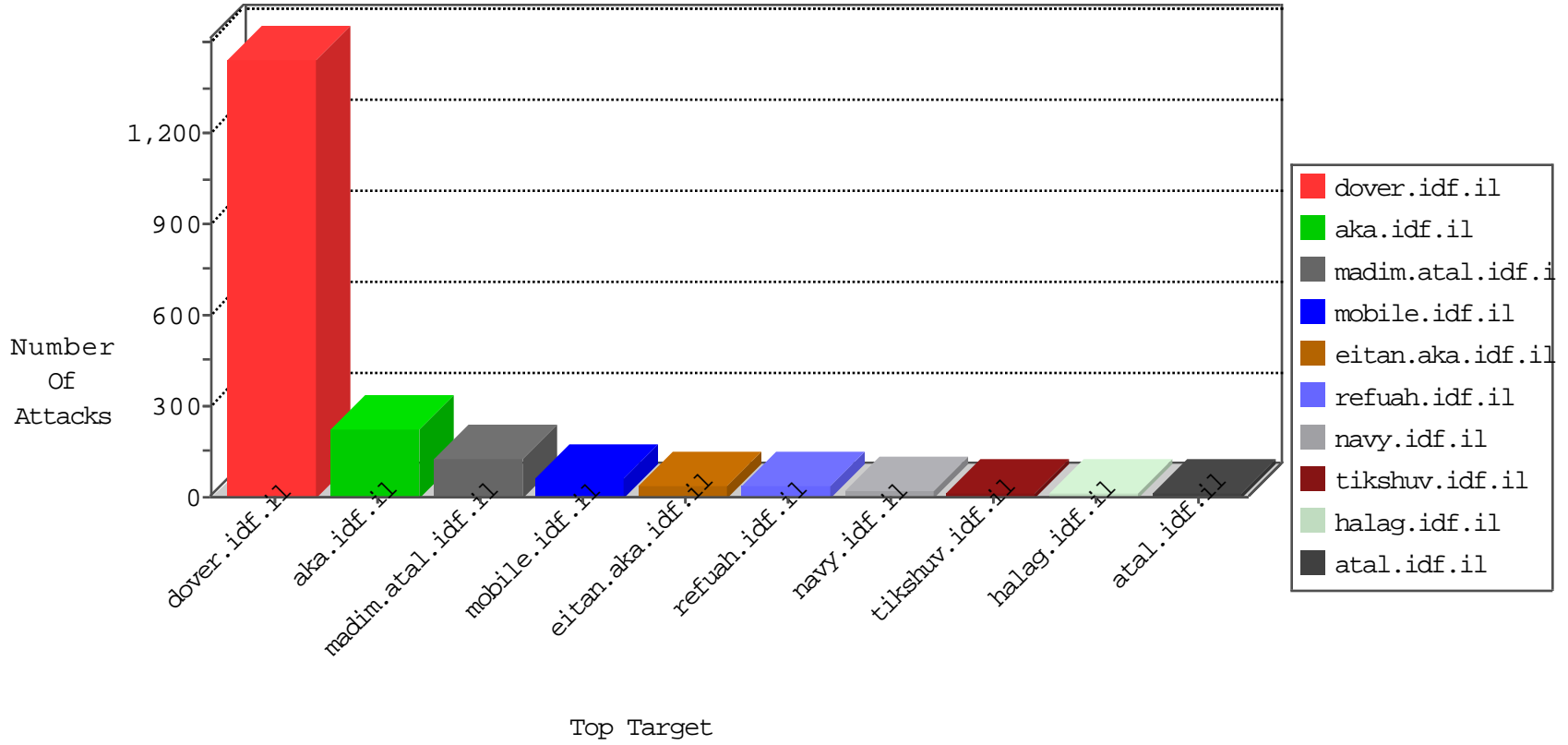


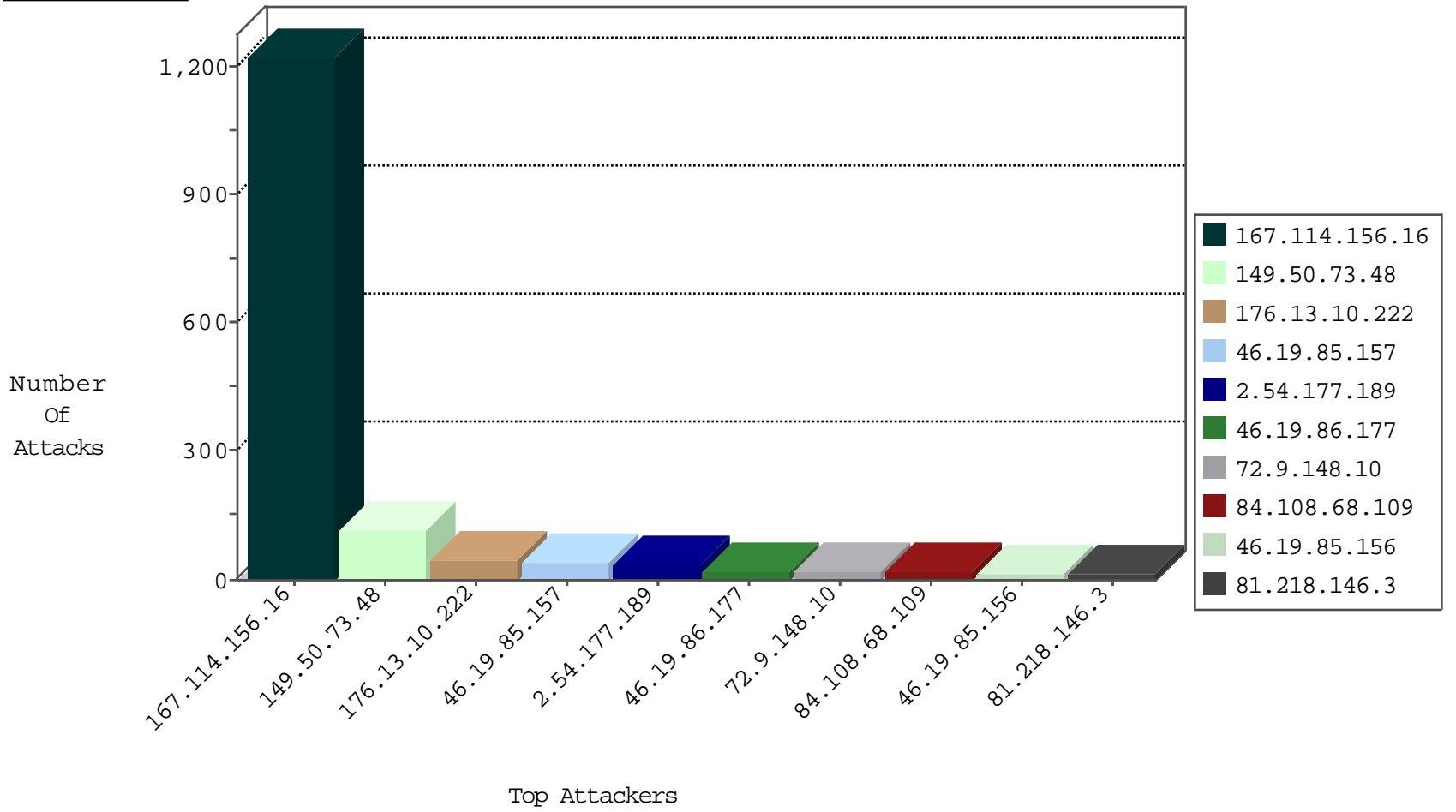
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3287
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	2
185.94.111.1		147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.125.77.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
107.150.56.254	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
176.13.12.107	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

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
5.29.187.252	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
23.252.161.191	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
89.255.21.58	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.31	China	nakchal.idf.i	ET SCAN NMAP -sS window 1024	1
149.50.87.208	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.10.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
46.19.86.177	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
81.218.146.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.183.123.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.199.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
2.54.177.189	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
89.138.108.143	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.108.68.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.181.10.229	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.177.167.165	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.54.177.189	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.38.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.140.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.177.189	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
72.45.160.170	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.166.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.177.189	Israel	147.237.77.243	mobile.idf.il	SYN Attack		reject	6
109.65.245.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.177.189	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.19	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.167.165	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.116.3.147	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
188.120.148.230	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
156.162.111.203		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
46.19.85.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.186.154.60	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.44	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.129.103	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.142.68.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
199.30.25.109	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.50.87.208	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.66.33.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.68.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	3
185.27.106.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.190.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.91.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
79.178.210.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.89.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.221.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.18.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.50.73.48	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
176.13.4.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
197.113.138.144	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.113.138.144	Block	2
5.102.217.15	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	2
80.246.139.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
41.100.185.32	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
94.230.93.84	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on ww.idf.il/error.htm	Block	1
79.182.235.236	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for ww.aka.idf.il/main/sachar/	Block	1
46.121.117.115	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
157.55.39.134	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
87.69.242.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.75.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.asp	Block	1
220.255.145.53	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on ww.idf.il/error.htm	Block	1
46.19.85.98	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
94.230.93.91	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on ww.idf.il/error.htm	Block	1
79.183.199.113	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2418.jpg	Block	1
31.13.112.123	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/&h=iaqg0aqf2&s=1	Block	1
94.230.93.59	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on ww.idf.il/error.htm	Block	1
79.177.167.165	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
46.19.85.98	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method c193e4000 in URL	Block	1
94.230.93.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on ww.idf.il/error.htm	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/contactus/contactus.aspx	Block	1
176.58.74.75	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
37.157.143.2	Bulgaria	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
94.230.93.62	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on ww.idf.il/error.htm	Block	1
79.182.146.186	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.134.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
81.218.146.3	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to ww.aka.idf.il/kamlar	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/shared/usercontrols/navmenu/	Block	1
180.76.15.144	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9687-he/refuah.aspx	Block	1
40.77.167.82	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
94.230.93.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.182.146.186	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to ww.aka.idf.il/xmlrpc.php	Block	1
46.32.120.173	Jordan	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.38.44	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
149.50.87.208	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/sct100\$scriptmanager1', document.getelementbyid('aspnetform'))	Block	1
85.65.202.55	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on ww.idf.il/https://ww.idf.il/	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3249.jpg	Block	1