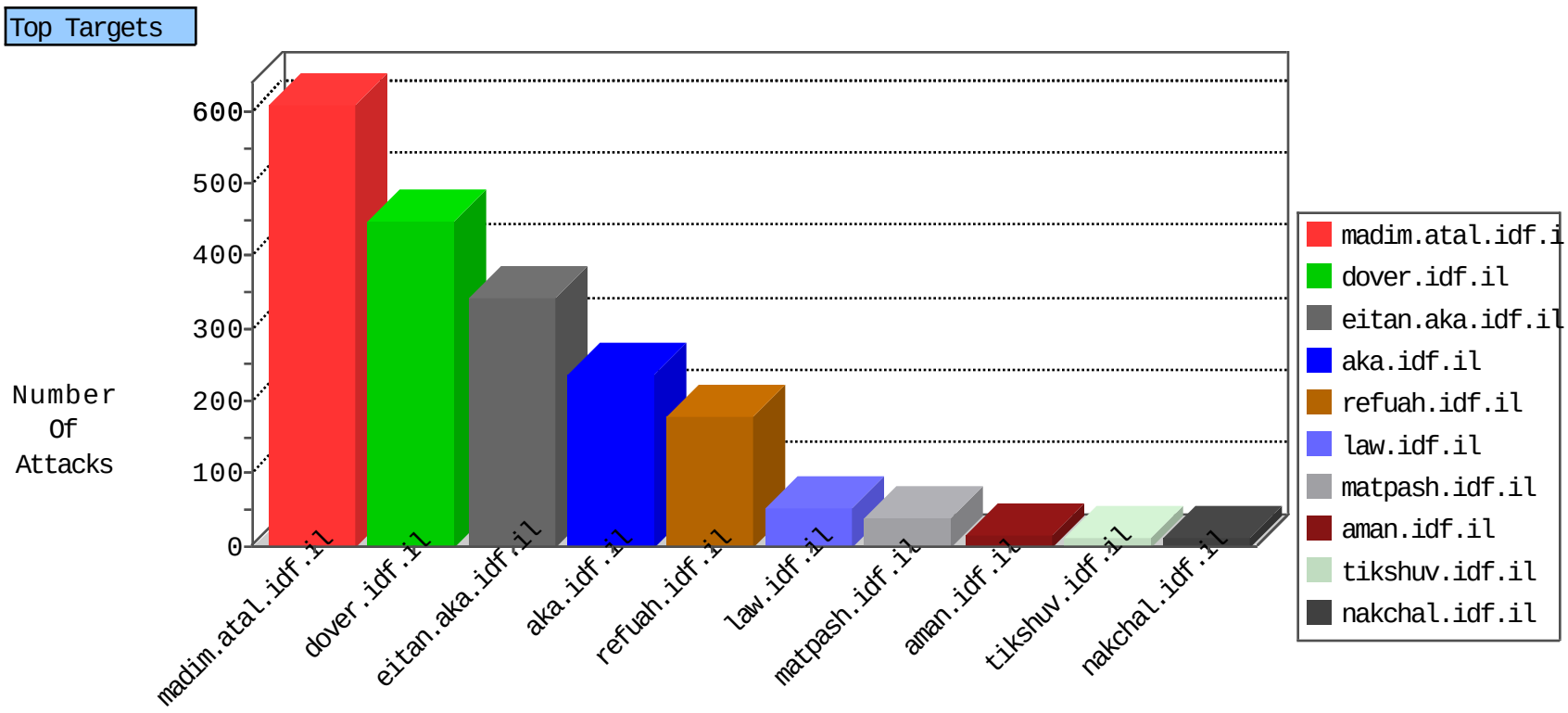
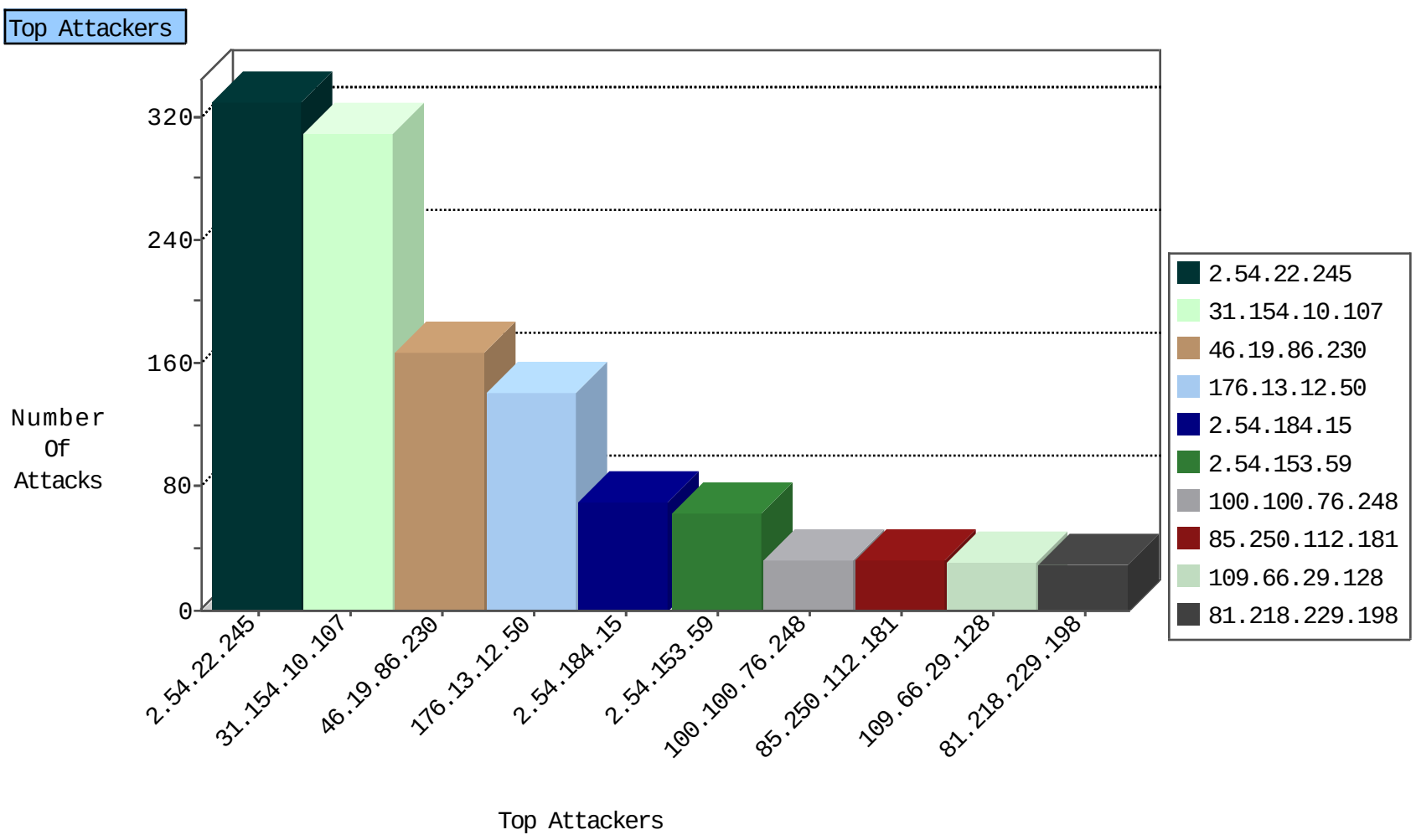
11-21-2015-11:04:07 to 11-21-2015-12:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-21-2015-11:04:07 to 11-21-2015-12:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	58
5.22.131.122	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	10
85.250.38.218	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
82.80.78.249	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
112.1.11.114	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
117.86.179.119	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
218.18.170.191	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
89.139.57.63	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
198.12.12.163	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

11-21-2015-11:04:07 to 11-21-2015-12:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.68.120	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.64.154.154	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-21-2015-11:04:07 to 11-21-2015-12:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.67	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
222.186.42.147	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
120.198.118.139	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
119.73.228.130	147.237.8.24	Singapore	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
85.104.57.121	147.237.8.27	Turkey	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.54.184.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.42.147	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
219.153.65.239	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
176.36.118.135	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
119.73.228.130	147.237.8.24	Singapore	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
119.73.228.130	147.237.8.24	Singapore	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
74.117.209.136	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.42.147	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

11-21-2015-11:04:07 to 11-21-2015-12:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.22.245	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	324
176.13.12.50	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	133
81.218.229.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
100.100.81.184		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
100.100.76.248		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
100.100.87.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
213.57.132.153	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
100.100.92.151		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
37.26.148.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.66.29.128	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	15
109.66.29.128	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
5.22.131.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.181.194.213	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.102.9.107	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	10
2.54.184.15	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
100.100.76.248		147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	10
109.65.124.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
199.16.156.125	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	9
199.16.156.124	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
183.79.221.34	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.12.50	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	8
2.54.184.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.177.55.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
91.182.231.138	Belgium	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
5.29.244.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.38.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.184.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
84.228.202.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.184.15	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
100.100.118.251		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.54.184.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.184.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
199.16.156.126	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
100.100.85.105		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.54.184.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.54.184.15	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
82.166.22.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.184.15	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
133.130.58.190	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.68.149.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.33.66.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
91.105.238.22	Russian Federation	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
185.3.146.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.64.24.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.54.184.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.10.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	151
31.154.10.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	134
46.19.86.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	125
2.54.153.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
46.19.86.230	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.230	Block	40
85.250.112.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
31.154.10.107	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 31.154.10.107	Block	23
2.54.28.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
94.159.141.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.37.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.126.62.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.22.131.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.173.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.109.189.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.108.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.107	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.107	Block	2
62.128.48.84	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.128.48.84	Block	2
176.13.14.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.58.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.148.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.224.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.22.245	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.22.245	Block	2
207.46.13.172	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109335.pdf×¦×‘×?-×″×″×¦×œ×″	Block	1
31.154.91.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.179.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.12.50	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
85.65.17.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/arabic/pages/default.aspx	Block	1
194.187.168.19	Poland	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/163-6843-	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
157.55.39.203	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/ishurim	Block	1
107.150.55.54	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /	Block	1
37.26.146.206	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/1133-22461-he/dover.aspx.	Block	1
81.218.229.198	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.229.198	Block	1
5.11.44.41	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nahal	Block	1
66.249.66.109	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.109	Block	1
109.66.29.128	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.86.230	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
194.187.168.24	Poland	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
176.12.143.207	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/flash/recruitlane/recruitlane.swf	Block	1
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	1
62.128.48.84	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
40.77.167.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1