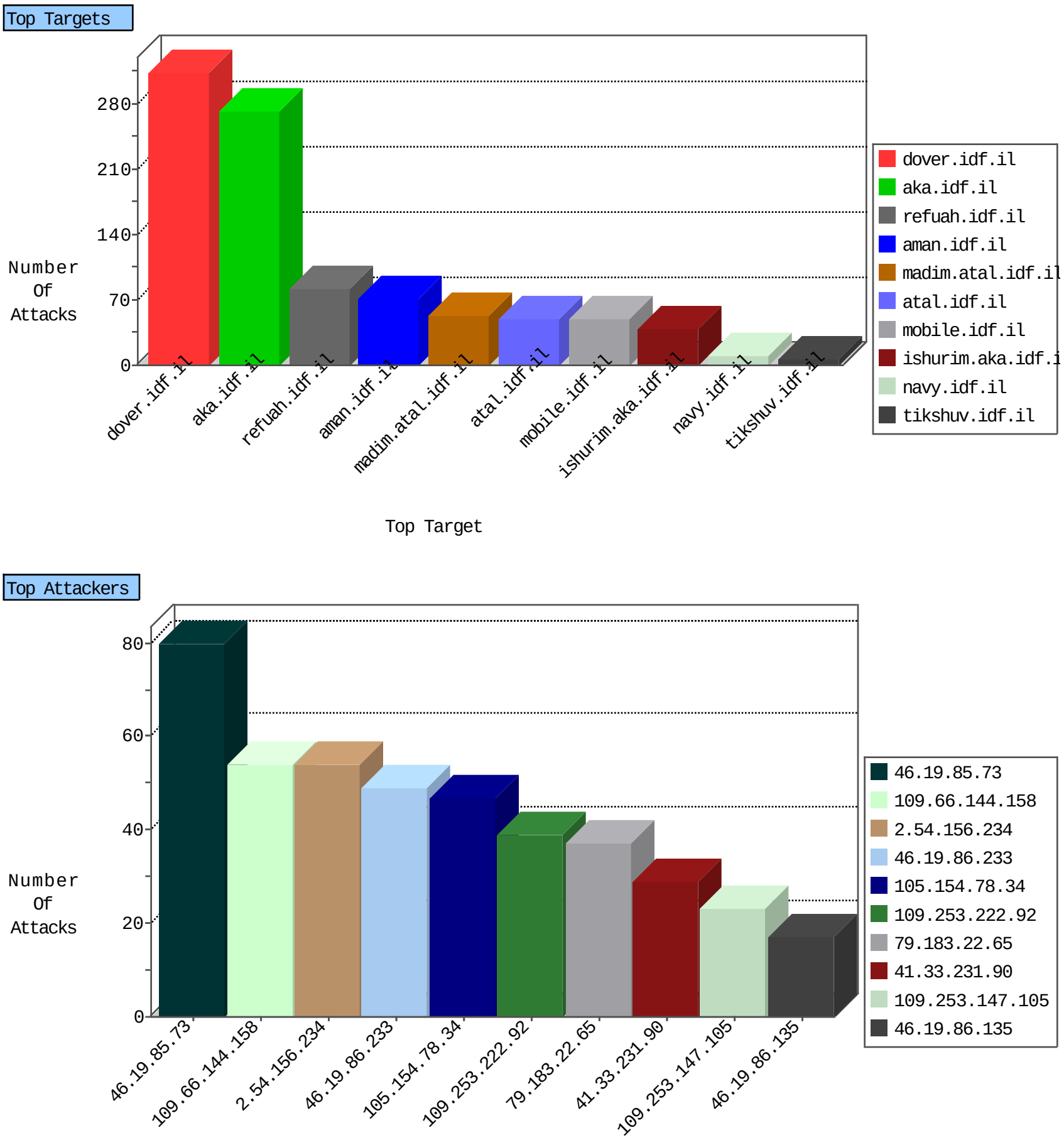
02-15-2016-15:04:04 to 02-15-2016-16:04:04

IDF Under Attack
Daily Report



02-15-2016-15:04:04 to 02-15-2016-16:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.73	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	42
105.154.78.34	Morocco	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
109.253.215.38	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
203.198.226.219	Hong Kong	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	3
84.228.177.151	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
2.54.186.35	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
107.150.60.77	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
46.117.239.0	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
93.158.203.154	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
84.228.238.19	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
107.150.60.76	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
171.108.29.119	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
93.158.203.154	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

02-15-2016-15:04:04 to 02-15-2016-16:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-15-2016-15:04:04 to 02-15-2016-16:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
149.78.207.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.64.213.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.84.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.102.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.156.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.195	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.161.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.165.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.105.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.60.248	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.34.57.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-15-2016-15:04:04 to 02-15-2016-16:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.66.144.158	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
105.154.78.34	Morocco	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	38
46.19.86.233	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.183.22.65	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
46.19.85.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
2.54.156.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
46.19.86.135	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.86.233	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
109.253.197.92	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
79.177.158.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.73	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
84.111.180.57	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
2.54.138.129	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.156.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
2.54.156.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
2.54.156.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.156.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
2.52.150.14	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.126.59		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.17.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.118.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.173.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.254.77	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
149.78.228.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.26.246	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
199.203.215.1	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.179.189.94	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
23.27.220.220	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
79.183.254.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
197.8.33.140	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.183.254.77	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
217.132.250.173	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.203.215.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.194.84.106	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.230.43.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.35.199.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.116.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.238.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.0.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.84.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.103.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.160.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

02-15-2016-15:04:04 to 02-15-2016-16:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.222.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
109.253.147.105	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	23
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.131.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.250.233.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.252	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
2.54.136.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.88.68.135	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.5.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	2
109.253.197.92	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
46.35.253.161	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation lang in www.law.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
87.69.62.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
5.22.135.156	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8/4148.pdf&gt	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
149.210.247.49	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/arabic/pages/default.aspx	Block	1
46.19.86.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
109.67.118.106	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.183.22.65	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
207.46.13.111	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16648-en/dover.asp	Block	1
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
10.104.40.143		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×¢×Ÿ×˜×•×“	Block	1
95.86.65.67	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.180.126.231	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-13372-he/dover.aspx	Block	1
157.55.39.28	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/main/stm	Block	1
109.67.202.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	1
207.46.13.187	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation ForumId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
132.71.96.64	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
62.90.235.67	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
95.86.125.3	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.75.20	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
157.55.39.62	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1360-he/atal.aspx	Block	1
109.253.133.174	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
46.35.253.161	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation DocID in www.law.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.241.237.211	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/general/general.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
62.219.225.96	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.mag.idf.il/602-2265-he/patzar.aspx	Block	1
46.19.85.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
104.194.26.205	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl91 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.35.253.161	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation folderid in www.law.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
2.54.186.77	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1

02-15-2016-15:04:04 to 02-15-2016-16:04:04