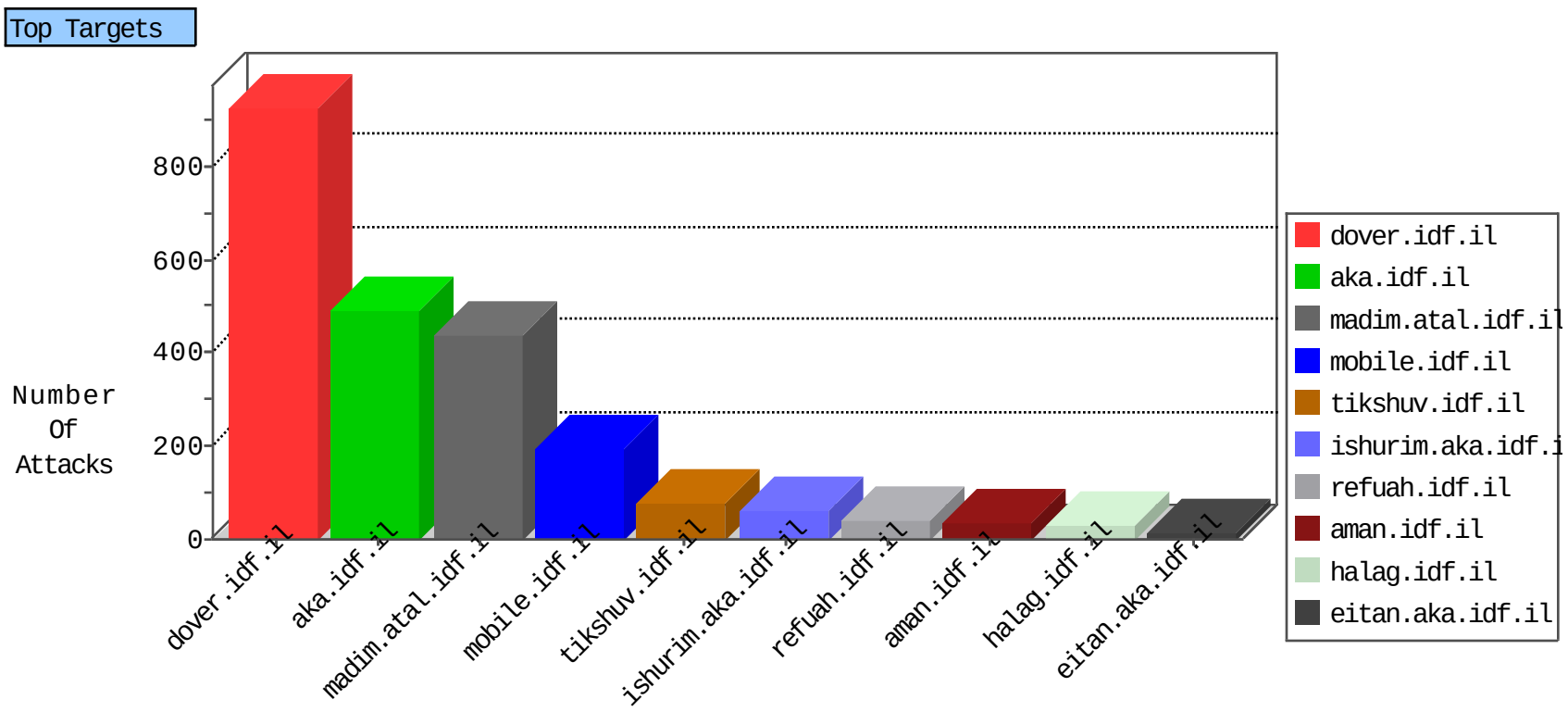
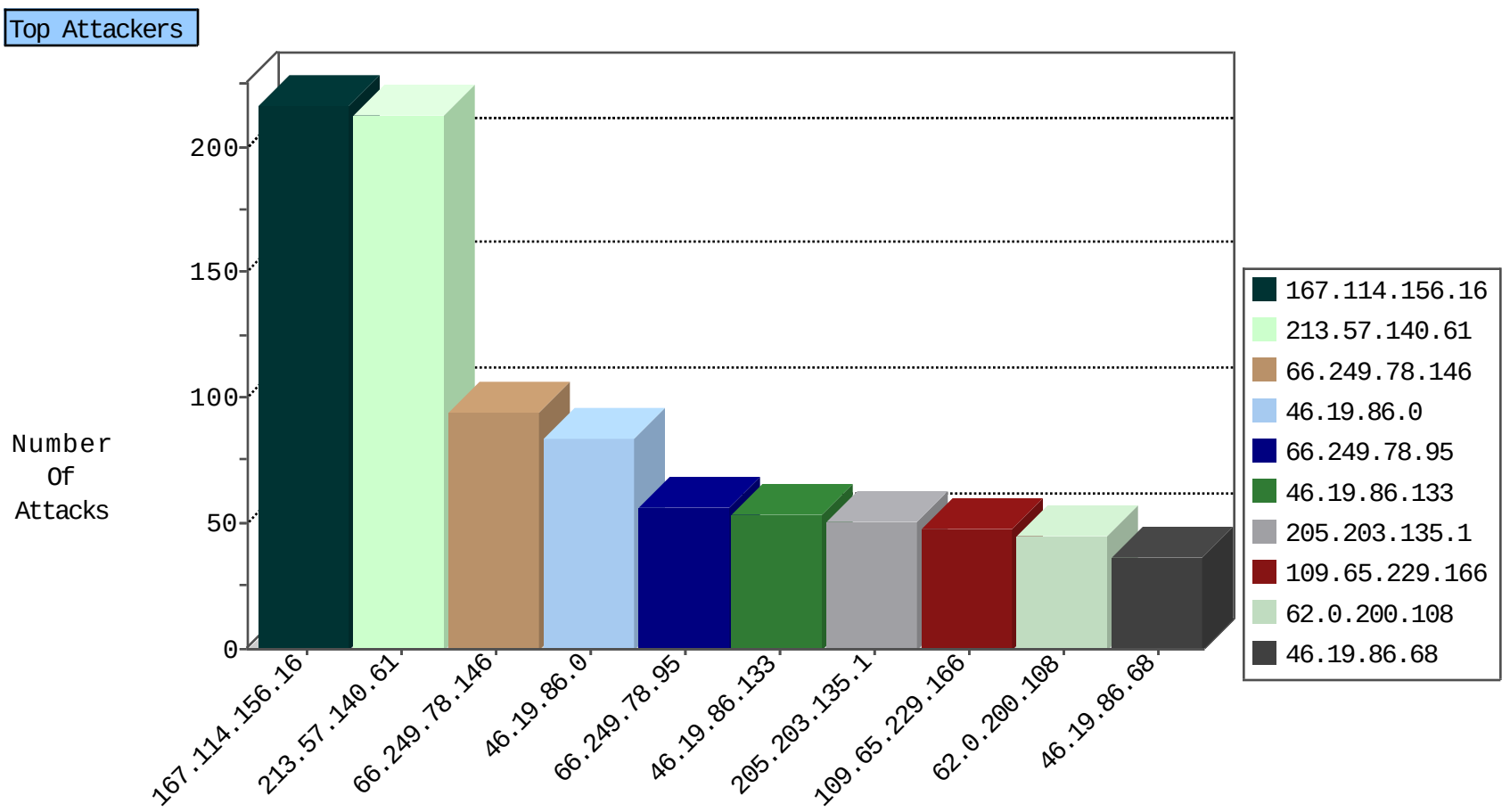
05-03-2016-11:04:02 to 05-03-2016-12:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-03-2016-11:04:02 to 05-03-2016-12:04:02

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	HTTP-POST-Segmented-DoS	dest-reset	8015
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4194
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	158
149.78.6.125	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	103
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
79.183.33.137	Israel	147.237.72.166	aka.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
204.42.253.130	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
71.6.216.41	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
98.217.84.130	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.161	China	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.49	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.39	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

05-03-2016-11:04:02 to 05-03-2016-12:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-03-2016-11:04:02 to 05-03-2016-12:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
132.64.167.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
2.53.154.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.90.185.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.20.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.171.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.208.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
212.179.221.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
208.100.26.228	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.179.210	147.237.72.166	Israel	aka.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
185.3.146.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.246.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.13.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.171.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.158	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
212.235.98.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.95	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.174.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.156.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1

05-03-2016-11:04:02 to 05-03-2016-12:04:02

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	93
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
109.65.229.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
37.26.148.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
132.66.61.185	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
39.36.90.188	Pakistan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
176.13.10.124	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
62.0.200.108	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	24
212.117.136.6	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	23
62.0.200.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
188.226.28.110	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.19.86.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
80.246.136.76	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
199.203.179.99	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.53.44.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
66.249.78.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
193.191.219.80	Belgium	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	12
89.145.95.40	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.78.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
198.58.103.114	United States	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	10
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.106.46.74	Palestinian Territory, Occupied	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	10
195.212.29.181	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
194.90.233.177	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.78.95	United States	147.237.77.216	dover.idf.il	drop		drop	9
46.19.86.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
132.64.182.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
176.13.23.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.219.168.120	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.65	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.13.17.132	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.137.5	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
176.13.6.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

05-03-2016-11:04:02 to 05-03-2016-12:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.140.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	213
46.19.86.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
46.19.86.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
80.246.136.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
46.19.85.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.53.176.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
109.253.199.199	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	9
185.27.105.123	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	8
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	7
85.250.165.26	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 85.250.165.26	Block	5
109.253.215.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
80.246.136.76	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.66.10.6	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
84.95.211.153	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	4
81.218.251.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	4
84.95.211.153	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 84.95.211.153	Block	4
81.218.251.250	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resources/content/images/mainpage/	Block	4
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.254	Block	3
80.246.140.171	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
185.27.105.123	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/	Block	3
131.253.25.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
65.55.210.153	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.23.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.53.182.115	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
212.199.251.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	2
2.55.139.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.2.206.118	Switzerland	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	2
2.53.165.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.121.124.255	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
62.90.234.249	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	2
212.179.197.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
2.53.179.101	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1362-16154-he/dover.aspx	Block	1
197.77.205.1	South Africa	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/wp-login.php	Block	1
132.71.108.91	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
93.172.21.22	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	1
54.159.195.37	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
193.43.245.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/gius	Block	1
84.94.106.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
37.26.146.146	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
2.53.42.191	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Illegal Byte Code Character in Method Tu7´•¯ñ	Block	1
199.203.226.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ס'ו'ג	Block	1
197.77.205.1	South Africa	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
109.253.195.127	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1437-he/atal.aspx	Block	1
212.199.251.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.251.227	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1

05-03-2016-11:04:02 to 05-03-2016-12:04:02