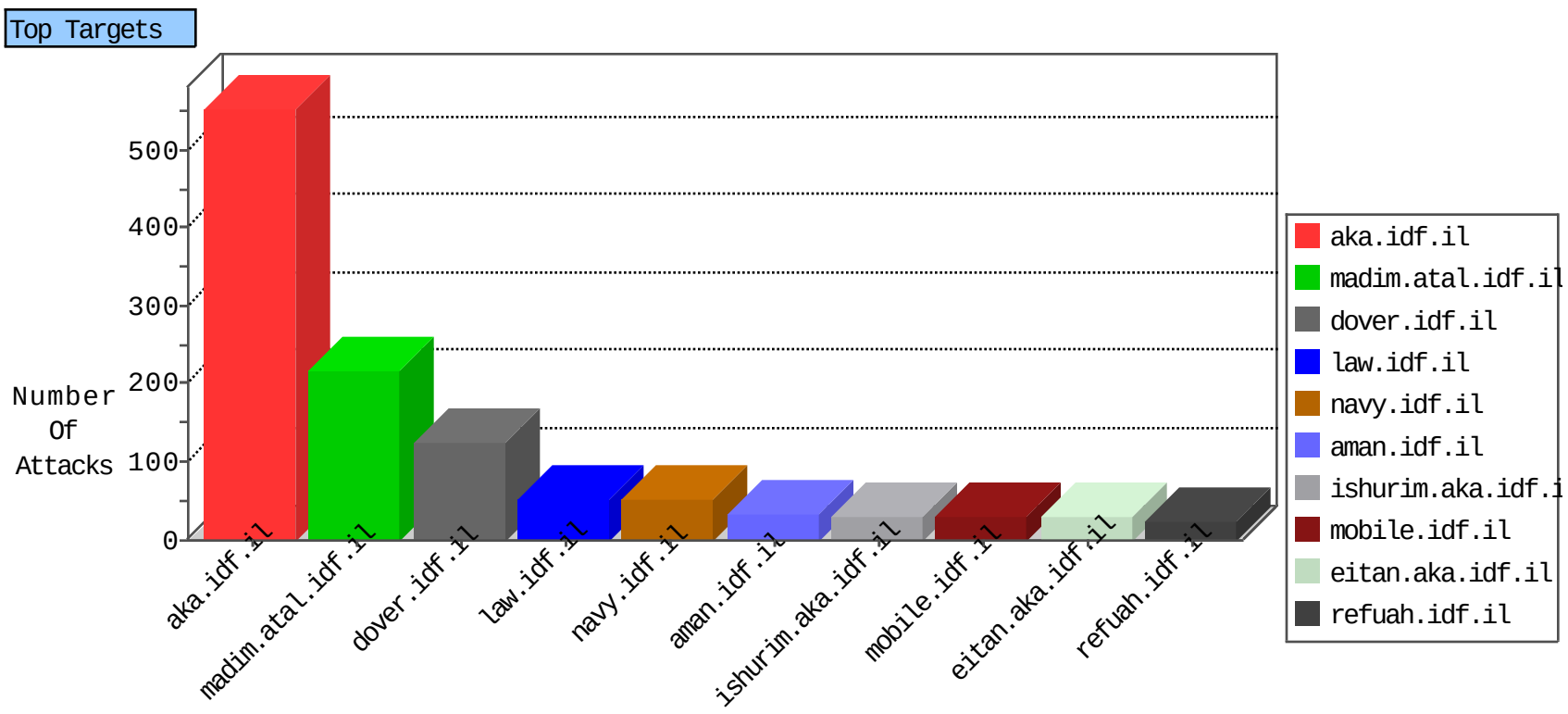
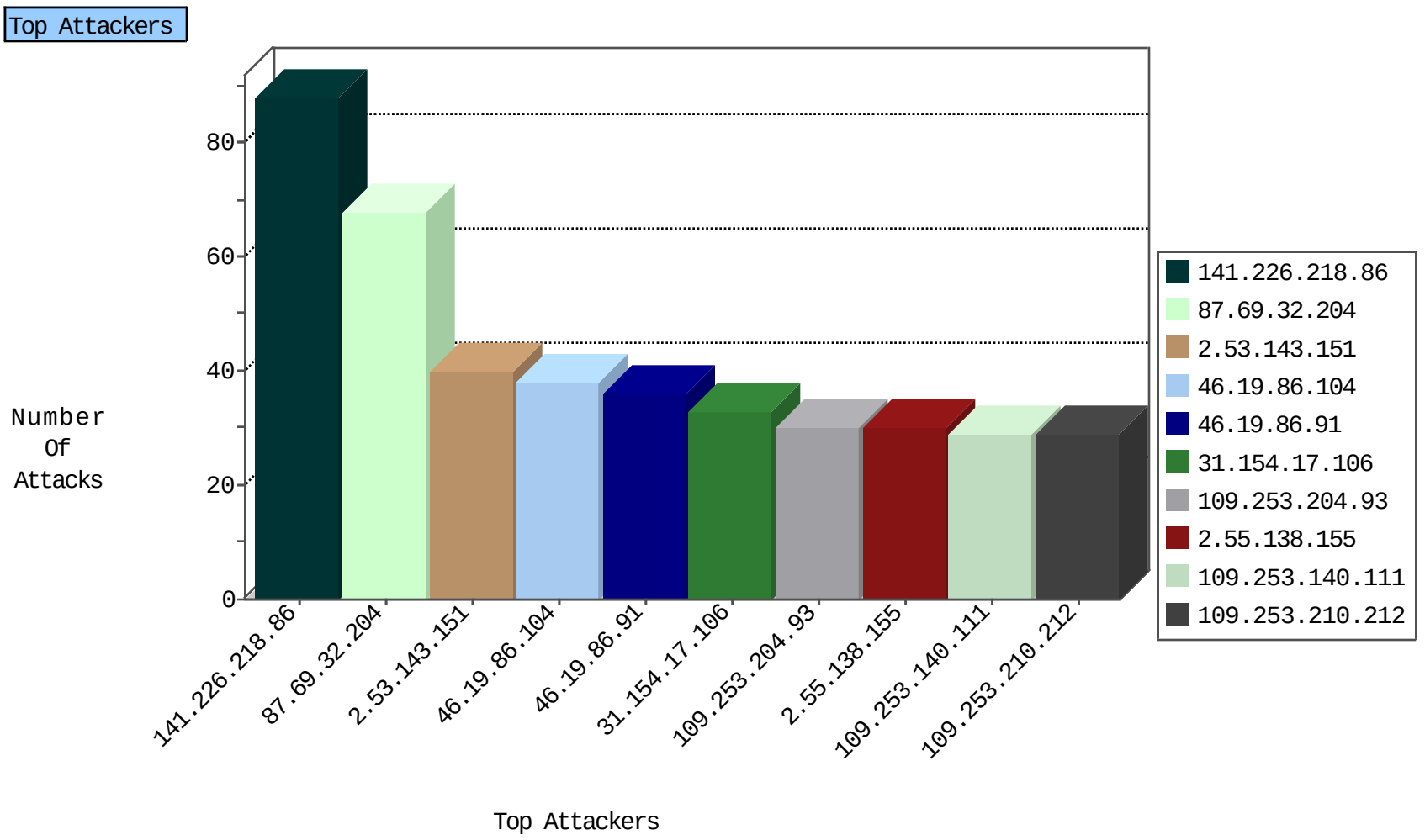
09-13-2016-19:04:09 to 09-13-2016-20:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-13-2016-19:04:09 to 09-13-2016-20:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.104.253	Israel	147.237.72.166	aka.idf.il	Black List	drop	6
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.167	ishurim.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
153.90.1.35	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-13-2016-19:04:09 to 09-13-2016-20:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
205.144.171.34	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
205.144.171.34	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
72.167.131.75	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
208.52.175.27	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.208.218.66	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.246.49.11	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
108.166.190.139	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
67.199.10.25	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
50.77.136.81	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
50.77.136.81	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
62.212.73.211	Netherlands	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-13-2016-19:04:09 to 09-13-2016-20:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
74.208.218.66	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	18
205.144.171.34	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
67.199.10.25	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	11
108.166.190.139	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
208.52.175.27	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
72.167.131.75	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	8
213.246.49.11	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	8
77.126.80.246	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
91.201.236.158	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
52.166.249.197	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
117.135.131.60	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.158	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
77.126.80.246	147.237.0.34	Israel	tikshuv.idf.il	Xenu Link Sleuth User Agent	1
66.249.76.97	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
163.172.129.15	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-13-2016-19:04:09 to 09-13-2016-20:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.69.32.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	35
2.53.143.151	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	35
87.69.32.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	33
31.154.17.106	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	33
109.253.204.93	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
212.76.108.46	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.86.91	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
109.253.213.28	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
80.246.139.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.86.91	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
109.253.197.113	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.91	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.253.211.182	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
176.13.229.113	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
176.13.230.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.136.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.178.54.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
85.130.136.66	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
85.130.206.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.130.206.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.86.18	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
87.71.24.162	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.85.39	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.130.242.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
77.239.224.35	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
85.130.242.146	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
109.65.162.56	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
85.130.242.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.226.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.206.214	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.138.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.219.208	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.177.186.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.19	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
84.94.223.204	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.161.147	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
109.65.17.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.13.251.80	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
178.199.147.77	Switzerland	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.204	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
85.64.14.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
85.130.136.66	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
85.64.14.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
31.13.166.218	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.115	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

09-13-2016-19:04:09 to 09-13-2016-20:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.226.218.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
2.55.138.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
109.253.140.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.253.210.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
68.100.45.173	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 68.100.45.173	Block	4
68.100.45.173	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	4
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	4
87.71.56.247	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
77.138.215.36	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	3
46.117.162.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.176.69.196	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.139.42.238	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.151.63.166	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.151.63.166	Block	2
173.26.144.152	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	2
87.68.53.33	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
77.127.70.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.63.166	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/pniotfindanswer.aspx	Block	1
139.162.13.205	Singapore	147.237.76.31	nakchal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.108.86.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.216.145	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
176.13.227.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.167.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.49.180	France	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
141.226.218.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
84.109.113.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
204.79.180.108	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/portalmiluim/templates/inner.asp	Block	1
46.19.86.255	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.65.147.86	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
80.246.133.51	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
85.64.63.128	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.178.54.7	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.54.7	Block	1
207.46.13.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/	Block	1
77.126.18.205	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.117.116.119	Israel	147.237.77.233	atal.idf.il	Unauthorized HTTP Method	Block	1
80.246.139.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.226.218.86	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	1
85.219.205.227	Poland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
5.29.103.4	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	1
79.178.54.7	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
77.126.80.246	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/main/	Block	1
46.117.116.119	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/1353-he/	Block	1
84.95.49.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.44.108	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
66.249.66.59	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
23.20.60.205	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
79.178.133.229	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-13-2016-19:04:09 to 09-13-2016-20:04:09