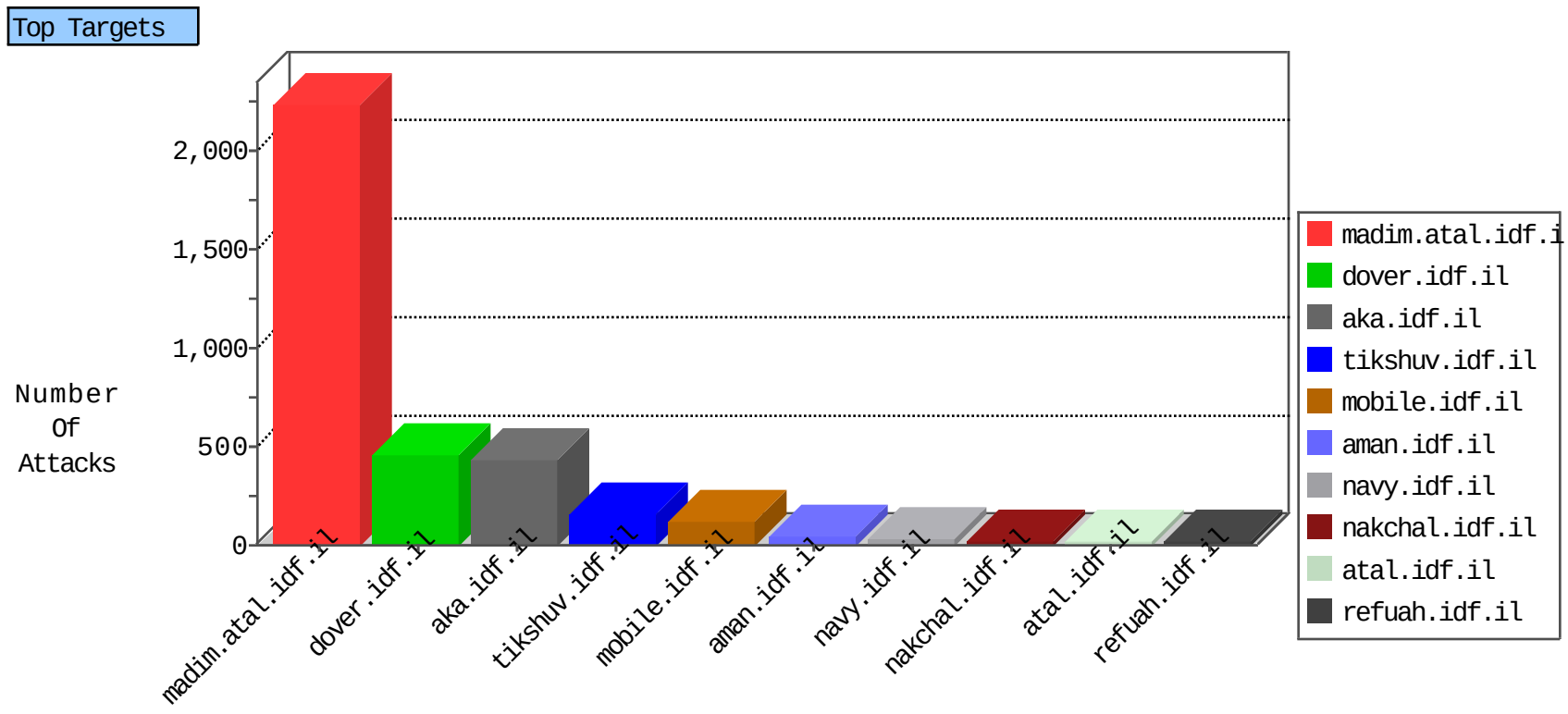
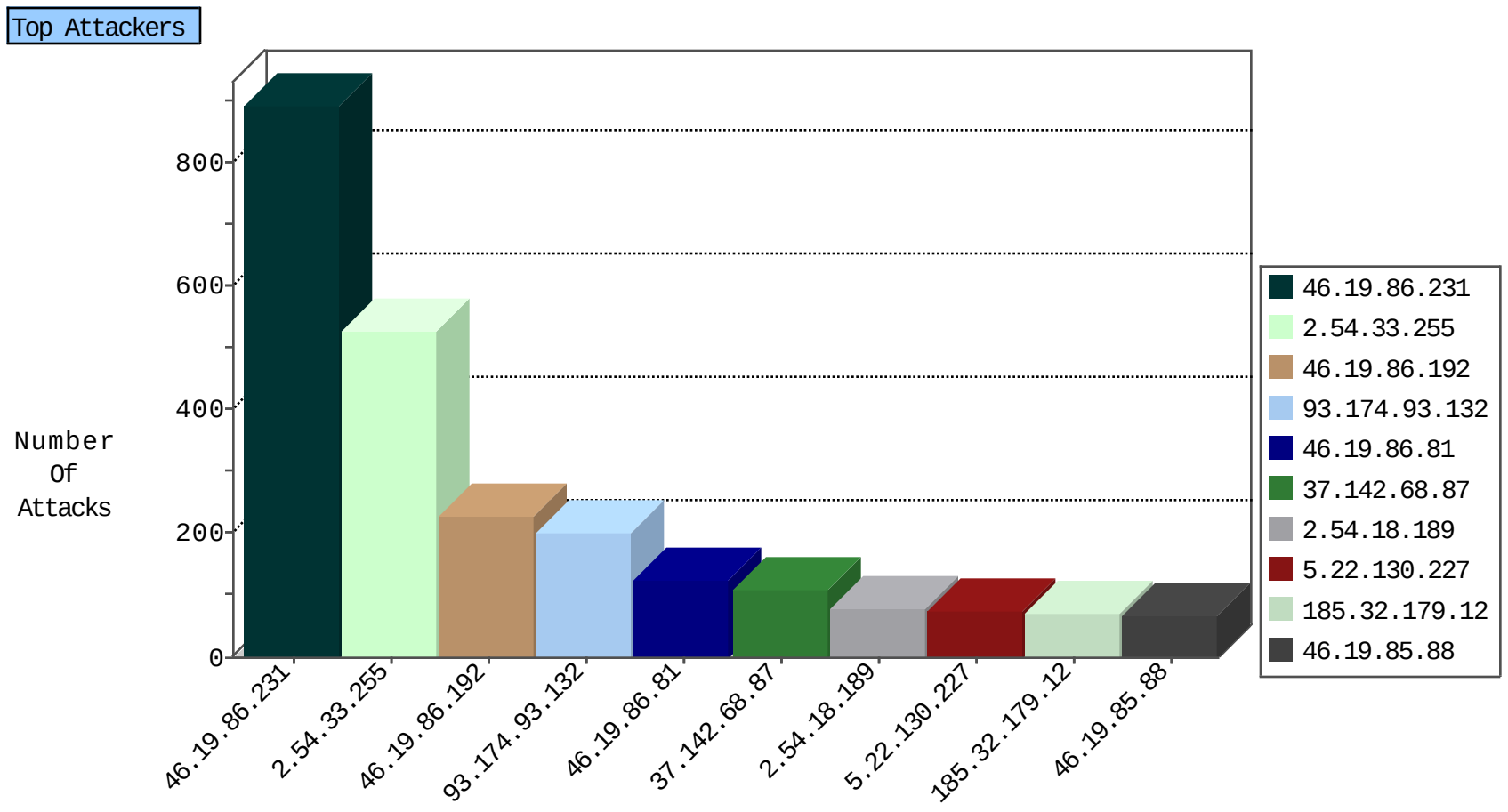
01-26-2016-17:04:01 to 01-26-2016-18:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-26-2016-17:04:01 to 01-26-2016-18:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	524
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	86
149.88.132.247	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
93.174.93.132	Netherlands	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
109.65.6.68	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
197.133.127.206	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
93.174.93.132	Netherlands	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	2
71.6.135.131	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
198.20.70.114	United States	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	1
142.54.169.166	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1

01-26-2016-17:04:01 to 01-26-2016-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
92.241.44.198	Jordan	147.237.77.216	dover.idf.il	13444: HTTP: WhatWeb User-Agent Header	Block	1
176.33.137.159	Turkey	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
176.58.117.133	United Kingdom	147.237.0.34	tikshuv.idf.il	3885: HTTP: PHP File Include Exploit	Block	1
191.232.39.241	United States	147.237.77.176	matpash.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1

01-26-2016-17:04:01 to 01-26-2016-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
82.80.59.137	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
175.6.228.149	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
46.19.85.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.13.173	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
5.28.165.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
120.199.111.137	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -f -sS	1
109.65.6.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.103.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.149.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
84.228.93.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.186.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.148.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.228.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
173.255.112.188	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.212.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
120.199.111.137	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 2048	1
114.112.90.54	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
98.25.0.11	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.84.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.84.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-26-2016-17:04:01 to 01-26-2016-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.174.93.132	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	186
213.8.245.58	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
197.133.127.206	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
37.26.147.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
149.78.49.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.86.84	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
149.78.49.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
83.53.215.36	Spain	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.192	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
80.179.14.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
64.233.173.151	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
64.233.173.151	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
5.102.254.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
31.210.187.207	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.253.204.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.192	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
79.181.50.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.93.243.46	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.181.183.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.210.188.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.65.157.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	drop	First packet isn't SYN	drop	8
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.180.175.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
5.102.254.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.102.254.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
197.133.127.206	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.88.132.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.138.196.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.5.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
149.88.132.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
85.250.173.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.88.132.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
79.182.188.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.173.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.88.132.247	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.120.17.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.94.56.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.52.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.211.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.62.200.215	Bulgaria	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
64.233.173.151	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
31.210.187.226	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

01-26-2016-17:04:01 to 01-26-2016-18:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	615
2.54.33.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	268
46.19.86.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	155
2.54.33.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	155
46.19.86.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	120
37.142.68.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
46.19.86.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	107
2.54.33.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
46.19.86.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	95
5.22.130.227	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
2.54.18.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
185.32.179.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
46.19.85.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
2.54.157.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
212.150.214.90	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	20
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
79.183.14.135	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.183.14.135	Block	12
2.54.0.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.54.130.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
5.144.62.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
79.183.14.135	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	5
37.26.147.254	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	4
79.179.204.54	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
176.33.137.159	Turkey	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.33.137.159	Block	4
37.26.146.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.108.93.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.4.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.33.137.159	Turkey	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.121.119.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.50.76.229	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.202.13	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.33.137.159	Turkey	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 176.33.137.159	Block	2
109.65.157.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.209	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.19.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
92.241.44.198	Jordan	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/70009.doc ×″×¦×″×¨×ª ×‘×¢×œ ×¨×™×©×•×Ÿ × ×″×™×’×″ - aka.&lt	Block	2
54.173.185.239	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/usercontrols/headerupper/	Block	1
31.210.187.226	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/	Block	1
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
197.189.206.93	South Africa	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
109.65.13.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.32.90	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1

01-26-2016-17:04:01 to 01-26-2016-18:04:01