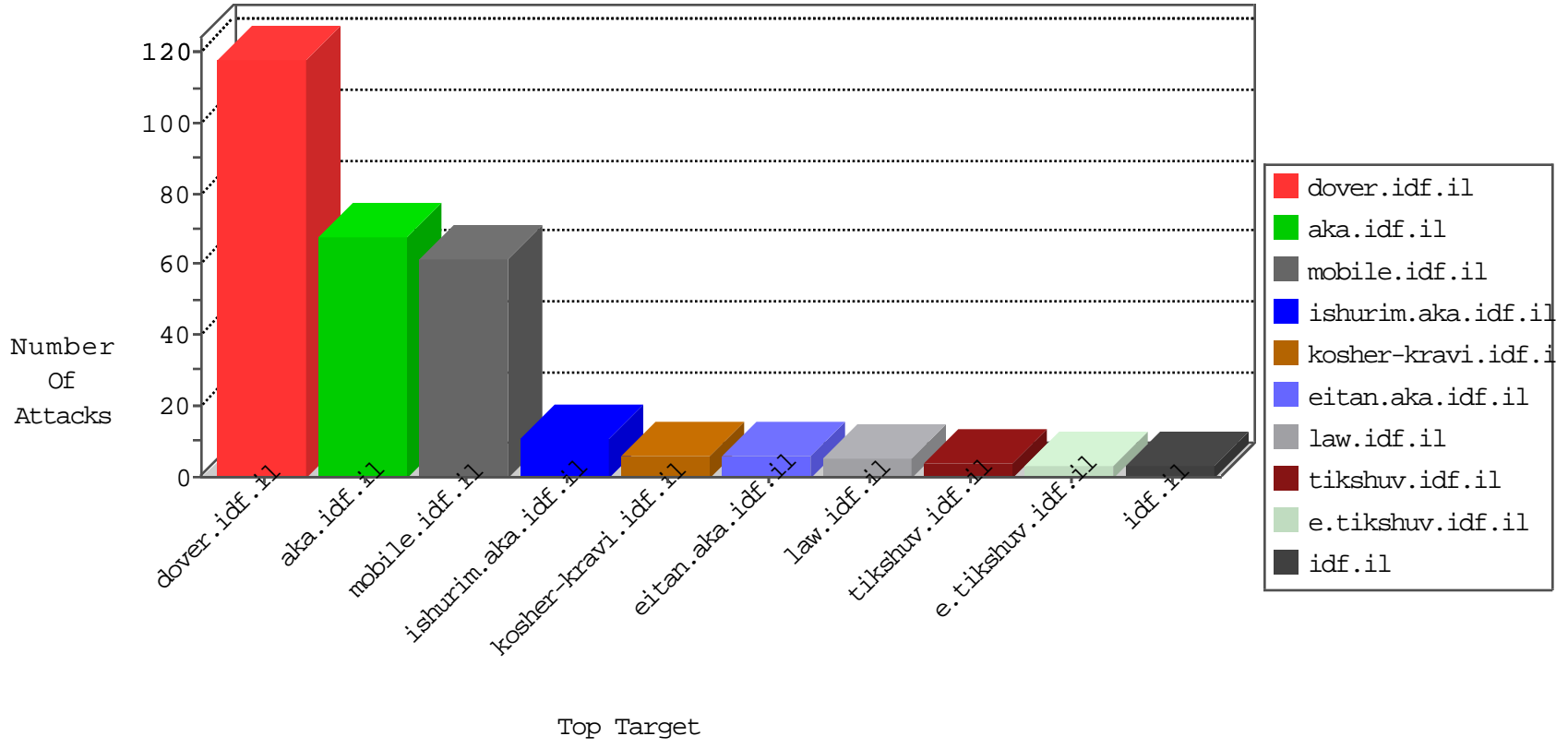


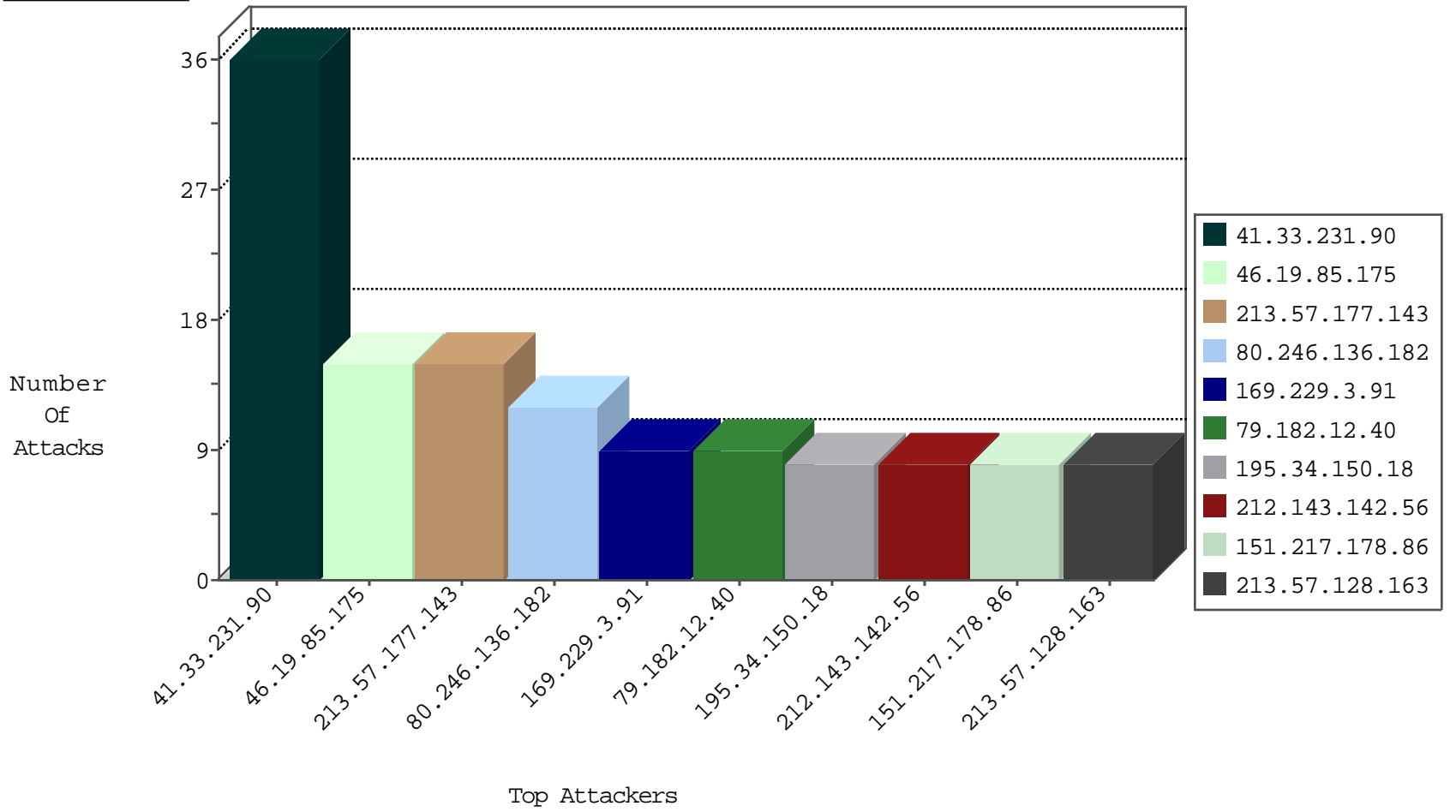
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.109.88.160	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.15	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
109.235.254.181	147.237.72.166	Turkey	aka.idf.il	ET SCAN NMAP -f -sS	1
80.82.78.8	147.237.0.33	Netherlands	idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
168.62.238.153	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
62.75.236.76	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.86	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.86	147.237.8.50		e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.86	147.237.0.34		tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.86	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
118.68.29.67	147.237.76.34	Vietnam	yohalan.idf.il	ET SCAN NMAP -f -sS	1
196.47.173.21	147.237.76.39	Cote D'Ivoire	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
109.235.254.181	147.237.72.166	Turkey	aka.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.76.39	Cote D'Ivoire	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
80.82.79.104	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.86	147.237.77.212		e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.86	147.237.8.50		e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.86	147.237.8.14		e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.86	147.237.0.19		madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
118.68.29.67	147.237.76.34	Vietnam	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
109.235.254.181	147.237.72.166	Turkey	aka.idf.il	ET SCAN NMAP -sS window 2048	1
196.47.173.21	147.237.76.39	Cote D'Ivoire	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.57.177.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.136.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.182.12.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.54	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
80.246.136.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.162.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.129.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.142	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
213.57.128.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	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
157.55.2.138	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
213.57.128.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
207.46.13.118	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.105.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3
82.81.11.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.204.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.32.179.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
70.39.186.218	Satellite Provider	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
71.82.189.216	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
5.29.143.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.11.105	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.3.144.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.64.75	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.160.204.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
141.212.121.189	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.29.127.12	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
141.212.121.178	United States	147.237.0.33	idf.il	drop		drop	1
86.176.225.63	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
141.212.121.190	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.29.143.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
117.197.244.183	India	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
210.44.144.110	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.6.31	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
54.176.195.13	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	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
24.218.80.94	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.179	United States	147.237.0.33	idf.il	drop		drop	1
2.54.26.3	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.177.143	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.182	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.175	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.160.204.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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	2
95.86.103.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
94.159.231.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
94.242.246.23	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.125.179.165	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
46.19.86.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.5.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
37.46.230.203	Ukraine	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on tikshuv.idf.il/site/general.aspx parameter catId	Block	1
85.250.134.94	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/0/310.pdf	Block	1
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_ses.20.8afc=*	Block	1
109.201.154.233	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.52.52.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.125.179.165	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
180.76.15.140	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.204.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
37.46.230.203	Ukraine	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
89.31.57.5	Italy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=dfa35b7a72af3d83.1451431524.1.1451431524.1451431524.;	Block	1
128.232.110.29	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
2.54.52.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.90.251.149	Germany	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.72.238.241	Block	1
46.166.190.158	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
40.77.167.50	United States	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on tikshuv.idf.il/site/general.aspx parameter catId	Block	1
89.145.95.43	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/l	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method %5B%22%22%2C%22%22%2C1451431524%2C%22https%3A%2F%2Fwww.google.co.il%2F%22%5D; in URL _pk_id.20.8afc=dfa35b7a72af3d83.1451431524.1.1451431524.1451431524.	Block	1
141.212.121.176	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
104.63.88.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
2.54.162.137	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
66.249.75.69	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
109.65.193.80	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
45.35.71.181		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.88.161.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
31.44.136.238	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/&sa=u&ved=0ahukewjk2uq_n4lkahxlbbokehvyadkqfghmaa&usg=afqjcnfd5s02zieedmbmfxvss2_oefusww	Block	1