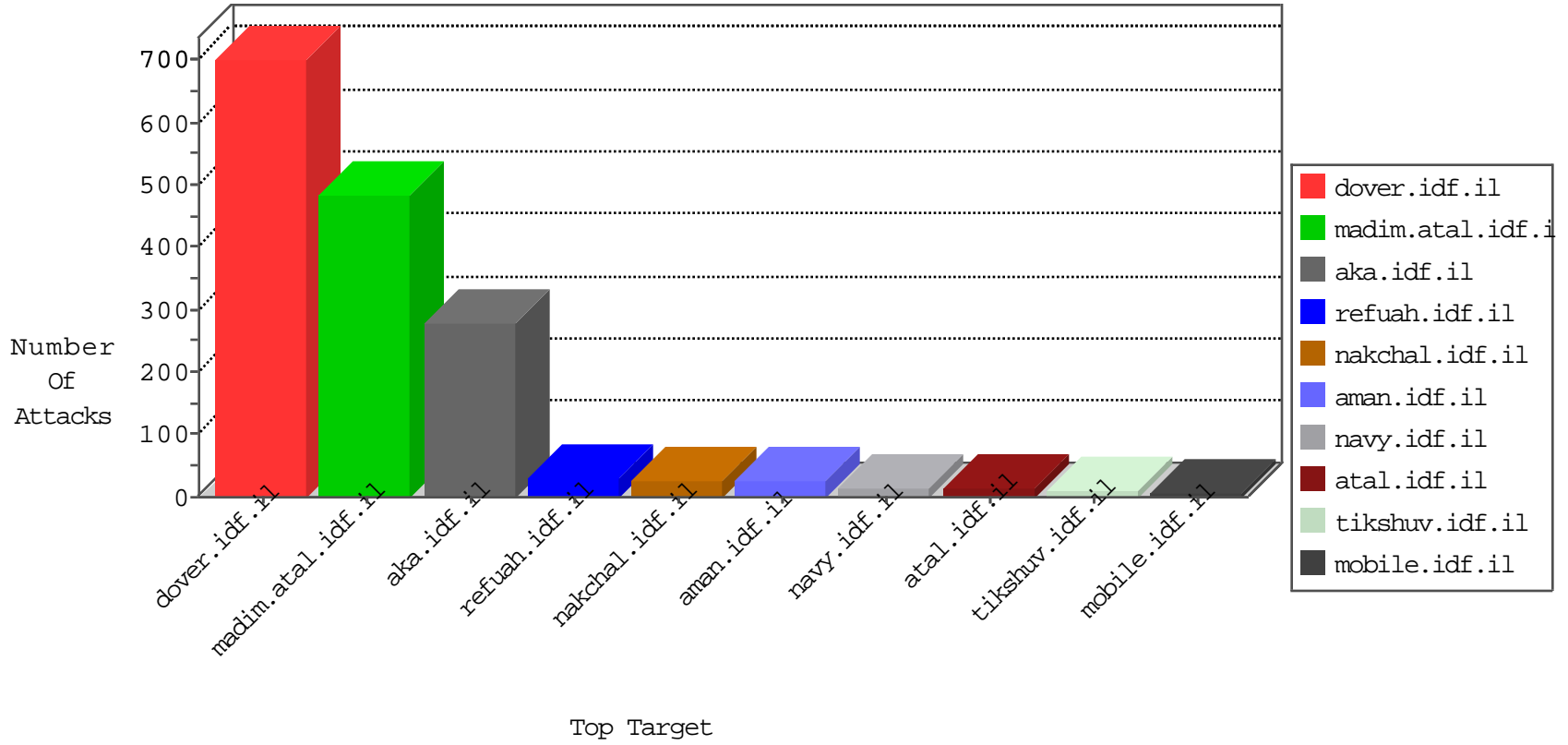


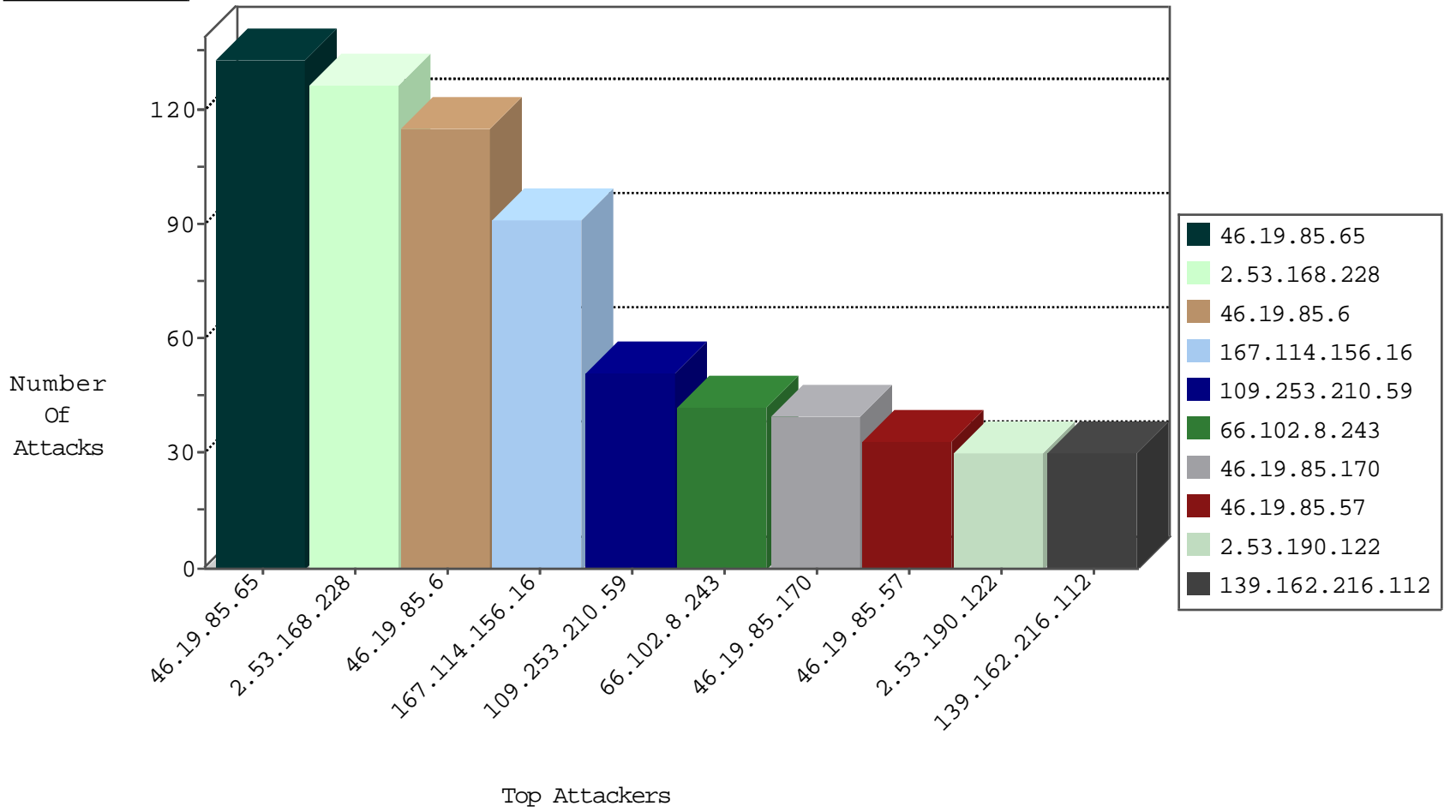
IDF Under Attack Daily Report



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	HTTP-POST-Segmented-DoS	dest-reset	3658
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1650
46.117.186.81	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	210
84.109.106.128	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	101
191.96.249.50	Chile	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
176.13.23.72	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
191.96.249.50	Chile	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
183.60.48.25	China	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
190.7.136.147	Colombia	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Https	drop	1

05-04-2016-20:04:06 to 05-04-2016-21:04:06

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
66.102.8.243	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	38
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.197	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
98.119.105.221	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
79.177.193.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.240.213.93	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.240.250.154	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
79.178.130.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
108.58.114.198	147.237.76.30	United States	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.53.190.122	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.85.57	Israel	147.237.76.31	nakchal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
184.185.138.126	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
131.123.60.0	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
188.161.117.73	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
162.243.104.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
197.89.8.78	South Africa	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
96.35.202.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
79.177.234.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.170	Israel	147.237.77.216	dover.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
24.229.110.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.177.234.39	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.124.43.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.21.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.111.2.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
62.90.193.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.222.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
84.111.2.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
89.138.123.36	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
94.230.86.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.250.254.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	5
66.102.8.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.154.173.103	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.22.135.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
70.48.100.92	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
149.101.37.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.168.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	126
46.19.85.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	121
46.19.85.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
109.253.210.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
2.55.43.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
46.117.20.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
87.70.62.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
131.253.25.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
131.253.25.229	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
89.138.33.141	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
109.253.213.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
146.142.1.10	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/mo	Block	3
89.138.33.141	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/	Block	3
46.120.17.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
79.182.61.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.144.58.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.217.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.156.76	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.121.13.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.7.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.52	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/yohalan/home/home.asp	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.81.212	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.94	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
2.53.7.228	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
212.179.21.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
75.145.80.29	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mo	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.120.17.107	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.17.107	Block	1
79.181.166.223	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
5.29.179.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
157.55.39.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
109.253.213.84	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/faq/mobile	Block	1
66.240.219.146	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
88.211.33.22	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 88.211.33.22	Block	1
79.176.63.84	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3392.jpg	Block	1
149.50.13.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https://twitter.com/	Block	1
89.138.161.249	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
185.120.126.7	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	1
88.211.33.22	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20877-he/dover..	Block	1
79.179.114.87	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kiosk/	Block	1
149.78.9.49	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1