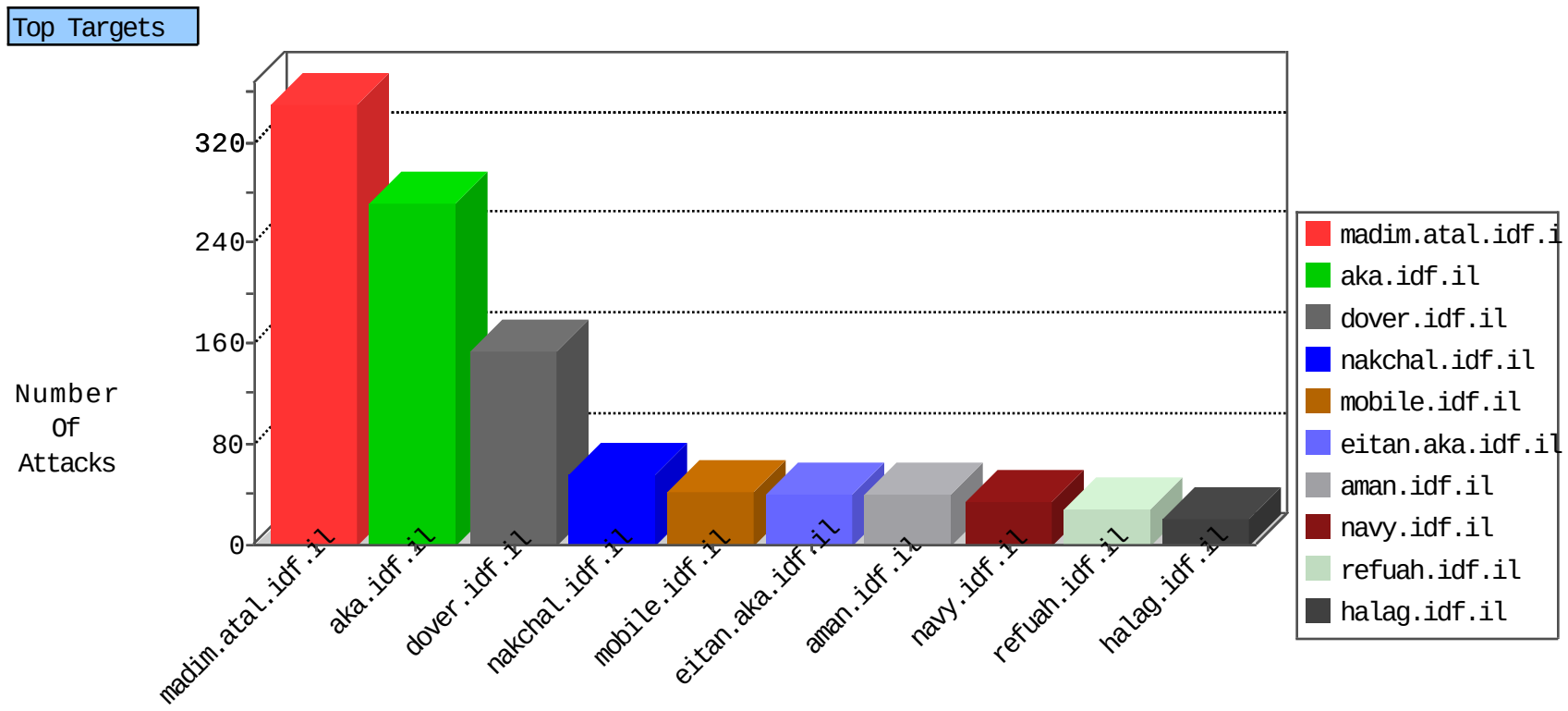
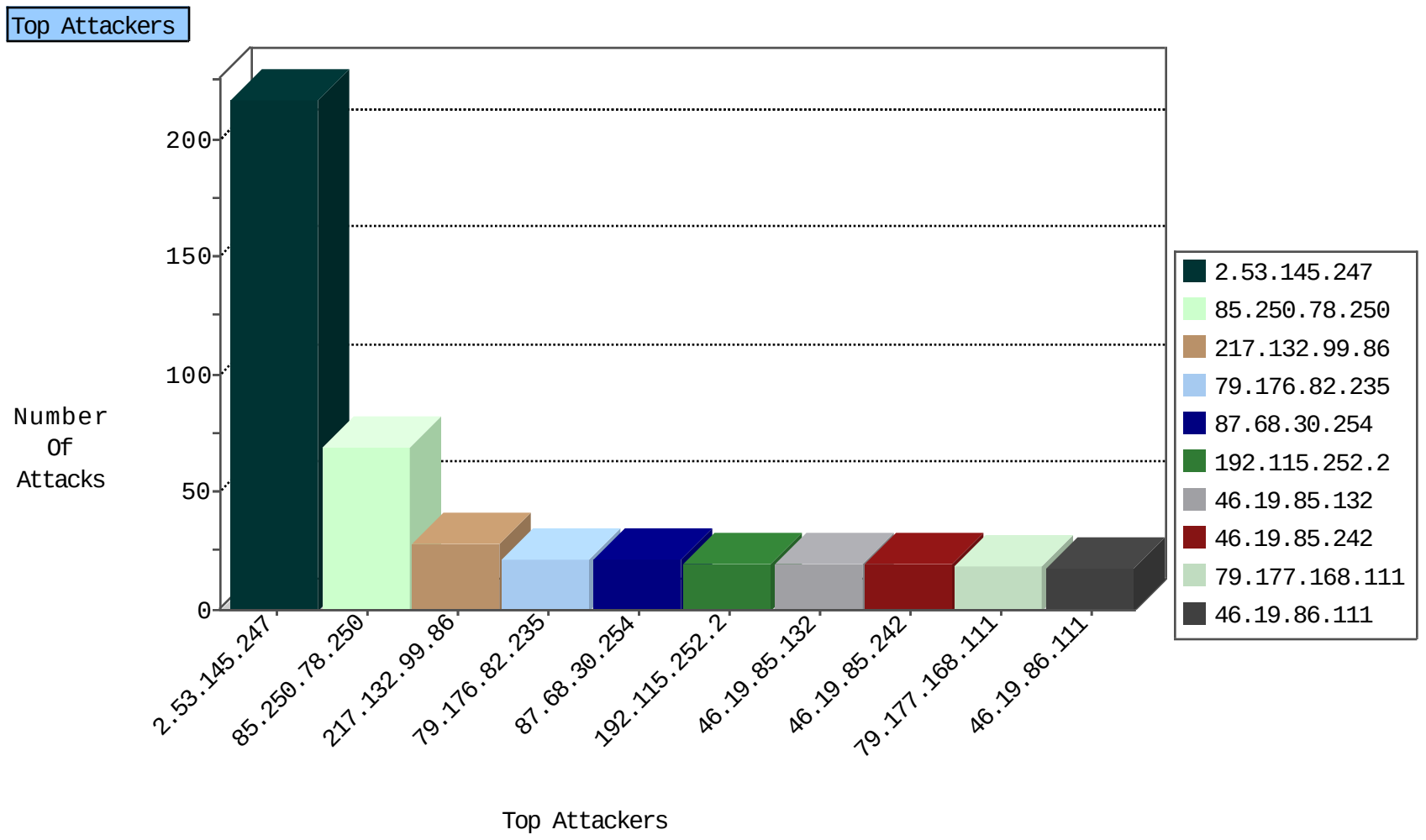
09-14-2016-17:04:01 to 09-14-2016-18:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-14-2016-17:04:01 to 09-14-2016-18:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.184.36	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	45
79.176.82.235	Israel	147.237.72.166	aka.idf.il	Black List	drop	21
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
141.22.213.34	Germany	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	2
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.221	United States	147.237.72.167	ishurim.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
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.254.215.12	France	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
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
41.35.16.58	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
204.85.191.11	United States	147.237.72.166	aka.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
129.93.229.138	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
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.217	e.idf.il	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

09-14-2016-17:04:01 to 09-14-2016-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
108.59.8.70	United States	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	1
109.236.90.209	Netherlands	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-14-2016-17:04:01 to 09-14-2016-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.53.5.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 2048	1
217.70.19.83	147.237.76.147	Russian Federation	chinuch.aka.idf.il	Tehila - Perl LWP with fake user agent	1
190.255.246.198	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.129.15	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
112.217.150.112	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
79.182.61.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
52.166.130.115	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.41.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 4096	1
220.231.195.122	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -f -sS	1
194.90.116.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
179.43.141.198	147.237.0.16	Switzerland	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
112.217.150.112	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
79.181.194.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
52.166.130.115	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1

09-14-2016-17:04:01 to 09-14-2016-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
87.68.30.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
79.177.168.111	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
50.24.30.72	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.225	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.242	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.242	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.10	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.10	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
176.13.7.88	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
109.67.129.56	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
112.210.52.158	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.182.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.138	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
77.127.23.111	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
176.13.231.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
81.218.66.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.61.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.43.114.244	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.149	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.111	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.5.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.111	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.146.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
46.19.86.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
176.13.231.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
109.186.75.173	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
79.180.100.177	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.93.24	Israel	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
217.132.121.190	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
50.252.152.33	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.134.252	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	4
31.154.49.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.192.197	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.172.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.129.56	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.35.26.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
84.109.160.151	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.235	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
176.13.231.158	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
37.26.149.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.129.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
98.231.98.228	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3

09-14-2016-17:04:01 to 09-14-2016-18:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.145.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	217
85.250.78.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
185.32.179.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
109.253.201.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
192.115.252.2	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	10
192.115.252.2	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 192.115.252.2	Block	9
46.121.115.171	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.115.171	Block	9
85.250.247.60	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7
82.81.97.250	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	6
176.13.238.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.3.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
31.168.89.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane/	Block	6
46.117.95.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.61.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.61.57	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
46.19.86.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.129.60	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.65.129.60	Block	2
2.53.63.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.242.233	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
77.138.128.113	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
87.69.199.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.122.184	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
77.138.200.10	France	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	2
2.53.153.245	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 2.53.153.245	Block	1
207.46.13.168	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
79.180.96.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
68.180.228.228	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane	Block	1
176.13.228.148	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
109.67.25.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
84.108.214.127	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/home.aspx	Block	1
37.26.148.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.125.16	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$hiddenUpdateQuestion in www.aka.idf.il/main/giyus/faq.aspx	None	1
147.235.236.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/	Block	1
109.65.26.124	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
2.53.172.154	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
80.246.130.84	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
77.127.23.111	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.231.18	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.67.129.56	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	1
37.26.149.235	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.177.168.111	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.30	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
2.55.171.247	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
77.138.47.201	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
109.67.129.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-14-2016-17:04:01 to 09-14-2016-18:04:01