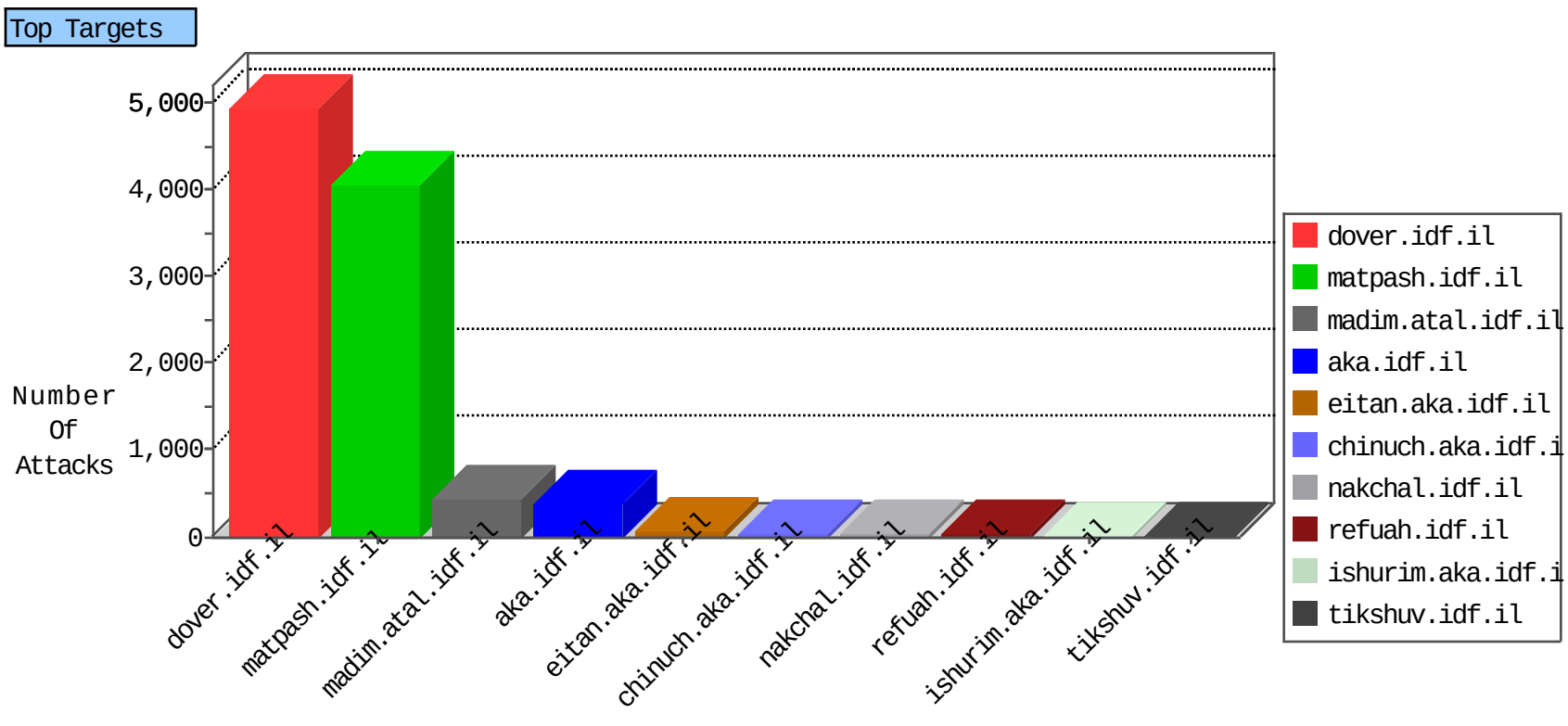
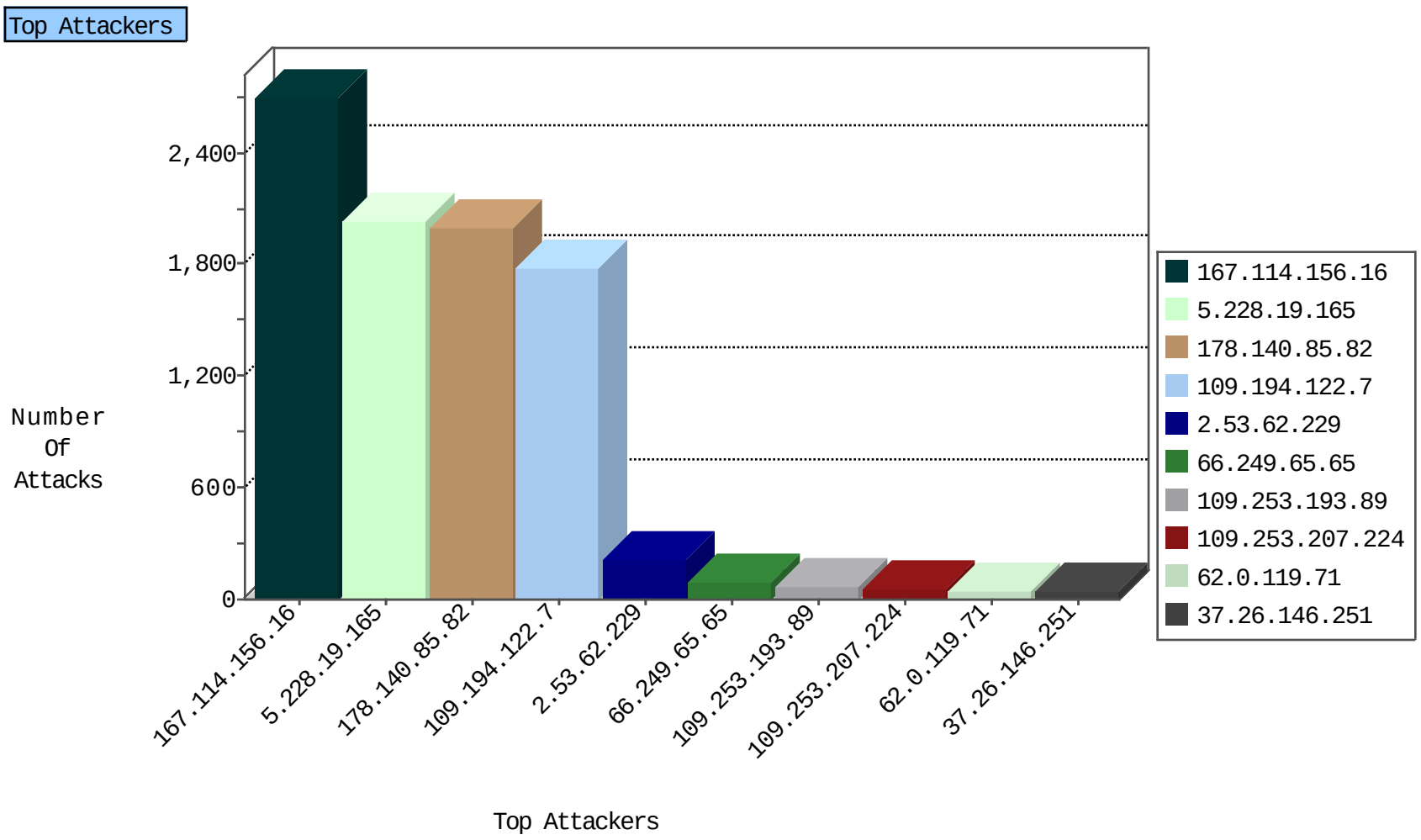
05-04-2016-14:04:03 to 05-04-2016-15:04:03

IDF Under Attack
Daily Report

Top Targets



Top Attackers



05-04-2016-14:04:03 to 05-04-2016-15:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2217
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	4
209.126.136.2	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
209.126.136.2	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
198.20.70.114	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

05-04-2016-14:04:03 to 05-04-2016-15:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-04-2016-14:04:03 to 05-04-2016-15:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.253.144.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.155	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.140.253.9	147.237.76.39	Morocco	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
5.29.182.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
181.194.52.255	147.237.72.166	Costa Rica	aka.idf.il	portscan: TCP Distributed Portscan	1
123.249.3.48	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.127.99	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.134.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.132	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.140.253.9	147.237.76.39	Morocco	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
2.53.182.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.217.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

05-04-2016-14:04:03 to 05-04-2016-15:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1890
5.228.19.165	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1378
178.140.85.82	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1369
109.194.122.7	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1292
5.228.19.165	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	647
178.140.85.82	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	619
109.194.122.7	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	488
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	92
62.0.119.71	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
2.55.156.154	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
37.26.146.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
62.0.34.177	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	28
176.13.16.213	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.142.125.227	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
62.219.117.118	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
162.243.71.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
162.243.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.246.136.171	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.108.104.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	9
80.246.130.63	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.228.19.165	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.142.125.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
5.34.164.224	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.121.80.30	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
80.246.130.63	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
149.88.12.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.46.84.213	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.151	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.108.104.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.64.113.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.118.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.110.17.24	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.130.63	Israel	147.237.0.34	tikshuv.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	6
87.71.106.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.55.134.87	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.244.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.62.153.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
132.66.227.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

05-04-2016-14:04:03 to 05-04-2016-15:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.62.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	214
109.253.193.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
109.253.207.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	56
37.26.146.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
176.13.14.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
46.19.85.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.134.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
84.111.91.185	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	4
79.180.109.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.1.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
95.35.185.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
195.77.247.14	Spain	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
131.253.25.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.234	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.11.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.185.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
131.253.25.175	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.246.137.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.22.129.140	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	2
134.191.232.68	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.111.91.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/6/	Block	1
31.154.33.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sacharqloging	Block	1
213.57.193.200	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2331.jpg	Block	1
37.26.147.185	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile	Block	1
81.218.241.25	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	1
2.53.171.162	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$txtPassword in www.aka.idf.il/main/giyus/faq.aspx	None	1
66.249.93.32	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	1
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.249	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
37.26.146.181	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
213.185.86.107	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.185.86.107	Block	1
79.180.136.140	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1119-he/nakhal.aspx	Block	1
66.249.73.179	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
37.26.148.138	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
81.218.241.25	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/1	Block	1
66.249.93.115	Israel	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../../images/shared/menustrech.png	Block	1
141.212.122.145	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
46.116.223.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
103.231.241.37	Philippines	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
79.181.162.216	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
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2808.jpg	Block	1
84.108.144.210	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
2.53.191.55	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
199.203.62.164	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/1321-he/refuah.aspc	Block	1
66.249.93.180	Israel	147.237.72.166	aka.idf.il	URL is Above Root Directory www.aka.idf.il/../images/search.jpg	Block	1
164.132.161.70	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/	Block	1
46.161.62.44	Kazakstan	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1133-he/dover.aspx	Block	1

05-04-2016-14:04:03 to 05-04-2016-15:04:03