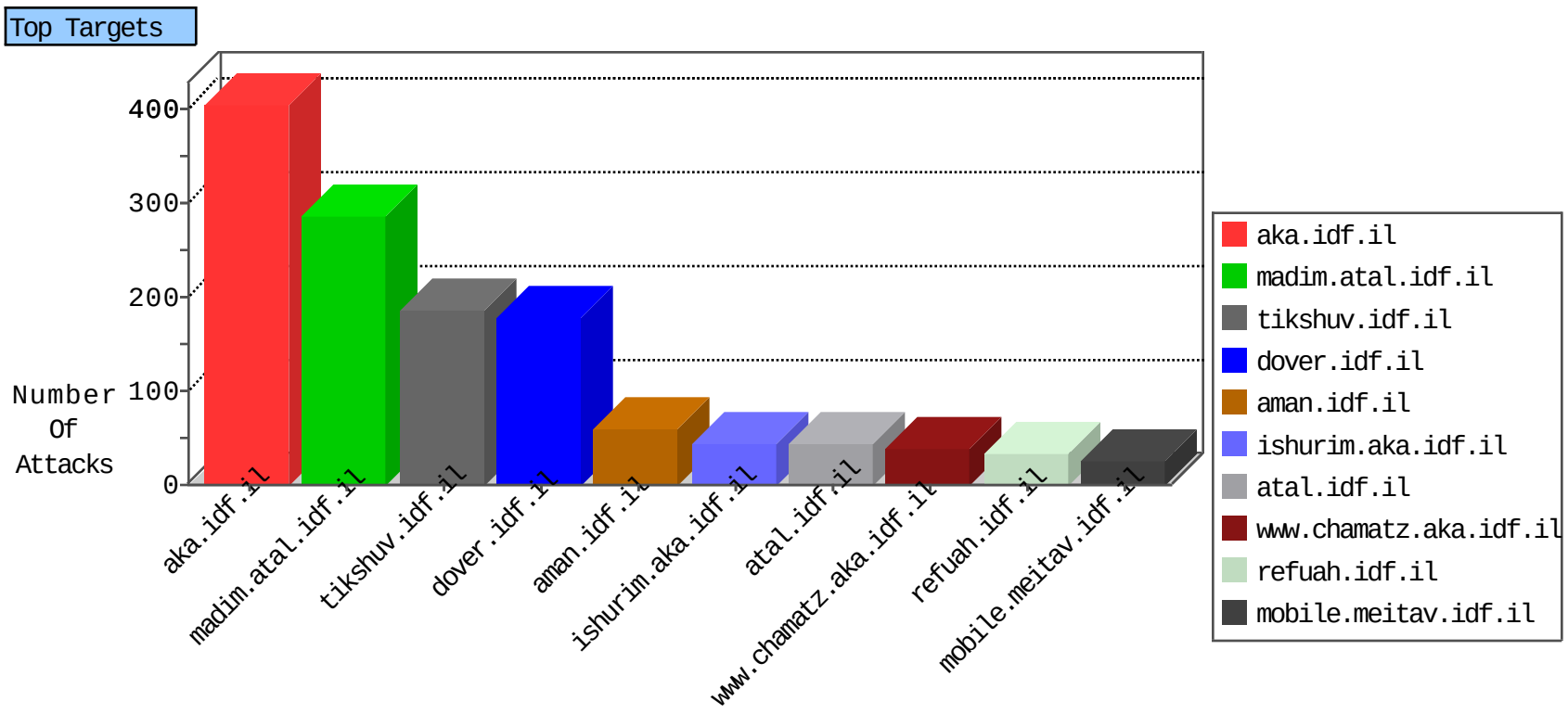
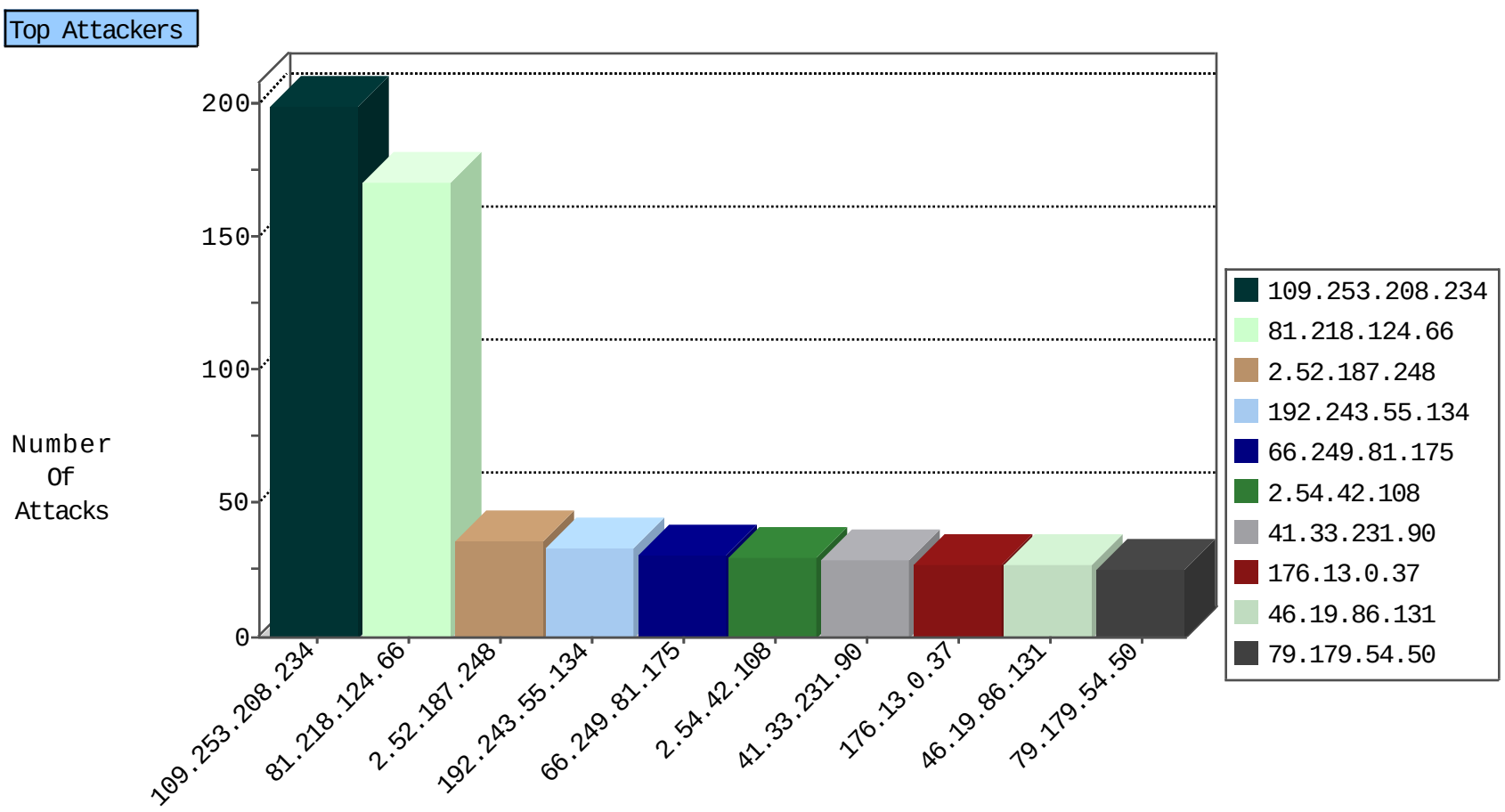
02-21-2016-12:04:03 to 02-21-2016-13:04:03

IDF Under Attack Daily Report





02-21-2016-12:04:03 to 02-21-2016-13:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
123.242.224.165	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
134.147.203.115	Germany	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	2
123.242.224.169	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
104.245.97.224		147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
123.242.224.166	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.130.5.201		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
104.245.97.224		147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

02-21-2016-12:04:03 to 02-21-2016-13:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.1.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
195.154.179.172	France	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Block	1
151.80.31.144	Italy	147.237.76.31	nakchal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-21-2016-12:04:03 to 02-21-2016-13:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.42.108	147.237.72.156	Israel	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
46.19.85.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
113.59.33.61	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
46.19.86.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.133.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.147.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.152.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.37.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.229.133.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.140.190	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
79.177.115.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.7.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
78.179.138.68	147.237.77.216	Turkey	dover.idf.il	portscan: TCP Distributed Portscan	1
113.59.33.61	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
66.249.81.212	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.194.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.186.172.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.153.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.70.48.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.117.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.108.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.158.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.243.55.134	147.237.77.216	Dominica	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.8.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.4.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.60.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-21-2016-12:04:03 to 02-21-2016-13:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
46.19.86.131	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.52.187.248	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	17
109.253.131.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.164.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.117.242.171	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
199.168.151.87	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
79.181.104.130	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
176.13.8.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
128.139.19.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.202.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
2.54.42.108	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
212.29.225.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.46.39.132	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.130.238.3	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
85.130.238.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.52.187.248	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.130.238.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.183.175.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.24.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.187.248	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.187.248	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.117.162.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.216.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.62.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.147.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.210.205.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.214.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.174.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.210.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.26.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.208	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
66.249.81.183	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
212.199.57.199	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.199.57.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
89.138.184.216	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
84.228.62.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.148.183	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
82.80.219.164	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

02-21-2016-12:04:03 to 02-21-2016-13:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.124.66	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 81.218.124.66	Block	169
109.253.208.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
109.253.208.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	72
176.13.0.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
79.179.54.50	Israel	147.237.76.39	mobile.meitav.idf.il	Distributed Suspicious Response Code	Block	22
176.13.1.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
2.54.28.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
80.246.138.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
195.154.179.172	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.154.179.172	Block	5
195.154.179.172	France	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
62.90.131.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.17.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
195.154.179.172	France	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 195.154.179.172	Block	3
109.253.139.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
157.55.12.93	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.162.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.226.189	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
79.176.97.99	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	2
176.13.21.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
65.55.210.190	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.182.20	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
195.154.179.172	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.179.54.50	Israel	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.150.168	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$78 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
176.13.8.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.81.218	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1
46.19.85.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.194.203.52	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
195.154.179.172	France	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
2.54.152.228	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
78.110.173.202	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/sendtofriend/sendtofriend.aspx	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
5.102.221.200	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
199.203.37.197	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
109.160.165.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam	Block	1
80.178.227.165	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
2.54.1.210	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Header Name	Block	1
66.249.81.221	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.241	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.19.86.62	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
217.194.206.108	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
176.13.0.37	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
64.79.85.205	United States	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in Method	Block	1
37.26.146.141	Israel	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Open Mode	None	1

02-21-2016-12:04:03 to 02-21-2016-13:04:03