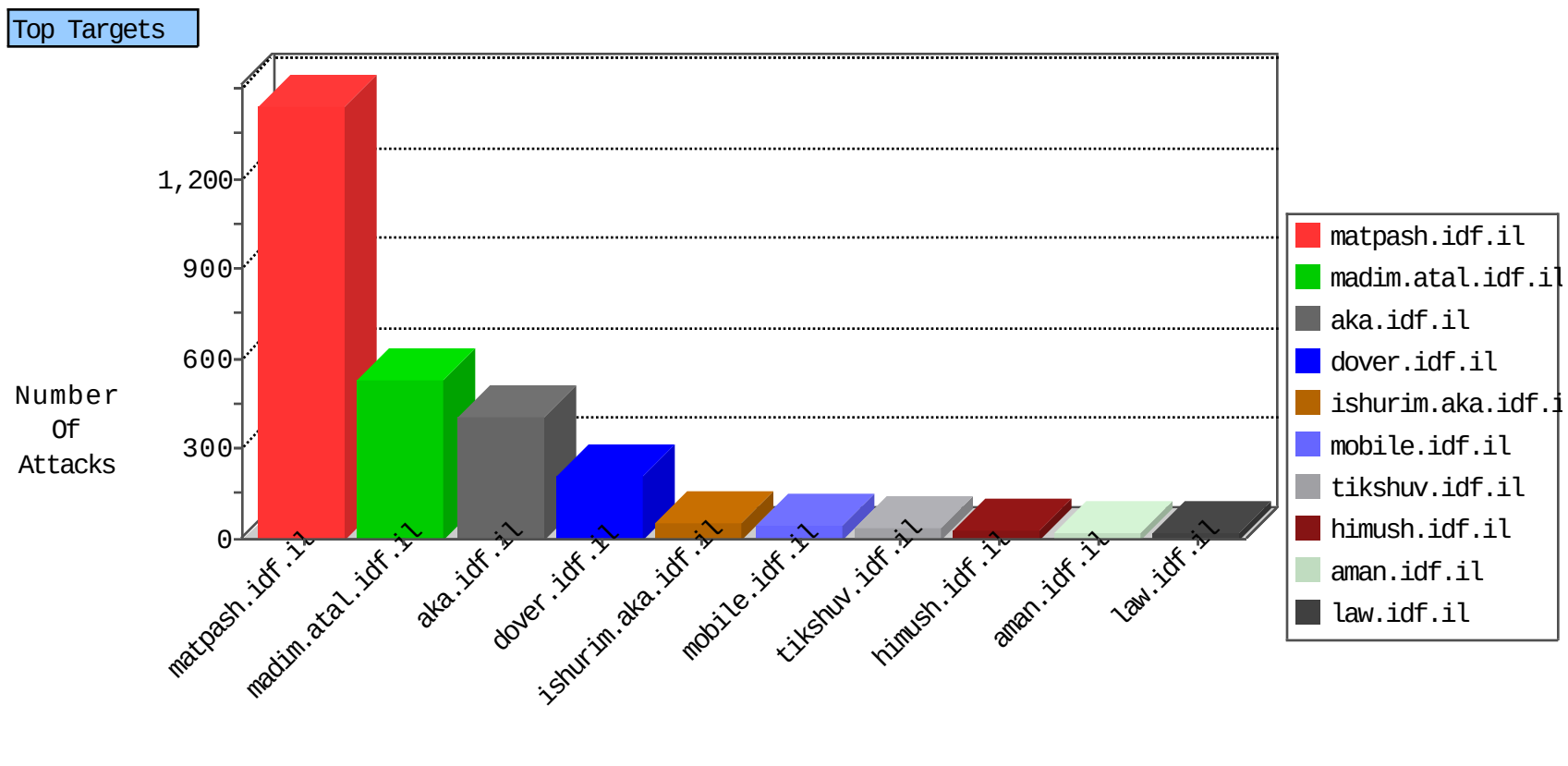
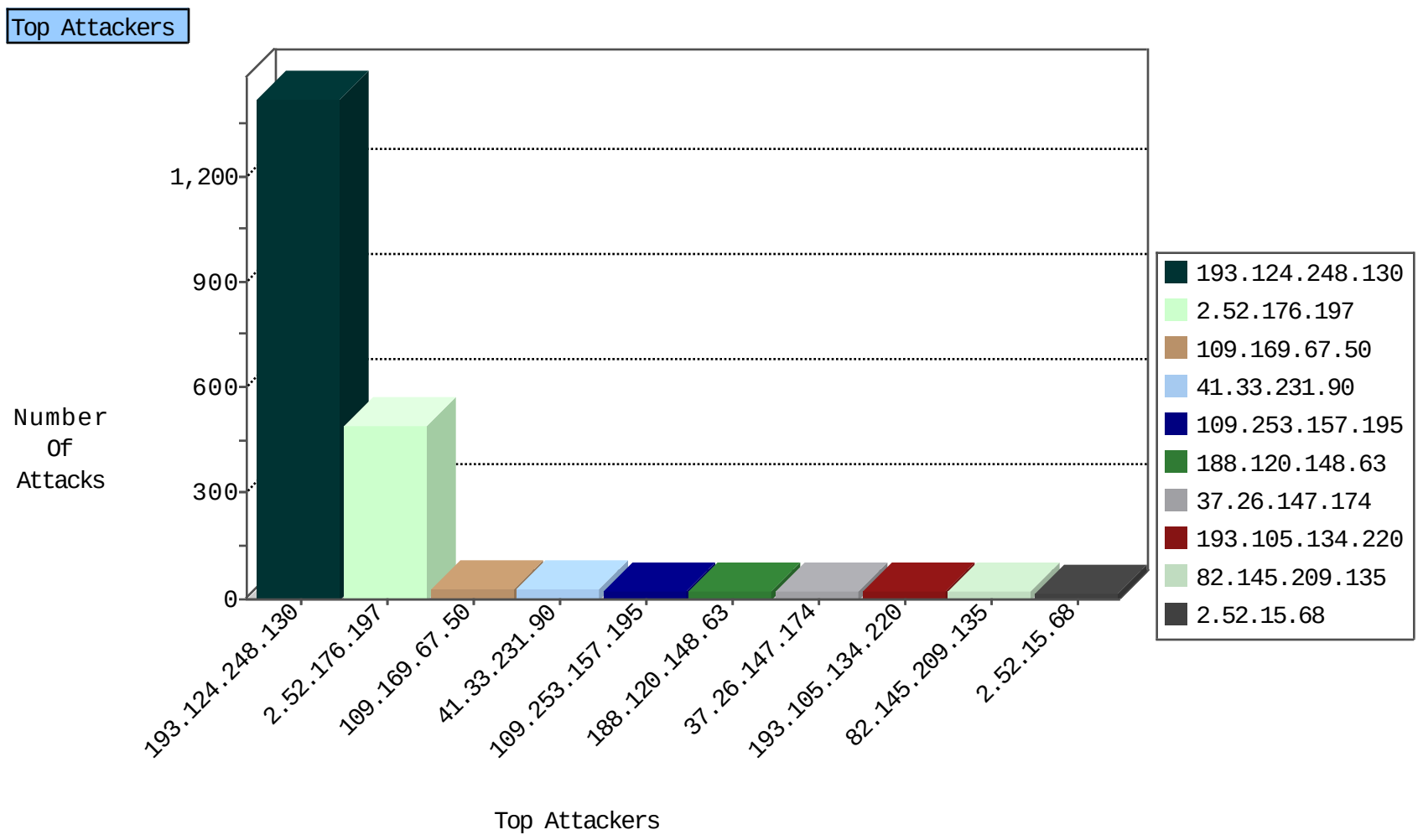
02-08-2016-18:04:06 to 02-08-2016-19:04:06

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-08-2016-18:04:06 to 02-08-2016-19:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.247.58	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
128.194.131.235	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
185.94.111.1		147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

02-08-2016-18:04:06 to 02-08-2016-19:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.134	Italy	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-08-2016-18:04:06 to 02-08-2016-19:04:06

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
109.253.157.195	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.102.9.28	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.153	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
179.43.141.234	147.237.77.243	Switzerland	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.127.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.58.169	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
119.62.123.227	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
218.83.155.86	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
212.47.237.95	147.237.77.235	France	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.114	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.101.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.165	147.237.77.212		e.dover.idf.il	ET SCAN Potential SSH Scan	1
79.183.136.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.165	147.237.76.197		e.himush.idf.il	ET SCAN Potential SSH Scan	1
183.82.106.200	147.237.72.217	India	e.idf.il	ET SCAN NMAP -sS window 4096	1
60.217.72.16	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
152.250.22.9	147.237.0.33	Brazil	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
14.158.242.161	147.237.76.34	China	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.58.169	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
149.78.39.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.58.169	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
119.62.123.227	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
212.199.218.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.25.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.47.237.95	147.237.0.15	France	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
89.138.169.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.77.178	Sweden	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.84.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.165	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.165	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1
60.217.72.16	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1

02-08-2016-18:04:06 to 02-08-2016-19:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
193.124.248.130	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1419
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
82.145.209.135	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
2.52.15.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.253.157.195	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
46.19.86.194	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	15
46.18.18.232	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.178.224.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.46.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
107.167.112.151	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
185.24.76.134	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
109.64.154.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.27.106.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.116.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.231.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.130.48	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.184.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.230.92.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.19.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.140.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.130.205.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.178.1.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.178.1.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.179.134.206	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	5
46.19.86.83	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.179.134.206	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.253.157.195	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.49.168	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
81.218.44.19	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.111.36.36	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.186.169.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
132.70.66.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.182.25.164	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.180.48.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.39.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
79.180.56.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.57.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.22.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.155.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.0.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.201.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-08-2016-18:04:06 to 02-08-2016-19:04:06

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.67.30.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-08-2016-18:04:06 to 02-08-2016-19:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.176.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	289
2.52.176.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
2.52.176.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	96
37.26.147.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
109.65.210.204	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
37.26.148.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.120.148.63	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Malformed URL	Block	3
46.19.85.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.5.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
94.23.242.48	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	2
188.120.148.63	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Unknown HTTP Request Method from 188.120.148.63	Block	2
31.154.2.110	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
109.67.148.123	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/rabanut/general.aspx	Block	2
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.120.148.63	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 188.120.148.63	Block	2
37.26.146.164	Israel	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Open Mode	None	2
188.120.148.63	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Method from 188.120.148.63	Block	2
109.65.99.54	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion $20 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
5.29.6.190	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
188.120.148.63	Israel	147.237.72.167	ishurim.aka.idf.il	Abnormally Long Request method	Block	1
149.88.36.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.109.74.111	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion $6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
188.120.148.63	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.169.67.50	United Kingdom	147.237.77.170	maarachot.idf.il	Multiple Malformed URL from 109.169.67.50	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19667-he/idfgdover.aspx)	Block	1
188.120.148.63	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Abnormally Long Header Line from 188.120.148.63	Block	1
109.169.67.50	United Kingdom	147.237.0.19	madim.atal.idf.il	Malformed URL *	Block	1
180.76.15.149	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9004-he/refuah.aspx	Block	1
80.179.225.230	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion $1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
213.57.92.115	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion $35 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
128.194.131.148	United States	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 128.194.131.148	Block	1
109.169.67.50	United Kingdom	147.237.76.42	refuah.idf.il	Multiple Malformed URL from 109.169.67.50	Block	1
46.216.245.56	Belarus	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/ Ð½Ð° Ñ€Ñƒ Ñ?Ñ?Ð°Ð¾Ð¼	Block	1
188.120.148.63	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple NULL Character in Header Name from 188.120.148.63	Block	1
5.62.131.135	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
149.88.37.219	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main-sachar	Block	1
84.228.216.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.93.125	Israel	147.237.0.34	tikshuv.idf.il	URL is Above Root Directory www.tikshuv.idf.il/../../images/shared/calendar/prev_but.gif	Block	1
188.120.148.63	Israel	147.237.72.167	ishurim.aka.idf.il	Unknown HTTP Request Method dÃ‘Ã©Ã§: in URL	Block	1
109.169.67.50	United Kingdom	147.237.77.176	matpash.idf.il	Multiple Malformed URL from 109.169.67.50	Block	1
188.120.148.63	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Abnormally Long Request from 188.120.148.63	Block	1
109.169.67.50	United Kingdom	147.237.72.156	aman.idf.il	Malformed URL *	Block	1
104.236.8.229		147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
181.225.132.66	El Salvador	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 181.225.132.66 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
80.246.130.209	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
128.194.131.148	United States	147.237.72.166	aka.idf.il	NULL Character in Method	Block	1
109.169.67.50	United Kingdom	147.237.76.200	eitan.aka.idf.il	Multiple Malformed URL from 109.169.67.50	Block	1
61.245.173.105	Sri Lanka	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
188.120.148.63	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Header Name Ã¦Ã..VÂ£1<Â¥}Ã„[[#2]]Ã˜ xk&VÃˆcÂŽ"Ãº1[[#29]]Ã”rÃ•![[#17]]Â¯Â?Ã¿j[[#3]]Ã—•Ã• [[#26]]Ã¦Â½r[[#24]]Â-Â¬ÃºÃ½Âªe/Â¸ [[#2]]`MMÂ§Â¥JÃ‘Â”<	Block	1

02-08-2016-18:04:06 to 02-08-2016-19:04:06