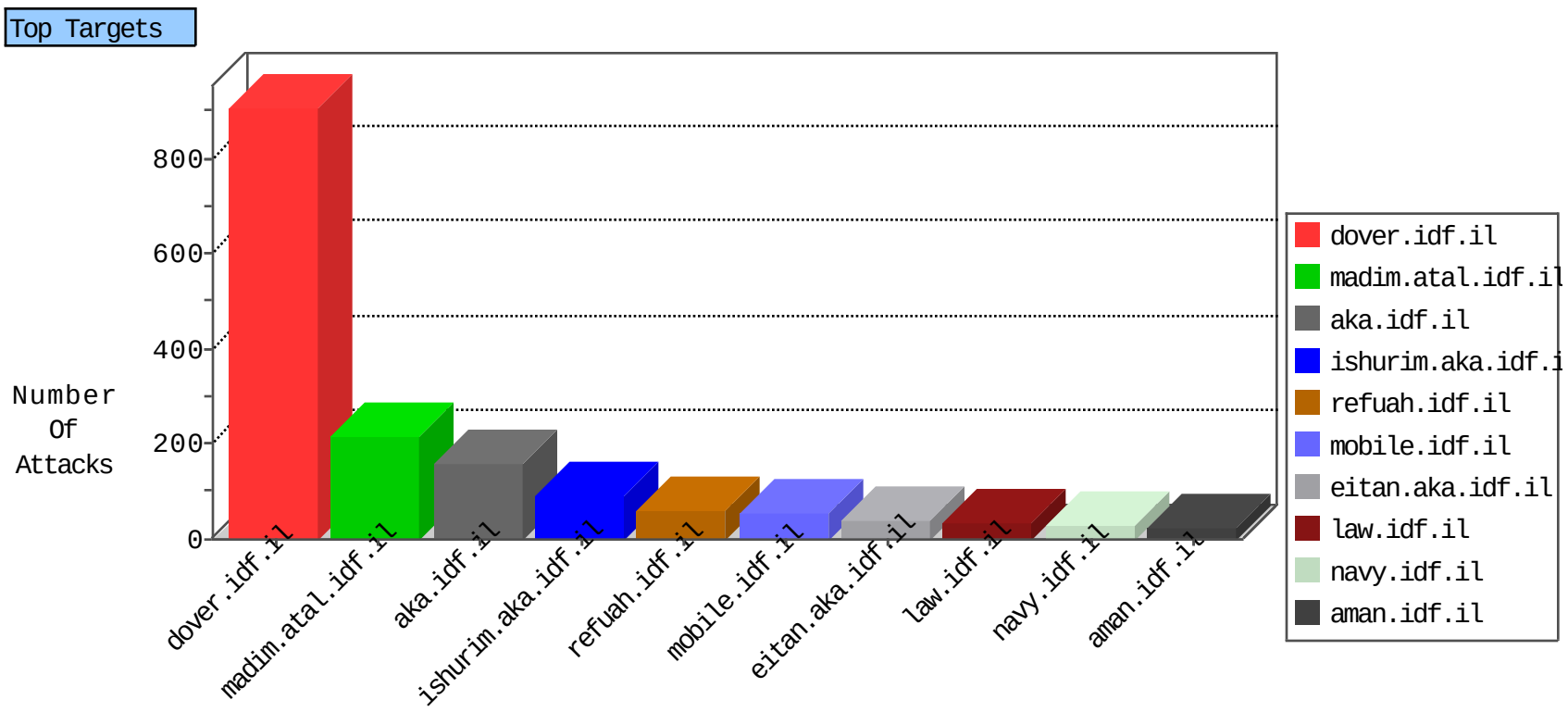
09-22-2016-09:04:00 to 09-22-2016-10:04:00

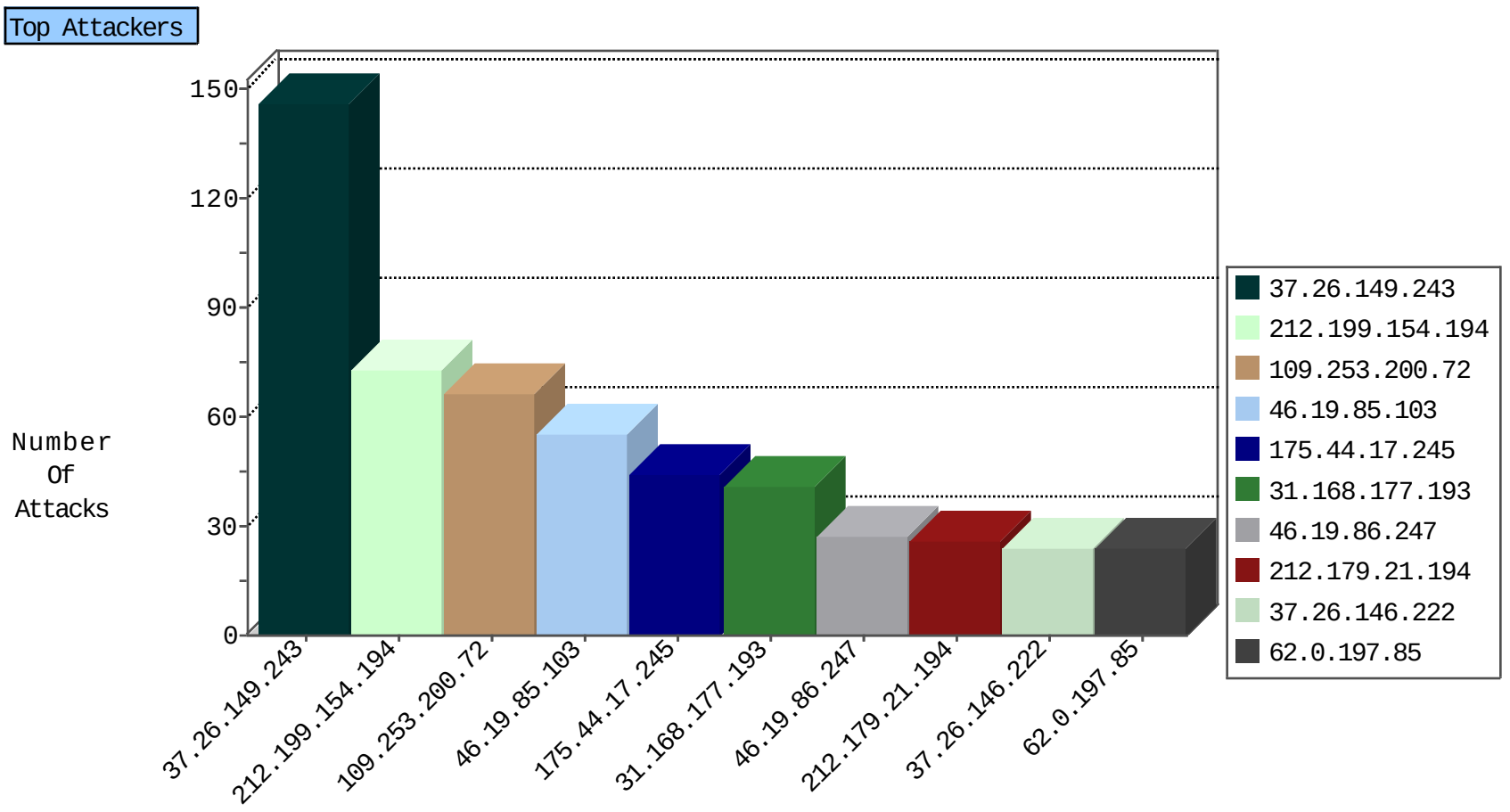
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-22-2016-09:04:00 to 09-22-2016-10:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	444
84.94.208.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
109.253.201.108	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
218.44.145.54	Japan	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	3
45.32.205.133	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1
66.240.219.146	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
5.29.112.129	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-22-2016-09:04:00 to 09-22-2016-10:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
36.110.147.67	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-22-2016-09:04:00 to 09-22-2016-10:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
211.149.246.60	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.146.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.234.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.14.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
118.103.126.194	147.237.8.46	Japan	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
89.138.176.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.111.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.117.59.18	147.237.72.166	Egypt	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.177.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.48.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.101.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.238.45	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
31.154.53.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.115.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.1.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.11.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.193.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.135.187.19	147.237.77.216	Czech Republic	dover.idf.il	portscan: TCP Distributed Portscan	1
41.230.31.128	147.237.76.86	Tunisia	navy.idf.il	ET SCAN NMAP -sS window 3072	1

09-22-2016-09:04:00 to 09-22-2016-10:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.168.177.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	36
46.19.86.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
37.26.146.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
79.180.238.213	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
109.253.200.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
62.0.197.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.103	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	13
192.116.218.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
141.226.162.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
213.57.70.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.146.251	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
31.146.114.66	Georgia	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
109.253.215.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
87.70.52.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
62.0.197.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.188.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
176.13.5.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.85.103	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.249.76.19	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.253.218.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.103	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
176.228.36.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.103	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
212.235.113.28	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.53.161.62	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
62.0.197.85	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
109.253.145.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
199.203.215.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.148.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.158.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.146.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.200.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.149.248	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
2.55.30.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.219.128.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
81.218.137.70	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
109.64.107.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.183.41.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.211.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.147.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.64.163	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

09-22-2016-09:04:00 to 09-22-2016-10:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	138
109.253.200.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
175.44.17.245	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 175.44.17.245	Block	17
175.44.17.245	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 175.44.17.245	Block	14
212.199.112.144	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	11
109.253.196.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
175.44.17.245	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	5
175.44.17.245	China	147.237.77.74	law.idf.il	PHP Attempt	Block	5
212.199.112.144	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	3
109.253.231.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.3.188	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
2.53.191.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.213.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.219.145.163	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/205-he/patzar.aspx	Block	2
217.194.196.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.102.9.30	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
192.115.134.93	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
31.210.186.60	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
46.19.85.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
175.44.17.245	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
66.249.64.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.26.146.207	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/guyus/	Block	1
85.250.114.255	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
212.199.154.194	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.199.154.194	Block	1
2.55.137.11	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
180.97.106.161	China	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in Method from 180.97.106.161	Block	1
66.249.76.19	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
198.20.69.74	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/robots.txt	Block	1
175.44.17.245	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.asp	Block	1
91.135.111.85	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/default.aspx "/mf1/e_shemesh2008$/desktop/שירותים/web/פורטל.lnk"	Block	1
46.135.187.19	Czech Republic	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
213.151.55.217	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
180.97.106.161	China	147.237.77.176	matpash.idf.il	Multiple NULL Character in Method from 180.97.106.161	Block	1
81.218.135.161	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
212.179.42.226	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
2.53.143.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.250.205	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
185.32.179.10	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.153	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
46.19.85.8	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.190.15	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1

09-22-2016-09:04:00 to 09-22-2016-10:04:00