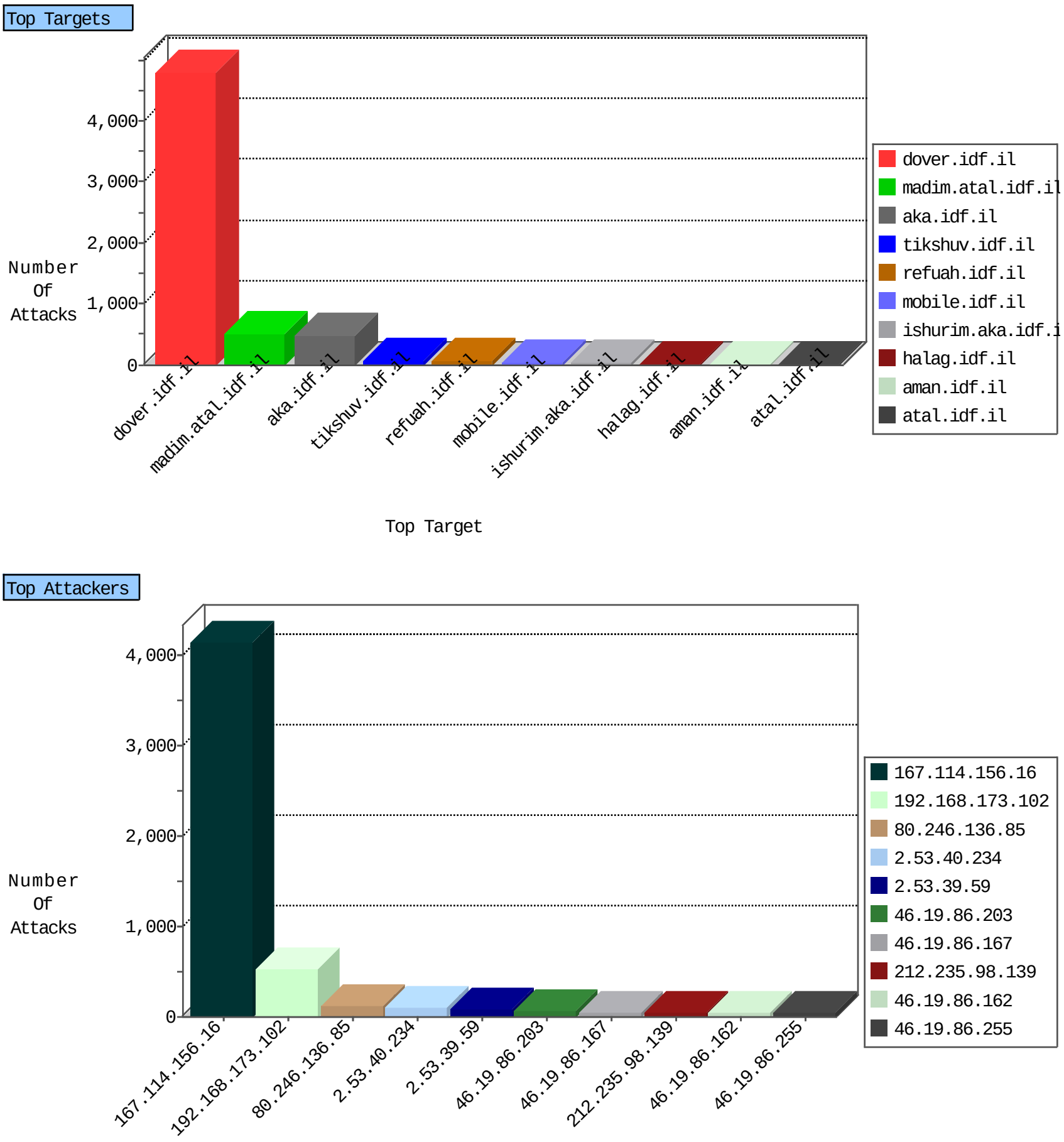
04-10-2016-10:04:08 to 04-10-2016-11:04:08

IDF Under Attack Daily Report



04-10-2016-10:04:08 to 04-10-2016-11:04:08

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	Block_Ip_Web_In	drop	4142
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
123.59.59.52	China	147.237.76.30	himush.idf.il	block-sp-traf1	forward	4
123.59.59.52	China	147.237.77.74	law.idf.il	block-sp-traf1	forward	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
74.91.17.179	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	2
173.208.197.254	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
81.218.13.130	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
69.30.226.219	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
74.91.17.182	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	2
69.30.202.226	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	2
69.197.185.20	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	2
74.91.17.182	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
69.30.202.227	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	2
74.91.17.178	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	2
74.91.23.110	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	2
69.30.226.218	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
185.94.111.1	Russian Federation	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
203.186.17.235	Hong Kong	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
178.135.82.30	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.98	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
93.201.86.227	Germany	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

04-10-2016-10:04:08 to 04-10-2016-11:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.126.142.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.4.32.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
62.210.97.48	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-10-2016-10:04:08 to 04-10-2016-11:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.215.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.0.15	Latvia	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
141.101.178.137	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
122.144.178.145	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
93.172.143.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
88.204.187.90	147.237.76.34	Kazakstan	yohalan.idf.il	ET SCAN NMAP -f -sS	1
62.84.116.68	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.37.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	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
122.144.178.145	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.67.174.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
88.204.187.90	147.237.76.34	Kazakstan	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
84.108.70.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-10-2016-10:04:08 to 04-10-2016-11:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	358
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	163
46.19.86.167	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
46.19.86.162	Israel	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	40
80.179.195.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
31.168.199.176	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
46.19.86.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
107.167.104.230	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
46.19.86.154	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
46.19.85.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
2.55.10.82	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.219.120.45	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
31.168.129.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
73.54.192.42	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.103	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	8
46.19.85.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
79.178.227.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.147.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
8.37.227.69	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	7
46.19.86.221	Israel	147.237.72.167	ishurim.aka.idf.i	drop	SAM rule	drop	7
176.0.29.250	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
85.130.128.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.203	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.199	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.90.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.53.42.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.185	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.199	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
217.194.203.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
197.0.197.180	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.86.11	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.52.162.71	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.31	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
46.19.86.186	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
87.71.22.53	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.78	Israel	147.237.77.233	atal.idf.il	drop	SAM rule	drop	5
106.38.241.149	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.160.242.40	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
8.37.227.81	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
31.168.192.177	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
2.54.195.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.168.192.177	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
2.53.40.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
2.53.39.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
46.19.86.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
176.13.6.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.52.190.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.85.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
176.13.3.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
46.19.86.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
212.235.115.168	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	6
185.130.5.163	Lithuania	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.130.5.163	Block	5
185.130.5.163	Lithuania	147.237.72.166	aka.idf.il	PHP Attempt	Block	5
212.235.115.168	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 212.235.115.168	Block	4
46.19.86.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
212.143.120.135	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	3
46.19.85.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.40.234	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	3
109.253.192.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
2.55.62.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.194.197.154	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 217.194.197.154	Block	2
176.13.7.182	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
31.168.103.115	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.103.115	Block	2
132.64.142.38	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	1
46.19.85.194	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
217.194.197.154	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
74.91.17.179	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
2.54.129.178	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/authenticationservice.asmx/getauthuser	Block	1
114.97.56.215	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1026-he/shared/usercontrols/headerupper/	Block	1
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 0.8afc=* in URL	Block	1
31.168.199.176	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
217.69.133.244	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/asp	Block	1
79.180.65.95	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl41 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
69.30.202.226	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
197.0.197.180	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
54.153.32.246	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
173.208.197.254	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
85.93.91.84	Germany	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.19.85.194	Israel	147.237.76.42	refuah.idf.il	Malformed URL asp.net_sessionid=lffm5g45da4znsfe2dpcegiv	Block	1
74.91.23.110	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
2.55.33.198	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
120.28.23.170	Philippines	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
37.8.72.182	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
217.194.159.14	Satellite Provider	147.237.72.166	aka.idf.il	Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
69.30.202.227	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
207.46.13.58	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1