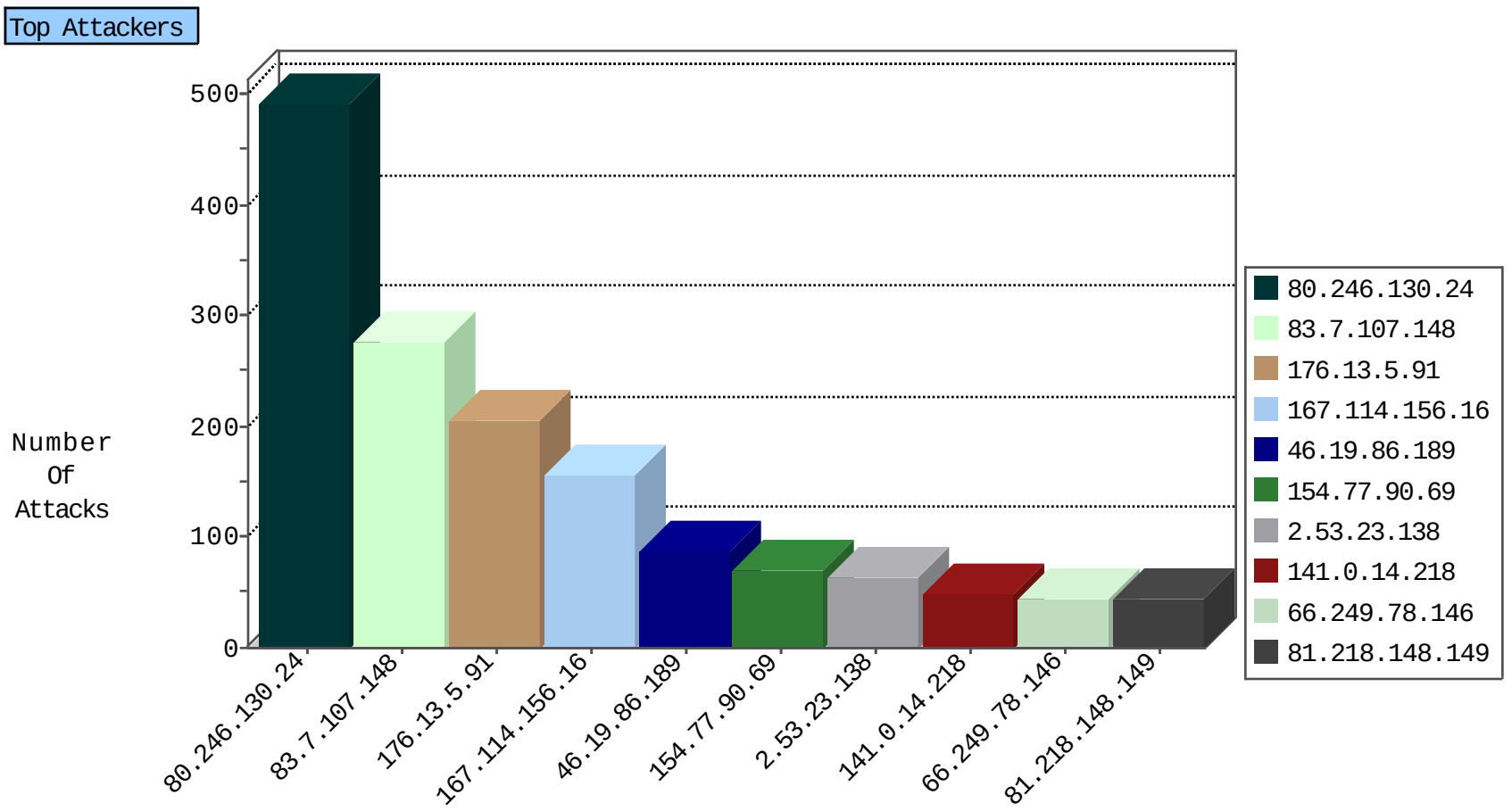
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-22-2016-17:04:05 to 04-22-2016-18:04:05

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	7254
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1073
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
40.76.83.120	United States	147.237.8.14	e.orchot.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
94.102.52.10	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
40.76.83.120	United States	147.237.76.200	eitan.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
186.234.253.18	Brazil	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
40.76.83.120	United States	147.237.77.235	sviva.idf.il	Frk_Purple_Con_Limit_Http	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
94.102.49.116	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

04-22-2016-17:04:05 to 04-22-2016-18:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-22-2016-17:04:05 to 04-22-2016-18:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.24	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
87.70.116.2	147.237.76.42	Israel	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.163	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
83.28.135.116	147.237.77.216	Poland	dover.idf.il	Xenu Link Sleuth User Agent	2
66.249.81.198	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	2
188.214.249.151	147.237.77.216	Romania	dover.idf.il	Xenu Link Sleuth User Agent	2
182.54.199.245	147.237.0.16	Malaysia	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.50	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
182.54.199.245	147.237.0.200	Malaysia	m4u.idf.il	ET SCAN Potential SSH Scan	1
182.54.199.245	147.237.0.33	Malaysia	idf.il	ET SCAN Potential SSH Scan	1
182.54.199.245	147.237.0.17	Malaysia	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.76.86	Turkey	navy.idf.il	ET SCAN NMAP -sS window 1024	1
182.54.199.245	147.237.0.34	Malaysia	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
182.54.199.245	147.237.0.19	Malaysia	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

04-22-2016-17:04:05 to 04-22-2016-18:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.24	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	471
83.7.107.148	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	276
46.19.86.189	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
154.77.90.69	Kenya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
2.53.23.138	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
141.0.14.218	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	48
176.13.5.91	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	46
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
81.218.148.149	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
51.36.64.217	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
176.13.5.91	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
189.201.137.253	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
93.185.238.152	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
84.95.211.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.228.236.190	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
193.183.105.68	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
193.227.170.194	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.53.51.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
196.121.104.190	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.26.146.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
80.246.130.24	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.177.52.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
189.122.130.131	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.146.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
206.226.72.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.64.115.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
75.33.126.176	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
95.86.104.64	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
189.201.137.253	Mexico	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
207.46.13.162	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
157.55.39.167	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.5.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	136
80.246.140.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
46.19.86.189	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.19.86.189	Block	7
80.246.139.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.139.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	5
80.246.139.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.189	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 46.19.86.189	Block	3
80.246.139.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.185.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.228.236.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
197.113.248.40	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
109.64.139.77	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 106 cookies	Block	1
69.197.185.21	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to www.yun.ph/	Block	1
178.150.15.43	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	1
84.228.236.190	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.139.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim1/templates/main.asp	Block	1
207.46.13.1	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/mail/kapats	Block	1
141.212.122.161	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
80.246.139.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
74.91.18.45	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on www.yun.ph/	Block	1
178.150.15.43	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
46.19.86.189	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
13.76.253.27	Singapore	147.237.77.74	law.idf.il	Parameter Type Violation pos in www.law.idf.il/163-6958-en/patzar.aspx	Block	1
107.150.32.60	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.yun.ph/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI in www.aka.idf.il/chinuch/faq/default.asp	None	1
207.46.13.14	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.189	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/mobile	Block	1
77.75.76.161	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/29/	Block	1
46.121.208.187	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
185.32.179.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
38.81.65.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
107.150.46.34	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/lomdim/forum/asp/showforum.asp	None	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/golani/	Block	1
156.197.114.205	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
46.19.86.189	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 46.19.86.189	Block	1
81.218.148.149	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
79.195.129.80	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
192.243.55.135	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcbwvzahvsyxzcdgfryw5vdf9oyxrhyxz1cmfcmi5wzgy=&infocenteritem=true	Block	1
46.19.86.2	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
107.150.46.37	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.86.189	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/opmissingperson/mobile	Block	1
80.246.130.24	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1