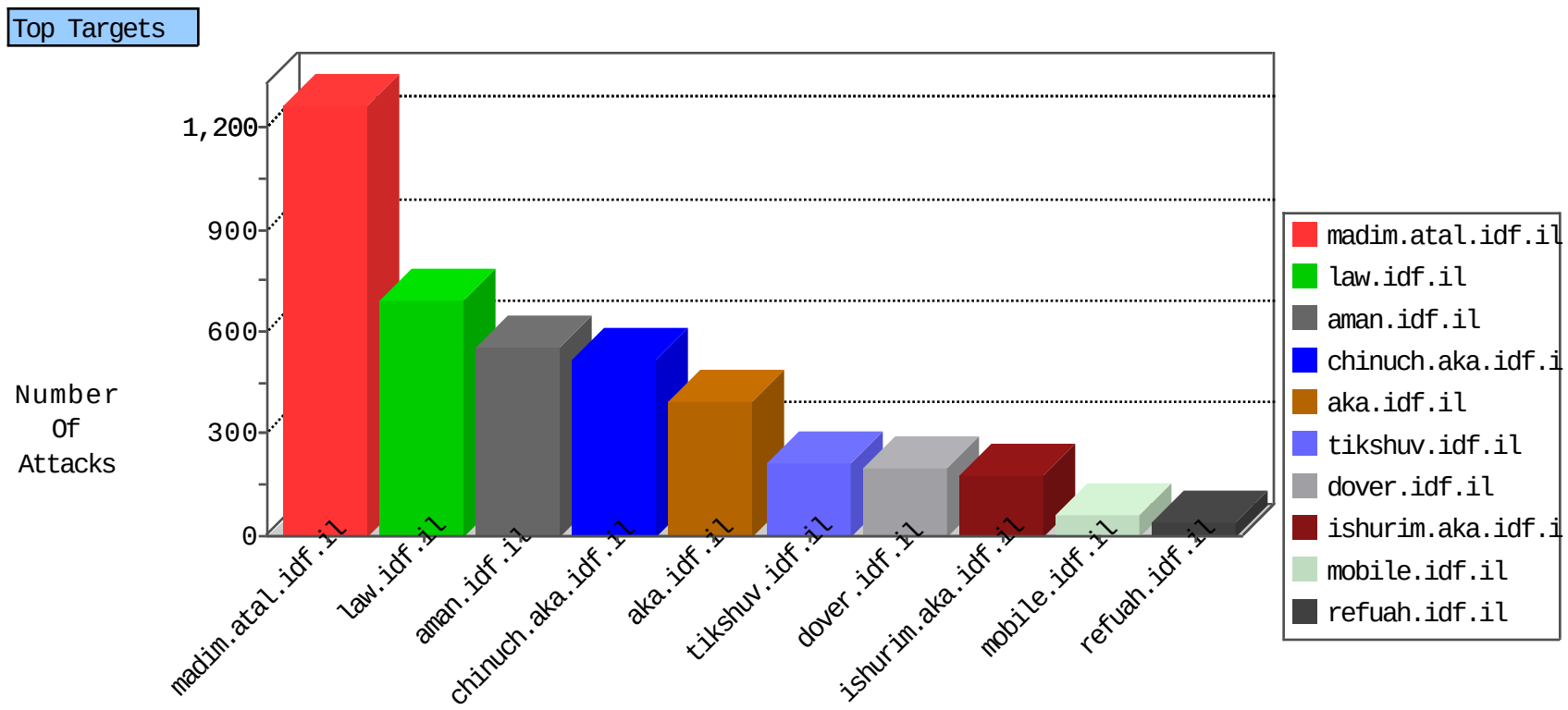
01-26-2016-15:04:04 to 01-26-2016-16:04:04

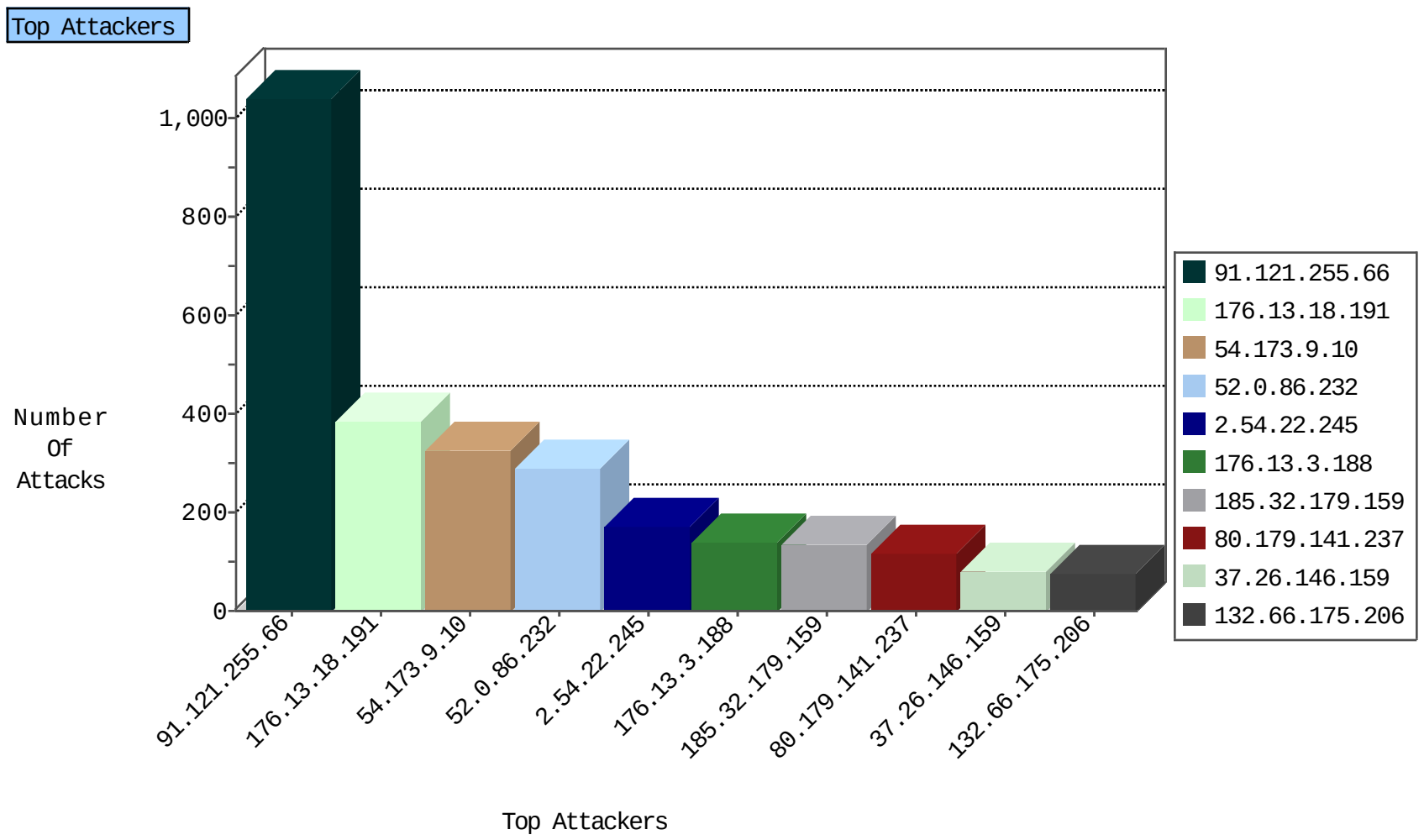
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-26-2016-15:04:04 to 01-26-2016-16:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	307
109.65.117.248	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
183.60.48.25	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.239.228.10	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Http	drop	2
142.54.169.166	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
81.218.208.46	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
142.54.160.213	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
142.54.169.162	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
188.138.17.205	France	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
142.54.169.163	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
81.218.208.46	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
119.244.208.1	Japan	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

01-26-2016-15:04:04 to 01-26-2016-16:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-26-2016-15:04:04 to 01-26-2016-16:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.142	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
194.246.79.135	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.64.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.94.75.226	147.237.77.216	Brazil	dover.idf.il	portscan: TCP Distributed Portscan	1
177.43.249.41	147.237.77.234	Brazil	halag.idf.il	ET SCAN NMAP -sS window 2048	1
149.88.206.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.150.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.188	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
46.19.86.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.32	147.237.72.166	Israel	aka.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
41.249.190.141	147.237.77.216	Morocco	dover.idf.il	portscan: TCP Distributed Portscan	1
183.107.21.167	147.237.72.166	Korea, Republic of	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.237.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.43.249.41	147.237.77.234	Brazil	halag.idf.il	ET SCAN NMAP -sS window 4096	1
177.43.249.41	147.237.77.234	Brazil	halag.idf.il	ET SCAN NMAP -f -sS	1
109.186.167.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.231.192.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.190.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.24.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-26-2016-15:04:04 to 01-26-2016-16:04:04

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	521
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	437
54.173.9.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	317
52.0.86.232	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	285
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	73
84.94.22.10	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
212.235.8.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
52.6.5.122	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
54.174.179.157	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	22
54.85.198.156	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	20
46.19.85.142	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
192.116.142.106	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	15
80.246.139.163	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.29.173.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
5.29.173.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	11
37.26.148.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.13.23.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.181.108.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.39.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.28.144.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.219.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.75.201	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.135.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.27.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.173.9.10	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.54.188.179	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.28.144.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.254	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.108.214.38	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
213.57.61.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.3.144.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
106.208.158.237	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.148.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
31.210.186.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.61.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.174.179.157	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
106.208.158.237	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.102.254.199	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.133.188	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	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
81.218.66.107	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	205
176.13.3.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
176.13.18.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
185.32.179.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
2.54.22.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	95
80.179.141.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	93
37.26.146.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	80
132.66.175.206	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
2.54.22.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	74
176.13.18.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	68
46.19.85.177	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
109.186.185.237	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.186.185.237	Block	47
2.54.46.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
2.52.134.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
46.19.85.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
185.32.179.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	31
80.179.141.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	23
79.179.216.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
176.13.3.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	23
109.253.199.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
89.139.28.233	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
176.13.18.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
2.54.36.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
2.54.24.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	6
176.13.18.14	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	6
176.13.23.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.158.121	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	6
109.253.205.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
79.176.35.92	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	5
2.52.48.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
212.235.8.225	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	4
212.235.8.225	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	4
176.13.13.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.33	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
79.176.35.92	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
36.81.181.73	Indonesia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
176.13.20.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
199.203.226.21	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 199.203.226.21	Block	3
212.235.8.225	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 212.235.8.225	Block	3
176.13.23.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.176.22.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.50.76.205	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/adguard-ajax-api/api	Block	3
79.180.195.15	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
176.13.23.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
217.132.128.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.50.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.179.120.254	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.179.120.254	Block	2

01-26-2016-15:04:04 to 01-26-2016-16:04:04