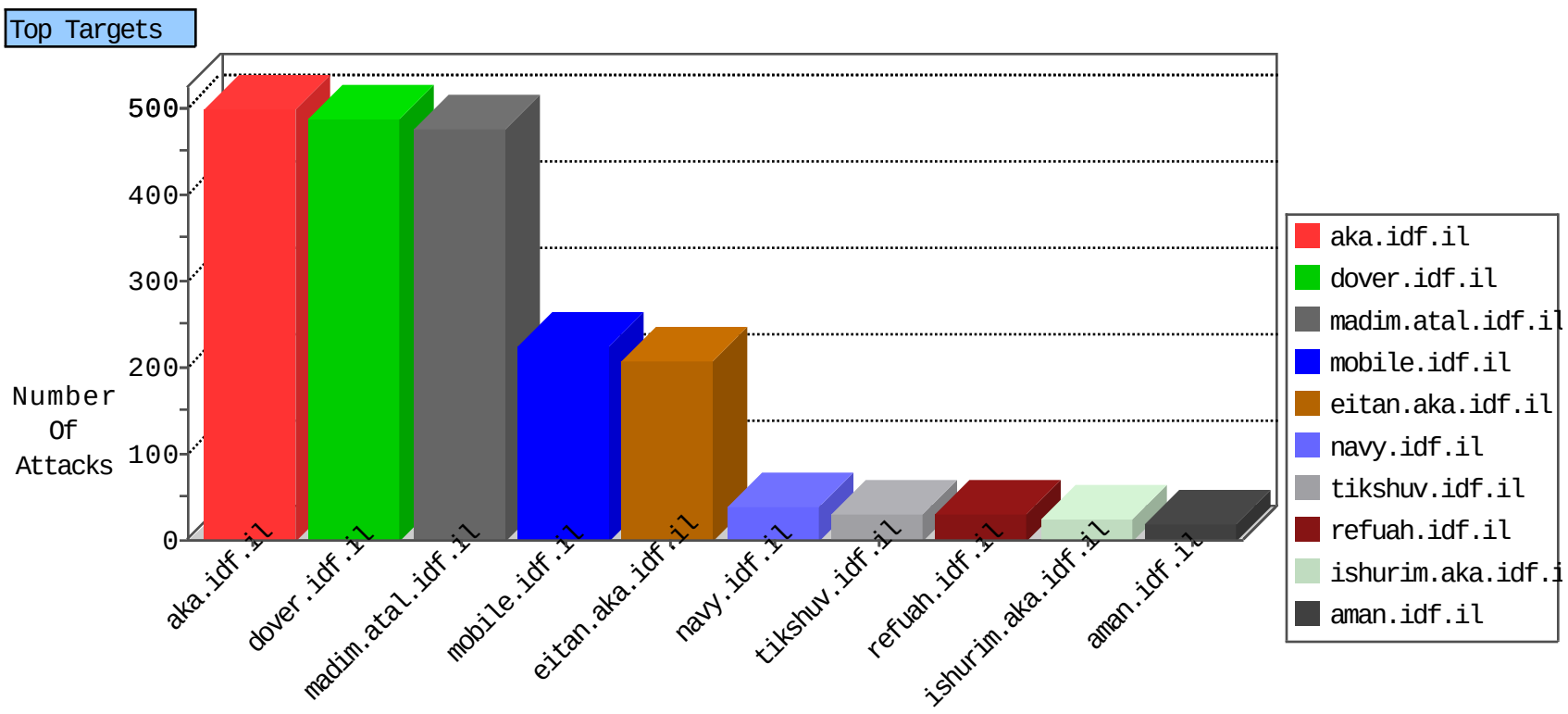
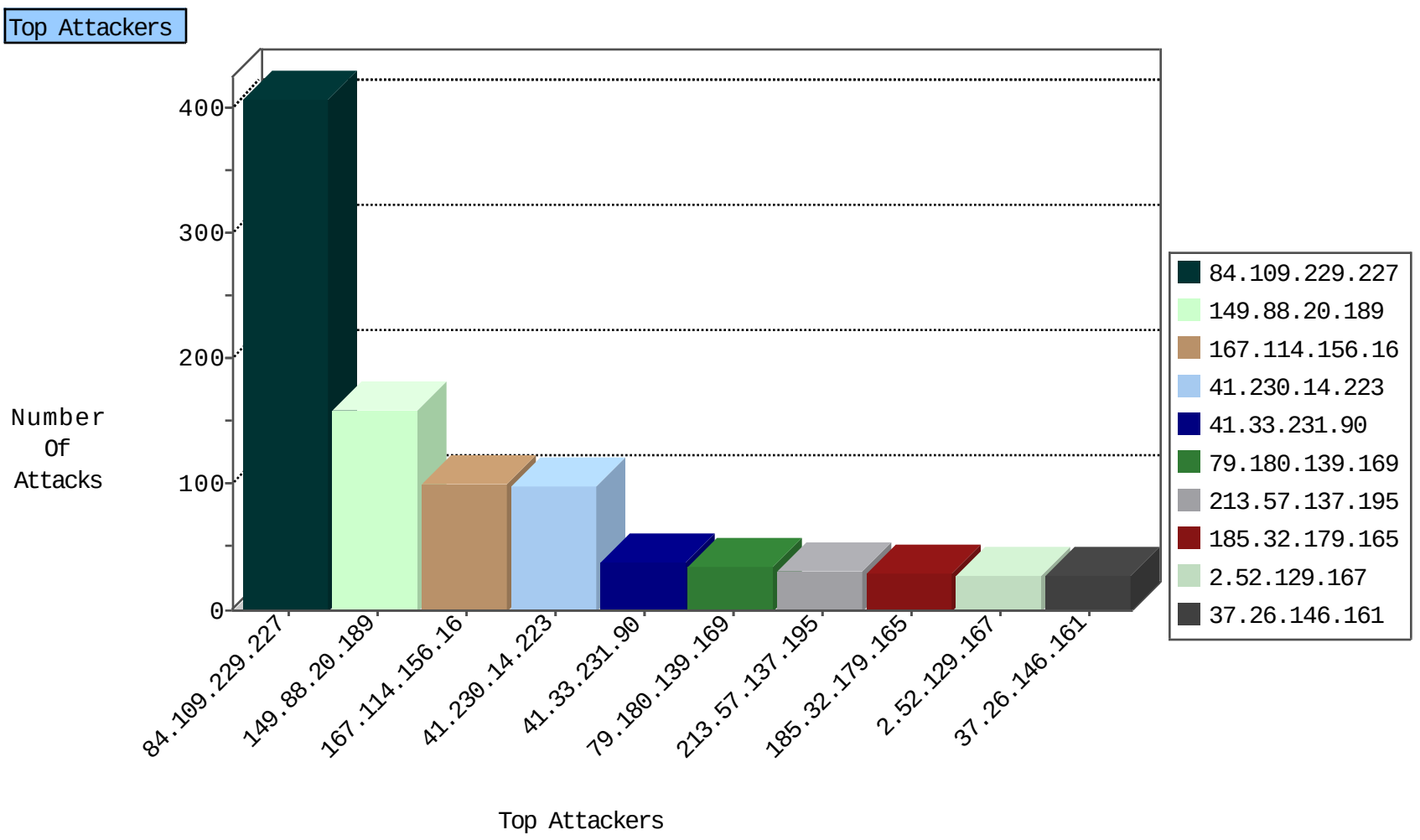
12-29-2015-19:04:06 to 12-29-2015-20:04:06

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-29-2015-19:04:06 to 12-29-2015-20:04:06

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	2496
37.26.148.245	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
85.65.140.67	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
66.249.80.83	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
84.108.32.166	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
204.93.161.17	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.177.55.135	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
213.8.46.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
188.42.240.225	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
150.70.173.10	Japan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.54.158.219	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

12-29-2015-19:04:06 to 12-29-2015-20:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.240.213.93	United States	147.237.77.179	e.mazi.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	2

12-29-2015-19:04:06 to 12-29-2015-20:04:06

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	3
184.51.154.10	147.237.77.216	Canada	dover.idf.il	Tehila - Perl LWP with fake user agent	2
139.91.210.41	147.237.76.38	Greece	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
185.3.146.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.215.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.252.84	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
77.125.6.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
59.126.188.243	147.237.76.34	Taiwan	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
202.59.169.38	147.237.77.19	Indonesia	law-forum.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.15.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.9.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
192.186.95.178	147.237.8.14	Canada	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
151.11.201.3	147.237.76.44	Italy	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
190.249.184.162	147.237.76.39	Colombia	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
139.91.210.41	147.237.77.212	Greece	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
190.147.129.99	147.237.76.38	Colombia	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
119.81.60.162	147.237.0.33	Singapore	idf.il	ET SCAN NMAP -sS window 1024	1
79.181.13.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.252.84	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
64.124.27.226	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
222.33.123.29	147.237.76.44	China	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
50.87.144.145	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
179.124.184.2	147.237.8.46	Brazil	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
197.115.25.107	147.237.77.216	Algeria	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
192.186.95.178	147.237.8.14	Canada	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
151.217.178.88	147.237.72.156		aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
190.249.184.162	147.237.76.39	Colombia	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
151.11.201.3	147.237.76.44	Italy	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
190.249.184.162	147.237.76.39	Colombia	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1

12-29-2015-19:04:06 to 12-29-2015-20:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.88.20.189	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	159
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.52.129.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
82.80.146.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
37.26.146.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
109.160.241.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
149.88.179.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.85.253	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
2.54.9.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
213.57.134.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
2.54.27.26	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
5.102.254.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.109.229.227	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.86.181	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
213.57.137.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
213.57.137.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
39.47.105.165	Pakistan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
94.194.9.232	United Kingdom	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.81.0.153	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
154.120.107.32	Nigeria	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	9
109.65.144.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
185.32.179.165	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
85.130.225.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.137.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
37.26.148.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
31.210.186.230	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
185.32.179.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.253	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.148.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.203.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.197	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
90.174.2.2	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.1.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.116.172.249	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.136.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
39.47.105.165	Pakistan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
79.178.10.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.28.34	Israel	147.237.77.170	maarachot.idf.il	HTTP Format Sizes	'Referer' header length exceeded maximum allowed length	monitor	6
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.128.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.3.203	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

12-29-2015-19:04:06 to 12-29-2015-20:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.229.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	225
84.109.229.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
84.109.229.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	64
79.180.139.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
37.26.146.161	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
79.179.136.109	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/resource/userfollowresource/create/	Block	6
2.54.9.111	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/milluim parameter Days	Block	6
109.160.209.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.52.129.167	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	4
149.88.179.43	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.54.9.111	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	4
176.13.18.113	Israel	147.237.76.30	himush.idf.il	Multiple Unauthorized URL Access from 176.13.18.113	Block	4
46.19.85.210	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
109.160.241.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
128.127.107.80	Netherlands	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
85.64.174.197	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
5.102.254.193	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.12.149.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.160.241.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
62.219.159.199	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.219.159.199	Block	3
37.26.147.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.197.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.41.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.102.254.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.28.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
93.172.74.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
87.69.222.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
176.13.15.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.179.21.194	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.13.6.180	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	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
79.180.139.169	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	2
109.160.207.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.27.26	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	2
5.102.238.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.235.8.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
178.67.201.179	Russian Federation	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
149.88.20.189	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templ@es/homepage/homepage.aspx	Block	1
87.69.105.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
201.130.153.192	Mexico	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
185.32.179.122	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.178.203.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.46.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method MlÂ™ Ã®OD[[#18]]gUGÂ¨dÂ°=[[#20]]Â£Ã·Â§2$Â¼`ÂŠ [[#18]]YÃ³Â¼"Â¥Ã¡JÂ†ÃƒÃ®Ã‡Âœ?GÃ˜Ã'Âˆ BÃ«sHÂ¬Ã¥s^FÃ¤Ã„ Â©Ã€ÂŽ,[[#17]]^ in URL	Block	1
176.13.11.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1

12-29-2015-19:04:06 to 12-29-2015-20:04:06