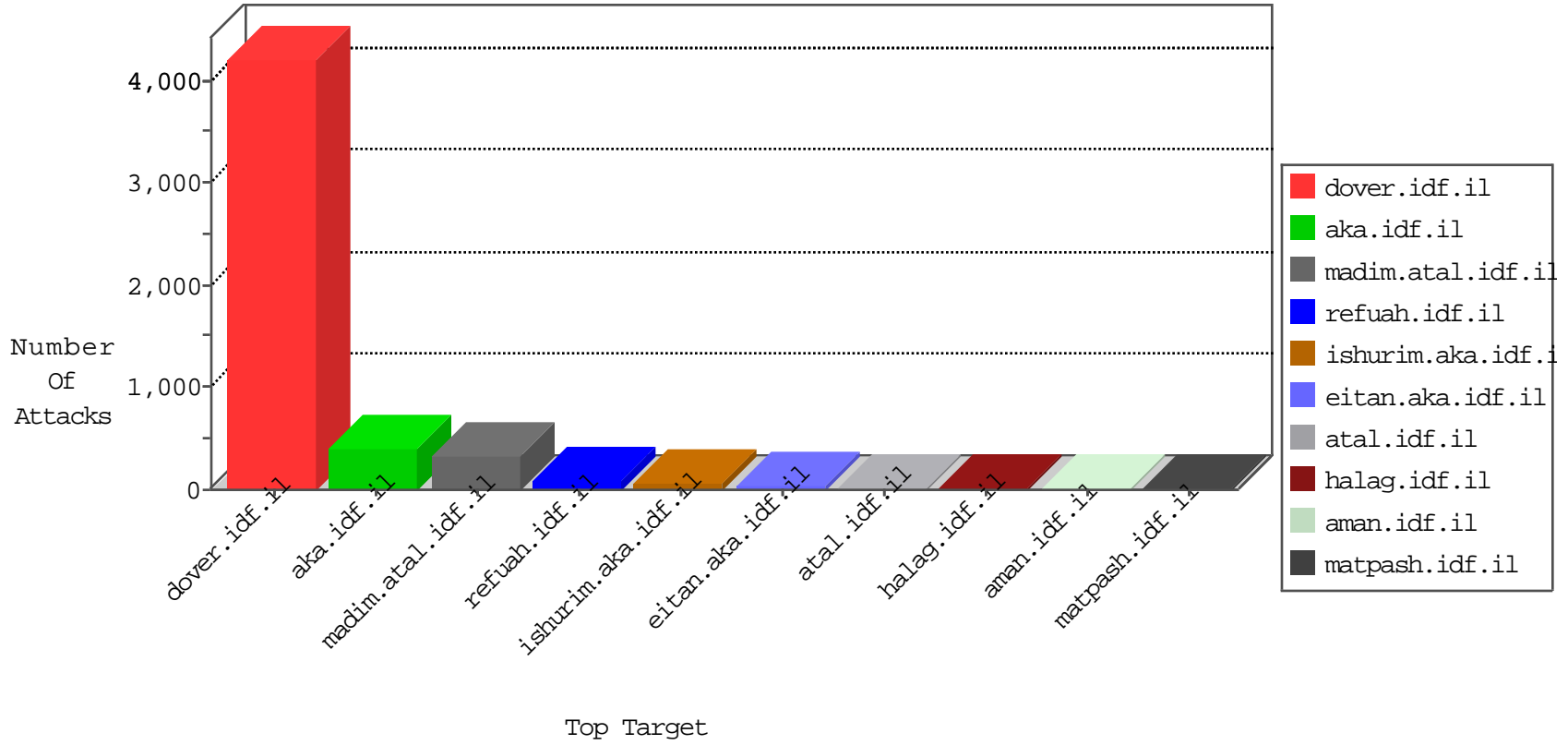


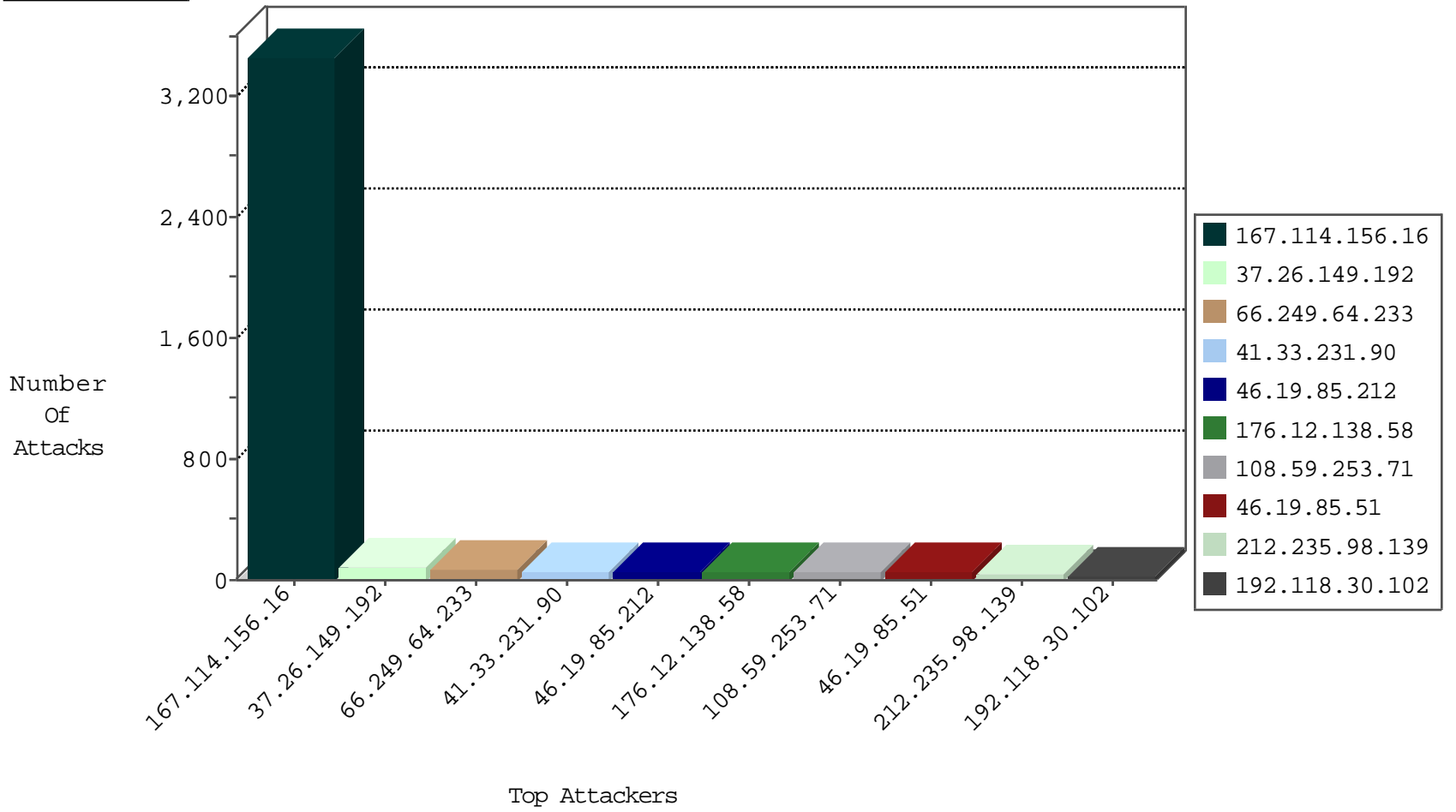
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.50	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3380
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	546
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	397
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
79.177.80.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
93.81.206.14	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	3
115.231.222.40	China	147.237.0.15	kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	2
109.248.153.111	Russian Federation	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
115.231.222.40	China	147.237.0.15	kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.90.209.69	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
82.80.46.158	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
151.80.31.130	Italy	147.237.76.200	eitan.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
213.244.82.58	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
151.80.31.142	Italy	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.99	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
87.68.158.61	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	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

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3267
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
84.109.126.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
77.158.88.41	France	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.51	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
62.0.203.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
77.158.88.42	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.51	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.86.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
77.158.88.40	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
162.243.199.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
100.100.11.157		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.217	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
157.55.39.254	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
86.15.36.175	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.182.165.40	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.65.209.88	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.181.241	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
176.13.21.58	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
85.130.223.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
62.0.251.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.54.129.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.64.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.239	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.177.6.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
176.12.138.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
46.19.85.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
176.13.1.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28
37.26.146.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
37.26.148.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
46.19.86.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
46.19.85.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
37.26.149.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	9
176.13.9.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
37.26.147.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
37.26.148.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
81.218.251.251	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
132.70.66.9	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 132.70.66.9	Block	5
176.13.22.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.8.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
207.232.36.85	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
80.246.136.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.22.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.61.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.19.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.158.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.181.150.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
176.13.16.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
132.70.66.9	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.246.136.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
207.232.36.85	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	2
176.13.20.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
5.29.75.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.229.35.56	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
62.0.100.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct125 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
123.125.71.29	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
212.76.106.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
207.46.13.181	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
2.54.24.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.91.63	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewj9zovihabjahvburokhyrxchkqfggnmaa&usg=afqjcnhcyyg7w1cq-yhd5_ammzoyodtwa	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
82.166.27.88	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1