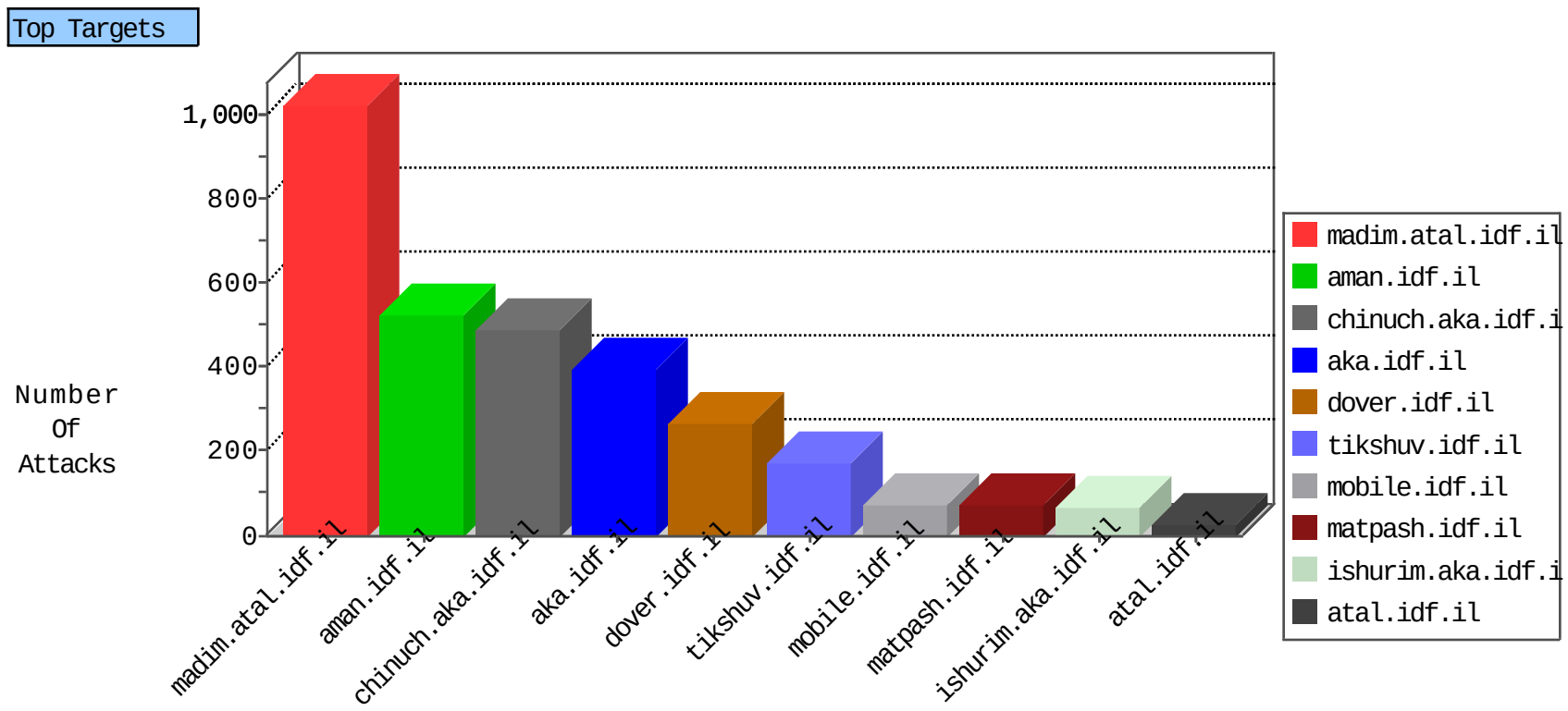
01-26-2016-14:04:02 to 01-26-2016-15:04:02

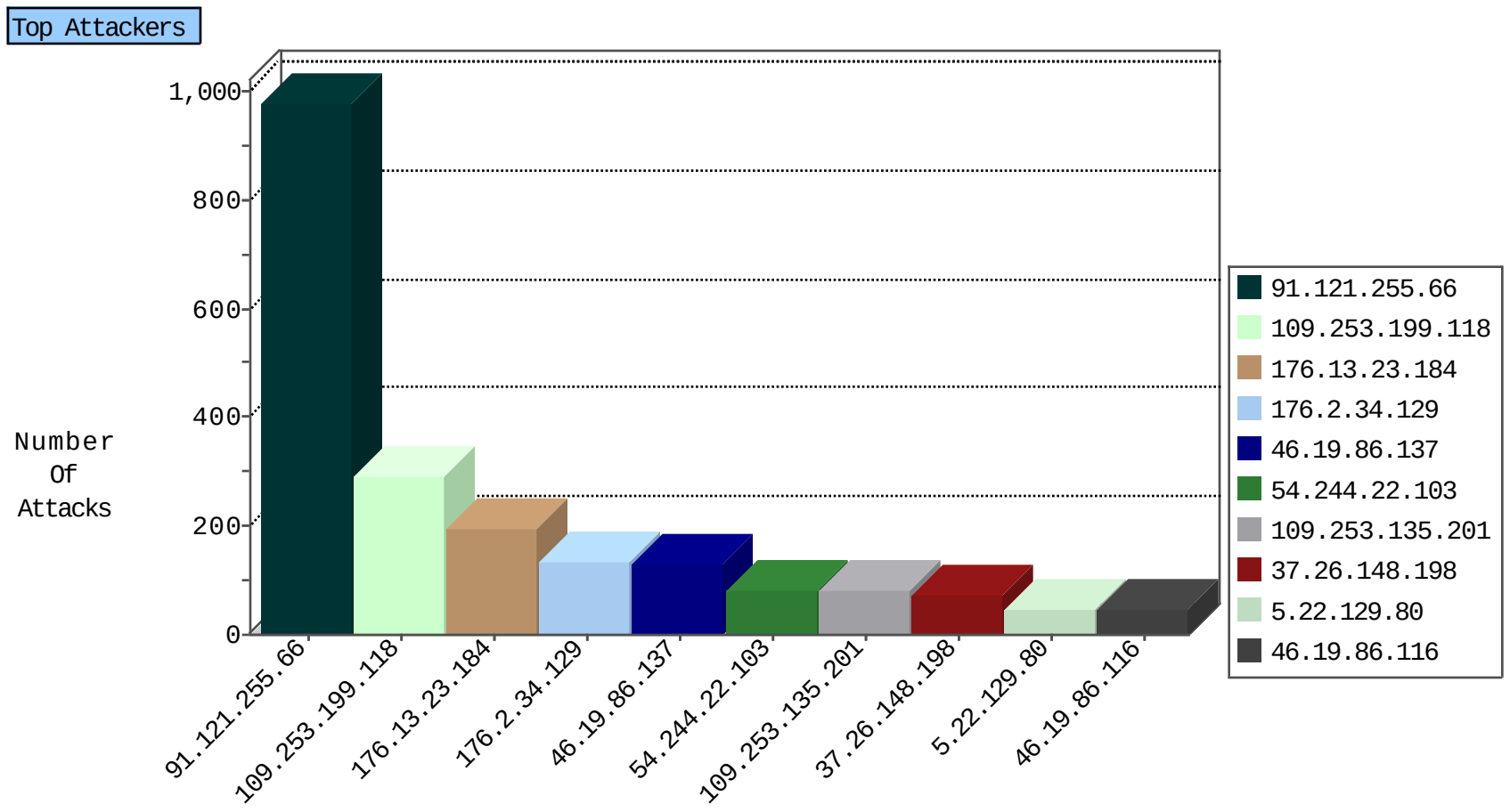
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-26-2016-14:04:02 to 01-26-2016-15:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
80.246.139.102	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
85.13.142.4	Germany	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
142.54.160.211	United States	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
81.218.56.125	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
142.54.169.164	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1

01-26-2016-14:04:02 to 01-26-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-26-2016-14:04:02 to 01-26-2016-15:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.139.102	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
80.82.64.68	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.171.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.216.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.1.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.39.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.0.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
93.183.201.2	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN Potential SSH Scan	1
84.108.79.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.68	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.202.208	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
37.143.82.50	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
188.97.198.69	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.229.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.141.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.130	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

01-26-2016-14:04:02 to 01-26-2016-15:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.121.255.66	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	465
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	431
176.2.34.129	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	135
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	70
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	48
5.22.129.80	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
2.52.7.2	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	34
46.19.85.237	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
91.121.255.66	France	147.237.72.156	aman.idf.il	SYN Attack		reject	26
37.26.149.178	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
46.19.86.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.253.199.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.182.208.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
37.8.120.72	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	9
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.148.184	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.149.222	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.253.156.30	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.234	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.192.251	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.139.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
80.246.139.102	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	drop	6
80.246.139.205	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.222	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.26.149.178	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
37.26.149.178	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
176.13.4.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.149.230	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.4.235	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
176.13.5.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.64.195	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.6.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.168.13.78	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.149.178	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
176.13.4.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.120.148.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.29.41.81	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.179.202.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.78.147	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

01-26-2016-14:04:02 to 01-26-2016-15:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.199.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	159
109.253.199.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	129
176.13.23.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
176.13.23.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	91
109.253.135.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
37.26.148.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
37.26.147.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	34
37.26.149.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
176.13.18.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
46.19.86.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
46.117.88.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
46.19.85.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
37.26.148.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
176.13.2.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
109.253.197.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	4
46.19.86.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.1.234	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	4
37.26.148.156	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	4
31.168.218.221	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	4
109.253.197.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.26.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.4.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.142.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.139.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.129.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.2.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
109.253.139.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	2
84.109.144.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.2.137	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	2
109.253.223.19	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.253.223.19	Block	2
79.182.208.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.147.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.109.106.239	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
95.35.75.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
149.78.123.140	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
213.151.38.124	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21570-he/idfgdover.aspx&sa=u&ved=0ahukewi4origvsfkahxd_ywkhdpcchcqfggimaa&sig2=0vpuxlxy2q-dk4jvkaasog&usg=afqjcngkxkptobpol8pgxzxftd95sstiiw	Block	2
109.253.199.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
212.150.71.177	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	2
46.19.86.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.150.159.66	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.54.17.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.96.48	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Malformed URL	Block	1

01-26-2016-14:04:02 to 01-26-2016-15:04:02