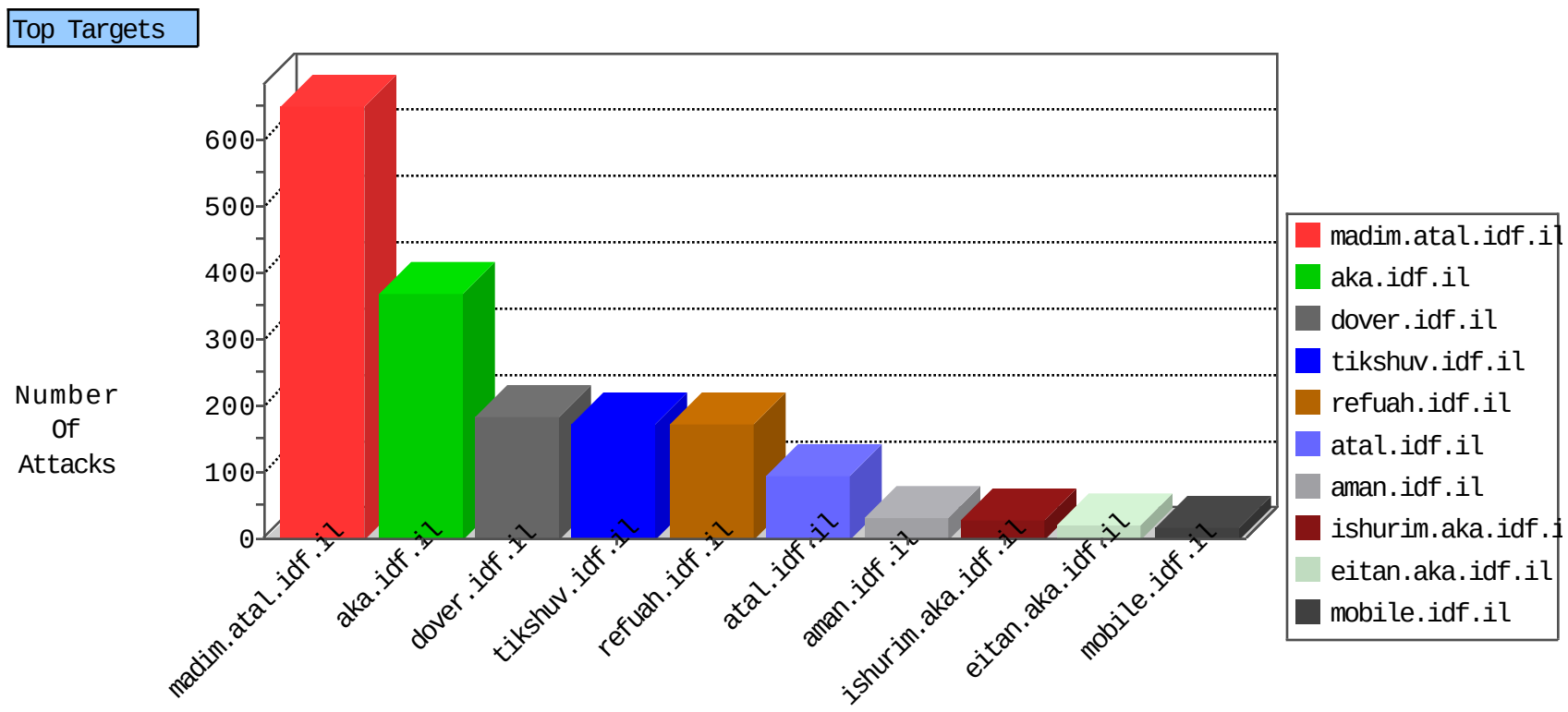
02-21-2016-09:04:04 to 02-21-2016-10:04:04

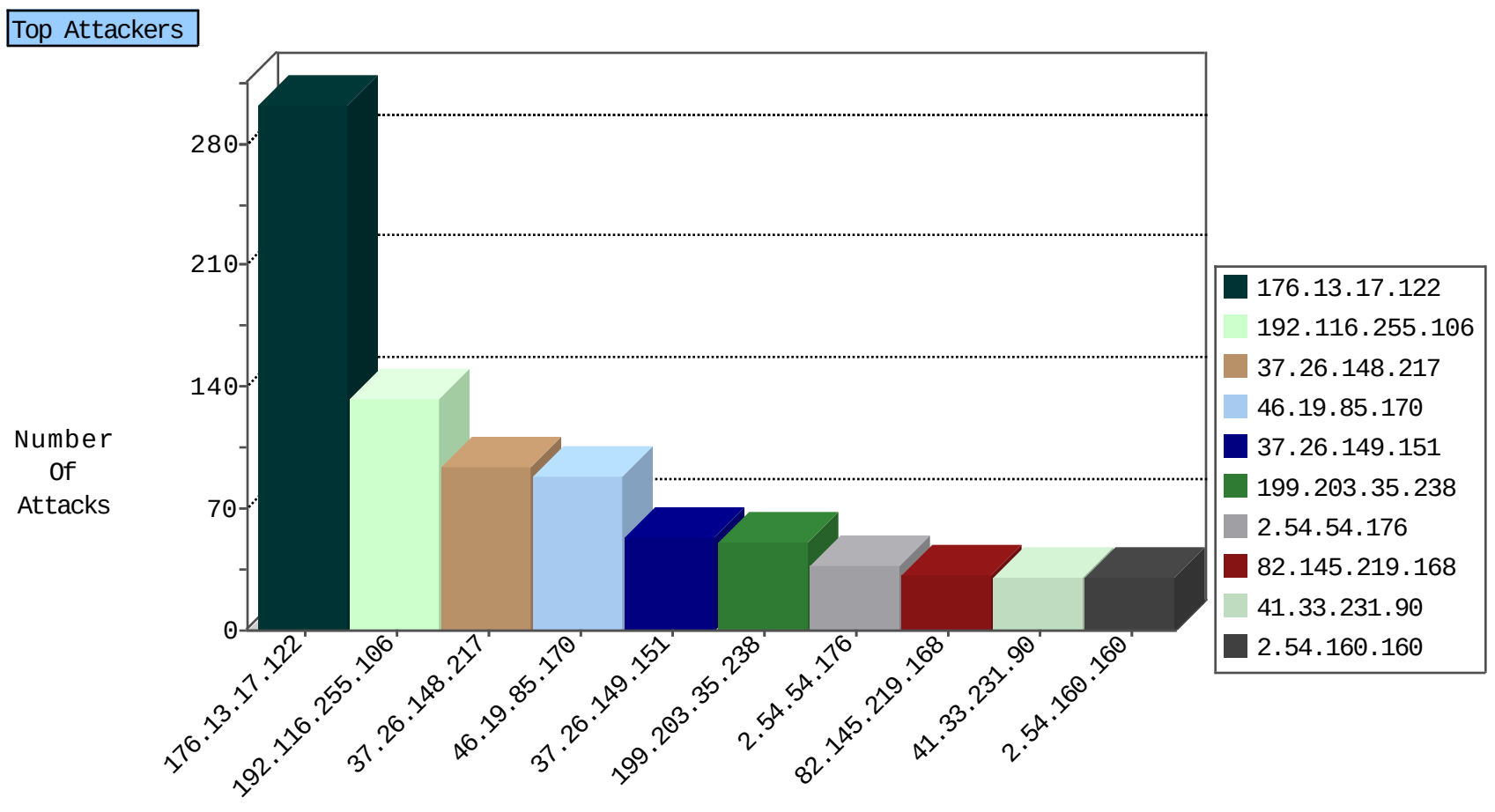
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-21-2016-09:04:04 to 02-21-2016-10:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.210	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	181
115.239.228.10	China	147.237.0.17	m.my-kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	2
115.239.228.10	China	147.237.0.17	m.my-kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1
185.94.111.1		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.7.227.195	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.7.227.196	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

02-21-2016-09:04:04 to 02-21-2016-10:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.3.143	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
84.228.217.94	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
82.166.154.239	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	3
157.55.39.216	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2

02-21-2016-09:04:04 to 02-21-2016-10:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
94.230.93.162	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.71.33.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.40.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.191	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	1
62.219.160.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.130.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
147.236.31.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.50.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.193.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.192.6.154	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.179.8	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-21-2016-09:04:04 to 02-21-2016-10:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.170	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
46.19.85.170	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	36
82.145.219.168	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
2.54.160.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
195.189.193.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
149.78.200.207	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
185.89.217.227		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
185.89.217.233		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
185.89.217.225		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
185.89.217.226		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
46.19.85.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.89.217.235		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
2.52.178.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.17.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.81	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	9
176.13.17.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
185.89.217.228		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
46.242.66.240	Russian Federation	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
185.89.217.230		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
185.89.217.234		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
80.246.136.202	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
185.89.217.232		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
46.19.85.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
64.62.219.89	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.224		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.147.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.150.224	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.44.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.229.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.231		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
82.80.132.76	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.89.217.229		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.26.148.148	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
79.181.197.170	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	4
93.173.200.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.130.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.116.255.106	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
212.143.227.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
132.66.234.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.6.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-21-2016-09:04:04 to 02-21-2016-10:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.17.122	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.17.122	Block	133
192.116.255.106	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 192.116.255.106	Block	120
176.13.17.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
37.26.148.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
37.26.149.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
199.203.35.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
176.13.17.122	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.17.122	Block	49
2.54.54.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
2.54.131.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
80.246.139.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
2.52.144.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	11
109.253.197.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
37.26.148.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
2.54.154.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
46.19.86.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
37.57.231.213	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.57.231.213	Block	4
147.236.38.29	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 147.236.38.29	Block	4
37.57.231.213	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
2.54.23.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.144.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.20.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.251.252	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
176.13.0.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.129.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.168	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$captchaText	Block	2
2.52.183.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.17.235	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
95.86.124.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/&sa=u&ved=0ahukewj3yvf6pyjlahxhbrqkhsyabukqfggimaa&usg=afqjcnh4ucr3bqpmkvh4yz9t7jscutsloq	Block	2
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
80.246.130.217	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.177.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.80.196.44	Block	2
2.52.27.166	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
80.246.138.243	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
132.74.150.53	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1406-he/atal.aspx	Block	1
94.205.92.144	United Arab Emirates	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
81.218.70.243	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/trans.gif	Block	1
184.105.247.195	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
79.180.60.105	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.42	Israel	147.237.77.233	atal.idf.il	Unknown HTTP Request Method px?&l=he&f=1440 in URL	Block	1
31.185.117.233	Bosnia and Herzegovina	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.118.48.248	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
80.246.138.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.201	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1

02-21-2016-09:04:04 to 02-21-2016-10:04:04