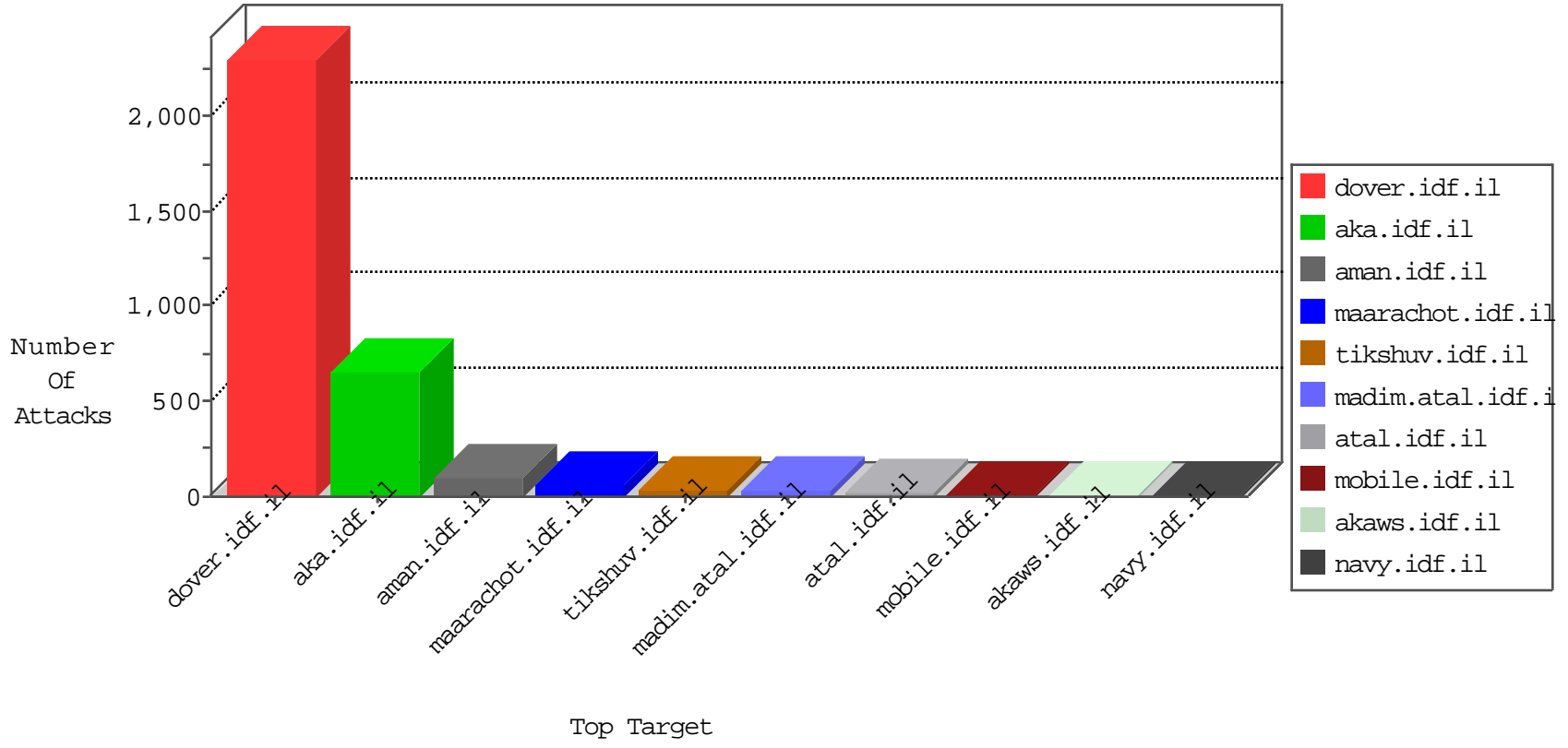


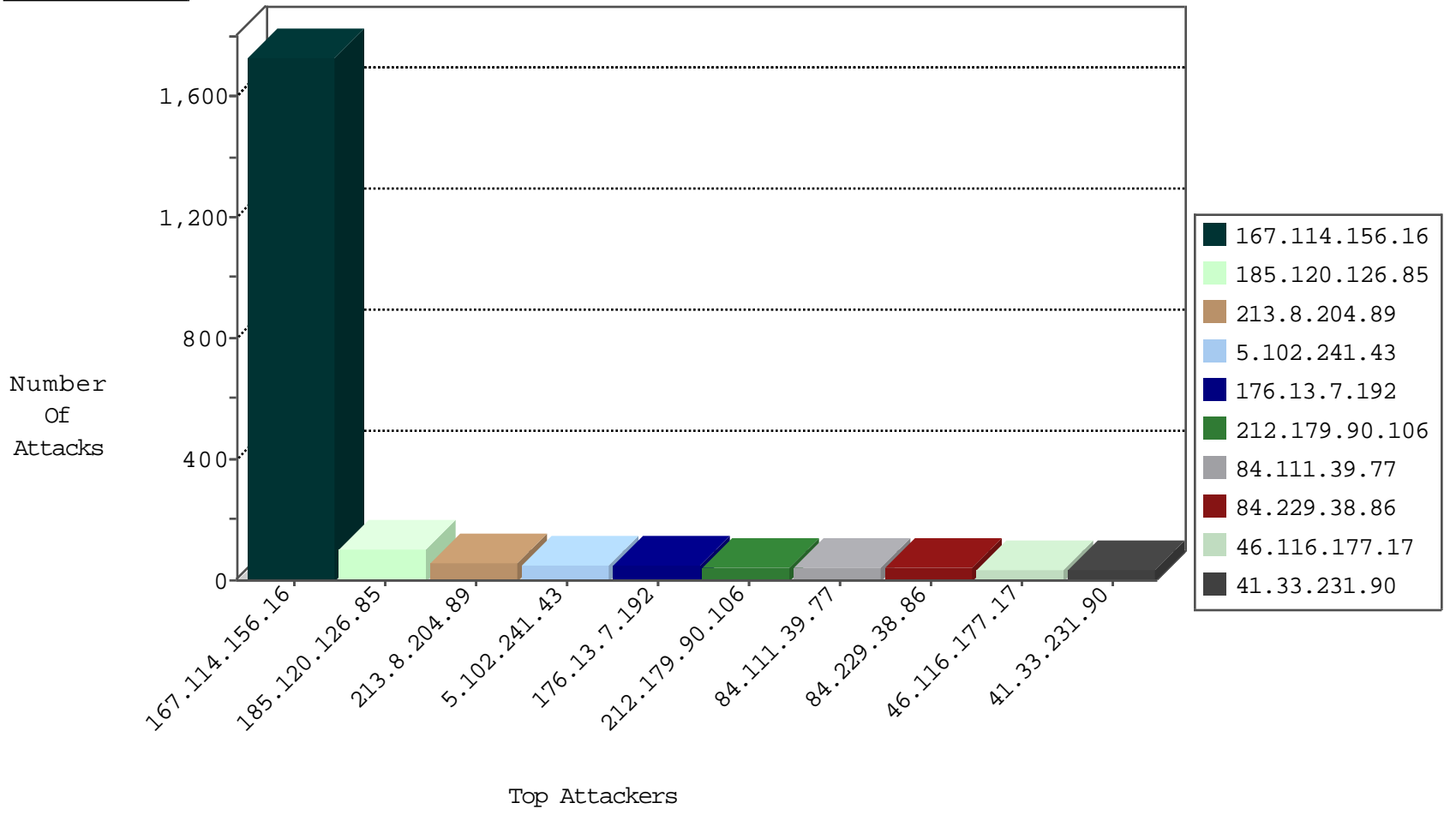
IDF Under Attack Daily Report



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	2596
130.75.2.26	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
168.235.196.104	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
77.247.178.132	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
113.188.214.169	Vietnam	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
113.188.214.169	Vietnam	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
27.5.164.254	India	147.237.77.216	dover.idf.i	C008: HTTP: Xenu UserAgent	Block	1
80.248.216.11	France	147.237.77.216	dover.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
106.38.241.147	China	147.237.77.216	dover.idf.i	C103: 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
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
134.213.133.4	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN NMAP -sS window 2048	1
36.72.228.72	147.237.77.205	Indonesia	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
220.231.195.122	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
220.231.195.122	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -f -sS	1
134.213.133.4	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN NMAP -sS window 3072	1
134.213.133.4	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN NMAP -f -sS	1
36.72.228.72	147.237.77.205	Indonesia	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
220.231.195.122	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.102.241.43	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	53
185.120.126.85		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
176.13.7.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
84.111.39.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
212.179.90.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
84.229.38.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.64.121.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
185.120.126.85		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	33
31.210.186.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
46.117.18.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
5.29.77.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
79.180.22.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
46.116.177.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
5.102.254.222	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
109.65.140.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
45.59.213.122		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
213.8.204.89	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
82.81.22.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
85.250.129.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
185.120.126.85		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
213.57.132.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
213.8.204.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
84.229.94.247	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
79.182.25.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
5.29.55.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
213.8.204.89	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
84.108.19.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
109.64.192.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
84.228.0.60	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
82.166.68.171	Israel	147.237.0.35	akaws.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
149.78.29.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
109.64.163.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.117.32.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
213.57.14.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.86.172	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
109.65.118.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
186.29.96.113	Colombia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
5.102.254.222	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.133.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
79.182.112.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
79.176.136.252	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
88.116.57.70	Austria	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
176.13.16.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
128.127.107.81	Netherlands	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.180.187.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
157.55.39.79	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
46.19.86.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.16.14	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
84.229.34.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/home/default.aspx	Block	1
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	1
141.212.122.80	United States	147.237.76.31	nakchal.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
66.249.64.224	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1397-he/atal.aspx	Block	1
2.54.47.137	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
66.249.79.121	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19396-he/idfgdover.aspx	Block	1
207.46.13.65	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19645-he/dover	Block	1
141.212.122.80	United States	147.237.76.86	navy.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
80.246.136.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
2.54.56.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.39.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
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
46.19.86.234	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 46.19.86.234 (Open Mode)	None	1
141.212.122.80	United States	147.237.77.233	atal.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
84.108.212.201	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	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
5.29.227.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.19.125	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTVALIDATIO in www.aka.idf.il/main/sachar/	None	1
109.201.154.198	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
46.182.30.45	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
141.212.122.129	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /x	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xyzy	Block	1
79.177.57.41	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$employmentStatesMonth in www.aka.idf.il/main/sachar/payslips.aspx	None	1
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.220.146.23	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.55	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1