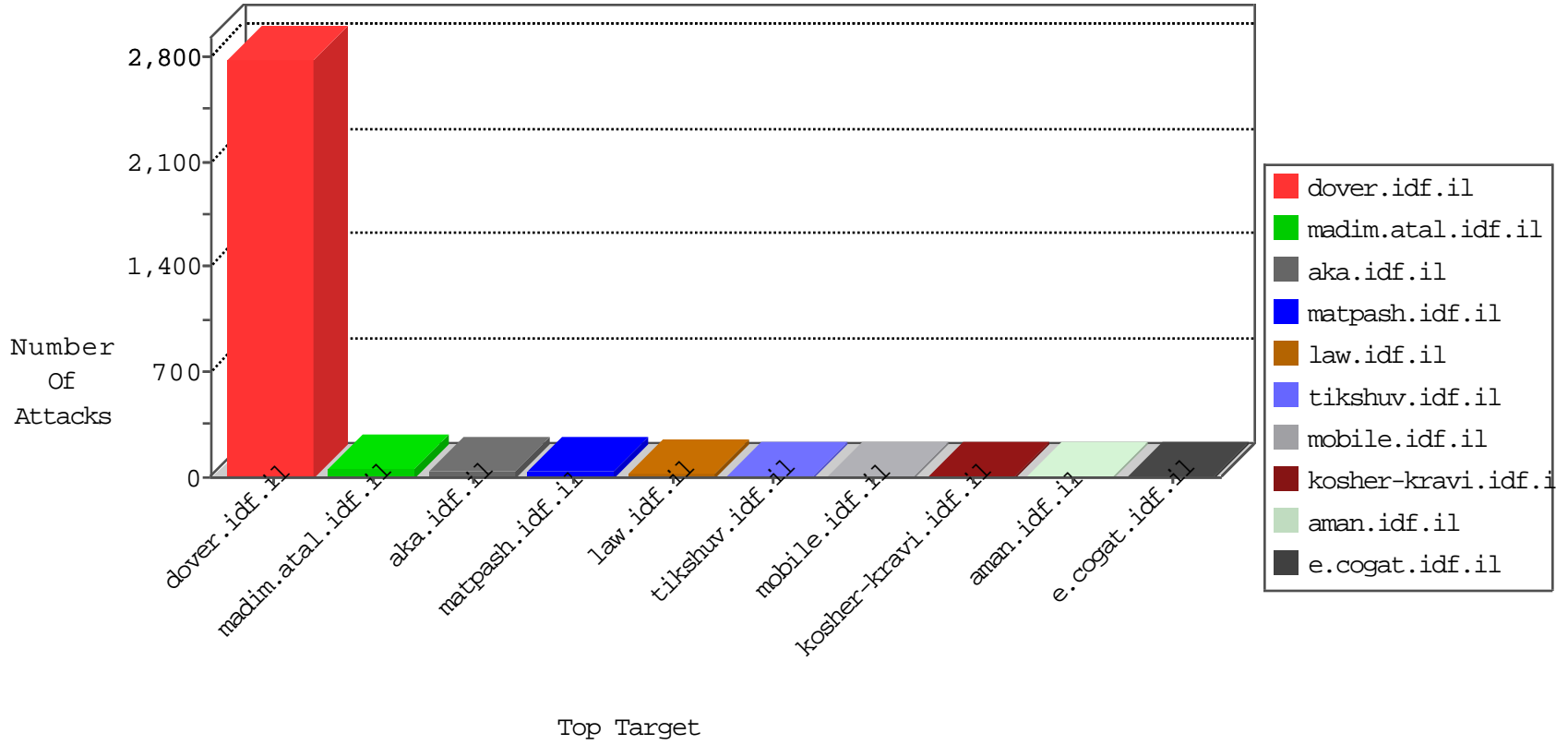


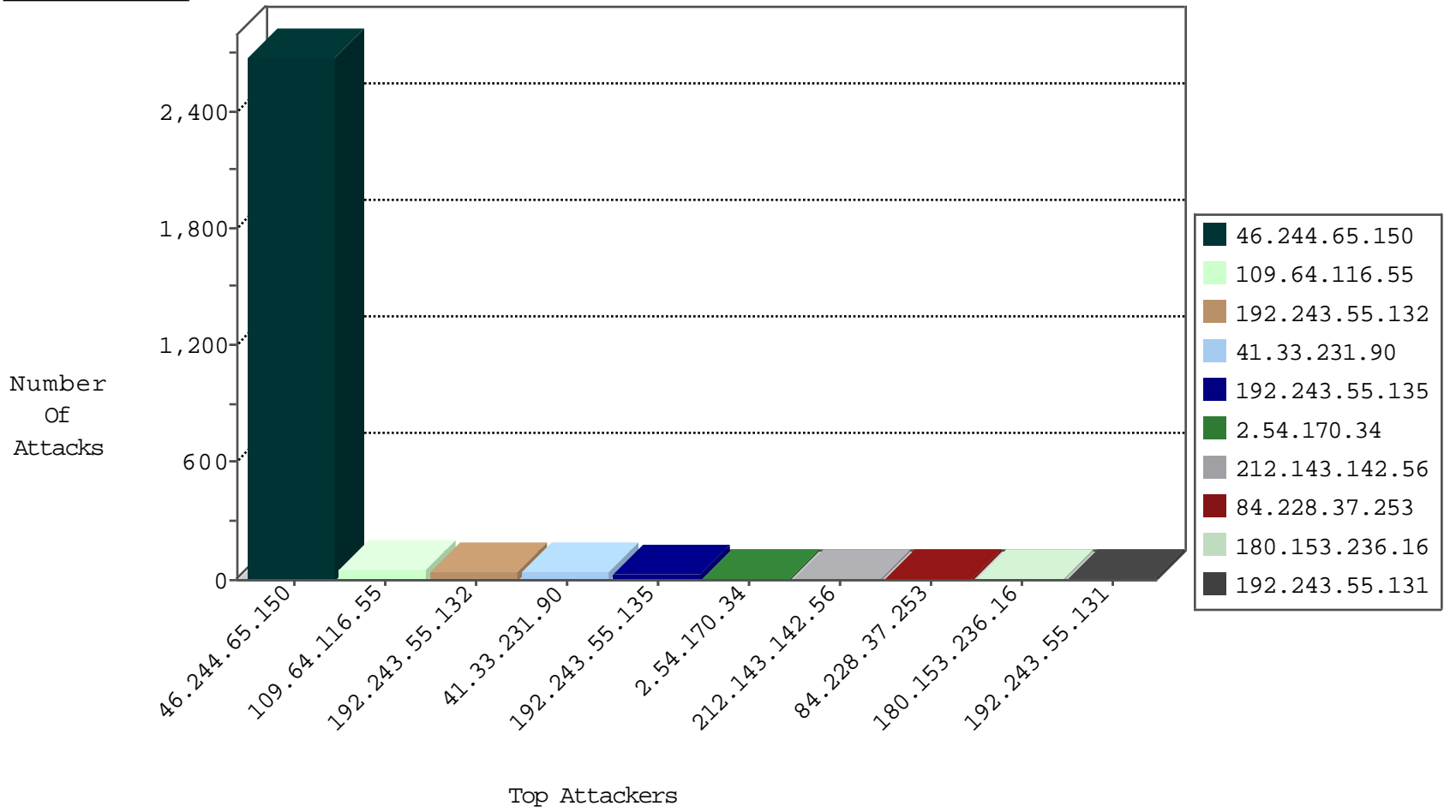
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.244.65.150	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2679
184.105.139.76	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.84	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.30	United States	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.100	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.80	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.84	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
164.132.54.194	Italy	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.120	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.80	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
184.105.139.88	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.80	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.100	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.210	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
207.46.13.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.105	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
122.228.207.118	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
113.76.90.49	147.237.0.17	China	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
185.130.5.159	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.135.176	147.237.76.44	Israel	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.228.207.118	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
113.76.90.49	147.237.0.34	China	tikshuv.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
195.216.176.244	147.237.77.61	Latvia	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.76.177	India	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
122.228.207.118	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	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	34
2.54.170.34	Israel	147.237.72.166	aka.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	7
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
84.228.37.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.135	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
94.230.84.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.161.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.180.139.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
83.130.106.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.178	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.48.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.102.200.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
180.153.236.16	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence		monitor	2
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.135	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
5.29.78.38	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
68.180.229.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.52.190.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.54	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
2.54.128.246	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.208	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
180.153.236.16	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
2.54.128.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.219	United States	147.237.0.34	tikshuv.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
109.64.116.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
46.19.86.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.76	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.76	Block	3
91.135.102.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.175.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
210.246.58.255	New Zealand	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
162.243.68.232	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 162.243.68.232	Block	1
66.249.79.195	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list1.htm	Block	1
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/navy/	Block	1
104.235.148.46		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.58.193	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/67785.pdf&sa=u&ved=0ahukewi69e_j06plahxd_q4khq5zay0qfggimaa&sig2=oa035hf7goylm7as2klygq&usg=afqjc nhdir0qtustf9tt2kmbjokxauigaq	Block	1
162.243.68.232	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/3950.pdfxy-and-dirtyed-the-oklaho ma-tornadows	Block	1
64.124.98.9	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
178.255.215.87	France	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
77.127.108.253	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/901-8613-he/tikshuv.aspx#.vtcj--ybol9	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
113.76.90.49	China	147.237.0.34	tikshuv.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
180.76.15.140	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
2.52.164.176	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation SearchText in www.refua.atal.idf.il/938-he/refuah.aspx	Block	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.183	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
184.105.139.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
17.167.248.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1