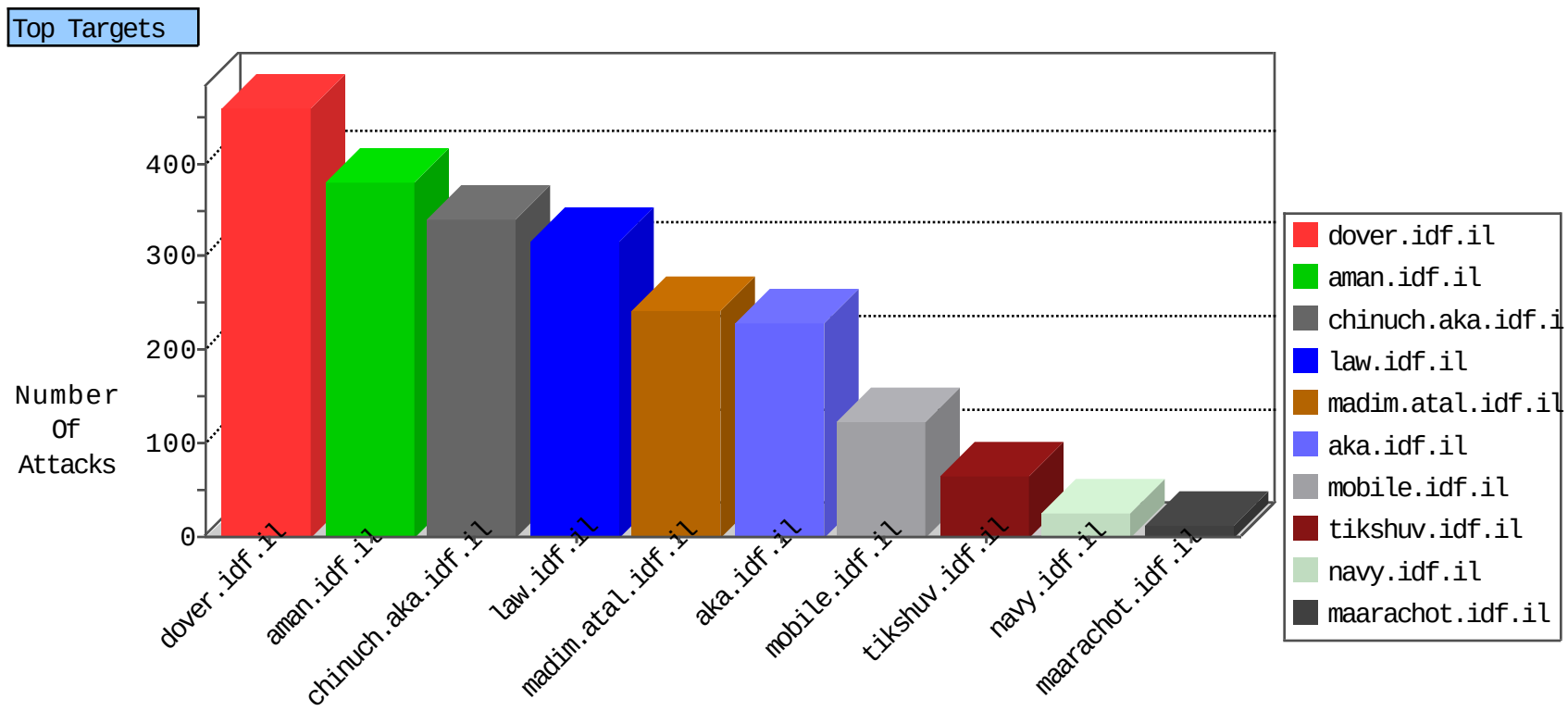
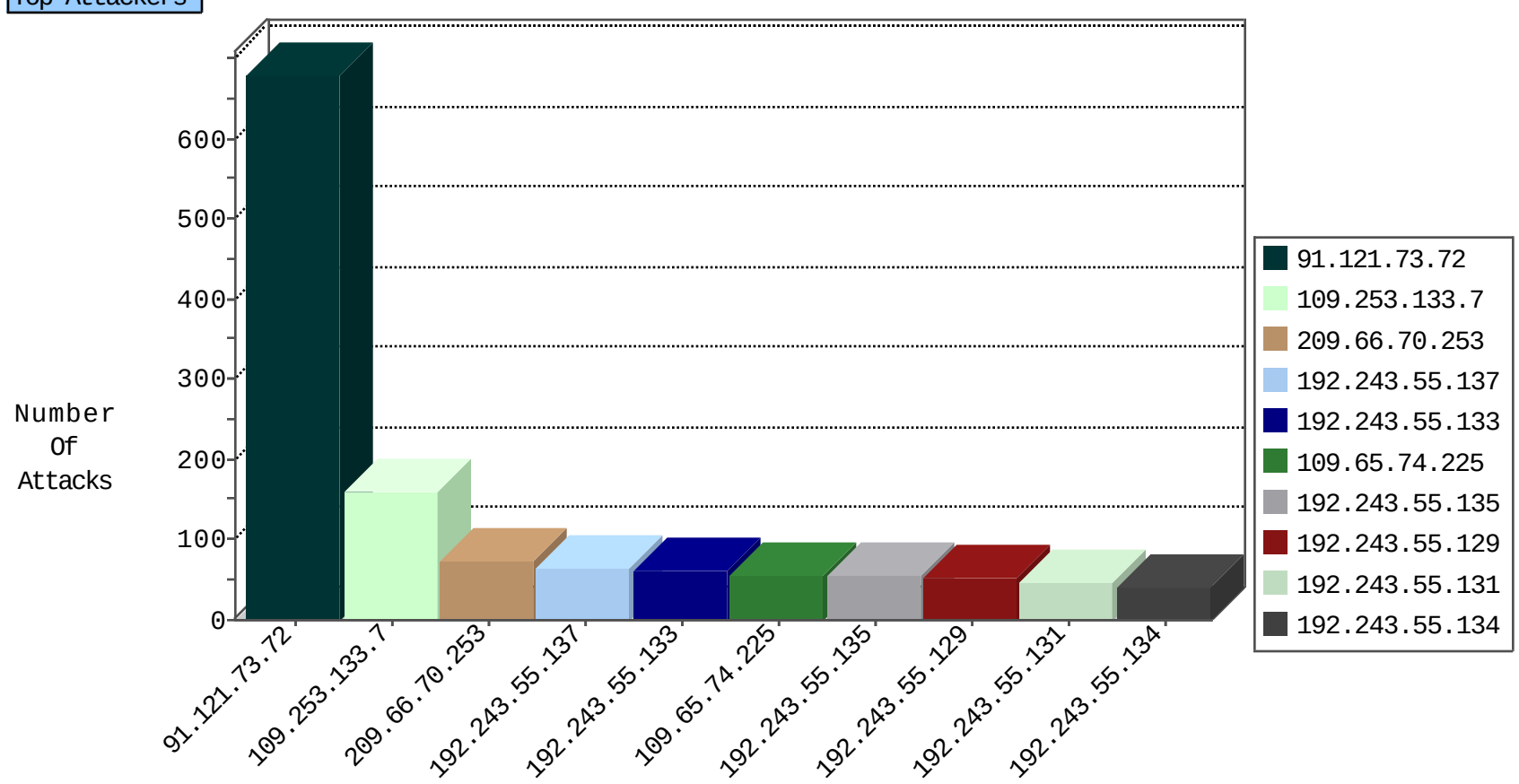
03-03-2016-17:04:06 to 03-03-2016-18:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-03-2016-17:04:06 to 03-03-2016-18:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.74.225	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	54
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
115.85.254.146	China	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
65.23.156.52	United States	147.237.0.19	madim.atal.idf.il	Invalid L4 Header Length	drop	1
164.132.54.194	Italy	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1

03-03-2016-17:04:06 to 03-03-2016-18:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.210.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
2.54.32.245	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.54.142.222	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.149.157	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.52.144.69	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.130	Italy	147.237.72.156	aman.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
212.235.31.253	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-03-2016-17:04:06 to 03-03-2016-18:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.66.70.253	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	25
82.221.48.130	147.237.76.42	Iceland	refuah.idf.il	Tehila - Perl LWP with fake user agent	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
52.7.206.250	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
193.106.52.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.125.56	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.162.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
147.235.236.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.130.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.215.89.20	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -f -sS	1
213.197.233.199	147.237.72.166	Netherlands	aka.idf.il	Tehila - Perl LWP with fake user agent	1
94.102.48.193	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.42.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.47.238.99	147.237.0.19	France	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.178.157.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.176.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.76.30	Sweden	himush.idf.il	ET SCAN NMAP -sS window 1024	1
37.9.122.202	147.237.72.166	Russian Federation	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.4.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.68.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.74.150.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.215.89.20	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
218.246.0.97	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
213.57.105.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.37.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.176.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.48.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-03-2016-17:04:06 to 03-03-2016-18:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.121.73.72	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	264
91.121.73.72	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	215
91.121.73.72	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	89
91.121.73.72	France	147.237.72.156	aman.idf.il	SYN Attack		reject	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
176.13.18.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
209.66.70.253	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
209.66.70.253	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
91.121.73.72	France	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	24
46.19.85.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
91.121.73.72	France	147.237.72.156	aman.idf.il	drop	SAM rule	drop	24
2.54.187.146	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	16
91.121.73.72	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
5.22.129.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
80.246.136.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
175.157.116.236	Sri Lanka	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
87.69.133.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
66.249.93.125	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
2.54.140.112	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.139.190.95	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
175.157.116.236	Sri Lanka	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
149.78.161.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
91.121.73.72	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.161	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.34.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.135	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

03-03-2016-17:04:06 to 03-03-2016-18:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.133.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	159
109.253.209.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
46.116.216.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
109.253.135.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
77.127.198.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.18.139	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.148	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
109.253.139.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
125.91.129.29	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	5
87.69.133.144	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
24.42.165.85	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/modiin/general	Block	3
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	3
46.19.85.9	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
192.117.158.210	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.117.158.210	Block	3
125.91.129.29	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 125.91.129.29	Block	3
83.130.108.89	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/ain/giyus	Block	3
80.246.136.115	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.181	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
125.91.129.29	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/plus/download.php	Block	2
213.57.143.74	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
82.221.48.130	Iceland	147.237.76.42	refuah.idf.il	PHP Attempt	Block	2
54.244.22.103	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.114.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.221.48.130	Iceland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/index.php	Block	2
4.79.123.3	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcdhphdmltxdezmzquzg9j&infocenteritem=true	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in URL	Block	1
72.186.5.22	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;list in www.aka.idf.il/kamlar/klali/default.asp	None	1
37.26.146.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.127.7	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21389-he/dover.aspx&sa=u&ved=0ahukewjttoaz6atlahumeiwkha_qc6uqfggfmak&usg=afqjcnexjm555oo0jti8231eng6vfumiqw	Block	1
81.218.204.97	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/general	Block	1
182.253.145.2	Indonesia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.83.81	United States	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	147.237.76.30	himush.idf.il	Malformed URL '„·''Ù¯ƒšit	Block	1
118.193.161.67	China	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
87.162.106.80	Germany	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
23.80.148.14	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/shared/usercontrols/headerupper/	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Unknown HTTP Request Method ûÙç1%-å20·ä_[[#4]]&[[#24]]Îí[[#27]]»˜M…áöåã3²ÏÎ^F³Ïcö´7[[#7]]ÇO in URL	Block	1
66.249.64.229	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/templates/shared/usercontrols/headerupper/	Block	1
137.226.113.7	Germany	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
38.81.65.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
192.117.158.210	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Unknown HTTP Request Method ³2#ö[[#12]]~•	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
118.193.161.67	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/utility/convert/index.php	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Method	Block	1
79.178.1.34	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.122	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1

03-03-2016-17:04:06 to 03-03-2016-18:04:06