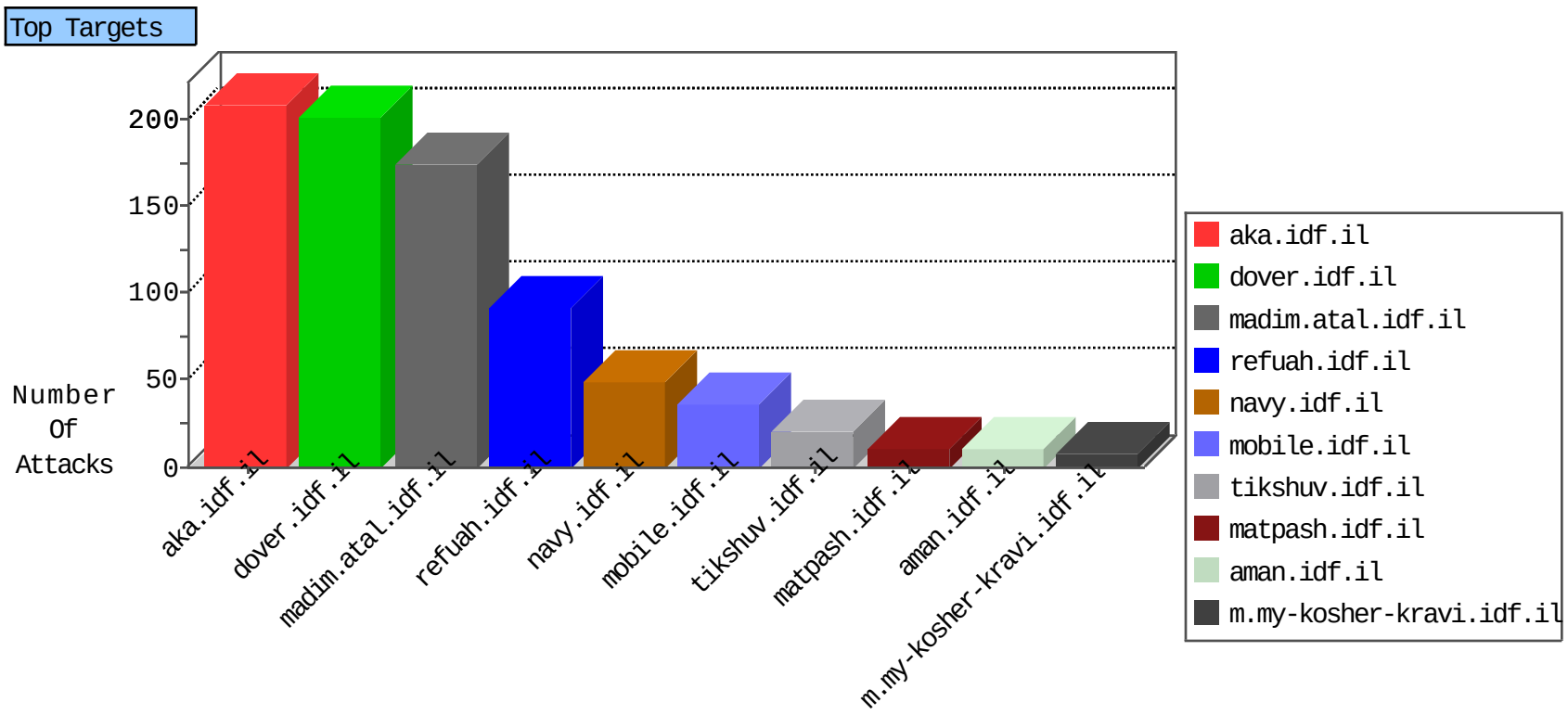
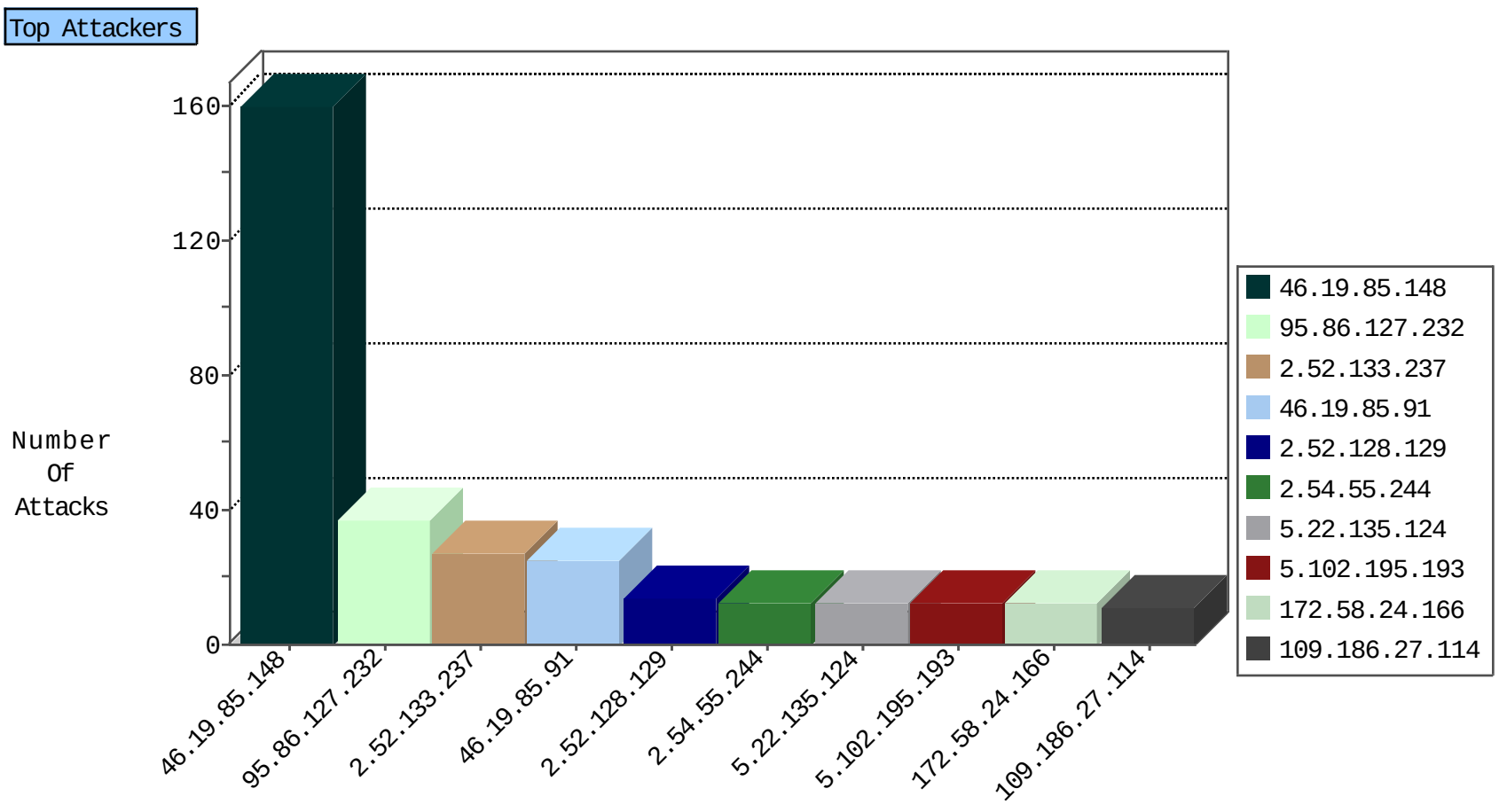
03-08-2016-22:04:06 to 03-08-2016-23:04:06

IDF Under Attack Daily Report



Top Target



Top Attackers

03-08-2016-22:04:06 to 03-08-2016-23:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
82.145.221.12	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
217.146.91.36	United Kingdom	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
104.156.246.165	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
218.77.14.202	China	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
104.156.246.165	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
217.146.91.36	United Kingdom	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
104.156.246.165	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
162.216.114.158	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
217.146.91.36	United Kingdom	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
104.156.246.165	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
217.146.91.36	United Kingdom	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
104.156.246.165	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

03-08-2016-22:04:06 to 03-08-2016-23:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.230.191	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.8.204.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
61.135.189.69	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
69.30.234.186	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
46.4.123.172	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
79.181.187.38	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
177.185.194.138	Brazil	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
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
62.128.48.46	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-08-2016-22:04:06 to 03-08-2016-23:04:06

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
221.226.31.210	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	147.237.77.176	India	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.0.17	Canada	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
94.102.53.233	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.179.60.212	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
221.226.31.210	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
218.246.0.97	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	147.237.77.176	India	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
202.71.25.29	147.237.77.176	India	matpash.idf.il	ET SCAN NMAP -f -sS	1
104.128.144.131	147.237.0.17	Canada	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.53.233	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.53.233	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
50.191.78.108	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

03-08-2016-22:04:06 to 03-08-2016-23:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.133.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
2.54.55.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
172.58.24.166	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.186.27.114	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.52.128.129	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.54.204.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.212	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
208.54.85.180	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.22.135.124	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.130.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.29.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.242.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.180.38.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.91	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.91	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.120.148.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.195.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.78.242.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
96.242.131.202	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.109	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
96.242.131.202	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
131.253.25.166	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.142.68.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.19.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
100.127.2.13		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.33	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
46.121.71.23	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.66.31.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.179.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.224.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.187.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.195.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.173.76	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
87.71.24.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.226.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.8.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.230.228.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.29.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.145.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.195.159	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
190.163.219.164	Chile	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
2.52.133.2	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.52.133.2	Block	7
2.54.191.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
95.86.127.232	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 95.86.127.232	Block	3
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.127.232	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 95.86.127.232	Block	3
95.86.127.232	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 95.86.127.232	Block	3
161.185.161.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.212.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.2.67	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
95.86.127.232	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 95.86.127.232	Block	2
2.52.133.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
95.86.127.232	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 95.86.127.232	Block	2
95.86.127.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
95.86.127.232	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 95.86.127.232	Block	2
94.230.93.79	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/imagevideogallerylobby/imagevideogallerylobby.js	Block	1
50.254.218.250	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
95.86.127.232	Israel	147.237.72.166	aka.idf.il	NULL Character in URL	Block	1
94.230.93.34	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/scriptresource.axd	Block	1
95.86.127.232	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL ″v[[#29]]nÿ[[#2]][[#31]][[#28]]¿/|pn :/[[#29]]lcµµ[[#31]]^'¬5[[›·#17[[]]#5³/w]]ᵀÊ¸]]03#[['_·–ƒb]]12#[[„1uƤf{m	Block	1
94.230.86.137	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.160.206.202	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
94.230.93.111	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/960.css	Block	1
95.86.127.232	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 95.86.127.232	Block	1
94.230.93.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
94.230.93.18	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sa_swfobject.js	Block	1
212.76.96.142	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/942-5061-he/patzar.aspx&sa=u&ved=0ahukewjxrmvq87hlahubjnikhq8jakeqfgglmae&usg=afqjcnh_iddvdzk1io6xr0mlnltaw1byna	Block	1
95.86.127.232	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 95.86.127.232	Block	1
95.86.127.232	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
87.71.45.222	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
141.212.122.209	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
94.230.93.82	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/clientscripts.js	Block	1
50.254.218.250	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1393-en/dover.aspx	Block	1
95.86.127.232	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.26.147.135	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
94.230.93.37	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/expand.js	Block	1
95.86.127.232	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version ¶O¤[[#28]]•-/[[#6]][[#0]][[#26]][[#11]]j·uK¯Â³7″B·…\[[#18]]'ÐÀ¤Ñâ[[#27]]vžC[[#3]]rA,[[#2]][[#14]]Ä1º[[[#23]] FÊ¹´=•	Block	1
94.230.93.2	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
176.13.7.8	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.186.185.117	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
94.230.93.114	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
94.230.93.63	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/scroller/jquery.jcarousel.css	Block	1
46.19.85.104	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
94.230.93.21	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/scroller/skin.css	Block	1
213.57.57.169	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/miluimday.asp	Block	1