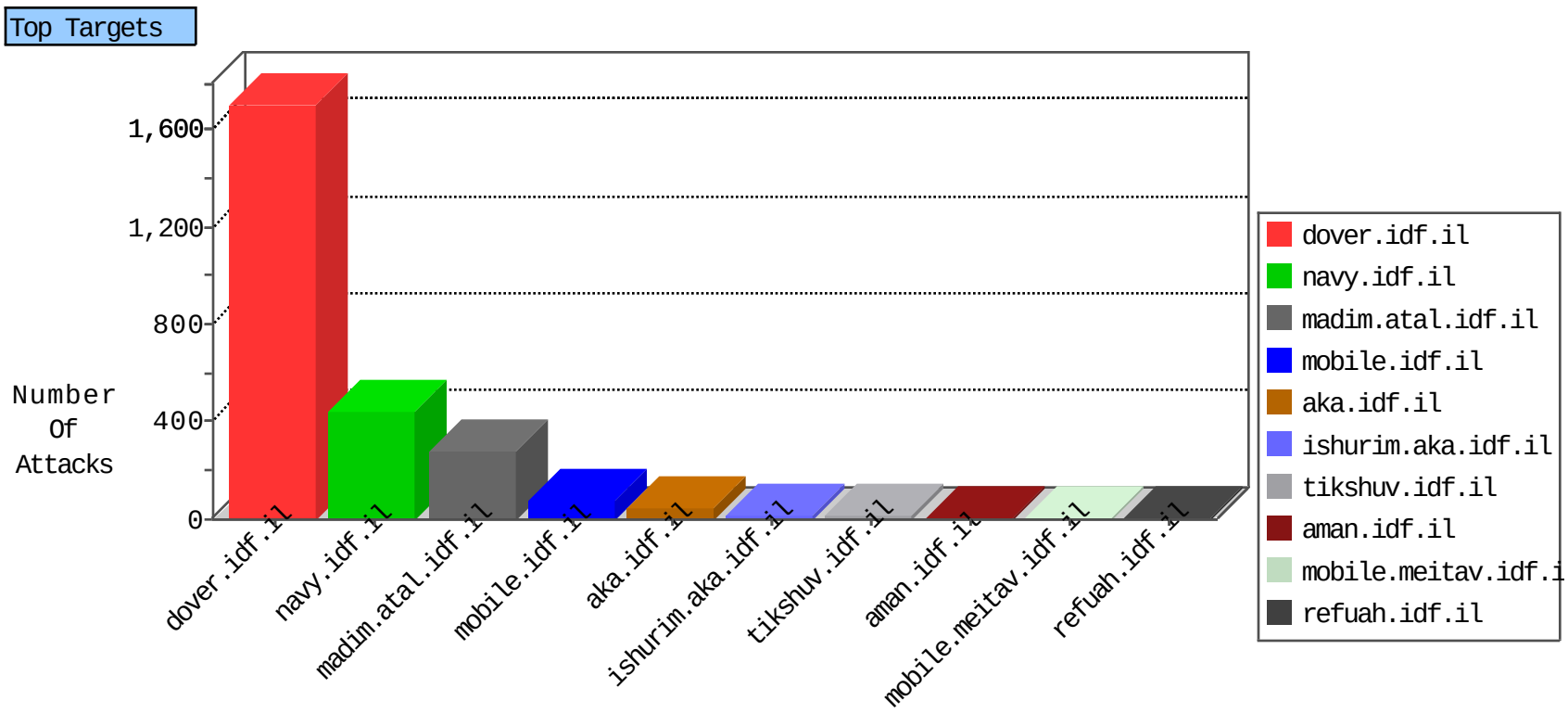
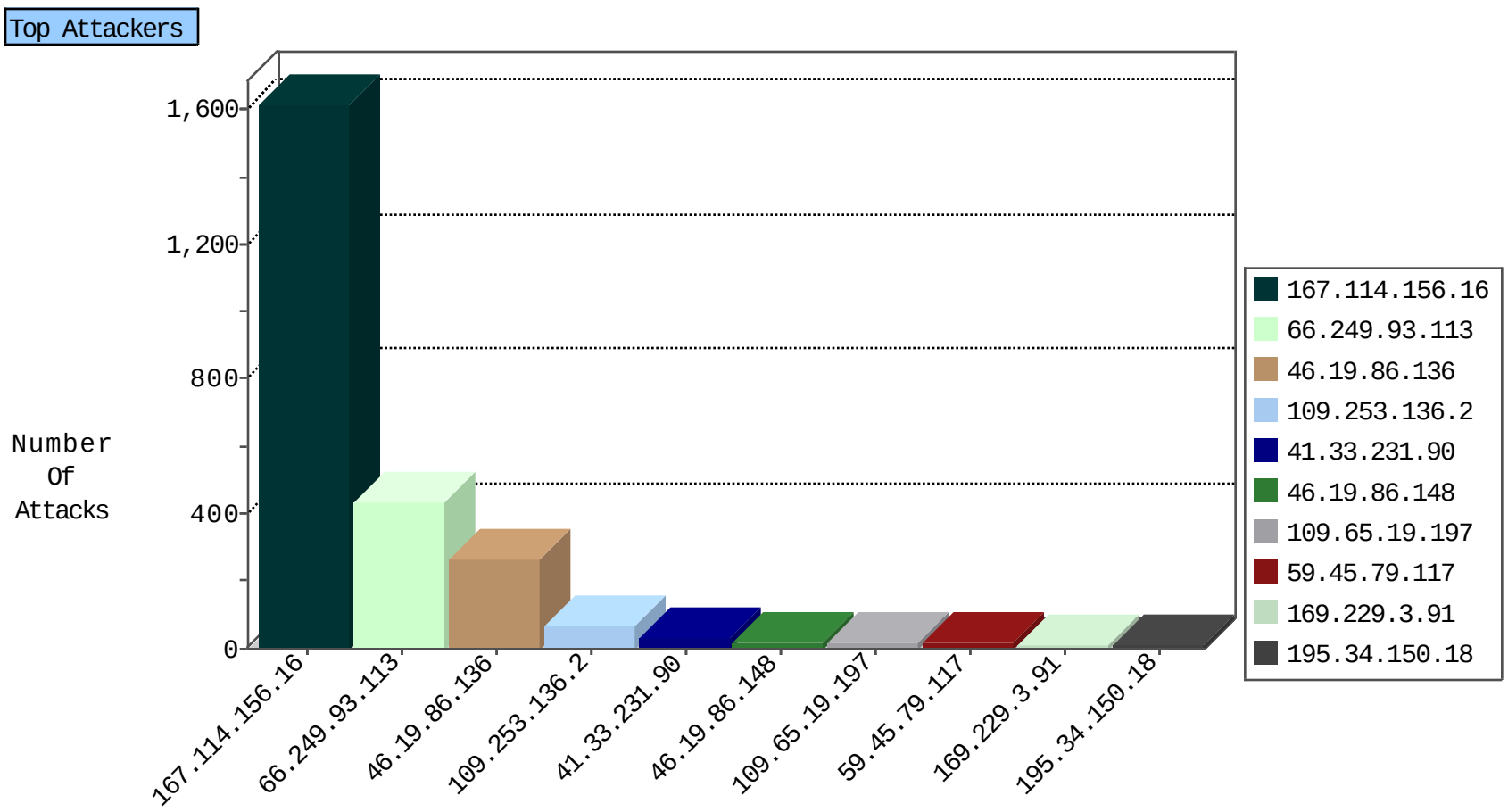
01-11-2016-01:07:22 to 01-11-2016-02:07:22

IDF Under Attack
Daily Report





01-11-2016-01:07:22 to 01-11-2016-02:07:22

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	DOS-Tool-SwitchbladG	dest-reset	3017
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2735
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
5.76.127.110	Kazakstan	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
5.76.127.110	Kazakstan	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
23.95.248.111	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

01-11-2016-01:07:22 to 01-11-2016-02:07:22

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-11-2016-01:07:22 to 01-11-2016-02:07:22

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.113	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	434
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
185.130.5.247	147.237.77.176		matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.247	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.247	147.237.76.176		test.ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.247	147.237.72.156		aman.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
183.82.106.200	147.237.76.31	India	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
117.25.155.164	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.247	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.247	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.247	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.247	147.237.8.14		e.orchot.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
183.82.106.200	147.237.76.31	India	nakchal.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
158.255.6.220	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
109.251.56.171	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.196	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1

01-11-2016-01:07:22 to 01-11-2016-02:07:22

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.136.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.86.148	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
172.56.20.91	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.142.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.86.136	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.102.254.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
204.79.180.97	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
149.88.35.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.78.153	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.52.39.203	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.177	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.253.196.101	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
149.88.35.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.108	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.126.213.161	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.21	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.52.39.203	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.178	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.70.81.143	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
169.229.3.91	United States	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1
141.212.122.176	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.65.87.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
172.56.34.218	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.21	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
5.22.131.23	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.178	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.103	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
217.148.45.113	United Kingdom	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
169.229.3.91	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.46.39.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.176	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
5.29.238.212	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.179	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	162
46.19.86.136	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.136	Block	93
109.253.136.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	16
109.253.136.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	15
109.65.19.197	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.65.19.197	Block	15
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	4
46.19.86.136	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.86.136	Block	3
37.26.147.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.179.132.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
65.55.210.15	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.179.132.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2277.jpg	Block	1
46.19.86.136	Israel	147.237.0.19	madim.atal.idf.i	Too Many 403: Response Code per Session	Block	1
84.108.250.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	1
157.55.39.47	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 157.55.39.47	Block	1
107.178.195.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
5.29.101.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
207.46.13.75	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
66.249.69.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1735	Block	1
84.111.187.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ishurim).	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
157.55.39.152	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
109.64.61.78	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/navmenu/mazi.idf.il	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
136.243.48.82	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	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
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
109.65.19.197	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	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
66.249.74.105	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/320/patzar.aspx	Block	1
141.212.122.97	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /x	Block	1
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	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9367-he/dover.aspx	Block	1
84.108.136.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
141.212.122.97	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /x	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.48.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1