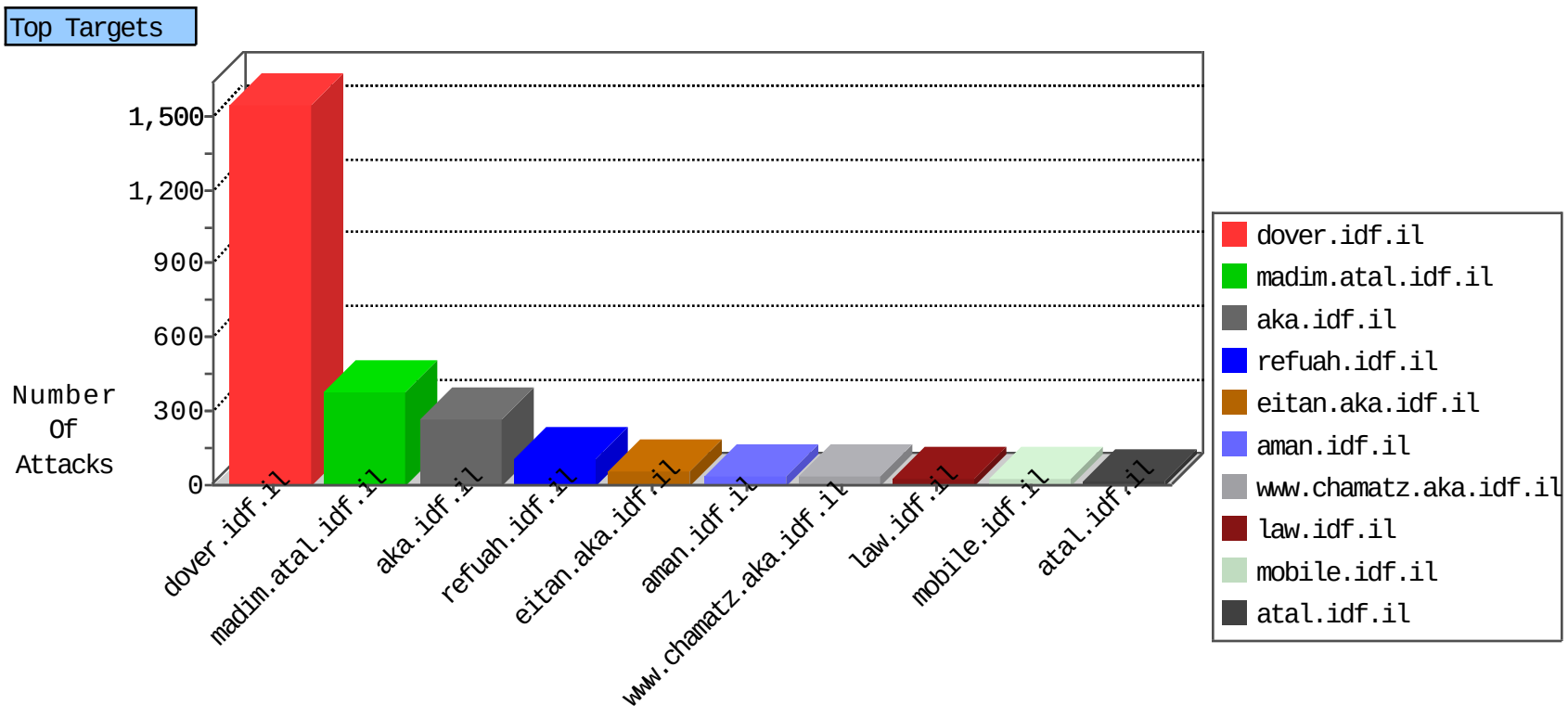
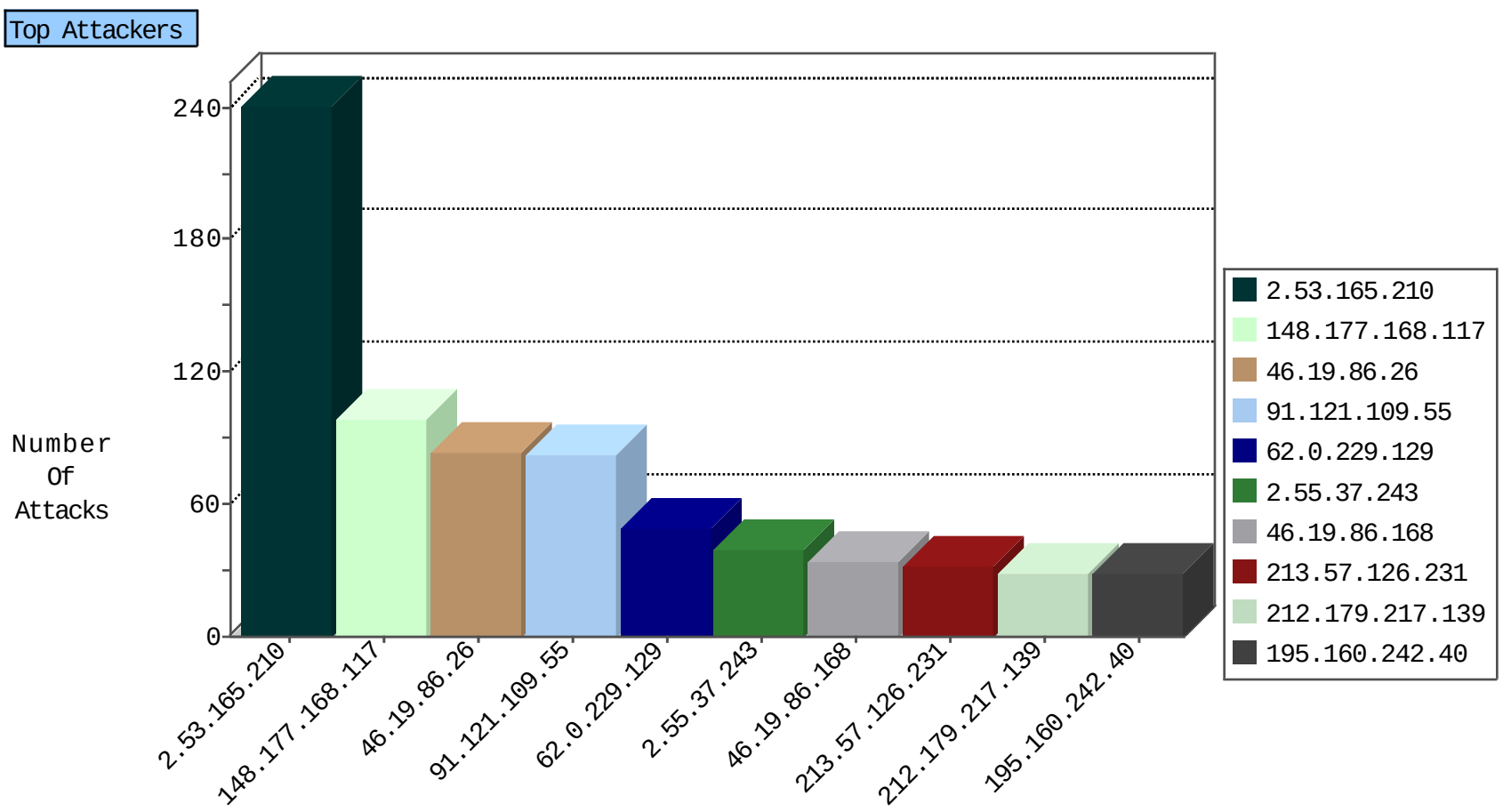
09-27-2016-11:04:08 to 09-27-2016-12:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-27-2016-11:04:08 to 09-27-2016-12:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.44.134.113	Denmark	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3011
85.130.139.108	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1307
66.249.69.228	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1179
85.255.7.155	Poland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	201
176.13.10.187	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
81.218.67.234	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
46.19.85.92	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
212.150.177.116	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
81.218.135.136	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
93.172.121.185	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
2.55.136.76	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
107.191.45.125	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
93.158.200.70	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
46.19.85.180	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.136.2	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
46.19.86.239	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.174.94.235	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1

09-27-2016-11:04:08 to 09-27-2016-12:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.121.109.55	France	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	52
91.121.109.55	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	16
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	10
91.121.109.55	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	8
91.121.109.55	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-27-2016-11:04:08 to 09-27-2016-12:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.83	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	2
217.132.102.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.48.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.149.222.5	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.228.13	147.237.77.226	Israel	www.chamatz.aka.idf.il	LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file	1
203.106.184.157	147.237.72.156	Malaysia	aman.idf.il	ET SCAN NMAP -sS window 4096	1
37.26.149.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.48.200.59	147.237.76.44	Peru	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
5.45.62.172	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	1
185.129.148.230	147.237.77.227	Latvia	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.144.18	147.237.76.201	Switzerland	e.atal.idf.il	ET SCAN Potential SSH Scan	1
109.65.15.17	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.70.22.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.25.65.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.212.207.80	147.237.8.50	India	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.48.200.59	147.237.76.44	Peru	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
31.154.19.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.178.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.53.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.93.185.10	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
179.43.144.18	147.237.76.199	Switzerland	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
87.71.6.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.102.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-27-2016-11:04:08 to 09-27-2016-12:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
148.177.168.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
213.57.126.231	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
62.0.229.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
109.253.144.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
62.0.229.129	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	19
148.177.168.116	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
2.53.190.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
2.81.180.122	Portugal	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.82	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
37.26.149.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
198.240.212.2	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.55.162.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
158.169.40.9	Belgium	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.168	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
185.120.124.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
80.246.138.85	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
2.55.37.243	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
176.13.14.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.173	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
2.55.37.243	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
62.0.227.33	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
176.13.244.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.179.217.139	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.82	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
194.114.146.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.179.217.139	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.179.217.139	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
2.53.14.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
192.114.91.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.253.136.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.168	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
46.19.86.148	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.120.35.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
141.226.162.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.176.54.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.67.146.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
31.168.118.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.116.166.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.120.186.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.125.37.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

09-27-2016-11:04:08 to 09-27-2016-12:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.165.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	241
46.19.86.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
2.53.156.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
132.64.217.111	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	8
37.26.149.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	7
176.13.238.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.136.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.129.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	5
132.64.217.111	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 132.64.217.111	Block	5
82.80.55.63	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/he/navy.aspx	Block	4
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
46.19.86.165	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	4
176.13.236.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.210.206.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
109.253.218.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.228	Block	3
81.218.251.252	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	3
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
46.19.85.226	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	2
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	2
109.253.142.164	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
217.194.197.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.139.33.36	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	2
2.55.23.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.84.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
31.154.36.100	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9	Block	1
81.218.57.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.102.175	France	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.14.187	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general	Block	1
84.95.226.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
46.19.85.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl41 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
2.55.132.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
79.181.56.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
75.190.16.11	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
188.163.107.176	Ukraine	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/blog/	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
37.26.147.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.198.183	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan	Block	1
2.53.53.201	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
84.111.157.224	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.69.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1

09-27-2016-11:04:08 to 09-27-2016-12:04:08