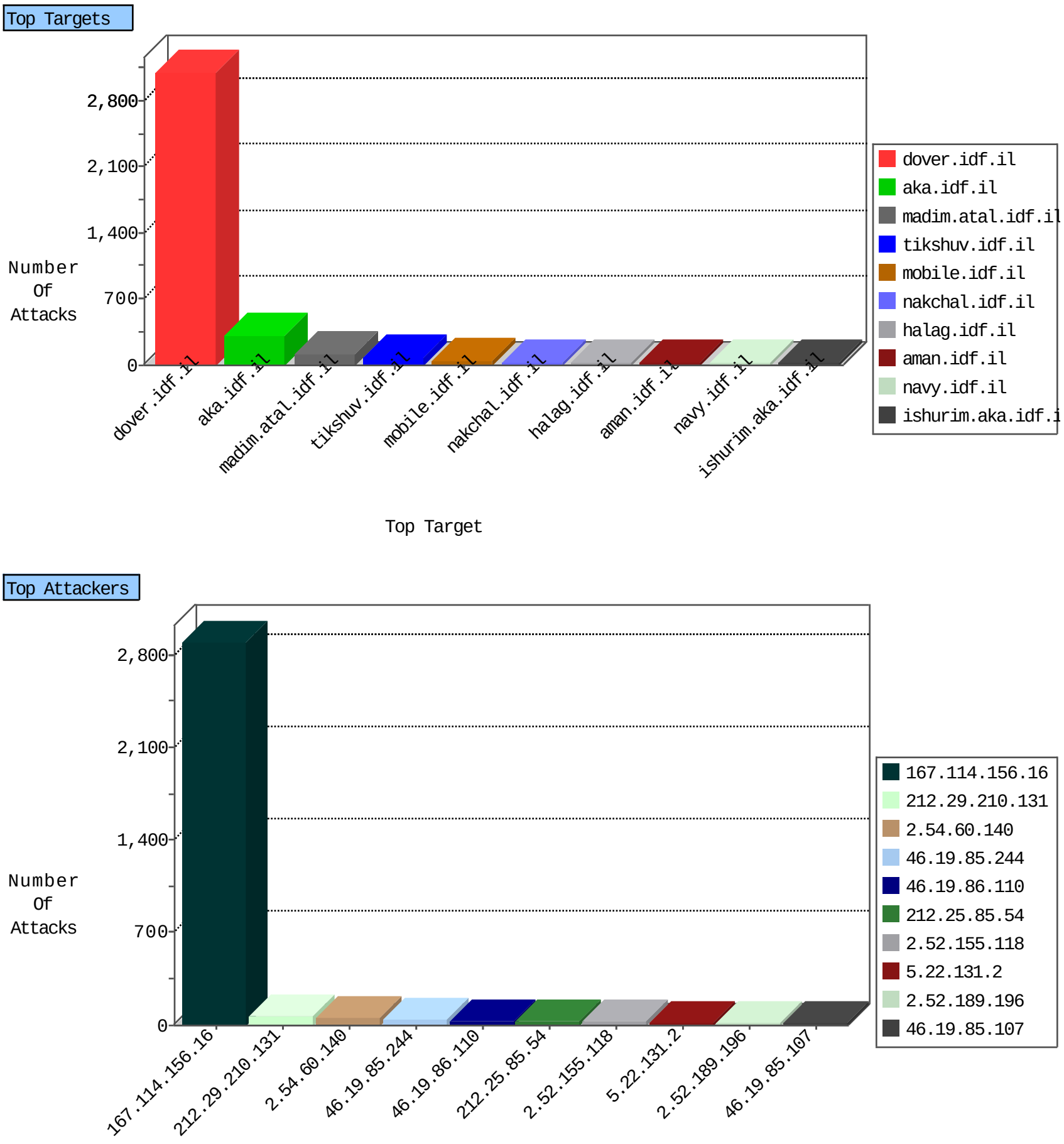
03-14-2016-20:04:01 to 03-14-2016-21:04:01

IDF Under Attack Daily Report



03-14-2016-20:04:01 to 03-14-2016-21:04:01

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	3456
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
31.171.155.29	Albania	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
199.58.80.184	Canada	147.237.0.15	kosher-kravi.idf.il	L4 Source or Dest Port Zero	drop	1
31.171.155.29	Albania	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1

03-14-2016-20:04:01 to 03-14-2016-21:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.22.131.2	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	21
61.135.189.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
109.65.2.78	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
69.197.177.50	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.242	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.242	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
212.47.234.93	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.242	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
46.19.85.244	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.198.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2

03-14-2016-20:04:01 to 03-14-2016-21:04:01

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

03-14-2016-20:04:01 to 03-14-2016-21:04:01

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	SYN Attack	SYN -> SYN-ACK -> RST	reject	48
46.19.85.244	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
212.29.210.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
212.29.210.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	33
2.52.155.118	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
2.52.189.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.120.126.195		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.2.202	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	11
2.54.168.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.175.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.68	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
46.120.95.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
176.13.9.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.120.95.243	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.23	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.121.76.48	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.229.198.81	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.120.95.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.64.212.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
84.94.180.12	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.22.130.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.186.188.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.67.133.17	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
5.102.254.231	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.120.148.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.250.114.37	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
84.196.115.145	Belgium	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.254.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.206.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.127.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.26.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.106.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.151.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.18.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.191.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.69.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.23	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
84.94.114.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.140	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

03-14-2016-20:04:01 to 03-14-2016-21:04:01

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
5.102.254.231	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.60.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	59
46.19.86.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
212.25.85.54	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	29
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
5.28.168.235	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	5
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	3
2.52.189.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.23.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
105.235.130.1	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
84.109.3.181	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.97	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
213.57.159.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
40.77.167.79	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/901-8504/tikshuv.aspx	Block	1
151.18.9.162	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
87.69.62.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
5.28.166.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1
79.179.31.156	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
192.118.73.36	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
176.107.194.231	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1566-en/d	Block	1
37.26.148.194	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.69	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1376-he/atal.aspx	Block	1
188.120.148.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/5/2325	Block	1
156.199.70.139		147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.149.29.18	Germany	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.254.241.6	United Kingdom	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
79.180.229.122	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
185.120.126.121		147.237.77.74	law.idf.il	PHP Attempt	Block	1
46.120.112.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.167.5	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/contactus.aspx	Block	1
109.65.129.151	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl75 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
85.65.103.155	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
188.143.22.196	Hungary	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
160.94.47.18	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.113.125.12	Romania	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 93.113.125.12	Block	1
31.184.238.200	Russian Federation	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
219.74.38.152	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/size220x0/16037.jpg	Block	1
79.183.134.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.120.126.121		147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
54.244.22.103	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.167.23	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.67.133.17	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
85.65.103.155	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.93.163	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
188.143.22.196	Hungary	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1

03-14-2016-20:04:01 to 03-14-2016-21:04:01