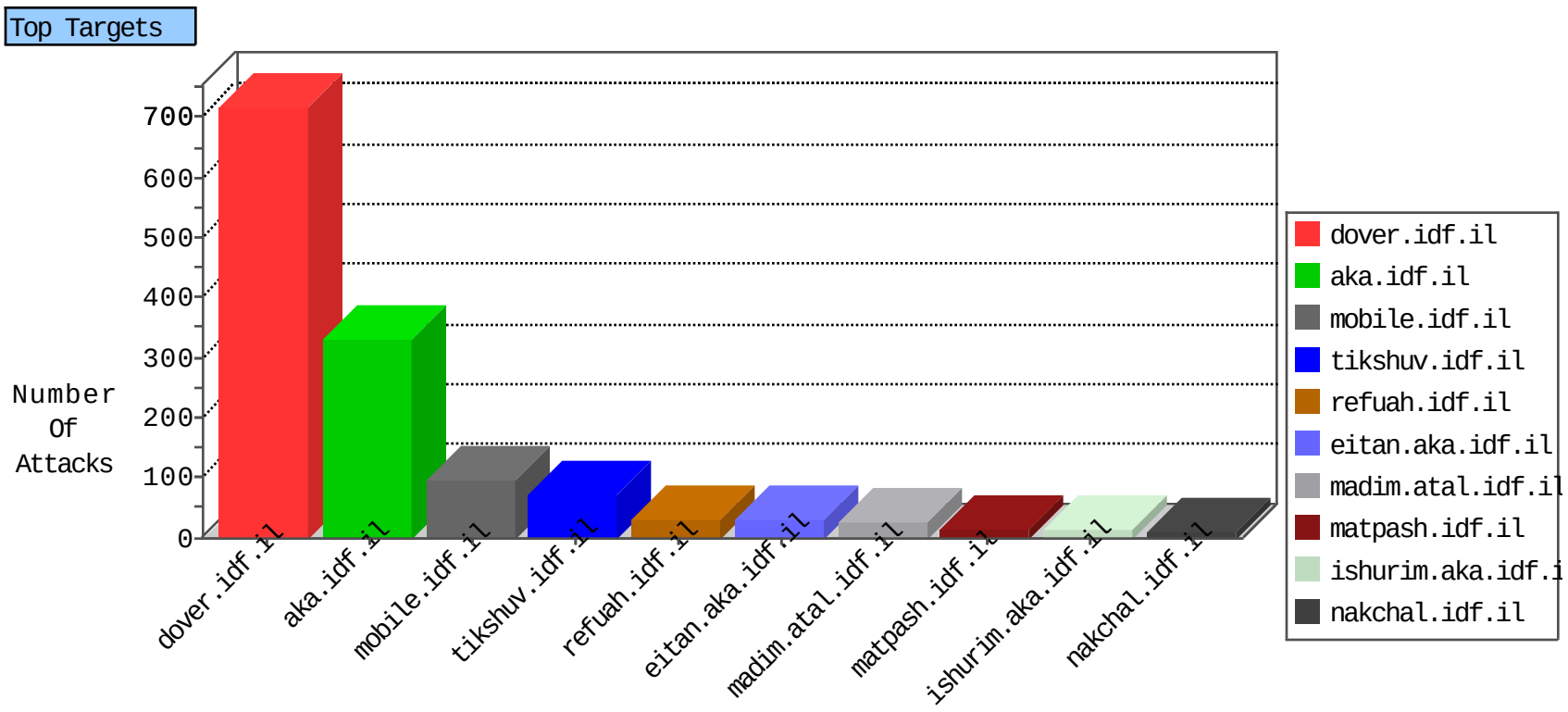
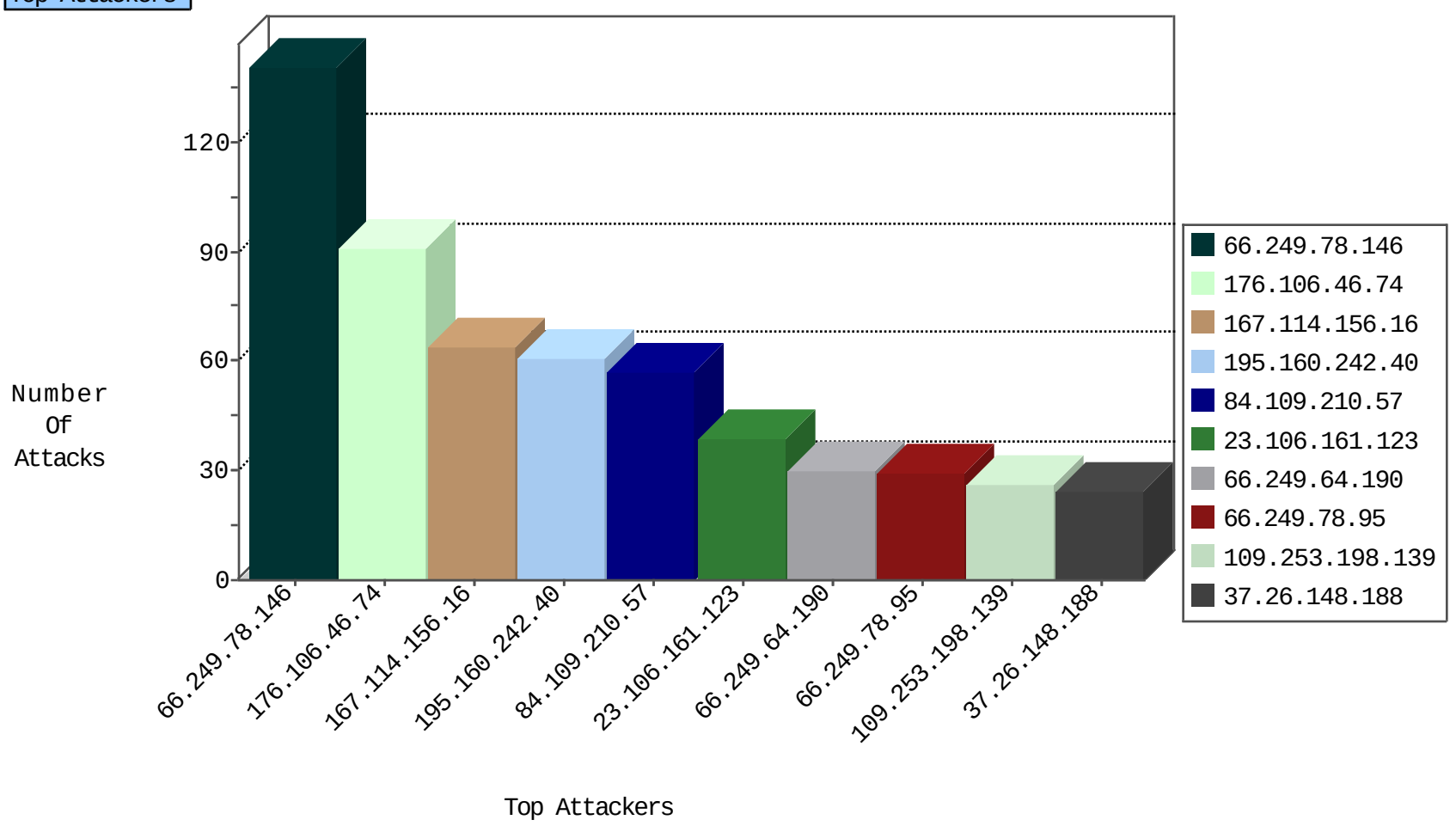
05-03-2016-08:04:09 to 05-03-2016-09:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-03-2016-08:04:09 to 05-03-2016-09:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.0.14.7	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3353
2.53.33.75	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2703
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2657
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2127
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	130
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
147.236.50.70	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
71.6.216.46	United States	147.237.76.196	e.sviva.idf.i	Block_Ntp_All_Net	drop	1

05-03-2016-08:04:09 to 05-03-2016-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-03-2016-08:04:09 to 05-03-2016-09:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.80.193.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.252.137.137	147.237.72.14	Poland	dover.idf.il(old	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
60.212.45.47	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -f -sS	1
2.55.41.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	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
163.172.140.23	147.237.77.178	United Kingdom	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
122.5.27.18	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 2048	1
82.102.169.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
78.164.126.12	147.237.77.216	Turkey	dover.idf.il	portscan: TCP Distributed Portscan	1
60.212.45.47	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 2048	1
5.22.131.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
192.116.241.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.70.66.9	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
122.5.27.18	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -f -sS	1

05-03-2016-08:04:09 to 05-03-2016-09:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	141
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
176.106.46.74	Palestinian Territory, Occupied	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	43
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
23.106.161.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.253.198.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
185.27.106.30	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
37.26.148.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
108.171.128.166	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
212.179.132.204	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
50.117.45.199	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	16
141.0.14.7	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.86.106	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.53.12.18	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
84.95.215.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
176.13.4.189	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.203.80	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.78.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
77.42.252.196	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.55.178.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.78.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.32.8	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
195.160.242.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
195.160.242.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.8.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.148.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.80.196.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.106.46.74	Palestinian Territory, Occupied	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.178.169.179	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.102.116.75	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.32.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

05-03-2016-08:04:09 to 05-03-2016-09:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.210.57	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	57
2.53.144.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
109.253.200.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
37.26.148.188	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
109.253.198.139	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	5
109.253.128.84	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	5
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew	Block	5
2.53.190.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
31.154.4.18	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.4.18	Block	3
109.253.203.80	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.223.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.116.177.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.149.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8871-he/refuah.aspx	Block	1
46.19.85.124	Israel	147.237.77.74	law.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.124	Block	1
192.118.10.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
31.154.4.18	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/error.png	Block	1
85.111.44.238	Turkey	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/index.php	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	1
218.71.150.50	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
164.132.161.52	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/paratroopers	Block	1
46.19.85.23	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
106.186.113.132	Japan	147.237.77.235	sviva.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8924-he/refuah.aspx	Block	1
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
192.118.10.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/main/kapatz/webresource.axd	None	1
37.26.146.208	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
85.111.44.238	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/index.php	Block	1
219.74.239.176	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
164.132.161.89	Italy	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/לכתבה המלאה	Block	1
46.19.85.23	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
109.65.29.119	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: ctl00$ctl00$cphMain$cphSachar$txtPassword in www.aka.idf.il/main/sachar/	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
46.19.86.50	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation SearchText in www.refua.atal.idf.il/938-he/refuah.aspx	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
91.231.193.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
220.255.146.147	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
176.13.8.49	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.23	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1437-he/atal.aspx	Block	1
17.142.155.148	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
109.65.29.119	Israel	147.237.72.166	aka.idf.il	Multiple Double URL Encoding from 109.65.29.119	Block	1
80.246.139.162	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl04.x in aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-23121-he/dover.aspx	Block	1
203.127.96.199	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.149.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
220.255.148.146	Singapore	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/robots.txt	Block	1

05-03-2016-08:04:09 to 05-03-2016-09:04:09