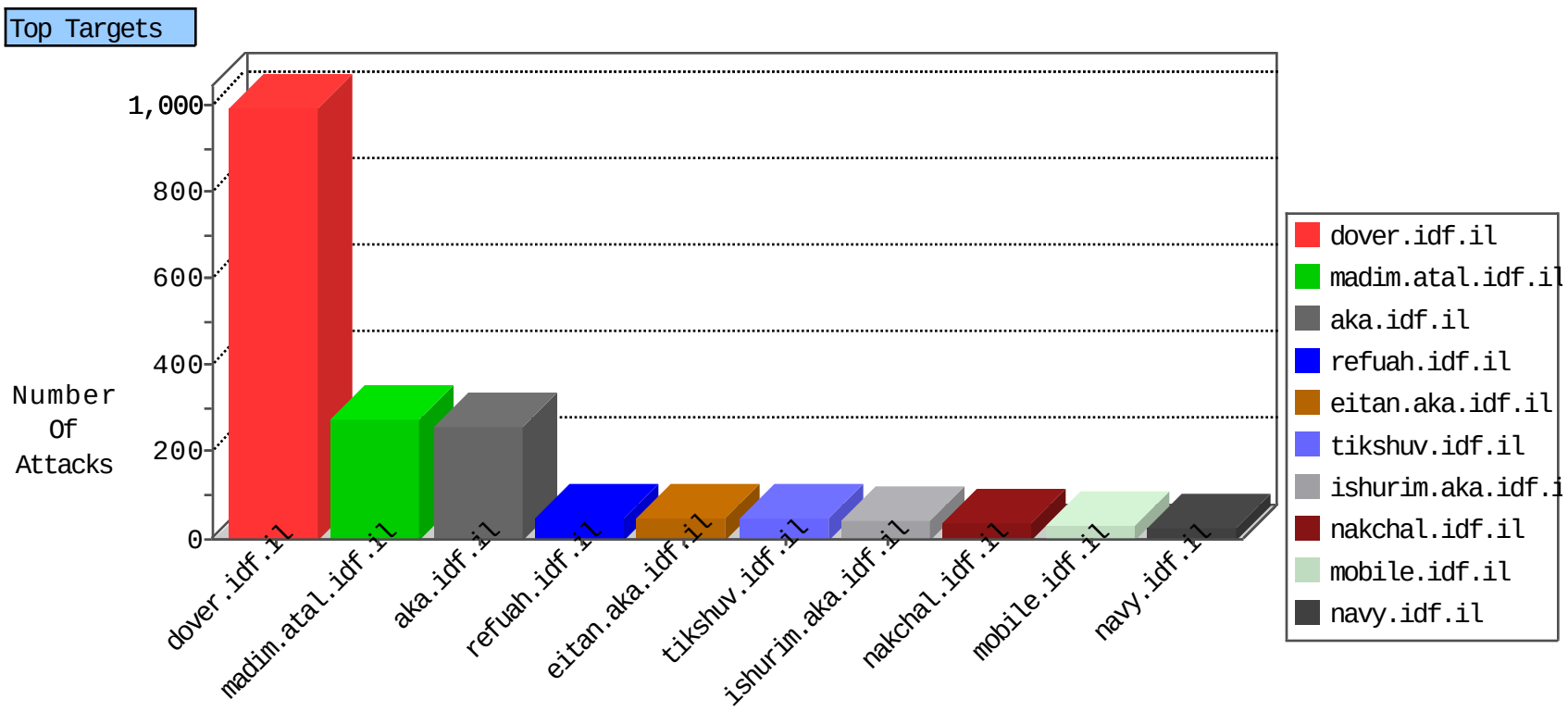
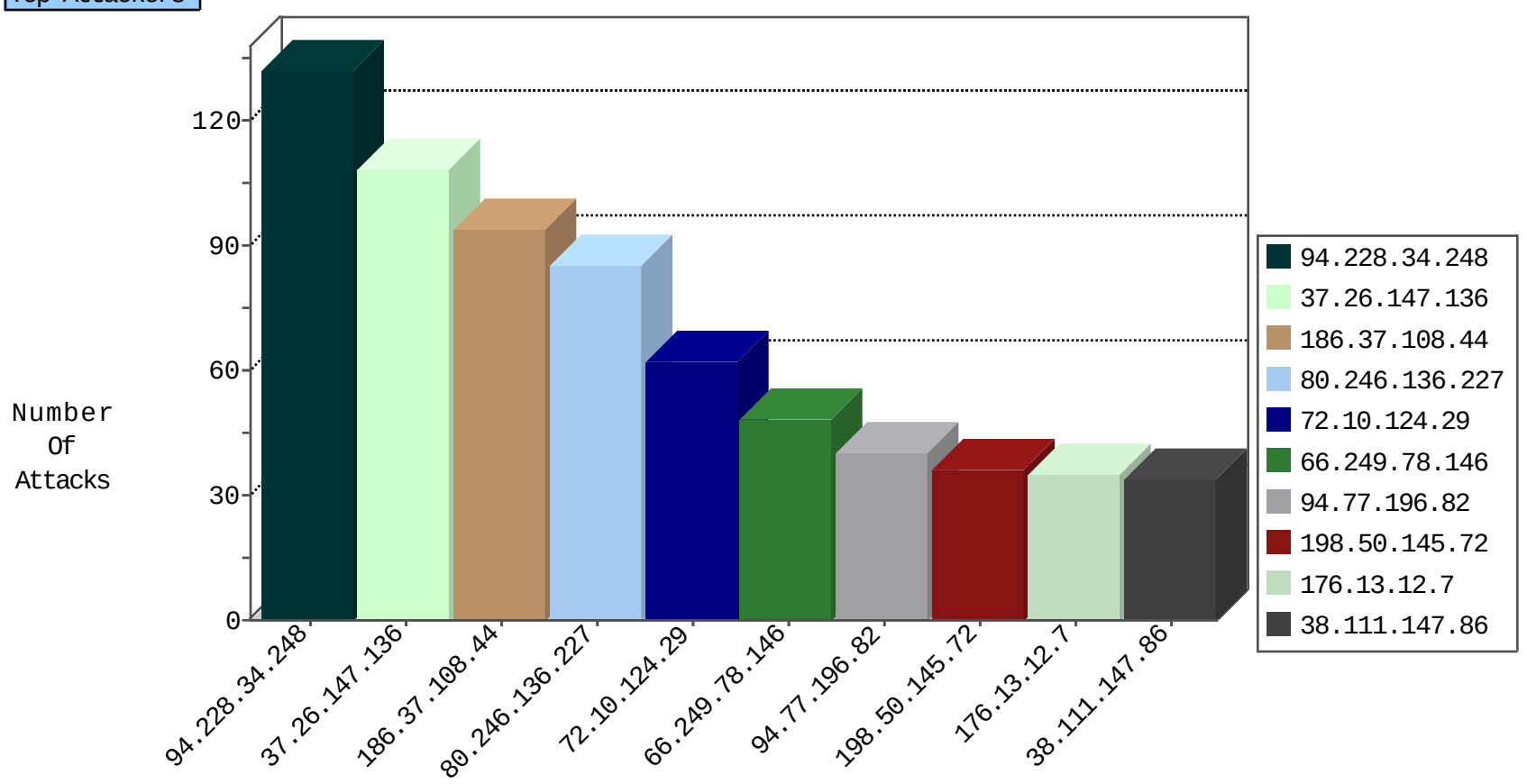
05-04-2016-16:04:02 to 05-04-2016-17:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-04-2016-16:04:02 to 05-04-2016-17:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.202.193	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2606
185.56.28.67	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
209.126.136.2	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
185.130.5.56	Lithuania	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
185.130.5.56	Lithuania	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.56	Lithuania	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

05-04-2016-16:04:02 to 05-04-2016-17:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-04-2016-16:04:02 to 05-04-2016-17:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.22.129.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
208.100.26.228	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.239.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
31.168.180.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.111.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.96.38	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.55.5.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.165.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.245.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.41.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.76.95.25	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
197.195.88.91	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.64.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.146.6.2	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
13.92.245.177	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
147.236.31.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.214.25.64	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.169.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.121.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.57.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.76.95.25	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
46.117.134.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

05-04-2016-16:04:02 to 05-04-2016-17:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
186.37.108.44	Chile	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
72.10.124.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
198.50.145.72	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
195.226.71.212	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.45	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
82.166.183.92	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
82.205.11.221	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
109.64.221.238	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
162.243.125.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
75.180.230.197	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
80.246.136.206	Israel	147.237.72.167	ishurim.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
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.146.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.198.151.43	Europe	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	11
5.29.64.181	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
82.102.169.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
181.49.177.171	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	9
168.9.26.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.179.9.115	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	9
84.228.248.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
209.22.221.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.179.9.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.179.9.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
83.150.36.3	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.179.9.7	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.0.100.227	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.29.64.181	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.0	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

05-04-2016-16:04:02 to 05-04-2016-17:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
37.26.147.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
176.13.12.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
37.26.147.136	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	23
176.13.11.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
46.19.85.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
131.253.25.207	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
81.218.22.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
176.13.2.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.3.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.22.130.64	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.142.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
79.181.131.9	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
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1245-he/atal.aspx	Block	1
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.156.204	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
192.114.23.211	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 192.114.23.211 (Open Mode)	None	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	NULL Character in Method	Block	1
46.19.85.189	Israel	147.237.0.34	tikshuv.idf.il	Malformed URL gzip,	Block	1
109.67.36.55	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 109.67.36.55	Block	1
5.102.230.177	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 5.102.230.177 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
212.76.105.156	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
80.178.186.11	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
178.168.81.61	Moldova, Republic of	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1242-he/atal.aspx	Block	1
46.19.85.105	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
2.53.157.0	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
83.68.225.42	Sweden	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/home.as'a=0	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
192.114.23.211	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.189	Israel	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method Accept-Encoding: in URL gzip,	Block	1
109.67.36.55	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/	Block	1
5.102.230.177	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
212.235.18.146	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/general/mobile	Block	1
80.178.186.13	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
178.168.81.61	Moldova, Republic of	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
168.9.26.2	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.111.114.55	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
2.53.165.149	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
75.180.230.197	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
31.154.152.121	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
213.254.241.5	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
80.178.187.228	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/71580.pdf	Block	1

05-04-2016-16:04:02 to 05-04-2016-17:04:02