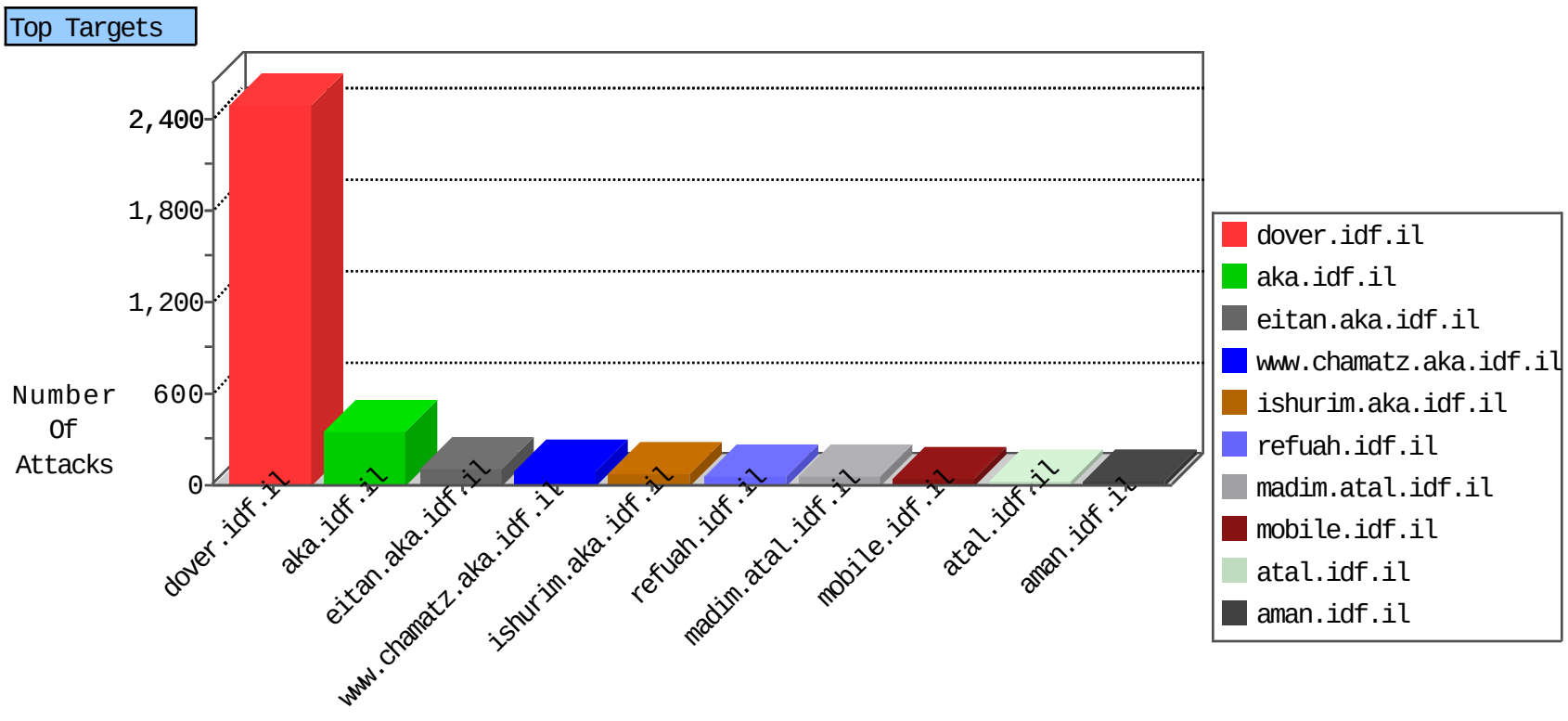
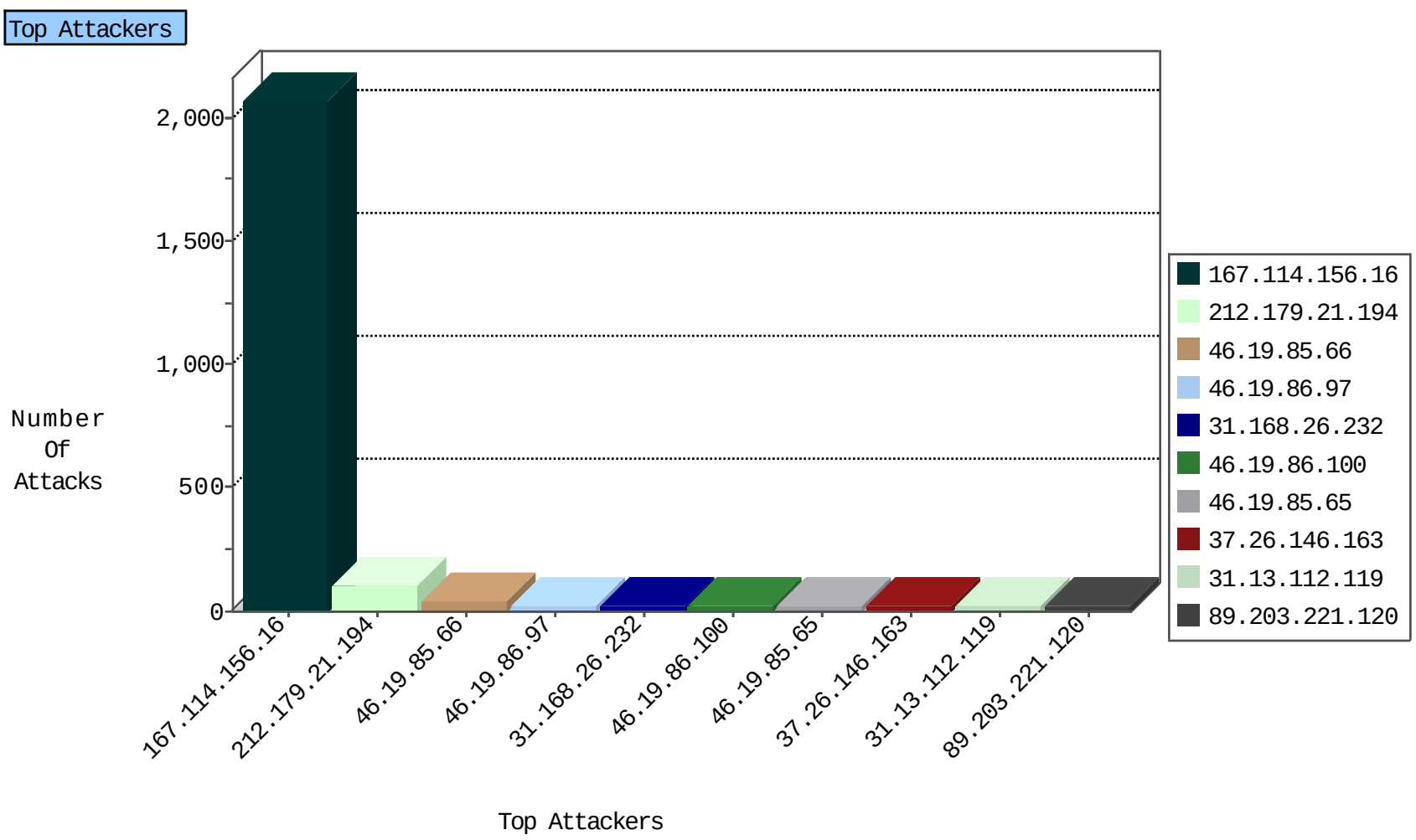
12-20-2015-14:04:04 to 12-20-2015-15:04:04

IDF Under Attack
Daily Report





12-20-2015-14:04:04 to 12-20-2015-15:04:04

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	3258
79.176.23.213	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
192.221.93.5	United States	147.237.72.217	e.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
49.229.85.221	Thailand	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
89.248.167.162	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
192.221.93.5	United States	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
222.254.180.216	Vietnam	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
89.248.167.162	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
223.197.50.121	Hong Kong	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
89.248.167.162	Netherlands	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

12-20-2015-14:04:04 to 12-20-2015-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.203.221.120	Czech Republic	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	18
77.109.139.87	Switzerland	147.237.77.216	dover.idf.il	1071: FPSE: authors.pwd Access	Block	1

12-20-2015-14:04:04 to 12-20-2015-15:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
192.221.93.5	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
106.3.45.131	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
46.172.71.251	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
106.3.45.131	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.183.36.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
46.151.54.178	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
41.140.253.9	147.237.0.33	Morocco	idf.il	ET SCAN NMAP -sS window 1024	1
2.54.36.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-20-2015-14:04:04 to 12-20-2015-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.66	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	43
31.13.112.119	Ireland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	20
31.13.112.123	Ireland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.242	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
31.13.112.118	Ireland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.97	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
31.13.112.117	Ireland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	12
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.179.218.166	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.160.79	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
46.19.86.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
84.228.212.228	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
37.26.146.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
31.13.112.120	Ireland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	10
109.67.136.37	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
109.64.159.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
31.168.26.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
46.19.85.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.148	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
31.13.112.116	Ireland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
212.143.35.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.166.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.155.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.13.112.122	Ireland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
46.210.145.160	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.61.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.19.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.137.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.10.107	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.80.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.116.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.1	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.179.98.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.4.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

12-20-2015-14:04:04 to 12-20-2015-15:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	80
46.19.86.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
176.12.147.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.52.173.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
80.246.136.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	3
79.183.23.97	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized HTTP Method	Block	3
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.125	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	3
46.19.86.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.13.21.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.180.11.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
5.29.222.96	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	2
176.12.137.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
62.0.101.185	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/275-he/patzar.aspx	Block	2
217.132.57.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
109.160.236.216	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
77.125.116.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane/	Block	2
79.183.23.97	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.183.23.97	Block	2
77.109.139.87	Switzerland	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.109.139.87	Block	2
2.52.15.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.207.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
46.19.85.65	Israel	147.237.76.42	refuah.idf.il	Multiple Malformed URL from 46.19.85.65	Block	1
85.250.206.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
74.6.53.182	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/old/wp-admin/	Block	1
66.249.78.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/rabanut/	Block	1
162.209.101.250	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
31.168.152.88	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/1	Block	1
213.151.49.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.62.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.92.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.115.55	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
77.109.139.87	Switzerland	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
46.19.86.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.196.68	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
39.42.68.149	Pakistan	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
84.94.119.243	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
176.13.4.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.185.98	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ main giyus	Block	1
212.179.21.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.64.50	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/rabanut/	Block	1
132.73.202.227	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.154	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
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	1
2.52.22.157	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

12-20-2015-14:04:04 to 12-20-2015-15:04:04