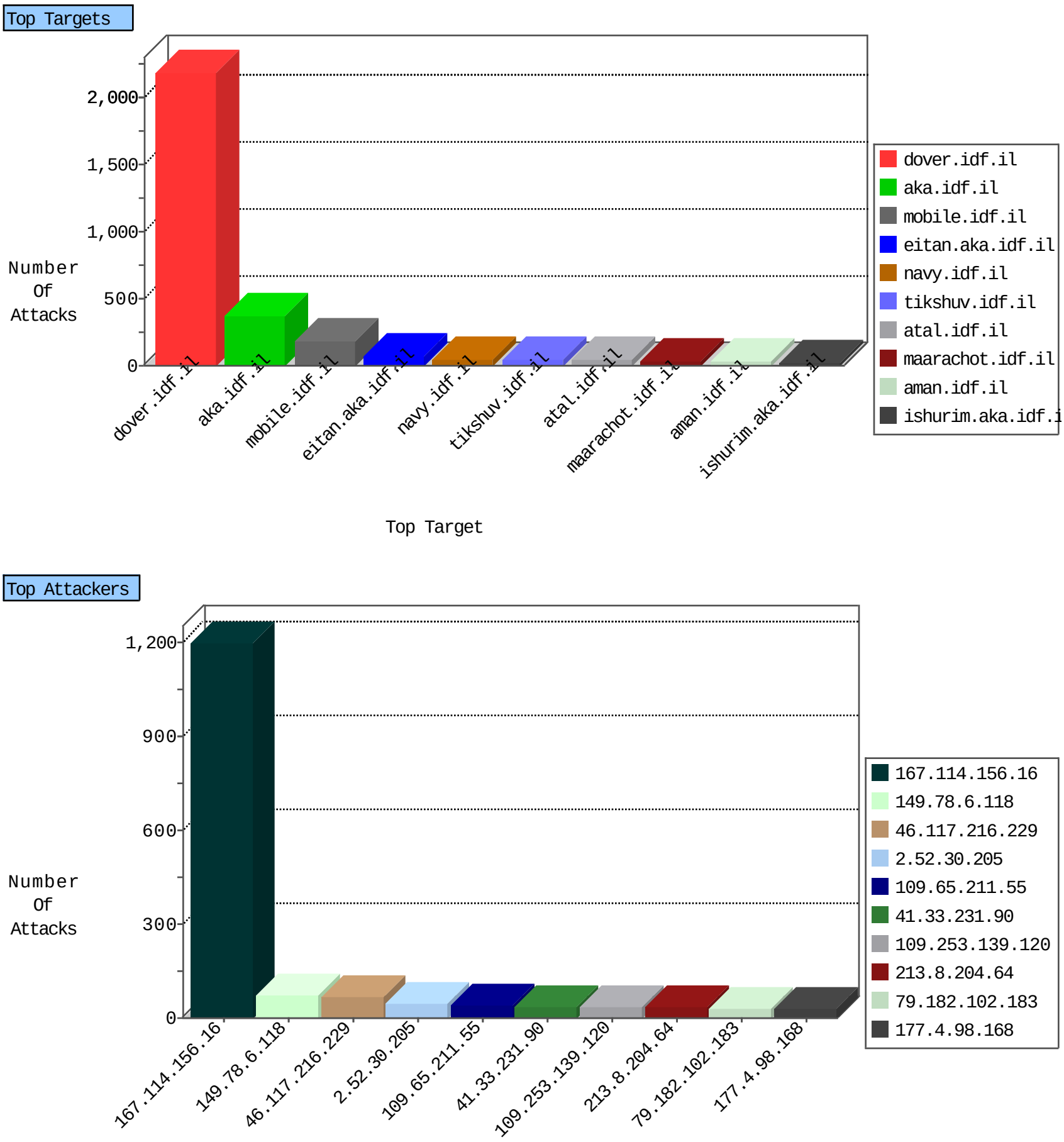
12-31-2015-19:04:09 to 12-31-2015-20:04:09

IDF Under Attack
Daily Report



12-31-2015-19:04:09 to 12-31-2015-20:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3261
2.54.171.50	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
205.197.242.187	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
64.233.172.171	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
106.75.199.192	China	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.37	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
119.138.17.207	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.37	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
123.151.42.61	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1

12-31-2015-19:04:09 to 12-31-2015-20:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.77.121	e.navy.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

12-31-2015-19:04:09 to 12-31-2015-20:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
109.67.216.104	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
46.117.216.229	147.237.77.216	Israel	dover.idf.il	SERVER-WEBAPP apache directory disclosure attempt	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.117.216.229	147.237.77.216	Israel	dover.idf.il	GPL WEB_SERVER apache directory disclosure attempt	2
79.181.130.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.129.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
141.255.166.37	147.237.0.15	Switzerland	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
79.176.36.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.0.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.77.121	United States	e.navy.idf.il	ET DROP Dshield Block Listed Source	1
31.11.79.220	147.237.0.200	Macedonia, the Former Yugoslav Republic of	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.129.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.198.216.130	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
2.54.154.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.218.176.152	147.237.76.34	Kazakstan	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.32.179.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.120.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
172.98.200.238	147.237.76.148		gqcenter.aka.idf.i	ET SCAN NMAP -sS window 4096	1
79.180.153.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.230.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.97.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
121.201.61.49	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
77.126.90.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.30.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 2048	1
212.199.57.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.68.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -f -sS	1
5.102.228.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.167.155	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
188.164.67.212	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.96.220	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.241.225.9	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

12-31-2015-19:04:09 to 12-31-2015-20:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.6.118	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	70
109.65.211.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.182.102.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
89.139.238.58	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
46.117.221.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
213.8.204.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
109.253.139.120	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
2.54.146.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.52.30.205	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
77.127.239.13	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
107.167.107.143	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
212.25.84.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
177.4.98.168	Brazil	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
105.196.15.229	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	13
105.196.15.229	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
46.19.85.134	Israel	147.237.77.216	dover.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	monitor	10
46.19.85.68	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
89.139.49.233	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
37.142.68.14	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
109.186.187.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
37.26.147.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.141.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.86.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.141.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
2.54.38.182	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.64.136.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
149.78.229.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
177.4.98.168	Brazil	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	7
37.46.39.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.30.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.226.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.199.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.126.85.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.117.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
101.164.228.136	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.30.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.130.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.30.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

12-31-2015-19:04:09 to 12-31-2015-20:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.216.229	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.117.216.229	Block	57
84.108.128.138	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.128.138	Block	18
213.8.204.15	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	12
109.253.139.120	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
213.8.204.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
37.26.148.173	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	5
109.66.111.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.181.36.220	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.181.36.220	Block	4
46.117.216.229	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	3
79.181.36.220	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
77.126.236.156	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/resource/userfollowresource/create/	Block	3
109.253.199.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.177.100.200	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/mas.aspx	Block	3
109.186.187.136	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.16.97	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
79.178.226.118	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
109.64.150.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.24.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.151.119	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	2
85.64.57.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
85.64.57.44	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
132.70.66.12	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 132.70.66.12	Block	2
79.177.177.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.64.136.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.178.0.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.117.205.102	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.117.205.102	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
84.108.152.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.187	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
109.64.116.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
85.130.244.119	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.104.58.65	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
61.135.190.71	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/shared/clientscripts/jquery/jquery-ui.js	Block	1
149.78.83.230	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.218.87.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.56.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.136.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.86.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
105.196.15.229	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
84.109.144.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
61.135.190.198	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/layout2.css	Block	1
176.12.138.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.13.99.97	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.166.170.3	Lithuania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1

12-31-2015-19:04:09 to 12-31-2015-20:04:09