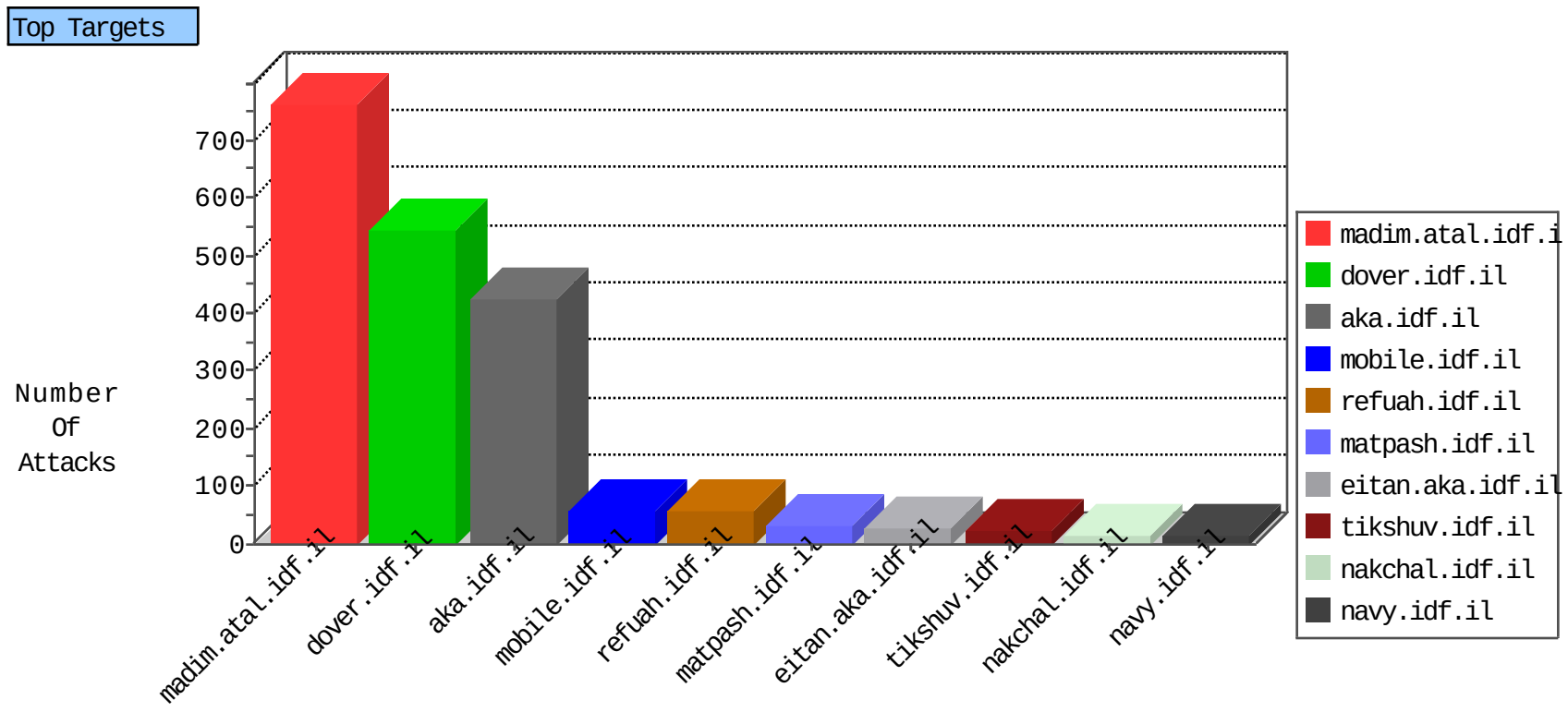
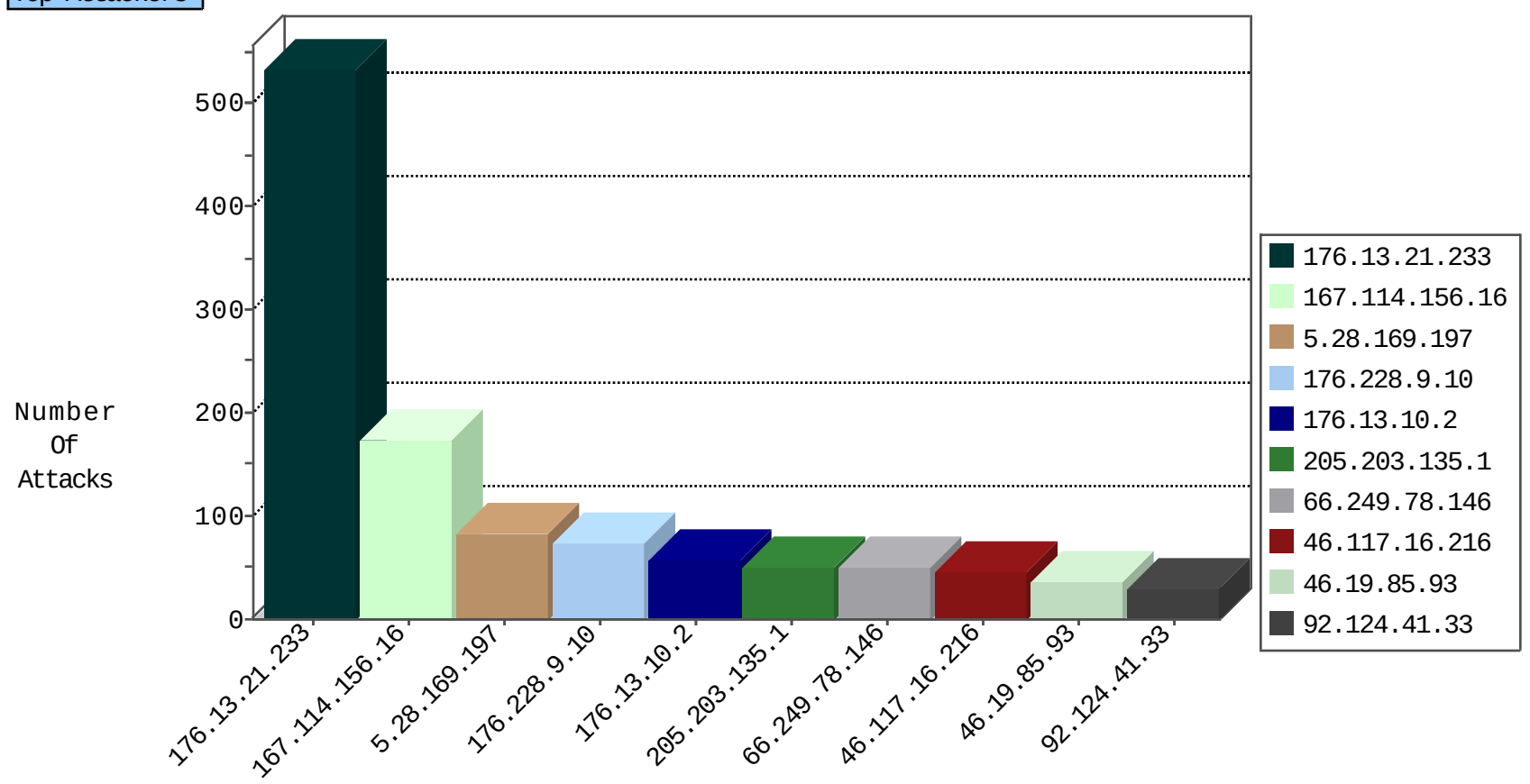
04-25-2016-12:04:08 to 04-25-2016-13:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-25-2016-12:04:08 to 04-25-2016-13:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	11948
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3855
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3188
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	9
84.108.75.232	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.179.234.185	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.28.19.26	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
120.132.50.135	China	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
185.103.252.98	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
212.60.246.66	Germany	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1

04-25-2016-12:04:08 to 04-25-2016-13:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-25-2016-12:04:08 to 04-25-2016-13:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
92.27.197.216	147.237.77.216	United Kingdom	dover.idf.il	Xenu Link Sleuth User Agent	2
66.249.64.197	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
119.156.54.17	147.237.77.216	Pakistan	dover.idf.il	Xenu Link Sleuth User Agent	2
92.27.197.216	147.237.72.166	United Kingdom	aka.idf.il	Xenu Link Sleuth User Agent	2
149.88.143.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.112.50	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
124.105.93.102	147.237.76.30	Philippines	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.67.112.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
84.108.75.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.146	147.237.0.19	Netherlands	madim.atal.idf.i	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
79.179.191.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
182.191.74.151	147.237.0.35	Pakistan	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.151.52.139	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
100.2.255.191	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.198.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.87.83.118	147.237.0.19	India	madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.64.253	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

04-25-2016-12:04:08 to 04-25-2016-13:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.21.233	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	146
176.13.21.233	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	alert	73
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
46.117.16.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
87.70.105.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
92.124.41.33	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	30
5.22.131.15	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
109.65.180.199	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
79.178.187.185	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
144.76.30.236	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.10.2	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
197.135.127.119	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.3.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
95.25.251.78	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
162.243.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.91	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
188.120.153.117	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
37.26.146.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
108.171.128.165	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
213.6.153.10	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.12.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.10.2	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	alert	6
79.183.57.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.241.32.185	Jordan	147.237.77.176	matpash.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
2.55.38.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.13.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.10.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.224	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.25.87	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.28.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.55.148.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.209.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.60.246.66	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.64.148.238	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.148.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.55.40.142	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
2.55.40.142	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

04-25-2016-12:04:08 to 04-25-2016-13:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.21.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	312
5.28.169.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	80
176.228.9.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
176.13.10.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
109.66.62.205	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 109.66.62.205	Block	18
46.117.16.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
79.180.145.160	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	5
79.177.167.172	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.177.167.172	Block	5
46.116.24.31	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
80.246.133.49	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
93.173.29.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.183.48.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	2
149.88.54.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.180.145.160	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.180.145.160	Block	2
84.228.249.165	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$61 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
62.0.111.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
144.76.30.236	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1392-en/cogat.asp	Block	1
109.66.62.205	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/dynamic_map/mobile	Block	1
80.246.133.32	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
120.132.50.135	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.mafengwo.cn/894-he/atal.aspx	Block	1
89.138.187.50	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
66.249.64.151	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
109.253.209.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.133.32	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
188.120.153.117	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
92.27.197.216	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/main/	Block	1
66.249.64.157	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/3384.jpg	Block	1
109.253.225.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
207.46.13.34	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
46.116.24.31	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 46.116.24.31	Block	1
144.76.30.236	Germany	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 144.76.30.236	Block	1
79.180.145.160	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
109.253.225.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
5.22.131.15	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
81.218.162.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/yassin7.	Block	1
144.76.30.236	Germany	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/מאיר שח aspx.מו	Block	1
176.13.21.233	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
66.249.64.253	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.253.225.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
212.174.76.22	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1

04-25-2016-12:04:08 to 04-25-2016-13:04:08