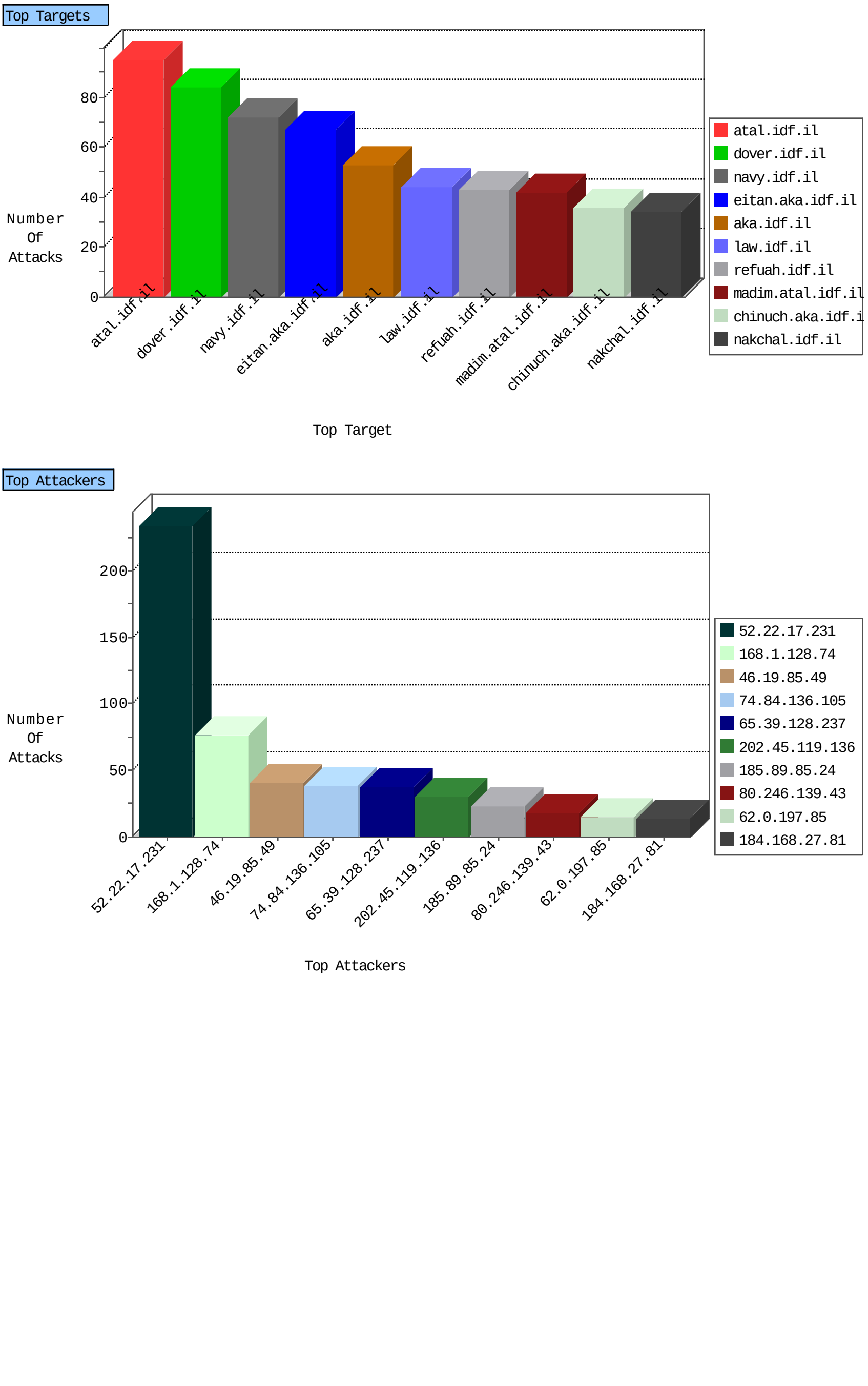
09-09-2016-08:04:09 to 09-09-2016-09:04:09

IDF Under Attack Daily Report



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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.135.131	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
109.65.4.192	Israel	147.237.76.31	nakchal.idf.il	Black List	drop	1
118.193.166.115	China	147.237.77.19	law-forum.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
24.86.161.214	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
65.39.128.237	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
65.39.128.237	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.27.81	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
65.39.128.237	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
64.34.186.9	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
74.84.136.105	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
192.99.167.90	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
74.84.136.105	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
74.84.136.105	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	2
198.20.69.74	United States	147.237.77.61	e.cogat.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

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

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
74.84.136.105	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	32
65.39.128.237	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
184.168.27.81	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
24.86.161.214	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	8
62.210.97.57	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.224.160.106	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
79.176.146.82	147.237.76.200	Israel	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
203.81.155.115	147.237.77.205	Korea, Republic of	prisha.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.69.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
163.172.129.15	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
150.242.238.99	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.168	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
150.242.238.99	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
93.174.94.142	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.49	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
52.22.17.231	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
52.22.17.231	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
52.22.17.231	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
52.22.17.231	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
52.22.17.231	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
52.22.17.231	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
52.22.17.231	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
52.22.17.231	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
185.89.85.24	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
80.246.139.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
62.0.197.85	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
66.249.69.81	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
141.226.218.22	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.69.85	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
209.208.126.125	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
176.13.239.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
212.179.140.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
202.45.119.136	Australia	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	6
62.0.251.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
202.45.119.136	Australia	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
202.45.119.136	Australia	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
49.32.64.227	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
202.45.119.136	Australia	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.182.63.248	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
5.117.254.78	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.253.157.88	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
84.111.115.169	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
202.45.119.136	Australia	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	4
5.117.254.78	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.49	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
168.1.128.74	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
168.1.128.74	United States	147.237.77.74	law.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
168.1.128.74	United States	147.237.77.233	atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
202.45.119.136	Australia	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
46.19.85.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.249.69.89	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.157.88	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
168.1.128.74	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
168.1.128.74	United States	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
109.67.98.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
202.45.119.136	Australia	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.32.179.90	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.237.133	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
185.32.179.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.250.92	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
168.1.128.74	United States	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
168.1.128.74	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
168.1.128.74	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.137.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.49	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	5
66.249.66.232	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.232	Block	2
109.64.181.224	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	2
77.138.191.81	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	2
168.1.128.74	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to /	Block	1
77.139.80.115	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
5.22.134.165	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
168.1.128.74	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
66.249.66.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/apple-app-site-association	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
212.179.140.133	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
66.249.66.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter WT.mc_id in www.aka.idf.il/ishurim/main	None	1
66.249.69.81	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
168.1.128.74	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to /	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/chamatz/gallery/showpicture.asp	Block	1
2.53.141.50	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Untraceable SSL Sessions from 2.53.141.50 (Open Mode)	None	1

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