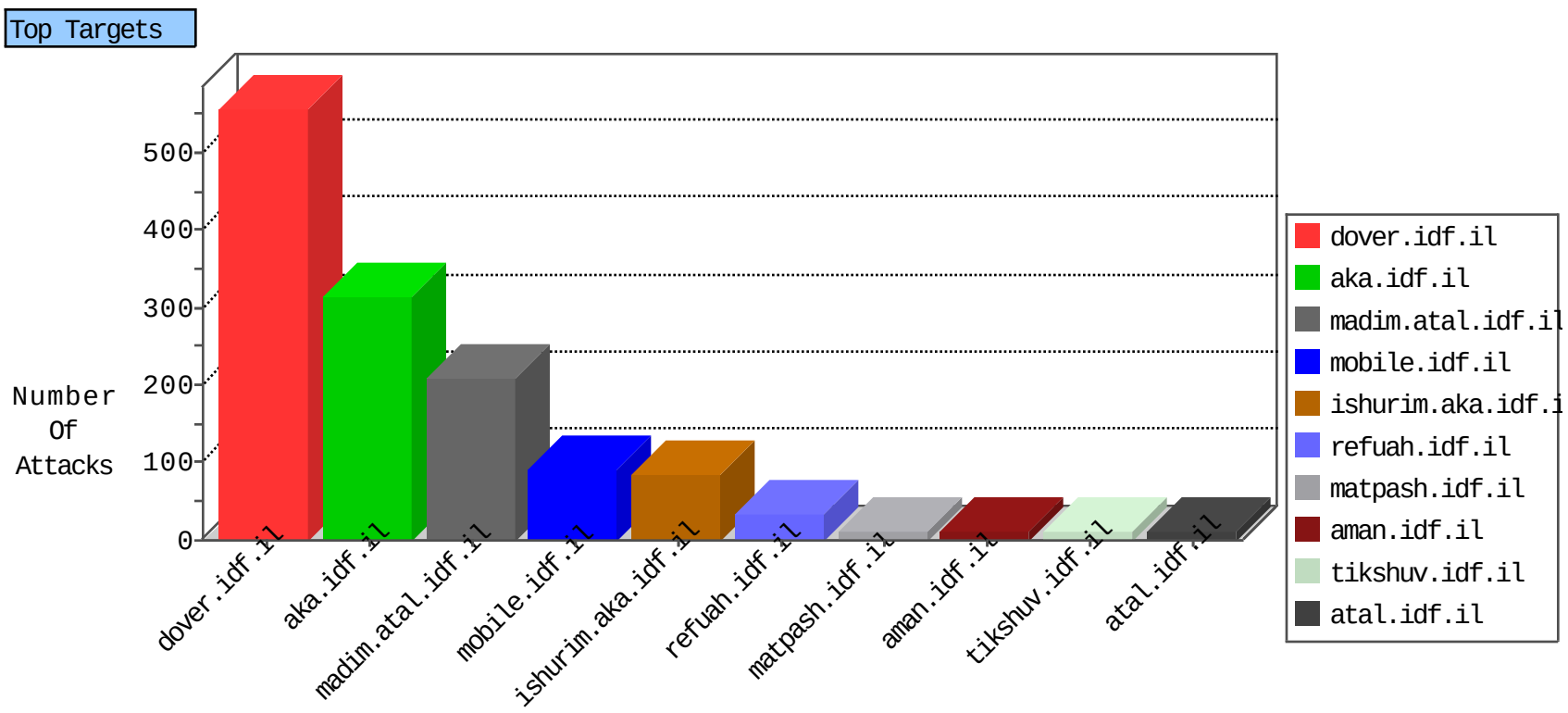
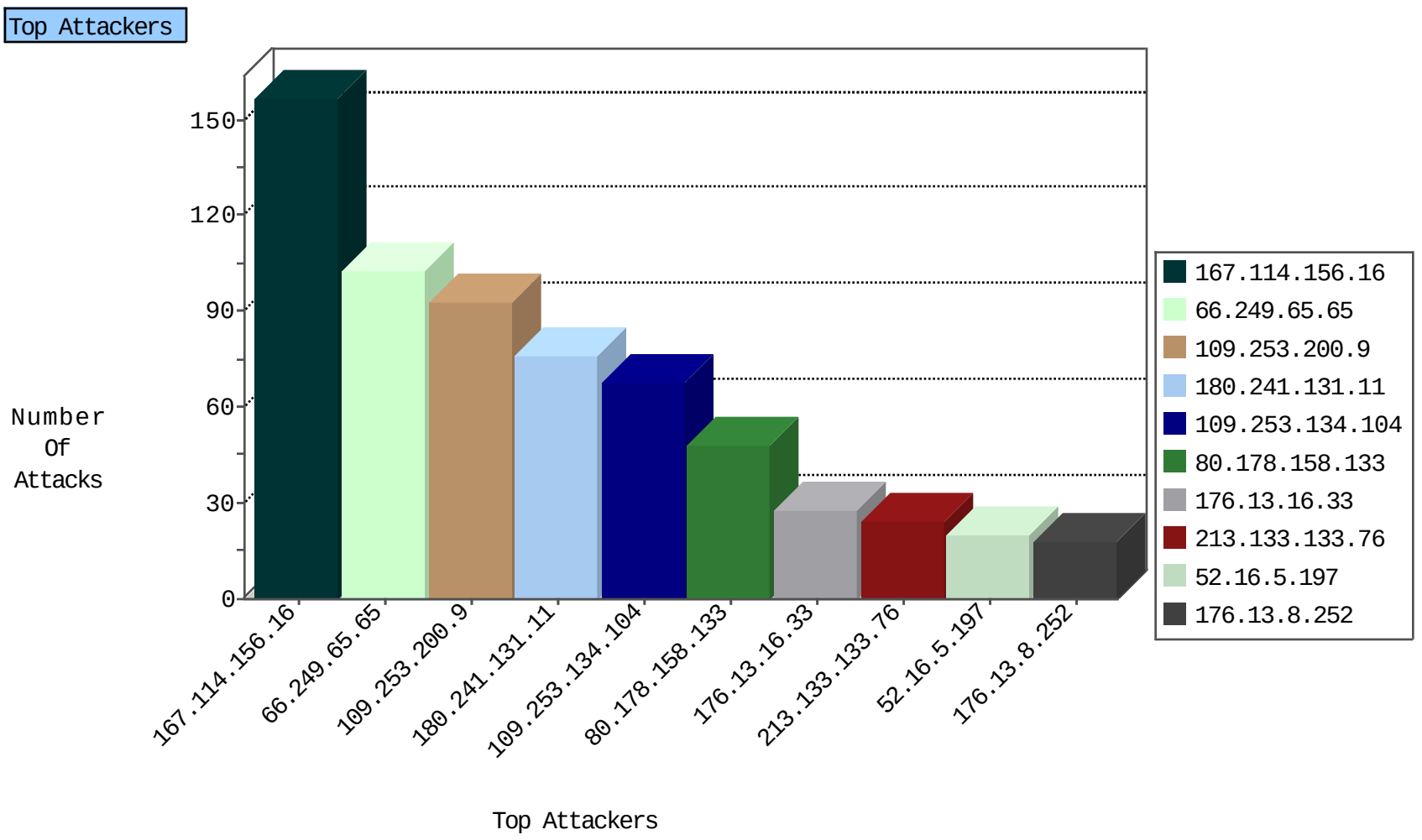
05-04-2016-11:04:03 to 05-04-2016-12:04:03

IDF Under Attack
Daily Report

Top Targets



Top Attackers



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

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	5607
84.94.83.36	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3418
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1737
82.145.218.194	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
66.249.65.65	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
192.167.90.244	Italy	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
38.229.1.13	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

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

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.204.172	147.237.76.200	Israel	eitan.aka.idf.il	Xenu Link Sleuth User Agent	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
104.192.0.19	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.138.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.76.112.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.3.144.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
159.18.125.235	147.237.77.235	Canada	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
2.53.137.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
159.18.125.235	147.237.77.235	Canada	sviva.idf.il	ET SCAN NMAP -f -sS	1
132.64.58.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.19	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
217.132.46.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.44.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.10.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.204.172	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1
185.3.144.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.204.172	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
159.18.125.235	147.237.77.235	Canada	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
140.101.84.1	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.19	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
180.241.131.11	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
80.178.158.133	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	48
176.13.16.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
213.133.133.76	United Kingdom	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	14
2.53.63.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.146.196	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
23.80.147.151	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.148.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.179.60.30	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
183.167.228.134	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
109.64.117.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
85.130.176.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.64.43.180	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.179.187.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.134.47	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.241.229.214	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.180.12.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.208.20	Israel	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	6
80.178.1.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
89.46.180.178	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
209.133.111.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.133.133.76	United Kingdom	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
2.53.152.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.9.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.18.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.69.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.61	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.80.196.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.79.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
217.64.86.6	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
89.147.0.199	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.128.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.77.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.176.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.193.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.4.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.200.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
109.253.134.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
176.13.8.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
109.253.212.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
2.53.45.61	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtID in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	9
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	7
176.13.16.33	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
2.53.63.35	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
65.55.213.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
131.253.25.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
132.66.235.47	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	4
80.246.138.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.139.171	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.244	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
84.94.193.214	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
131.253.25.185	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.149	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	3
87.71.67.116	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.71.67.116	Block	3
131.253.25.208	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.67.128.73	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
31.168.90.180	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
176.13.11.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.211.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.180.12.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
62.90.35.105	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
212.179.60.30	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	2
184.105.139.70	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/3249.jpg	Block	1
141.255.158.88	Netherlands	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
46.43.106.2	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
213.254.241.4	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
93.173.177.169	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.180.209.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.179.60.30	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 212.179.60.30	Block	1
185.120.126.52	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.120.126.52	Block	1
141.255.158.88	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/size100x0/3211.jpg	Block	1
109.253.214.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.117.62.227	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
193.47.165.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
79.183.178.118	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.176.49.120	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1

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