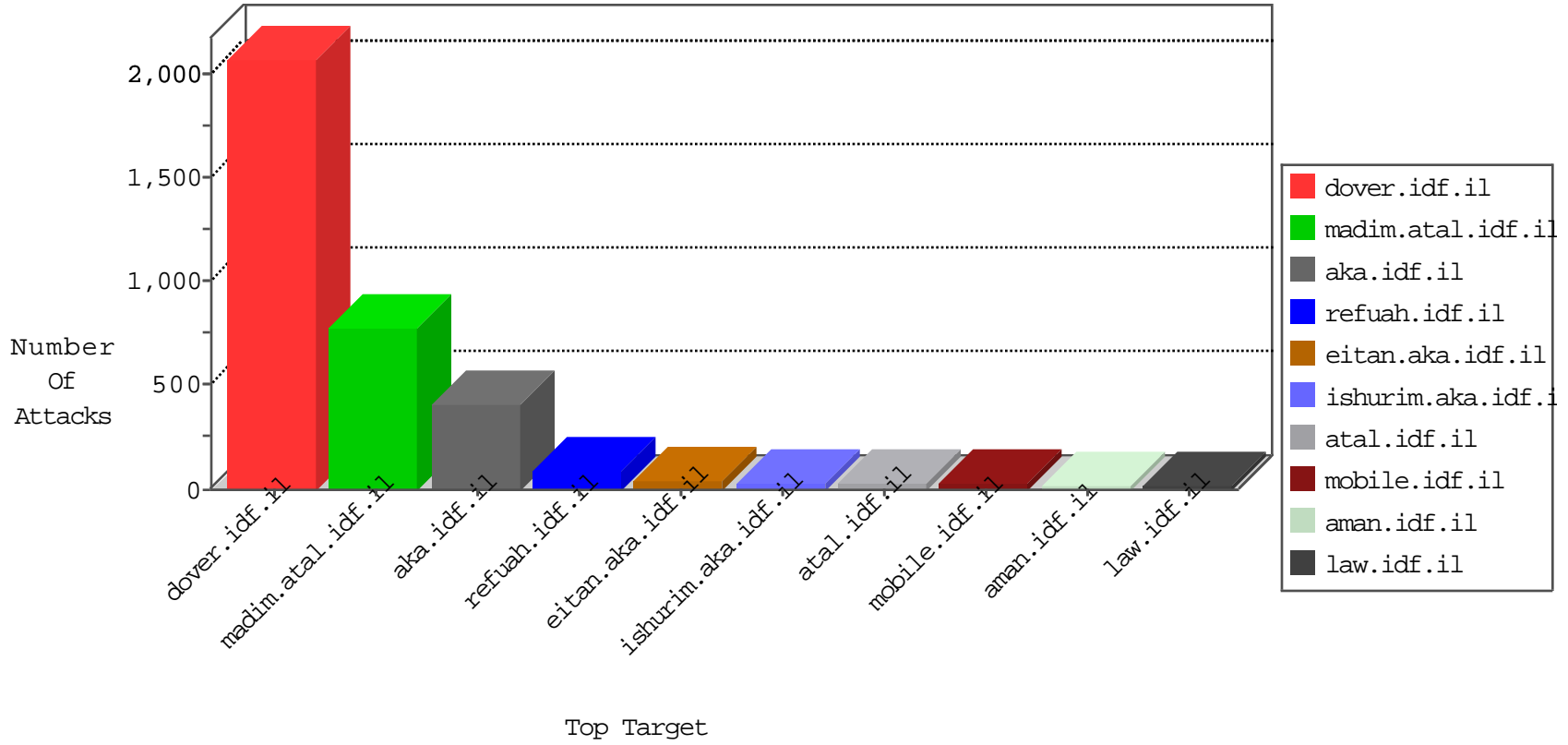


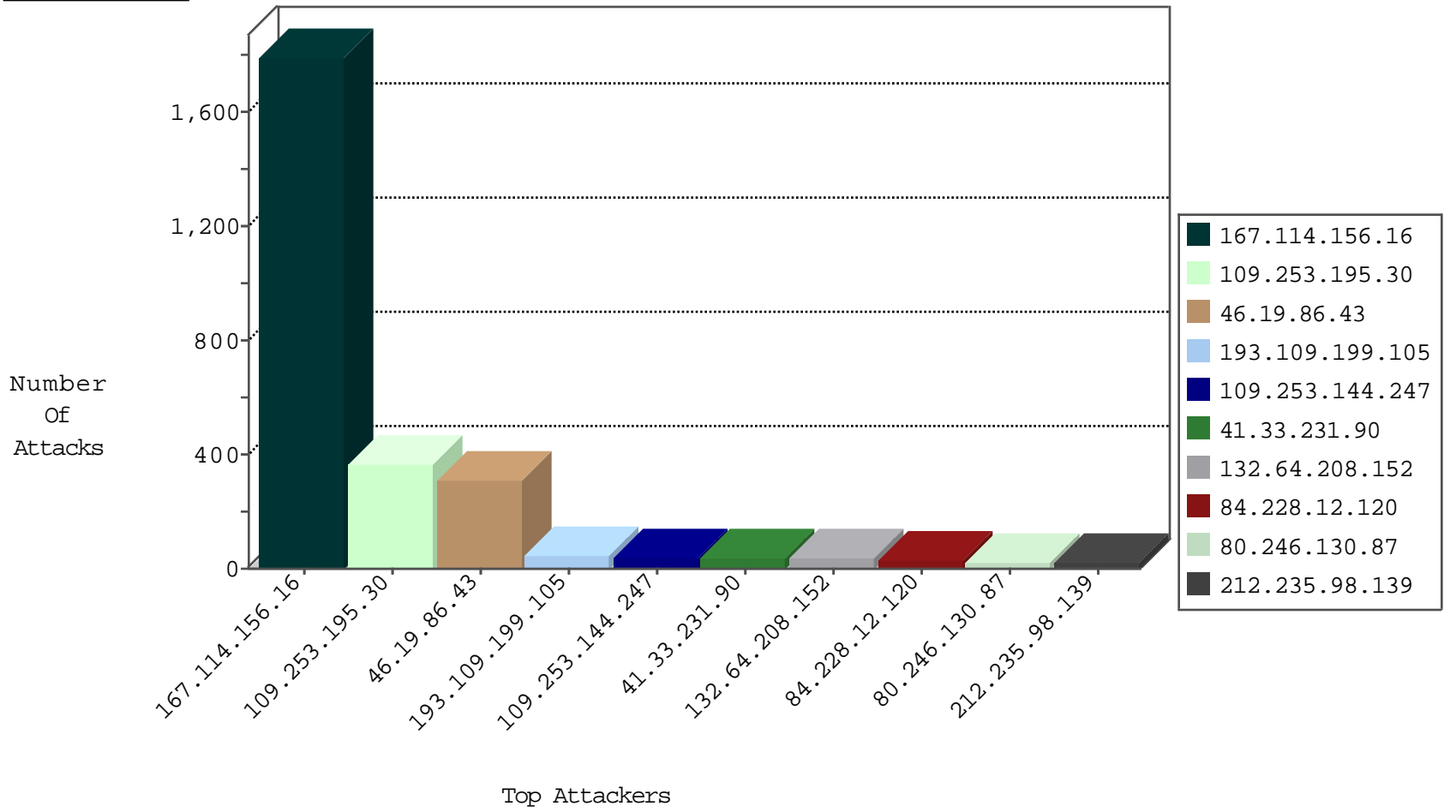
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3104
193.109.199.105	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24
46.20.15.11	Turkey	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

12-27-2015-14:04:00 to 12-27-2015-15:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
151.217.178.88	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.219.99.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.56	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.86.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.133.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.210.186.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.167.162	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.167.162	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.167.162	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.167.162	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.105.134.220	147.237.8.45	Sweden	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
84.110.110.95	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
176.13.17.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.119.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.56	147.237.77.205		prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.86.216	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.31	147.237.76.34		yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.167.162	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.52.46.17	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.167.162	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.167.162	147.237.76.177	Netherlands	noore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.167.162	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
89.139.181.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.108.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
132.64.208.152	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
84.228.12.120	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
80.246.130.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
80.246.133.52	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
193.109.199.105	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.54.47.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
79.181.160.118	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
84.94.193.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.177.34.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.183.248	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.180.164.179	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
79.180.164.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
193.109.199.105	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.144	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.154.89	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.202.185	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
79.183.129.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.102.254.45	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.101.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.183.129.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.174.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.204.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
62.219.165.242	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
84.94.193.22	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	6
46.117.20.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.235.98.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.22.134.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.189.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.140.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
213.8.204.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	5
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.186	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
85.130.189.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.186	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.219.110.87	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.253.144.247	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.130.189.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.210.186.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.128.127	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	229
109.253.195.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	194
109.253.195.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	142
46.19.86.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	77
109.253.144.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
109.253.195.30	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 109.253.195.30	Block	25
109.253.133.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
176.13.10.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
95.108.132.178	Russian Federation	147.237.77.74	law.idf.il	Distributed Suspicious Response Code	Block	8
109.253.144.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
79.179.183.139	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.179.183.139	Block	6
176.12.137.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.159.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
80.246.136.176	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
46.19.86.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.214.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.18.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.172.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.125.63	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	3
2.54.28.36	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00\$ContentPlaceHolder1\$txtLastName	Block	2
81.218.116.129	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
213.57.43.106	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	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
87.68.34.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.102.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
80.246.137.100	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 80.246.137.100	Block	2
46.19.86.43	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
46.19.86.173	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	2
158.69.52.102	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
65.208.151.116	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripts/jquery/' + url + '	Block	1
37.26.148.181	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
84.110.110.95	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
184.105.139.67	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
31.13.109.117	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.166.186.202	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
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	1
149.78.184.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.159.144.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.67.183.198	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
46.19.85.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.188.136	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/resource/userfollowresource/create/	Block	1
194.90.76.213	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1384-he/dover.aspx	Block	1
109.253.202.229	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.186.172.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.146.189	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.15.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
65.208.151.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1