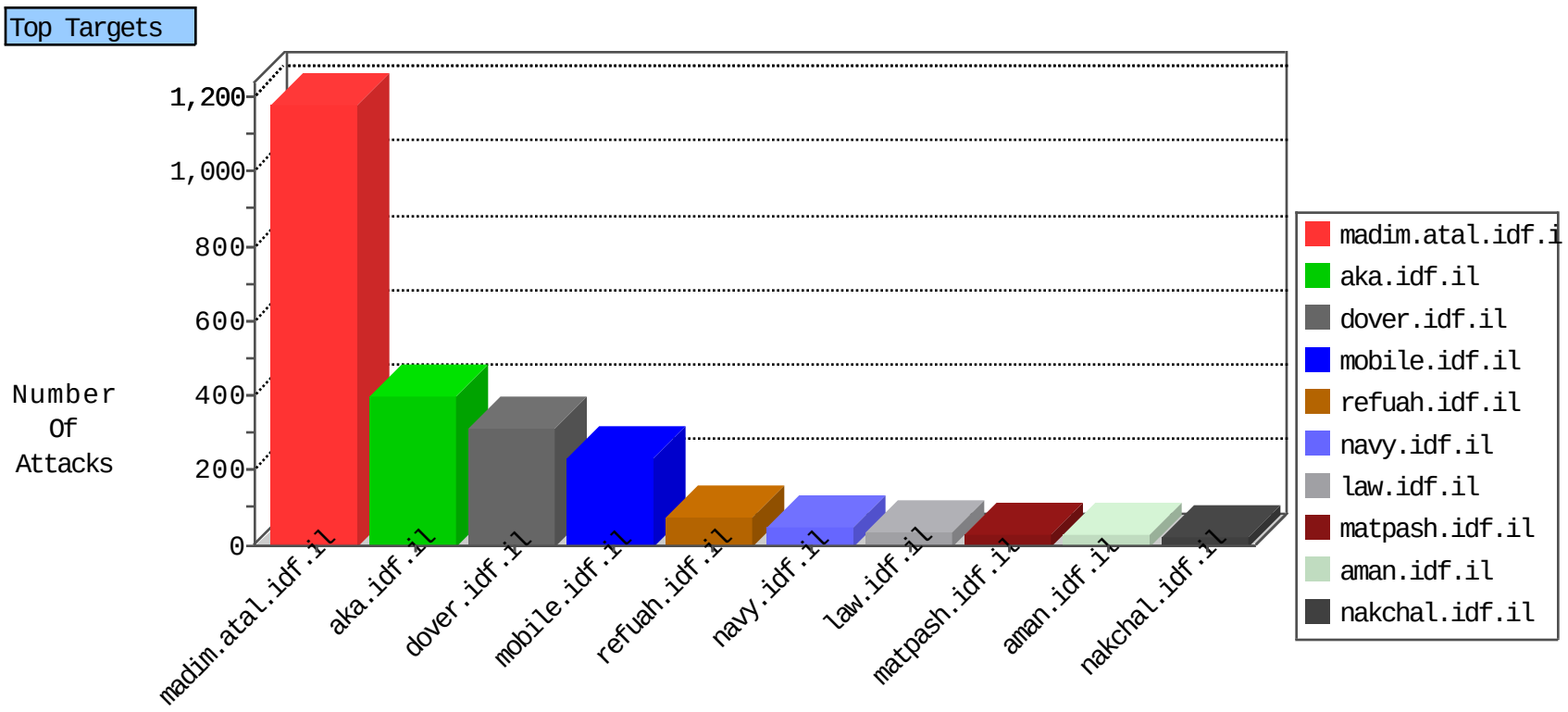
02-01-2016-18:04:08 to 02-01-2016-19:04:08

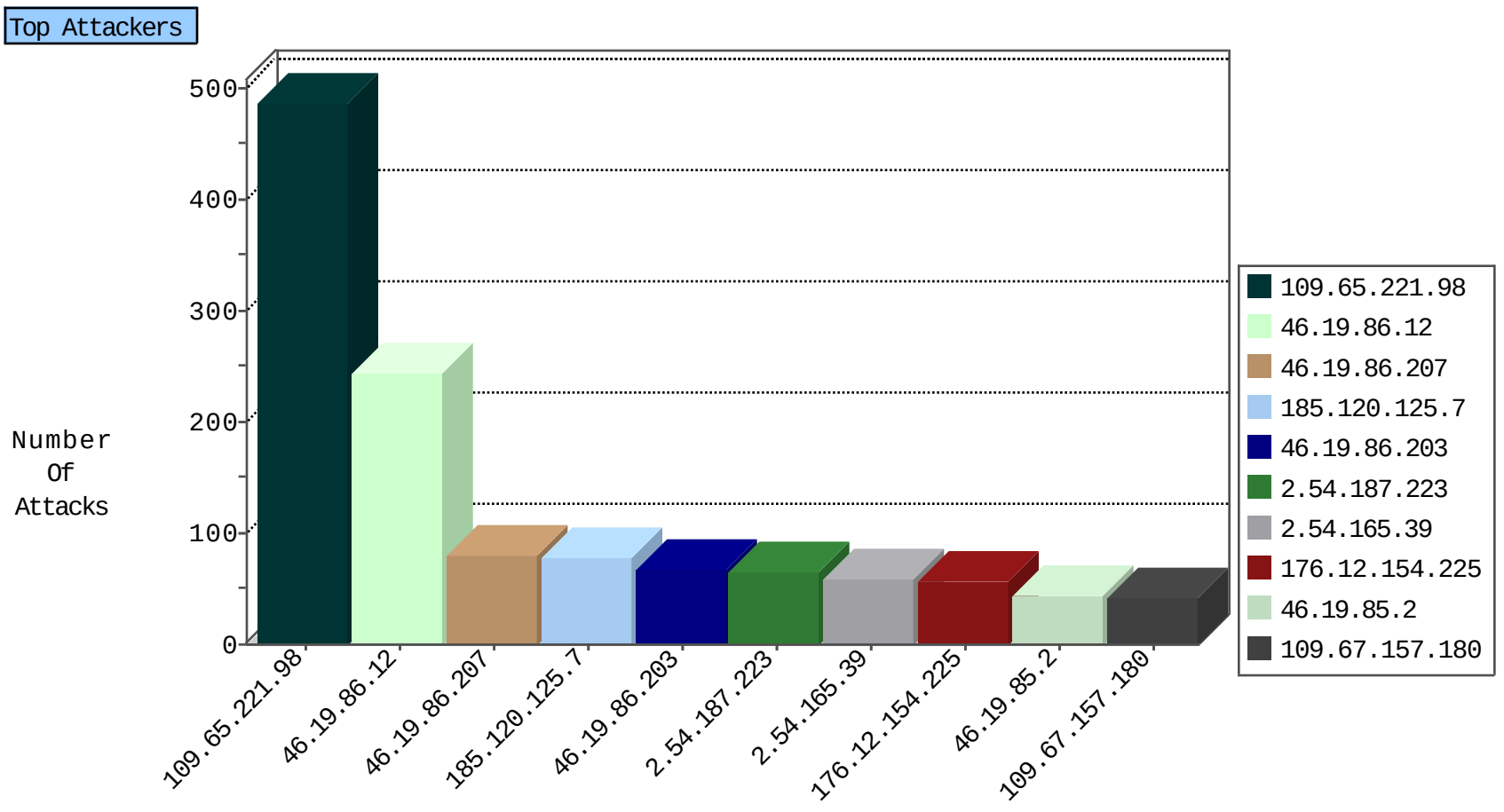
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-01-2016-18:04:08 to 02-01-2016-19:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.245	Israel	147.237.77.243	mobile.idf.il	TCP handshake violation, first packet not syn	drop	7603
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
31.168.19.190	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
74.91.28.59	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
10.0.0.5		147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
82.221.105.7	Iceland	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
142.54.169.165	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	drop	1

02-01-2016-18:04:08 to 02-01-2016-19:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.97.48	France	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	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

02-01-2016-18:04:08 to 02-01-2016-19:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.65.137.228	147.237.77.176	Israel	matpash.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	16
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
91.218.15.202	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
91.218.15.202	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
185.3.147.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.52.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
153.31.112.20	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.184	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
125.65.165.215	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
37.142.64.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.1.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.163.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.11.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.218.15.202	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
91.218.15.202	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.76.198	Ukraine	e.yohalan.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
168.62.238.153	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.25.255	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.80.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.128.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.28.135.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.170.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-01-2016-18:04:08 to 02-01-2016-19:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
109.67.157.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
141.0.14.82	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	38
79.180.112.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
80.246.130.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
12.12.162.124	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	24
176.12.155.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
149.50.87.198	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
109.64.163.241	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	16
46.19.85.233	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
2.52.170.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.136	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.136	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
157.55.39.175	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.180.127.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.181.201.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.228.213.79	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.170.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.135.198	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
89.139.149.59	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.157	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.147.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
176.12.155.113	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.210.186.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.67.221.134	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.12.155.85	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.155.113	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.102.228.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.141.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.150.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.195.17	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.176.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.145	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.12.154.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.226	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.148.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.155.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.165.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.102.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.66.25.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.226	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

02-01-2016-18:04:08 to 02-01-2016-19:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.155.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.221.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	322
109.65.221.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	165
46.19.86.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	119
46.19.86.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	94
46.19.86.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
176.12.154.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
2.54.187.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
2.54.165.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
46.19.85.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	33
46.19.86.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	31
46.19.86.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	22
46.19.85.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
109.67.221.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
2.54.187.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	11
46.19.86.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
104.12.80.51	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 104.12.80.51	Block	9
84.108.0.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
149.50.87.198	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
2.54.0.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.12.155.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.170.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.0.159	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
2.54.182.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
104.12.80.51	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 104.12.80.51	Block	3
176.12.155.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.12.155.171	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
77.127.225.123	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	2
109.64.195.17	Israel	147.237.0.34	tikshuv.idf.il	Suspicious Response Code	Block	2
176.12.154.199	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
50.93.201.50	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
79.181.98.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.150.15	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.65.137.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	2
46.19.85.254	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
77.126.215.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
84.228.213.79	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.181.201.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
5.144.58.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
94.230.86.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
188.143.232.37	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	1
79.183.21.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
37.157.214.192	Armenia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.117.157.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
84.108.52.49	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
176.67.122.16	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin/	Block	1