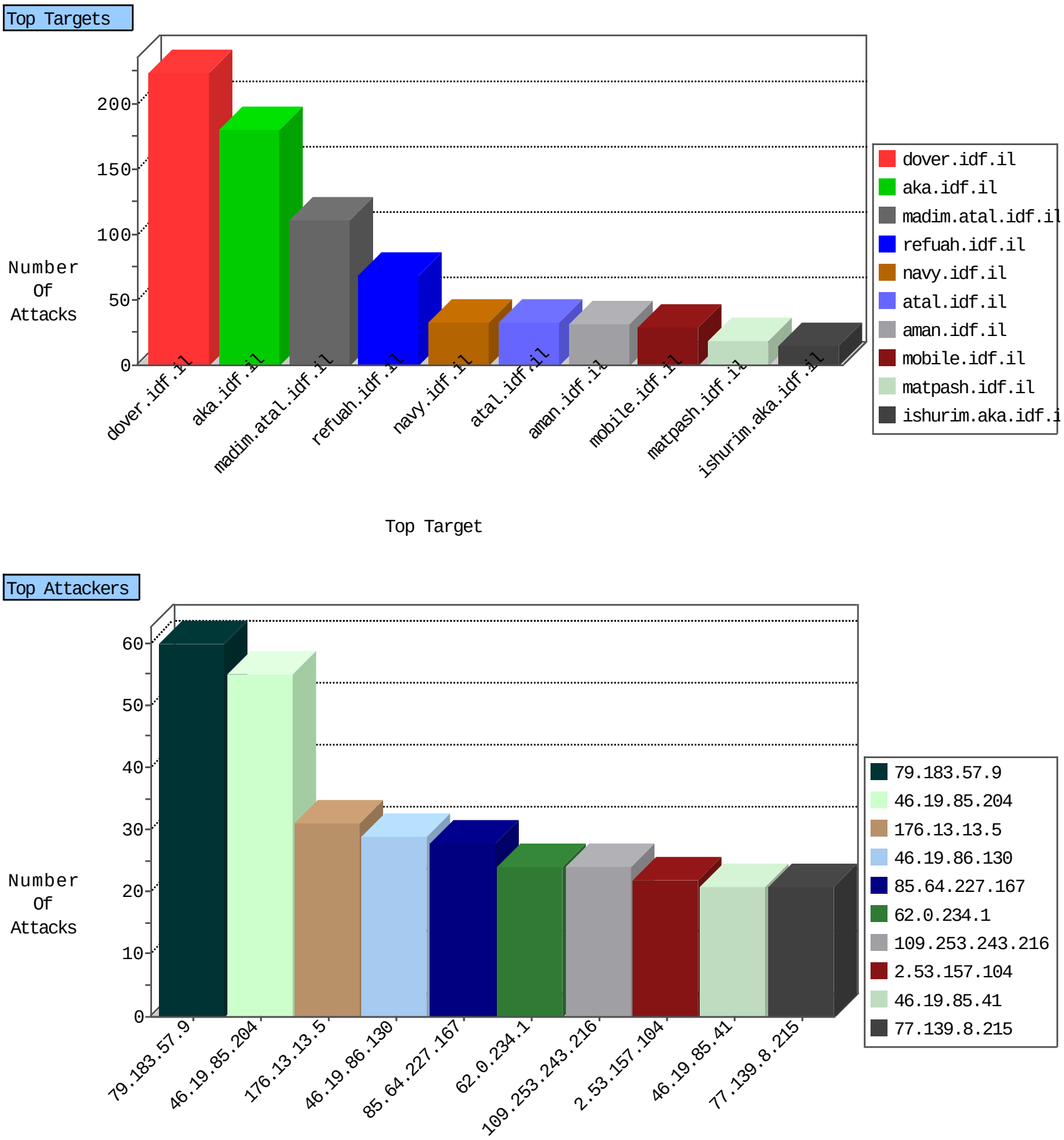
09-19-2016-08:04:09 to 09-19-2016-09:04:09

IDF Under Attack Daily Report



09-19-2016-08:04:09 to 09-19-2016-09:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.164.19	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
93.172.135.123	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
2.53.40.49	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
176.13.17.204	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.35	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
176.13.13.5	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
46.121.112.167	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
222.186.50.142	China	147.237.0.34	tikshuv.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
134.117.226.180	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.212.113.178	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-19-2016-08:04:09 to 09-19-2016-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-19-2016-08:04:09 to 09-19-2016-09:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
42.60.245.132	147.237.8.14	Singapore	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
222.186.56.179	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.143.227.35	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN NMAP -sS window 3072	1
42.60.245.132	147.237.8.45	Singapore	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
42.60.245.132	147.237.0.34	Singapore	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
93.172.135.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.237.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
54.82.204.124	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
222.254.34.165	147.237.77.176	Vietnam	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
49.144.120.199	147.237.76.200	Philippines	eitan.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.143.227.35	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN NMAP -sS window 4096	1
42.60.245.132	147.237.8.50	Singapore	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.37.148.18	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
109.67.190.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
42.60.245.132	147.237.0.17	Singapore	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
81.218.226.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.91.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.15.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.6	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
54.82.204.124	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

09-19-2016-08:04:09 to 09-19-2016-09:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.57.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
85.64.227.167	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
62.0.234.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
77.139.8.215	France	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
46.19.85.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
82.81.142.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
80.246.136.134	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	16
109.253.158.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
46.19.86.130	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.116	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
79.183.57.9	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
79.183.57.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
37.46.38.180	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.243.150.194	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.85.204	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
62.0.225.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.130	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
46.19.86.130	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.253.146.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.98.189	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	6
24.6.190.73	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
78.93.44.206	Saudi Arabia	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
93.143.31.158	Croatia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
24.6.190.73	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
78.93.44.206	Saudi Arabia	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
24.6.190.73	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.97	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.204	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.55.48.24	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.200.205.22	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
42.60.245.132	Singapore	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	4
2.53.56.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.183.57.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	3
176.13.0.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.6	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.204	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.204	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
62.0.224.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2

09-19-2016-08:04:09 to 09-19-2016-09:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.13.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.253.243.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
2.53.157.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
176.13.2.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
109.253.131.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
185.27.106.29	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
109.253.139.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.191	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
2.53.142.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.140.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.209	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
213.57.80.87	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.86.33	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.53.58.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.64.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/library/generaldoc.asp	Block	1
93.172.148.107	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
213.57.70.6	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/rights/asp/news.asp	Block	1
176.195.108.174	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
109.160.255.82	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	1
109.253.245.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
2.55.31.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/6782.jpg	Block	1
46.19.86.97	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.19.86.97	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/home/def...78&catid=38978	Block	1
85.64.227.167	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.138.68.125	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/kamlar/home/default.asp	Block	1
194.242.175.3	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
27.145.42.31	Thailand	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
91.199.69.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/forms	Block	1
80.246.139.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
195.200.205.2	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1
37.46.38.180	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
109.253.146.31	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

09-19-2016-08:04:09 to 09-19-2016-09:04:09