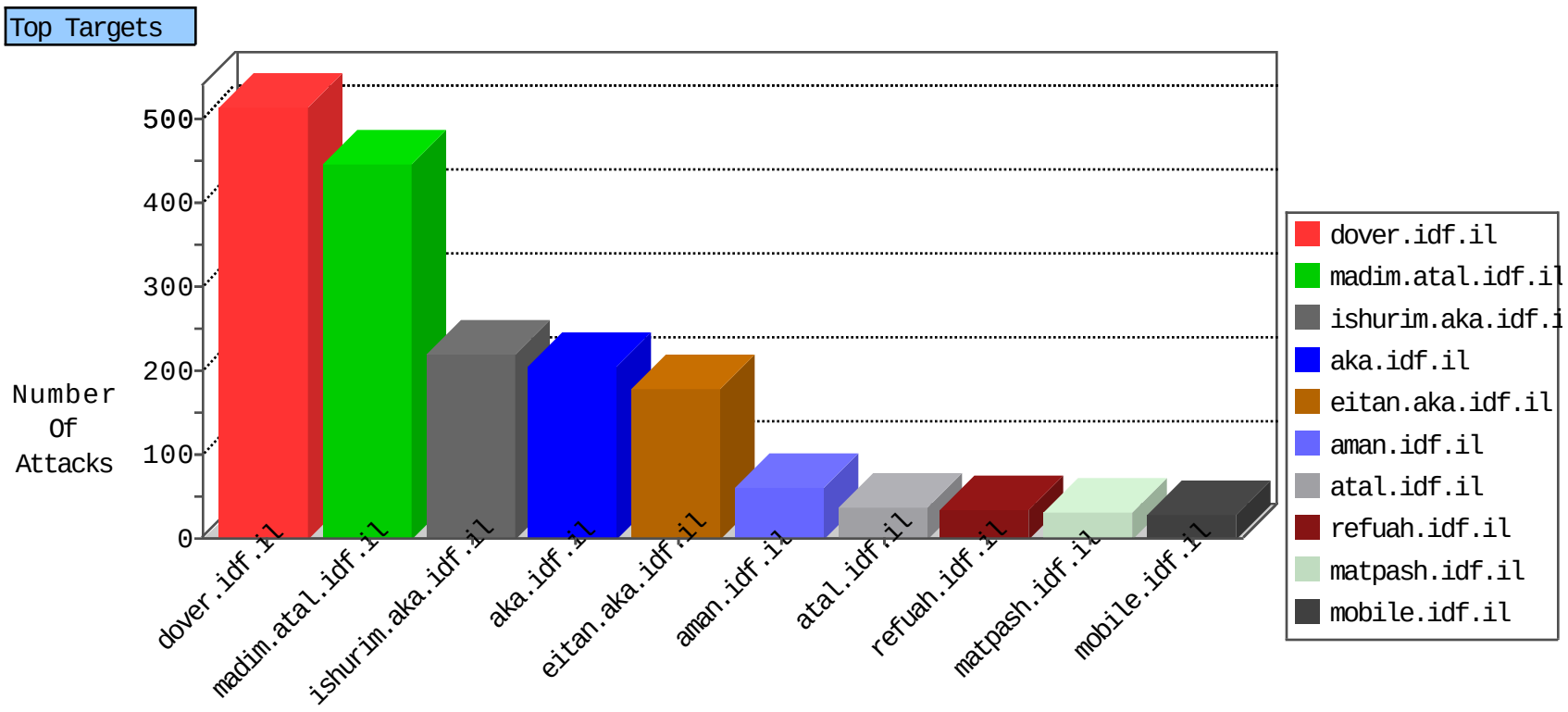
02-14-2016-19:04:01 to 02-14-2016-20:04:01

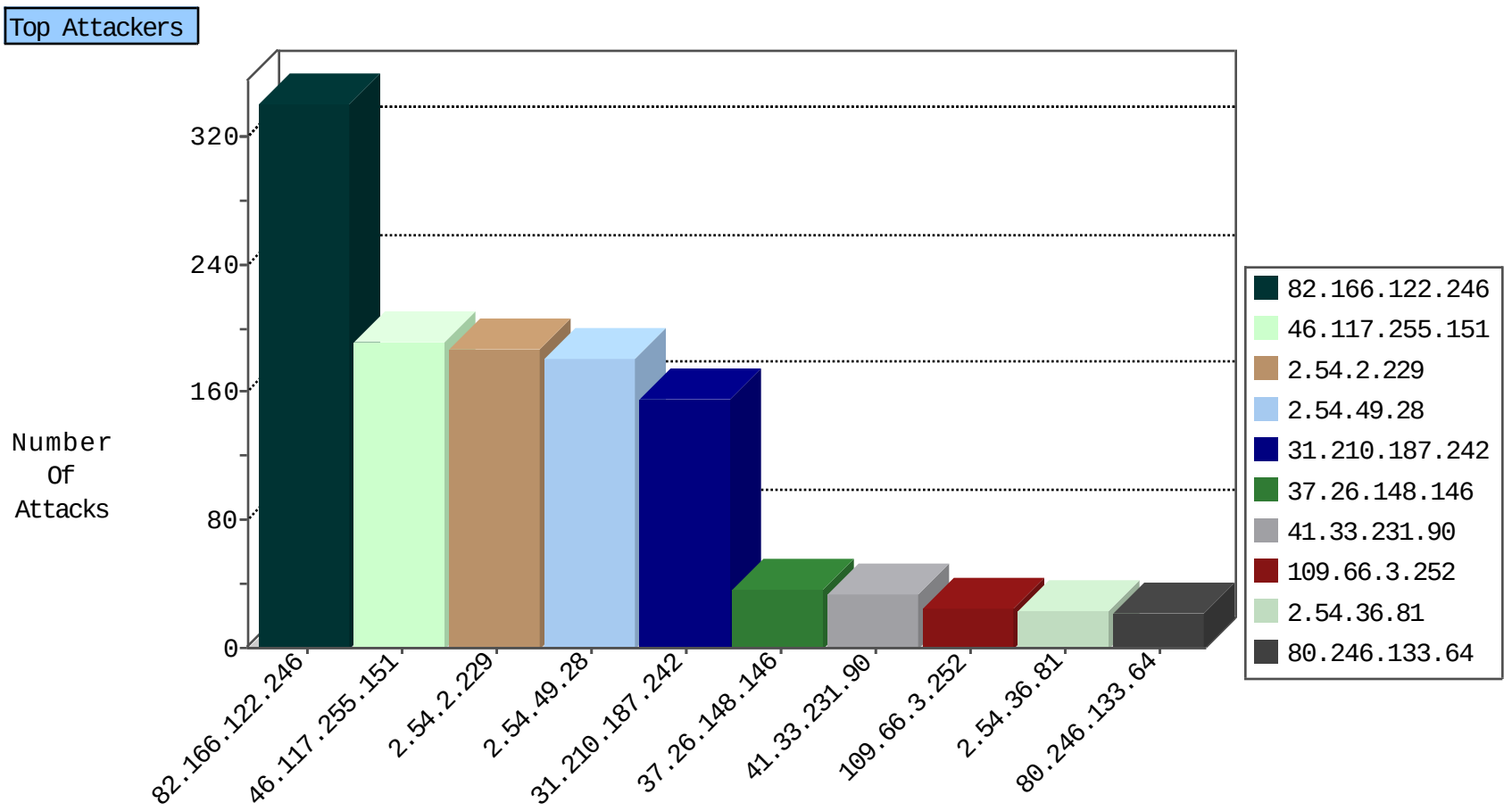
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-14-2016-19:04:01 to 02-14-2016-20:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.146	Israel	147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	26
157.55.39.147	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
201.48.16.165	Brazil	147.237.72.167	ishurim.aka.idf.il	Frk_Under_Attack_Con_Tcp	drop	1
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

02-14-2016-19:04:01 to 02-14-2016-20:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.231	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-14-2016-19:04:01 to 02-14-2016-20:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
132.74.95.21	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
176.223.4.179	147.237.72.217	Romania	e.idf.il	ET SCAN NMAP -sS window 3072	1
79.178.29.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.208.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.216	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.159	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.177	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
89.139.171.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.34.177	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.117.208.243	147.237.76.197		e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.47	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
180.128.252.1	147.237.76.38	Thailand	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
79.180.214.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.223.4.179	147.237.72.217	Romania	e.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.182.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.133.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.97.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.164.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.172.140	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.159	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.177	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.94.171.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
81.182.80.64	147.237.76.44	Hungary	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
190.205.119.220	147.237.72.156	Venezuela	aman.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
79.182.161.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-14-2016-19:04:01 to 02-14-2016-20:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	338
46.117.255.151	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	192
31.210.187.242	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	150
80.246.133.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
46.19.86.84	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
2.54.158.182	Israel	147.237.76.200	eitan.aka.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	12
2.54.28.106	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
84.95.54.83	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	10
79.180.102.231	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.88.94.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.58.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
93.173.237.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.182.116.176	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.3.252	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.53.255	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.147.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.17.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.151.42.39	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.180.188.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.162	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.29.212.105	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.32.179.58	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.66.3.252	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
31.210.187.242	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.148.146	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
37.26.148.146	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.66.3.252	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.178.184.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
188.120.154.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.76.96.31	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.66.3.252	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
31.186.183.83	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.66.3.252	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.131.243	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.206.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.63.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.27.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.34.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.239	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

02-14-2016-19:04:01 to 02-14-2016-20:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.49.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
2.54.2.229	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.2.229	Block	102
2.54.2.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
2.54.49.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
2.54.36.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
2.52.137.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
79.180.24.146	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.180.24.146	Block	14
2.54.131.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	7
23.254.138.210	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 23.254.138.210	Block	5
2.54.7.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.9.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.8.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.135.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.136.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.49.28	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	3
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1842-he/dover.aspx	Block	3
2.54.45.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.49.28	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ********** ********** ********** **********, Observed ********** ********** ********** **********	None	1
85.65.49.191	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.181.8.3	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
2.50.197.241	United Arab Emirates	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.66.90	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/â€Ž	Block	1
128.232.110.28	United Kingdom	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
84.94.42.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
207.46.13.23	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/homepage/	Block	1
79.176.138.167	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	1
37.26.147.209	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
149.78.254.138	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$76 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
85.65.230.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/_vti_bin/webs.asmx	Block	1
80.246.133.64	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
176.13.17.248	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
141.0.15.39	Europe	147.237.77.176	matpash.idf.il	Parameter Type Violation search in www.cogat.idf.il/1035-ar/cogat.aspx	Block	1
2.54.25.197	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
84.108.186.33	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
212.179.3.44	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
79.177.33.69	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$3 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
37.26.148.146	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
149.88.187.112	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/112457.pdf	Block	1
93.173.40.156	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18485-he/dover.aspx	Block	1
178.40.135.110	Slovakia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1785-he/dover.aspx	Block	1
141.212.122.112	United States	147.237.76.39	mobile.meitav.idf.i	Unauthorized URL Access to /x	Block	1
84.108.186.33	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
212.179.3.44	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/xmlrpc.php	Block	1
79.178.51.30	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.86.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.218	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/giyus/qanda/default.asp	None	1
109.66.0.22	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.66.0.22	Block	1

02-14-2016-19:04:01 to 02-14-2016-20:04:01