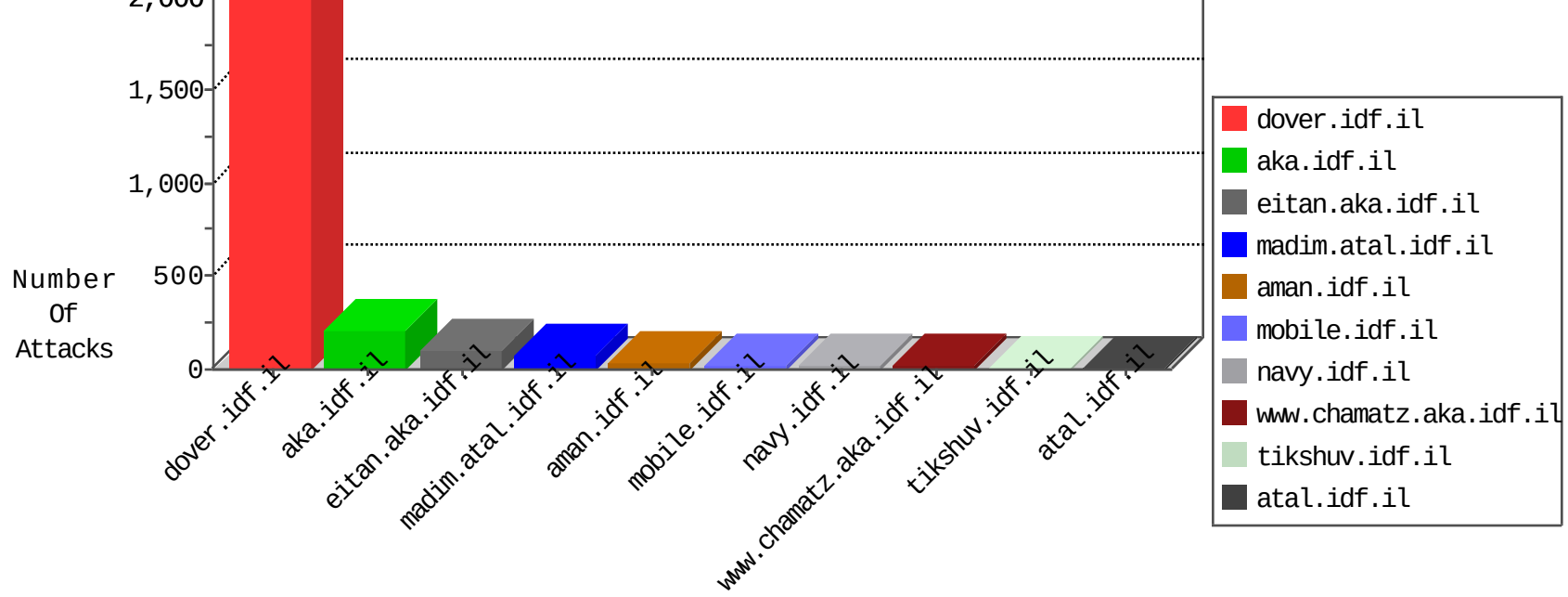
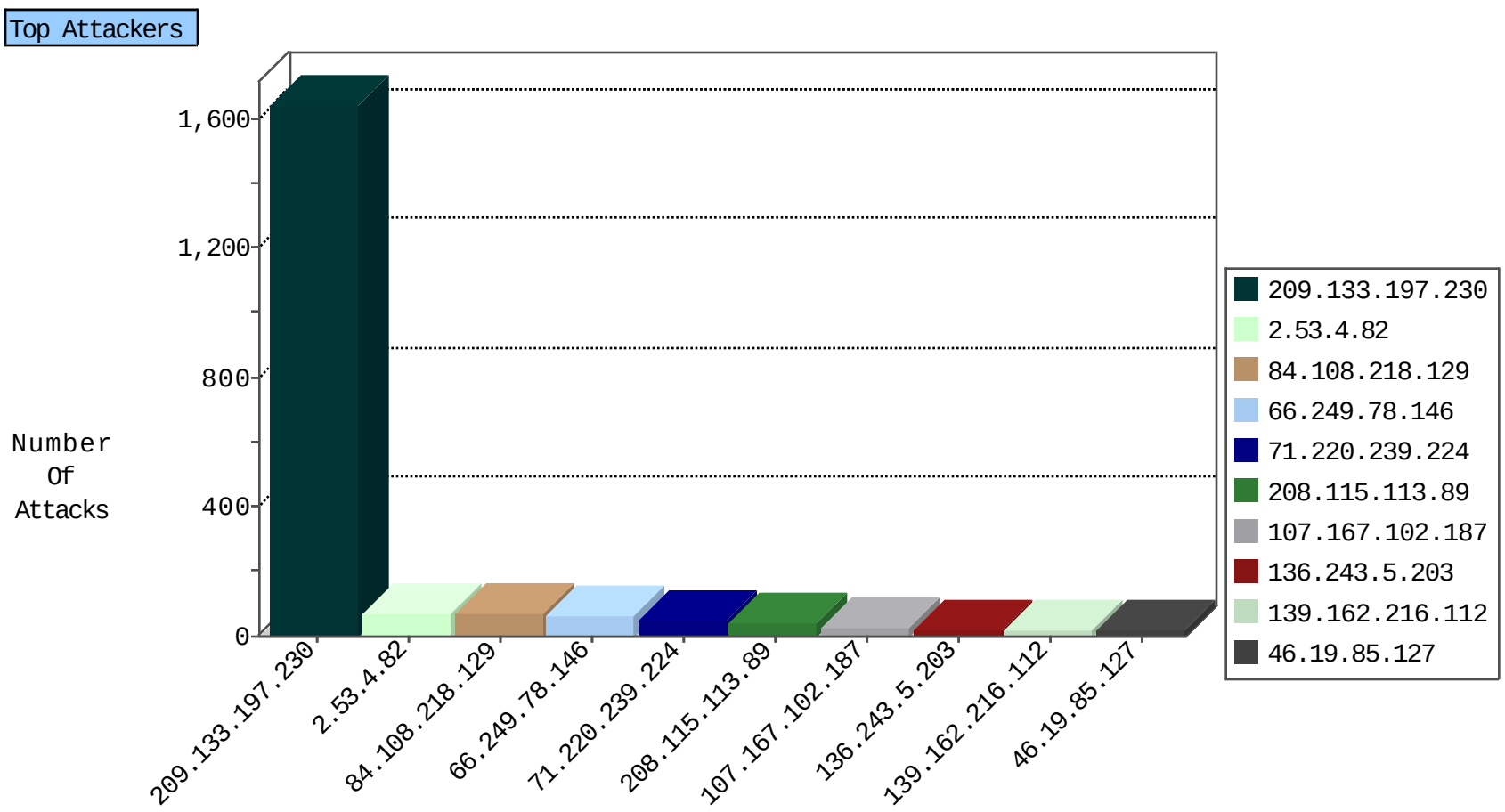
04-25-2016-21:04:06 to 04-25-2016-22:04:06

IDF Under Attack Daily Report





04-25-2016-21:04:06 to 04-25-2016-22:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.102.6.191	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1255
82.145.219.81	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
201.238.254.156	Chile	147.237.76.196	e.sviva.idf.il	L4 Source or Dest Port Zero	drop	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
183.60.48.25	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
89.46.102.242	Romania	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
31.148.219.200	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
123.59.59.52	China	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
89.46.102.242	Romania	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
45.63.20.231	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.162	China	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
94.102.52.10	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

04-25-2016-21:04:06 to 04-25-2016-22:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-25-2016-21:04:06 to 04-25-2016-22:04:06

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	3
185.130.5.99	147.237.0.16	Lithuania	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
152.250.137.78	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.82.78.38	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
58.218.204.211	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
196.203.149.99	147.237.76.198	Tunisia	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
58.218.204.211	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.198	Lithuania	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.39	Lithuania	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.0.19	Lithuania	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.0.15	Lithuania	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
139.217.27.204	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
58.218.204.211	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
58.218.204.211	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.77.205	Latvia	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.201	Lithuania	e.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.148	Lithuania	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.31	Lithuania	nakchal.idf.il	ET SCAN Potential SSH Scan	1

04-25-2016-21:04:06 to 04-25-2016-22:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
209.133.197.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1643
84.108.218.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
71.220.239.224	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
107.167.102.187	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
213.57.211.155	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.243.150.194	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
143.176.92.255	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
188.72.103.228	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.46.39.59	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
204.16.69.128	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.102.6.188	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.130.235.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
149.78.38.113	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.130.235.64	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.210.186.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.56.81	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.231.136.15	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
118.173.143.81	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
66.102.6.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.46.38.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
72.38.202.49	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
66.96.128.60	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
46.19.85.127	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.127	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.136	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
87.70.21.115	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
85.130.235.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.154.167.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.188.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.77.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.18.131	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
2.53.4.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
46.19.85.22	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.85.22	Block	10
46.116.6.243	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
2.53.143.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.64.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.22	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
203.127.96.212	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily	Block	1
84.110.209.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
61.161.130.241	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/docs/funcspecs/3.jsp	Block	1
180.76.15.14	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20050529.htm	Block	1
2.53.138.216	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
94.23.19.178	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/מאיר שחמון.aspx	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
212.24.144.226	Czech Republic	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
149.78.144.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.8.102.57	Italy	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
180.76.15.155	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
109.160.160.49	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.160.160.49	Block	1
69.30.219.2	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
87.69.168.165	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 87.69.168.165	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/smalim.aspx	Block	1
185.5.223.12	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
5.102.195.120	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/resources/images/icons/favicon.png	Block	1
130.185.155.10	Sweden	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
82.102.220.191	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
87.69.168.165	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
197.49.127.210	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
130.185.155.10	Sweden	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
84.110.209.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$62 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
61.161.130.241	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/docs/funcspecs/3.jsp	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
87.70.67.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1

04-25-2016-21:04:06 to 04-25-2016-22:04:06