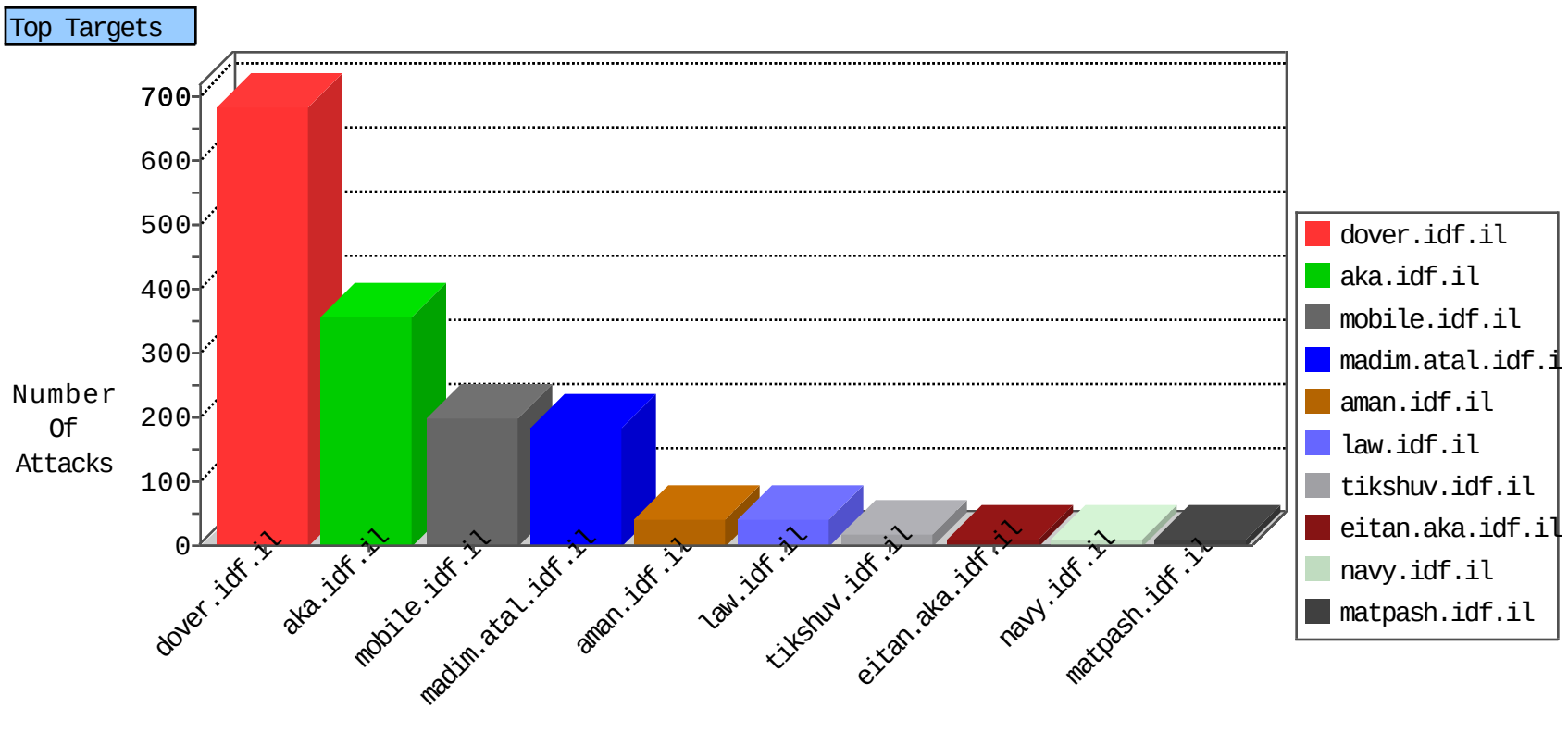
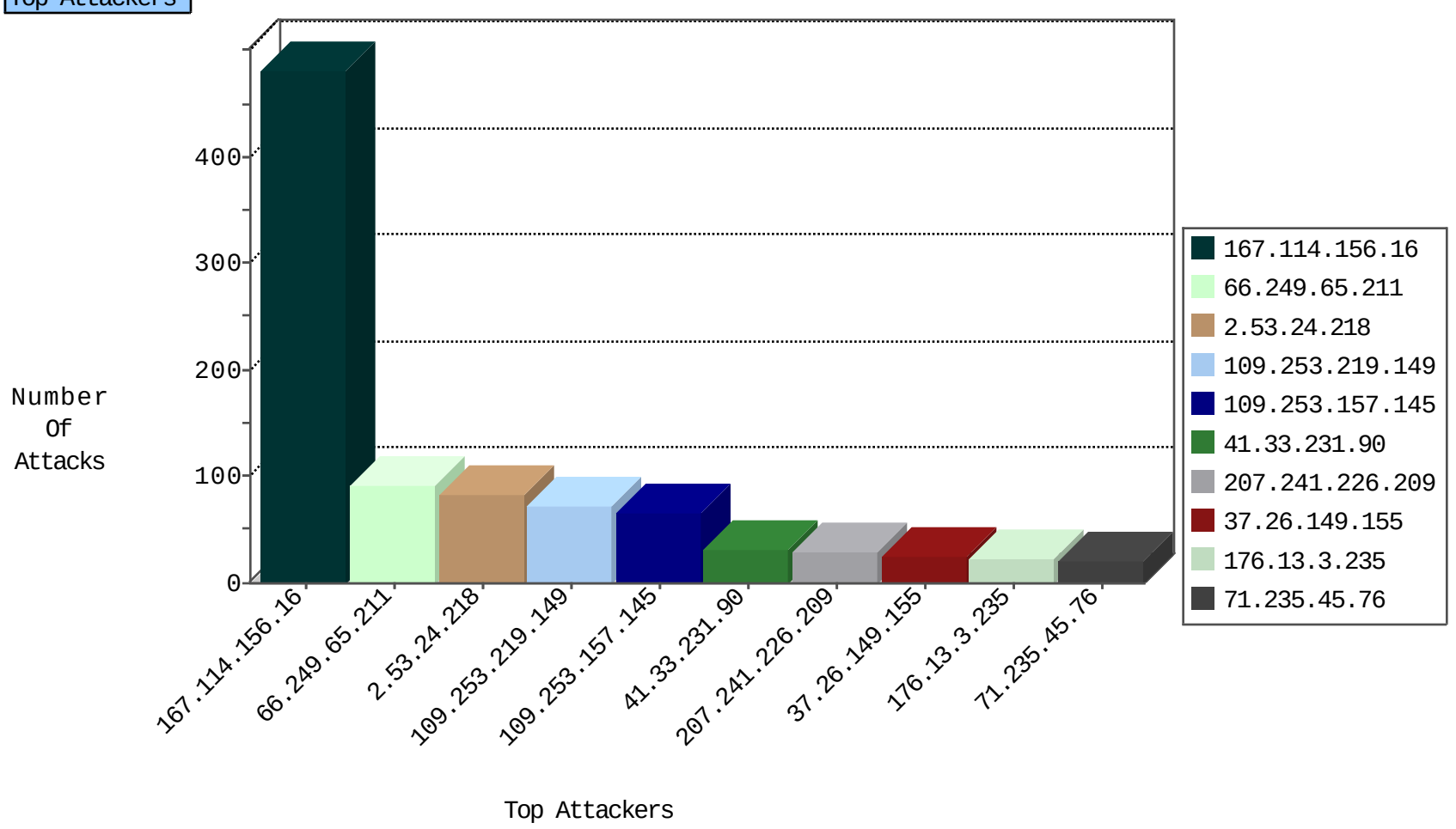
04-21-2016-19:04:08 to 04-21-2016-20:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-21-2016-19:04:08 to 04-21-2016-20:04:08

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	21788
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3610
217.132.57.83	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	204
31.148.219.11	Netherlands	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
66.249.65.211	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1

04-21-2016-19:04:08 to 04-21-2016-20:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-21-2016-19:04:08 to 04-21-2016-20:04:08

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
193.201.227.52	147.237.76.86	Ukraine	navy.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.52	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
195.81.248.101	147.237.72.217	United Kingdom	e.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.52	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.52	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.162	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
66.223.201.10	147.237.76.30	United States	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
207.241.226.209	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1

04-21-2016-19:04:08 to 04-21-2016-20:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.211	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
109.253.219.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
207.241.226.209	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	29
2.53.146.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
37.26.149.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
176.13.3.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.53.16.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.141.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
198.204.249.34	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.85.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.64.41.192	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
79.180.127.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.22.134.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
165.24.252.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.158.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
213.8.204.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.180	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.50.123.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.7.110	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.180	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
71.235.45.76	United States	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
79.181.160.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.187.51	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.144.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.124.13.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
71.235.45.76	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
5.22.134.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.124.13.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
185.3.144.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.71.17.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.185.155.10	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.3.147.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
71.235.45.76	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
185.120.126.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.150.97.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.136.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.210	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.84.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.25.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-21-2016-19:04:08 to 04-21-2016-20:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.26.149.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.203.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3

04-21-2016-19:04:08 to 04-21-2016-20:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.24.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	77
109.253.157.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
109.253.219.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
109.66.37.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
176.13.3.235	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
37.26.149.155	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
17.138.55.96	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templatecontrols/generic/	Block	4
85.64.160.160	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	4
109.253.141.14	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.219.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.16.92	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
17.138.55.96	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
79.179.19.111	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
79.181.32.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
157.55.39.139	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/giyus/giyus/general.aspx	None	1
51.255.65.72	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list2005b.htm	Block	1
207.46.13.106	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/iturim/iturim.aspx	None	1
84.94.64.162	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/mobile	Block	1
66.249.65.211	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1148-he/chinuch.aspx	Block	1
165.123.2.106	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
157.55.39.139	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in aka.idf.il/rights/asp/info.asp	None	1
79.177.232.238	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
207.46.13.4	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/giyus/general.aspx	Block	1
157.55.39.139	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/news/	None	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
117.25.108.95	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/trackback/	Block	1
40.77.167.86	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/popups/popup.aspx	None	1
207.46.13.106	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/tizmoret/gallery/	None	1
84.111.165.15	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.111.165.15	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/scriptresource.axd	Block	1
157.55.39.139	United States	147.237.72.166	aka.idf.il	Unknown Parameter cat_id in aka.idf.il/iturim/asp/wars.asp	None	1
207.46.13.26	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
157.55.39.139	United States	147.237.72.166	aka.idf.il	Unknown Parameter catld in aka.idf.il/yohalan/main/main.asp	None	1
40.77.167.86	United States	147.237.72.166	aka.idf.il	Unknown Parameter sOpenLinkIn in aka.idf.il/giyus/main/	None	1
149.50.123.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.115	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/list.asp	Block	1
84.111.165.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/gitus	Block	1
66.249.65.218	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
181.137.221.232	Colombia	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
157.55.39.139	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/eitan/mesiratmeida/	None	1
207.46.13.106	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.106	Block	1
79.179.140.33	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
157.55.39.139	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/brothers/skira/default.asp	None	1
46.19.85.190	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
149.78.237.41	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1

04-21-2016-19:04:08 to 04-21-2016-20:04:08