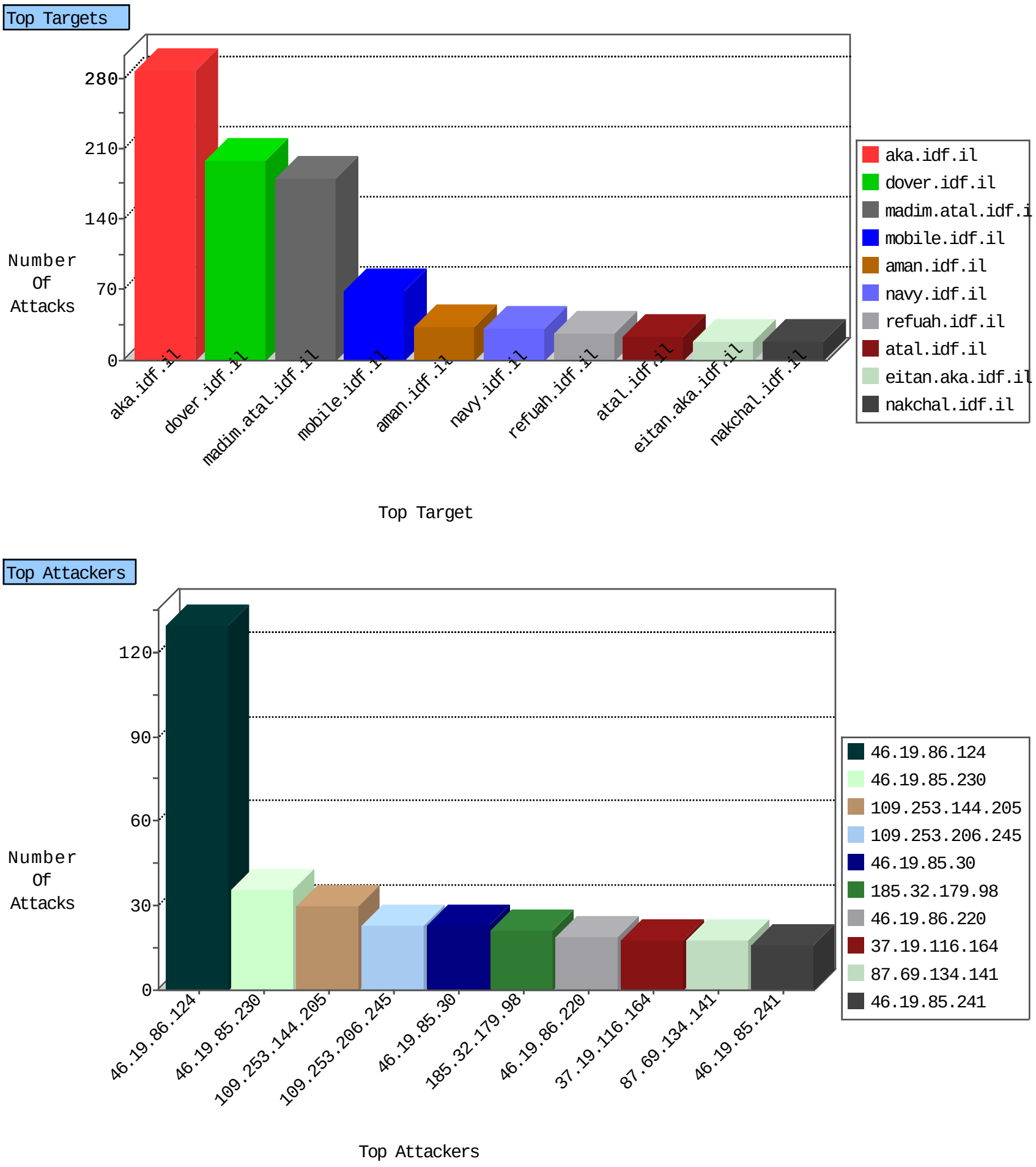
09-14-2016-20:04:05 to 09-14-2016-21:04:05

IDF Under Attack Daily Report



09-14-2016-20:04:05 to 09-14-2016-21:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.4.48	Israel	147.237.77.216	dover.idf.il	Black List	drop	8
68.0.200.128	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
109.66.4.48	Israel	147.237.77.226	www.chamatz.aka.idf.il	Black List	drop	5
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
143.85.70.18	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
129.97.74.12	Canada	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	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
94.76.8.228	Bahrain	147.237.0.35	akaws.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
217.132.115.154	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.99	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.198	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.11	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
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
94.76.8.228	Bahrain	147.237.0.17	m.my-kosher-kravi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-14-2016-20:04:05 to 09-14-2016-21:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.32.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
220.181.124.109	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-14-2016-20:04:05 to 09-14-2016-21:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.76.8.228	147.237.0.16	Bahrain	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	3
180.97.106.37	147.237.76.177	China	ncore.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
142.4.108.129	147.237.0.33	United States	idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
116.71.128.85	147.237.76.200	Pakistan	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.8.228	147.237.0.17	Bahrain	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.32.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
189.161.173.106	147.237.0.19	Mexico	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
23.91.75.231	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.103.198.32	147.237.0.200	Turkey	m4u.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.0.17	China	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
163.172.129.15	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
118.103.142.140	147.237.76.200	Bhutan	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
116.71.128.85	147.237.76.196	Pakistan	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.8.228	147.237.0.35	Bahrain	akaws.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
46.227.67.158	147.237.77.74	Sweden	law.idf.il	ET SCAN NMAP -sS window 1024	1
185.103.198.32	147.237.77.216	Turkey	dover.idf.il	ET SCAN Potential SSH Scan	1
185.103.198.32	147.237.0.34	Turkey	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

09-14-2016-20:04:05 to 09-14-2016-21:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.253.144.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.30	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
87.69.134.141	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.85.230	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
84.108.62.154	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
185.32.179.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
196.145.152.231	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.32.179.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
37.26.148.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.241	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.19.116.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	9
37.19.116.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
185.120.126.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.121.136.82	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
87.69.32.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
87.69.32.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
68.0.200.128	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.146.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.206.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
143.85.70.18	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.180.152.86	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
87.69.52.217	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
66.249.75.179	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.7.206	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.230	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
207.46.13.115	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.207	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.86.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.207	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.178.30.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.149.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.206.245	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
109.253.206.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.206.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
5.102.195.172	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
77.125.3.222	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
37.26.146.134	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.58	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.181.58.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.182.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.146.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

09-14-2016-20:04:05 to 09-14-2016-21:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	130
109.253.213.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
77.139.154.161	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	10
79.176.109.162	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	8
77.139.64.144	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.64.144	Block	7
31.154.81.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.67.24.64	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	6
109.67.24.64	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	4
36.37.170.126	Cambodia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	4
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	3
46.19.86.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.81.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
94.230.92.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.185.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.250.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.210	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.181.165.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.206.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.138.96.4	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugtafkidim.aspx	Block	2
46.19.85.241	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
207.46.13.136	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/maslulim/leftarrowdisabled.gif	Block	1
197.32.136.143	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	1
85.65.0.213	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
77.138.241.243	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
189.218.121.121	Mexico	147.237.72.166	aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
46.19.86.242	Israel	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method 32q0vjotya45 in URL	Block	1
104.58.22.154	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/kiosk	Block	1
201.173.80.85	Mexico	147.237.76.42	refuah.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
31.13.100.115	Ireland	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/ במי דה ולא תדרג את השאלון לא תזומן למיונים ותשובץ על-פי צרכי הצבא. בהצל חה	Block	1
189.219.94.87	Mexico	147.237.77.234	halag.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
187.185.113.44	Mexico	147.237.72.156	aman.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
46.19.86.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.117.154.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus	Block	1
31.210.186.176	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/ishurim/exampcert/	Block	1
201.166.236.191	Mexico	147.237.76.147	chinuch.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
85.65.98.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
189.218.121.121	Mexico	147.237.72.167	ishurim.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
177.239.62.96	Mexico	147.237.76.200	eitan.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
46.116.57.32	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/guyus	Block	1
109.65.129.60	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
40.77.167.64	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/66414.jpg	Block	1
201.173.178.227	Mexico	147.237.77.235	sviva.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
31.13.100.117	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/ במידה ולא תדרג את השאלון לא תזומן למיונים ותשובץ על-פי צרכי הצבא. בהצלחה	Block	1
189.219.159.202	Mexico	147.237.76.39	mobile.meitav.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
79.183.13.39	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatus in www.aka.idf.il/main/sachar/payslips.aspx	None	1
189.214.64.247	Mexico	147.237.76.30	himush.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
212.199.95.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.250.98.46	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1

09-14-2016-20:04:05 to 09-14-2016-21:04:05