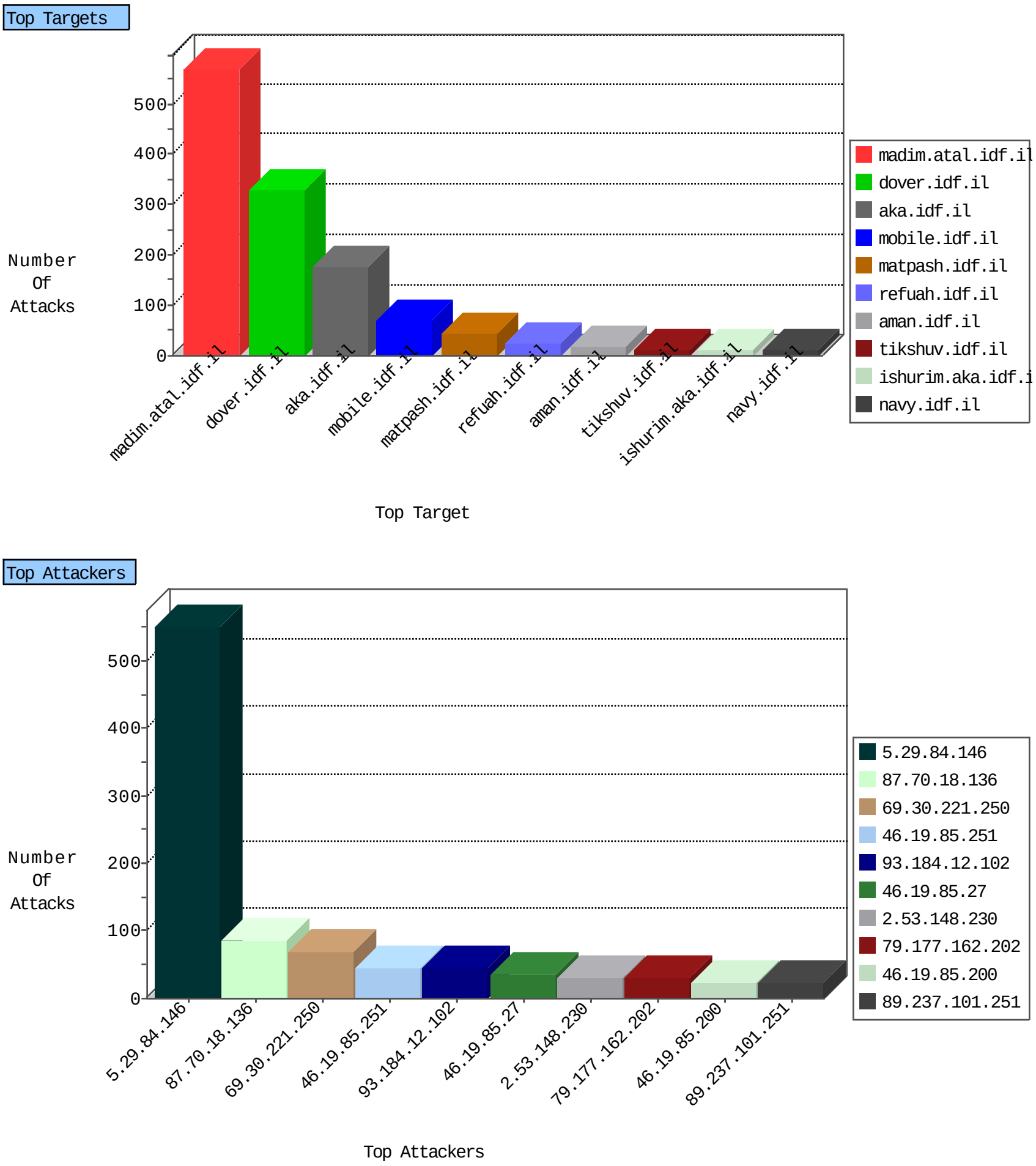
09-17-2016-19:04:04 to 09-17-2016-20:04:04

IDF Under Attack Daily Report



09-17-2016-19:04:04 to 09-17-2016-20:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	9
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.221	United States	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
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.35	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.35	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-17-2016-19:04:04 to 09-17-2016-20:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.221.250	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	49
69.30.221.250	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	14
178.32.203.32	Poland	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	8
69.30.221.250	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.221.250	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.221.250	United States	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-17-2016-19:04:04 to 09-17-2016-20:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.99.218.218	147.237.76.147	Brazil	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
177.99.218.218	147.237.76.147	Brazil	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
121.12.233.254	147.237.77.179	China	e.mazi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.60.153.178	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.46	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.35.65	147.237.77.170	Israel	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
218.17.117.22	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
31.24.228.20	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
209.89.37.88	147.237.72.167	Canada	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
202.155.58.28	147.237.0.19	Indonesia	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
177.99.218.218	147.237.76.147	Brazil	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
139.162.13.205	147.237.76.42	Singapore	refuah.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
109.60.153.178	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
95.181.183.108	147.237.77.216	Russian Federation	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	1
93.174.93.46	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
41.180.9.40	147.237.76.31	South Africa	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
209.89.37.88	147.237.72.167	Canada	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
209.89.37.88	147.237.72.167	Canada	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1

09-17-2016-19:04:04 to 09-17-2016-20:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.70.18.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
93.184.12.102	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
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
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
46.117.245.122	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.27	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
89.237.101.251	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
89.237.101.251	France	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
80.246.133.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
46.19.85.27	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
93.172.140.117	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.27	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
79.176.140.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.130.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.86.133	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.27	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
79.183.25.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.131.47	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
66.249.65.44	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.237.101.251	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
93.184.12.102	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
87.69.79.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.53.131.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
77.126.12.31	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.53.131.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.116.45.226	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
84.229.8.167	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
141.0.15.127	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
95.35.140.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
176.13.6.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.180.74	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	3
2.53.21.100	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
77.126.12.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.102.195.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
187.159.239.203	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.102.195.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.177.221.152	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	2
176.13.234.128	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
188.120.154.227	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.62.8	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.138.98.162	France	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
87.69.225.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.108.73.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
40.85.132.92	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-17-2016-19:04:04 to 09-17-2016-20:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.84.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	547
46.19.85.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.53.48.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
5.29.84.146	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	3
176.13.242.232	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	2
109.65.14.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.138.164.24	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/faq.aspx	Block	2
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	2
77.139.208.184	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan/main/main.asp	Block	1
46.120.147.79	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
157.55.39.75	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/size220x0/sip_storage	Block	1
80.246.133.177	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
77.138.108.157	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/chinuch/klali/default.asp	Block	1
5.102.254.6	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
104.131.94.218	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
79.177.83.186	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.64.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
87.68.30.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.164.24	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.164.24	Block	1
37.26.147.213	Israel	147.237.76.42	refuah.idf.il	URL is Above Root Directory www.refua.atal.idf.il/../images/shared/mailthisclose.png	Block	1
79.181.20.168	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.181.20.168	Block	1
66.249.66.101	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
201.141.227.204	Mexico	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
87.71.53.168	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
114.98.244.254	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1038-he/idfg.aspx/trackback/	Block	1
79.181.20.168	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/ain/giyus	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
93.172.222.35	Israel	147.237.0.19	madim.atal.idf.il	Multiple Untraceable SSL Sessions from 93.172.222.35 (Open Mode)	None	1
77.139.171.158	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
80.246.130.86	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.228.251	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
93.172.222.35	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1

09-17-2016-19:04:04 to 09-17-2016-20:04:04