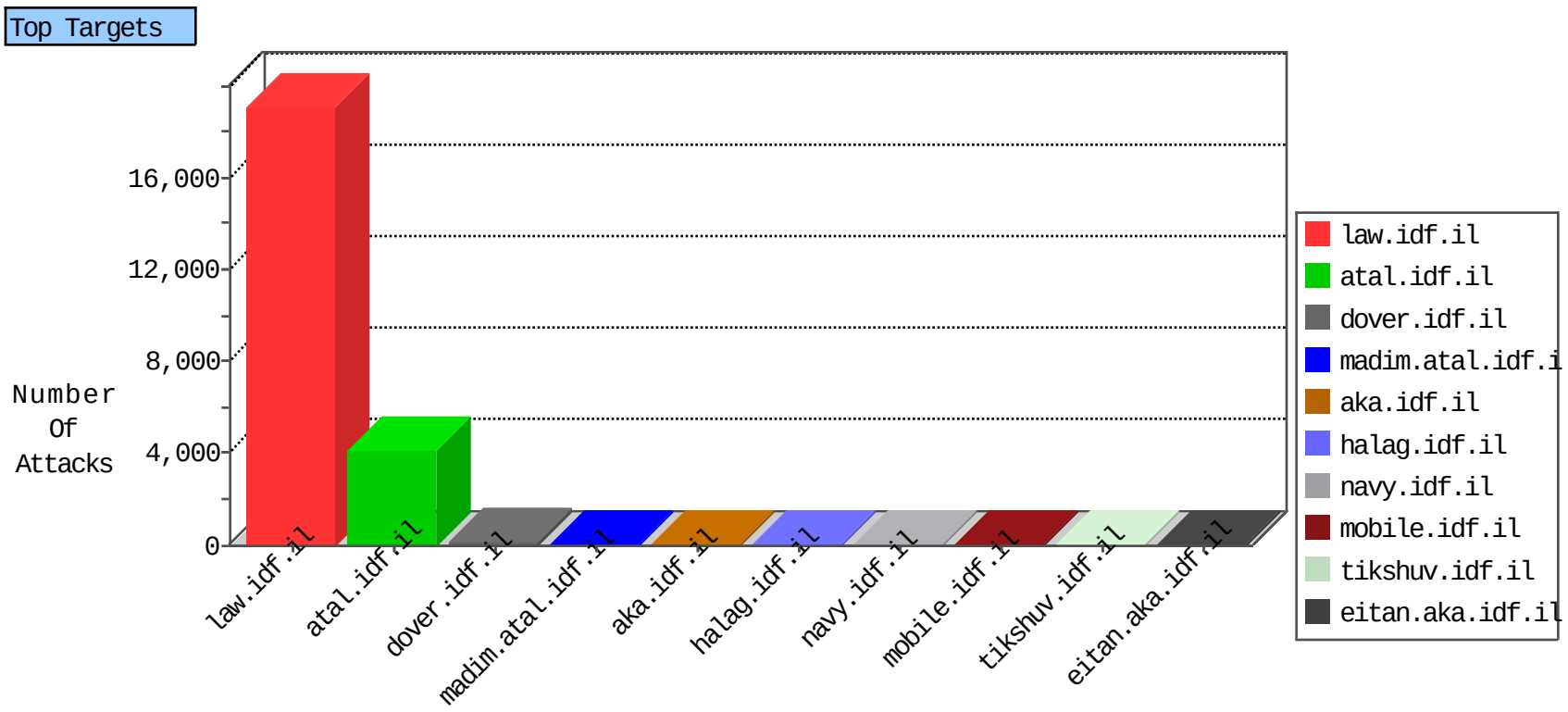
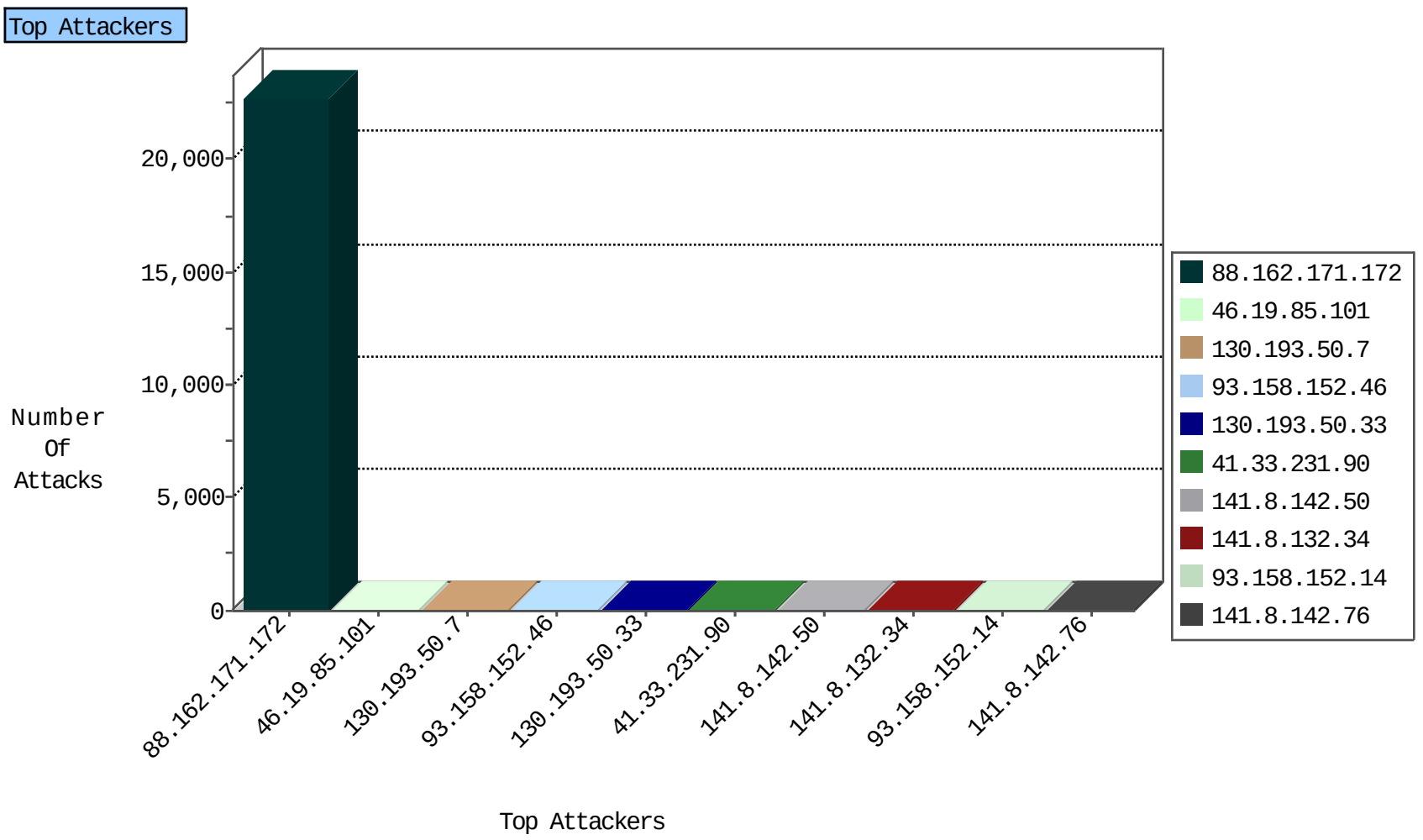
02-03-2016-06:04:06 to 02-03-2016-07:04:06

IDF Under Attack Daily Report





02-03-2016-06:04:06 to 02-03-2016-07:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.8.184.29	Russian Federation	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	659
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
88.162.171.172	France	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
115.236.67.147	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
200.86.119.192	Chile	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.79	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	1
200.86.119.192	Chile	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
85.25.43.94	Germany	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
200.86.119.192	Chile	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
200.86.119.192	Chile	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
5.255.253.30	Russian Federation	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1

02-03-2016-06:04:06 to 02-03-2016-07:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.49	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.59	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-03-2016-06:04:06 to 02-03-2016-07:04:06

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	4
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
104.128.144.131	147.237.77.61	Canada	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.113	147.237.77.121	Ukraine	e.navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
37.200.225.36	147.237.72.156	Oman	aman.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.76.200	United States	eitan.aka.idf.il	ET DROP Dshield Block Listed Source	1
196.47.173.21	147.237.8.45	Cote D'Ivoire	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.84	147.237.0.19	Ukraine	madim.atal.idf.i	ET SCAN Potential SSH Scan	1
145.255.2.133	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.61	Canada	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.113	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.2	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.8.45	Cote D'Ivoire	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
189.167.47.240	147.237.77.216	Mexico	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
145.255.1.5	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN NMAP -sS window 1024	1

02-03-2016-06:04:06 to 02-03-2016-07:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
88.162.171.172	France	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	18343
88.162.171.172	France	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4178
88.162.171.172	France	147.237.77.74	law.idf.il	drop		drop	150
130.193.50.7	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	46
93.158.152.46	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	40
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
141.8.142.50	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	31
88.162.171.172	France	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
88.162.171.172	France	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
141.8.132.34	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	18
141.8.132.71	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	16
141.8.142.76	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	16
93.158.152.14	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	16
88.162.171.172	France	147.237.77.74	law.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	16
130.193.51.29	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	14
5.255.253.80	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	14
93.158.152.75	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
93.158.152.5	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
178.154.189.26	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
93.158.152.44	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
5.255.253.103	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
141.8.183.1	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
141.8.184.29	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
5.255.253.30	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
93.158.152.64	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
141.8.132.52	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
93.158.152.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
5.255.253.24	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
130.193.37.18	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
66.249.66.42	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
141.8.142.12	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
5.255.253.124	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
93.158.152.47	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
5.255.253.82	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
130.193.51.17	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
5.255.253.86	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.217.14.172	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
188.120.148.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.138.36	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
68.180.231.40	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
66.249.66.45	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.14.95.223	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
130.193.51.26	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
2.54.191.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.78.161	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

02-03-2016-06:04:06 to 02-03-2016-07:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
212.179.134.162	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.134.162	Block	4
80.246.136.99	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
188.143.232.13	Russian Federation	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.143.232.13	Block	2
88.162.171.172	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 88.162.171.172	Block	2
188.143.232.24	Russian Federation	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 188.143.232.24	Block	2
189.167.47.240	Mexico	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 189.167.47.240 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
176.14.95.223	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
88.162.171.172	France	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 88.162.171.172	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
40.77.167.33	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/megurim/skira/default.asp	None	1
185.3.135.42	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
98.143.148.107	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/check	Block	1
85.10.210.199	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
189.167.47.240	Mexico	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Heartbleed Attack	None	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
177.154.145.101	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
2.54.158.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
88.162.171.172	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
73.219.221.183	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
174.129.237.157	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
88.162.171.172	France	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
189.167.47.240	Mexico	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sa_swfobject.js	Block	1
5.22.129.128	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
178.162.205.26	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
74.82.47.2	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
46.116.54.227	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
188.143.232.13	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/900-he/	Block	1
176.12.154.66	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
88.162.171.172	France	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 88.162.171.172	Block	1
192.173.144.3	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/ui.datepicker.js	Block	1
5.22.129.128	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 5.22.129.128	Block	1
178.162.209.232	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
88.162.171.172	France	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layoutdev.css	Block	1
176.12.155.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
88.162.171.172	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
212.179.134.162	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
68.37.43.82	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/tfasim.aspx	Block	1
5.255.253.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
180.76.15.14	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list7.htm	Block	1
88.162.171.172	France	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 88.162.171.172	Block	1
84.177.12.104	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1

02-03-2016-06:04:06 to 02-03-2016-07:04:06