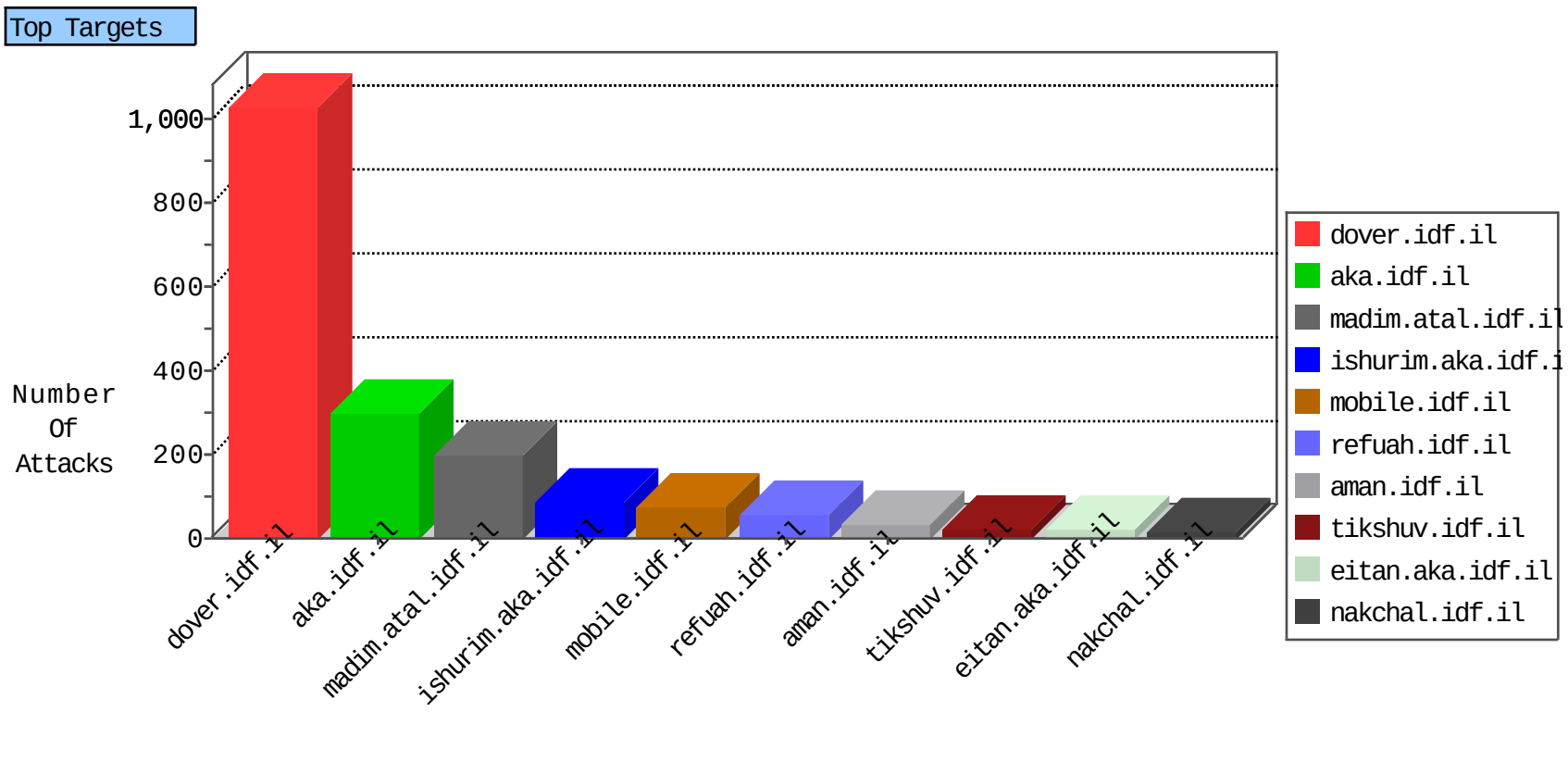
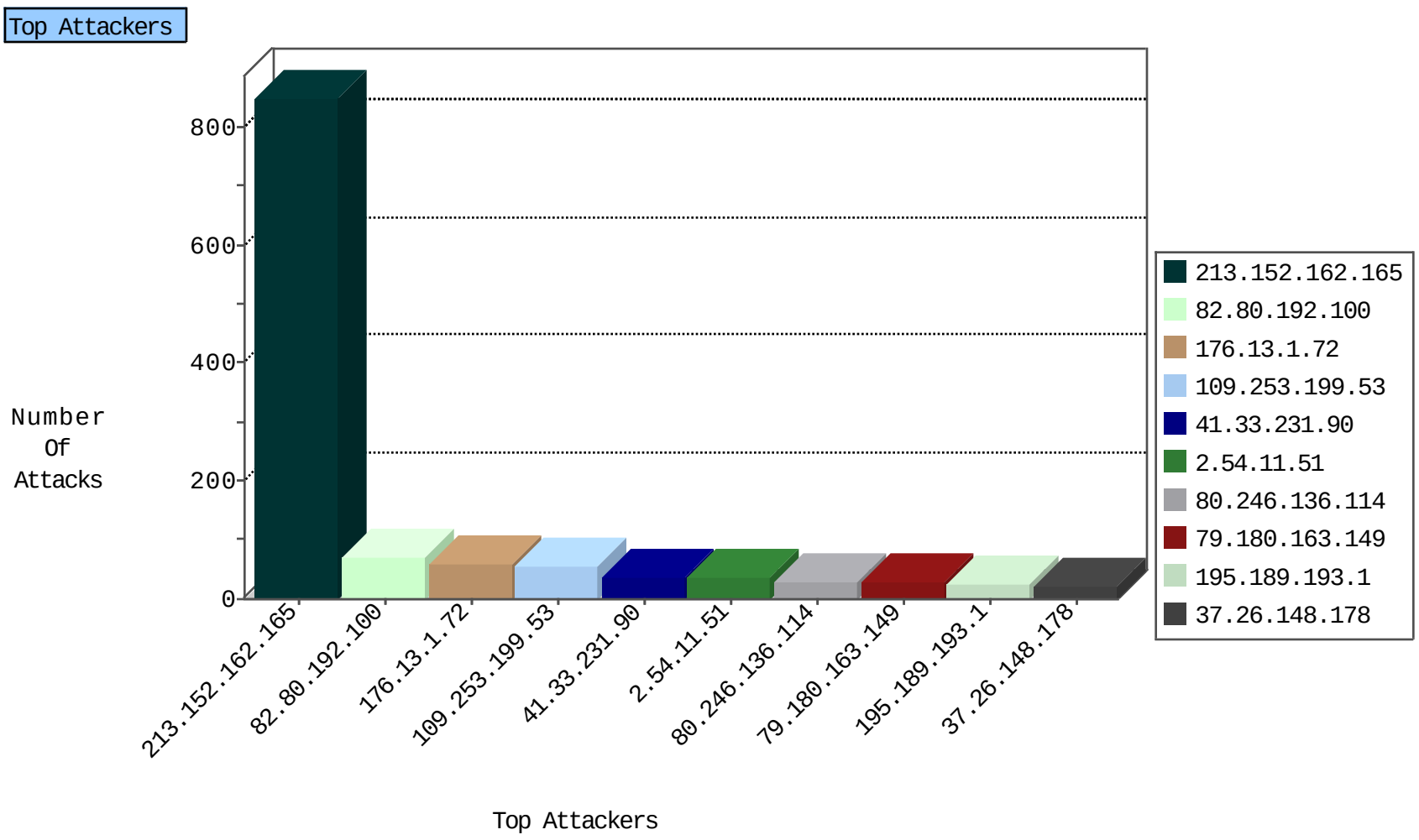
02-21-2016-08:04:01 to 02-21-2016-09:04:01

IDF Under Attack
Daily Report





02-21-2016-08:04:01 to 02-21-2016-09:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.152.162.165	Netherlands	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	3166
213.152.162.165	Netherlands	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1711
213.152.162.165	Netherlands	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	144
70.199.77.29	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	5
213.152.162.165	Netherlands	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
198.20.70.114	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets_Con_Limit	drop	3
208.67.1.70	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
66.249.64.195	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
208.67.1.70	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.70	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
216.238.145.2	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

02-21-2016-08:04:01 to 02-21-2016-09:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
138.134.102.15	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
46.19.85.96	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
209.88.183.193	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1

02-21-2016-08:04:01 to 02-21-2016-09:04:01

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
84.94.97.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.174.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.115.113.89	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.249	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.15.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.120.153.246	147.237.8.24	Russian Federation	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
91.208.139.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
74.201.85.87	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.203.239.133	147.237.77.121	Pakistan	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
93.120.153.246	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN Potential SSH Scan	1
93.120.153.246	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN Potential SSH Scan	1

02-21-2016-08:04:01 to 02-21-2016-09:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.152.162.165	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	610
213.152.162.165	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	93
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
80.246.136.114	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
195.189.193.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
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
46.19.86.203	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.108	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
79.177.38.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.52.229	Israel	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	8
80.246.139.73	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.26.148.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
64.19.78.242	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
82.166.190.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
109.253.206.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.3.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.158	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.113.242.177	Ukraine	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.125.109.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.180.213	Israel	147.237.72.156	aman.idf.il	SYN Attack		reject	6
37.26.148.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.146.6.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.185.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.236.238.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
149.78.96.42	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.248	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
2.54.180.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
62.219.164.85	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.180.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.77	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
2.54.180.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
46.116.255.77	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
66.249.93.56	Israel	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
46.121.29.39	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.26.148.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.66.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.54.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.153.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.192.100	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 82.80.192.100	Block	70
176.13.1.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
109.253.199.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
2.54.11.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
79.180.163.149	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.163.149	Block	26
2.54.23.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.13.4.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
37.26.149.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.52.144.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.203	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
95.86.115.160	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 95.86.115.160	Block	4
80.246.136.114	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.17.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
209.88.183.193	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
109.253.194.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.197.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.116.255.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.2.80	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
46.19.85.213	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
2.54.143.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.72.221	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$78 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
95.86.122.30	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
37.26.148.220	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtID in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
209.88.183.193	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 209.88.183.193	Block	2
82.81.14.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.206.191	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
95.86.115.160	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1824-he/dover.aspx	Block	1
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method .; in URL _pk_ses.20.8afc=*	Block	1
84.36.245.163	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/	Block	1
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
79.180.163.149	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/images/common/hrhorizontal.gif"	Block	1
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
124.82.223.21	Malaysia	147.237.72.167	ishurim.aka.idf.i	PHP Attempt	Block	1
38.81.65.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
209.88.183.193	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/back.png	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	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
79.182.109.92	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
195.189.193.1	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
131.253.25.245	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sa_swfobject.js	Block	1
40.77.167.44	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
95.86.115.160	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
212.117.157.74	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation search in www.logistics.atal.idf.il/1205-he/halag.aspx	Block	1
82.80.192.100	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many 404: Response Code per Session	Block	1