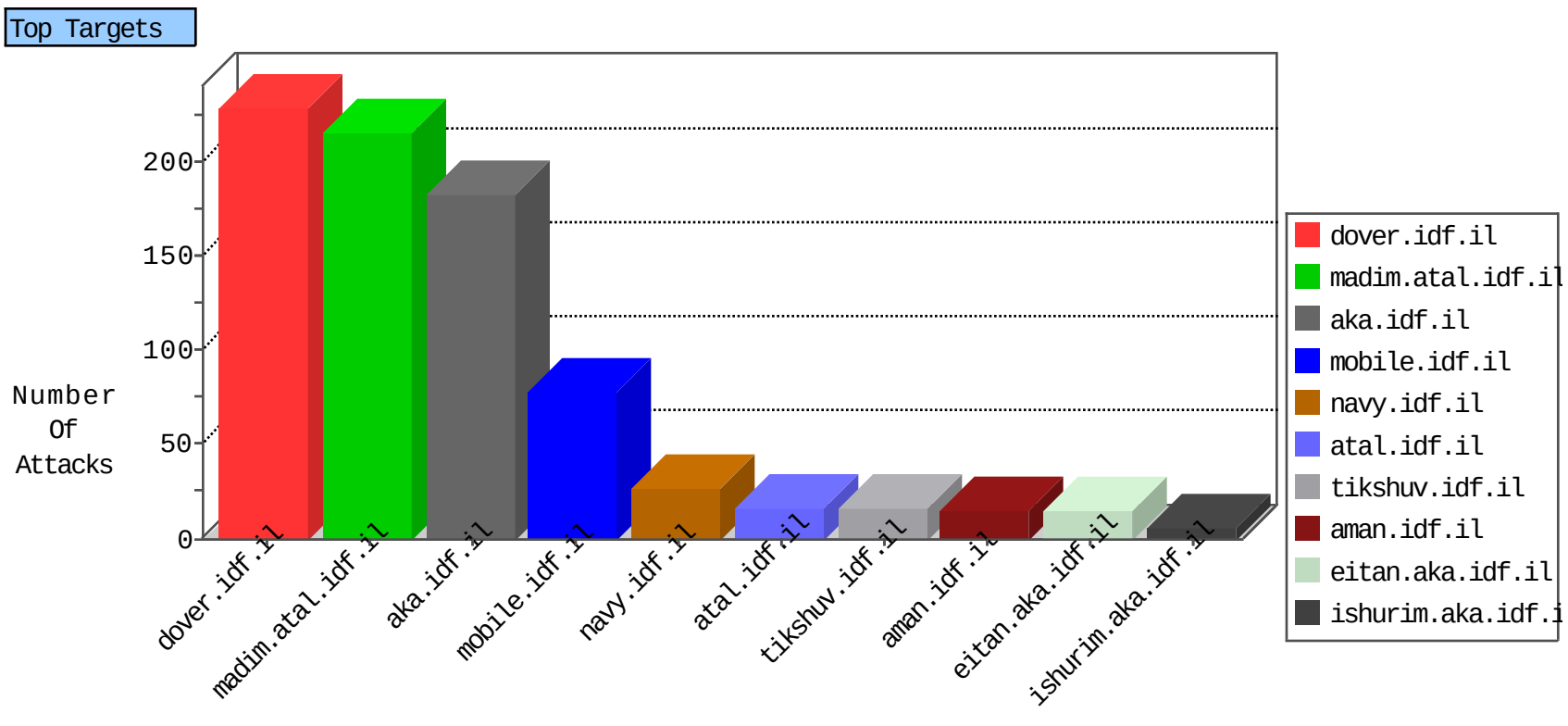
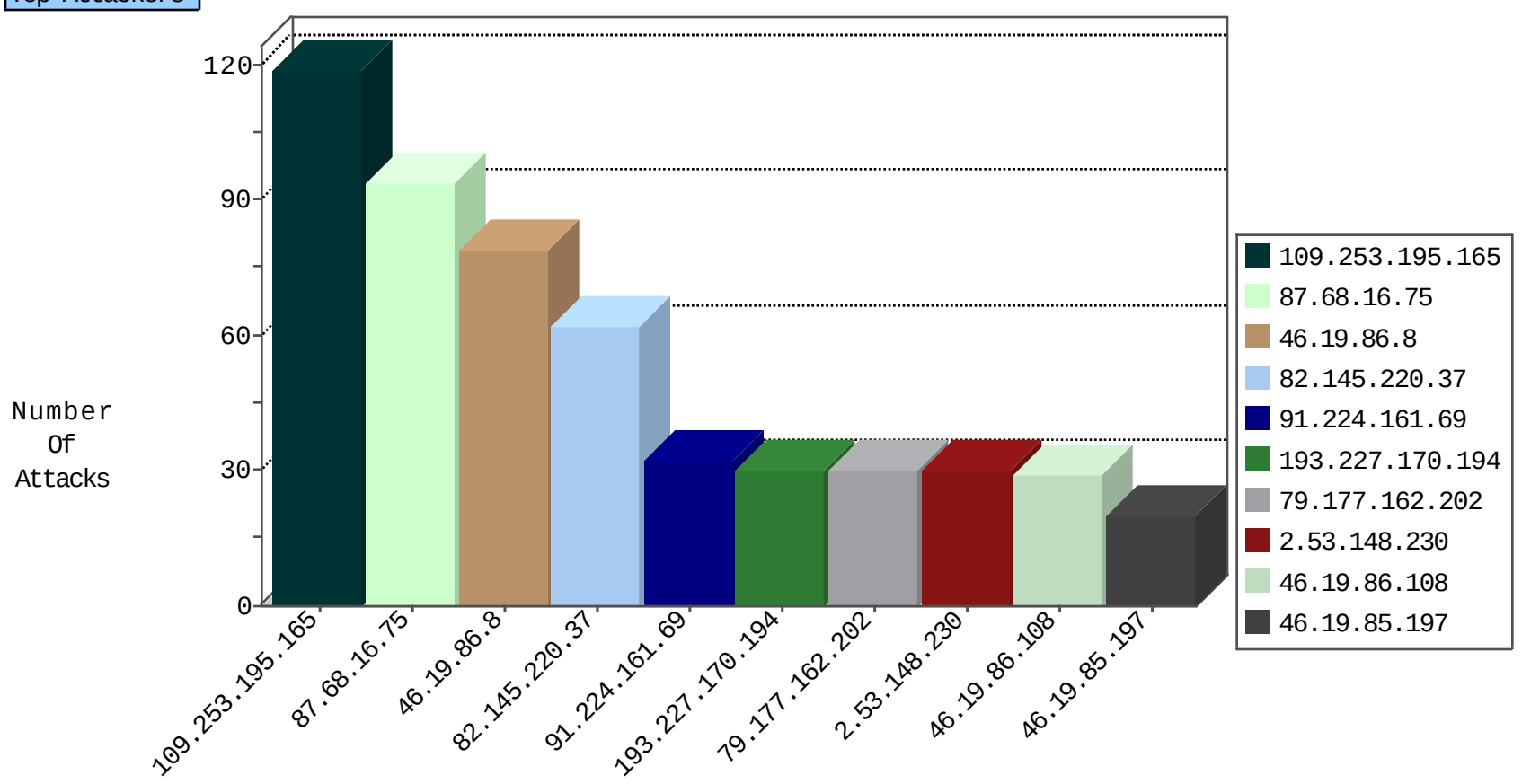
09-17-2016-15:04:09 to 09-17-2016-16:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-17-2016-15:04:09 to 09-17-2016-16:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
216.48.80.12	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
109.123.125.156	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
109.123.125.157	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
176.67.161.245	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
141.22.213.35	Germany	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
109.123.125.158	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
91.224.161.69	Netherlands	147.237.8.14	e.orchot.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
123.59.59.52	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	1
193.227.170.194	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-17-2016-15:04:09 to 09-17-2016-16:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-17-2016-15:04:09 to 09-17-2016-16:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.224.161.69	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	2
91.224.161.69	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
91.224.161.69	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
91.224.161.69	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	2
91.224.161.69	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	2
91.224.161.69	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	2
91.224.161.69	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	2
91.224.161.69	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.3.23.130	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.224.161.69	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
45.55.6.174	147.237.76.200	United States	eitan.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

09-17-2016-15:04:09 to 09-17-2016-16:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.145.220.37	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
2.53.148.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.177.162.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
193.227.170.194	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
188.120.154.81	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.86.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
84.109.228.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.229.13.254	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
87.71.6.166	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
196.100.132.57	Kenya	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.100.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.53.188.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.138.173.217	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.69	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
100.92.113.255		147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	4
185.3.147.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.138.114.117	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
66.249.93.137	Europe	147.237.0.34	tikshuv.idf.il	Directory Traversal	directory traversal overflow	monitor	3
46.19.85.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.246.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
77.125.66.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.93.129	Europe	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.179	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
66.249.93.133	Europe	147.237.0.34	tikshuv.idf.il	Directory Traversal	directory traversal overflow	monitor	3
46.19.86.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
188.120.148.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.108.46.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.125.66.197	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
109.253.192.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.40	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
77.125.66.197	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
109.64.82.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.64.230.174	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
66.102.8.157	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.221.188	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.40	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.134.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
5.102.242.58	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.102.8.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.15.251	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.177.100.94	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
46.19.85.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.93.135	Europe	147.237.0.34	tikshuv.idf.il	Directory Traversal	directory traversal overflow	monitor	2
176.13.246.14	Israel	147.237.77.216	dover.idf.il	SYN Attack		monitor	2

09-17-2016-15:04:09 to 09-17-2016-16:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.195.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	119
87.68.16.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.68.16.75	Block	93
46.19.86.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
109.253.156.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.64.28.57	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
79.182.118.81	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
77.138.194.135	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniot.aspx	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
176.24.111.208	United Kingdom	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
23.227.179.178	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name ©1K¯€•%ï[[#18]][[#25]]×4	Block	1
84.110.179.206	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
46.19.85.3	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/defapx	Block	1
77.139.123.234	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.124	Block	1
23.227.179.178	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
84.229.49.101	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
79.178.252.215	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/family	Block	1
23.227.179.178	United States	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 4	Block	1
77.138.8.23	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
109.253.231.129	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
2.53.32.206	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.93.135	Israel	147.237.0.34	tikshuv.idf.il	Distributed URL is Above Root Directory	Block	1
23.227.179.178	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 23.227.179.178	Block	1
77.138.45.57	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.64.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
120.22.18.160	Australia	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
5.22.134.241	Israel	147.237.72.166	aka.idf.il	Unknown Parameter https://www.aka.idf.il/main/giyus/docId in www.aka.idf.il/main/giyus/general.aspx	None	1
84.109.228.174	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sip_storage/files/	Block	1
68.180.228.159	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1930-he/cogat.aspx	Block	1
45.55.6.174	United States	147.237.76.200	eitan.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.64.81.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius/general	Block	1

09-17-2016-15:04:09 to 09-17-2016-16:04:09