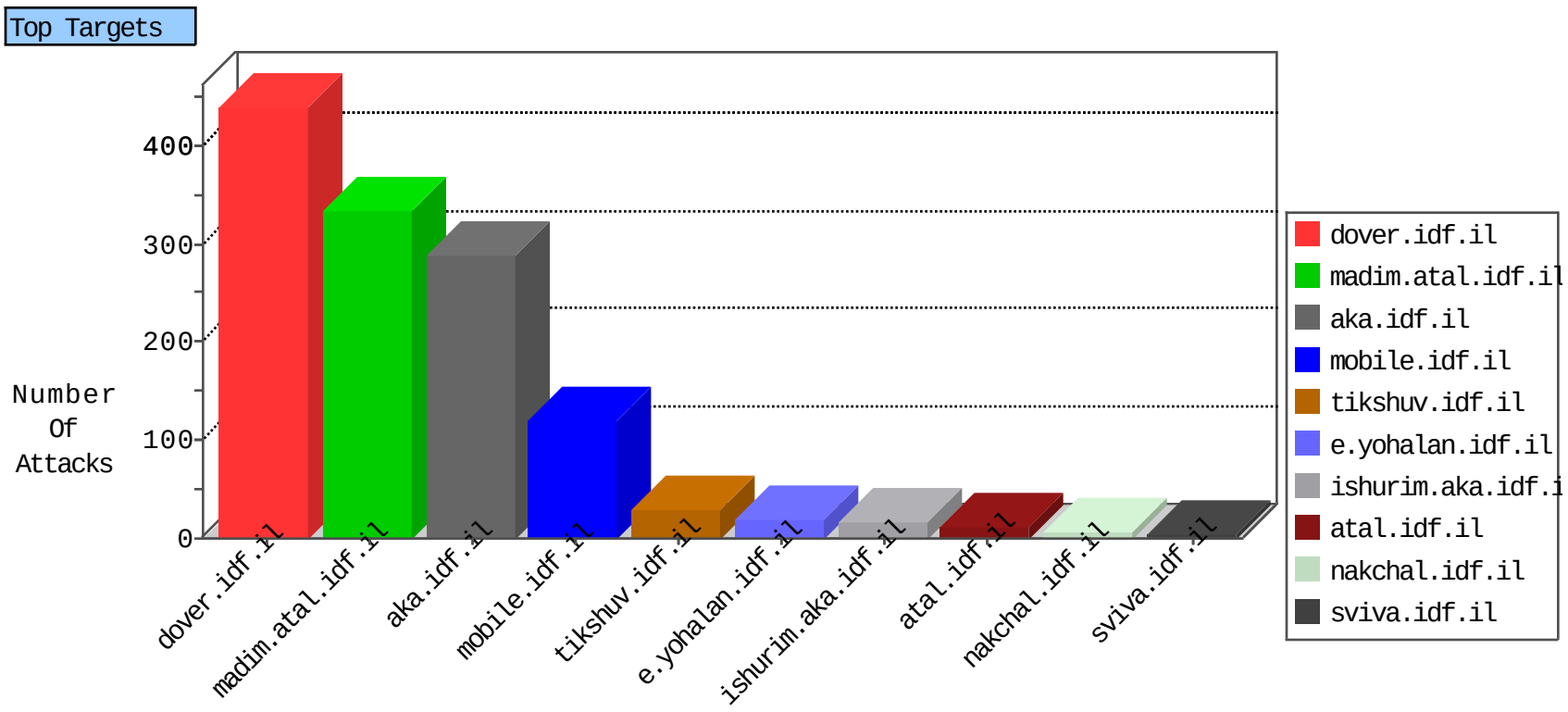
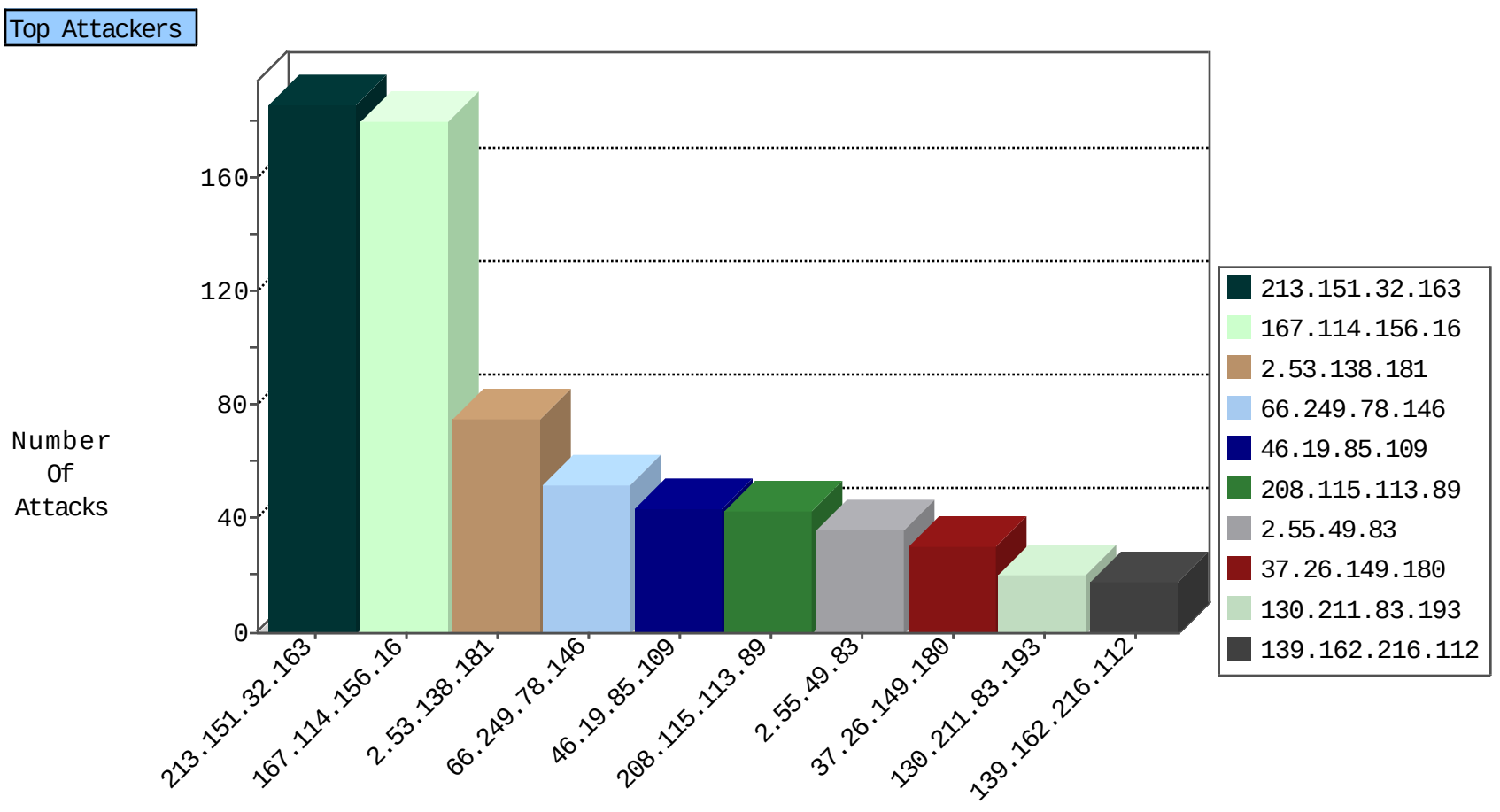
05-01-2016-07:04:01 to 05-01-2016-08:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



05-01-2016-07:04:01 to 05-01-2016-08:04:01

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	8073
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	482
89.139.241.142	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
123.151.149.222	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
124.232.150.230	China	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1

05-01-2016-07:04:01 to 05-01-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
130.211.83.193	United States	147.237.72.166	aka.idf.i	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	10
130.211.83.193	United States	147.237.72.166	aka.idf.i	22095: HTTP: Joomla Image Manager folderRename Security Bypass Vulnerability	Block	10

05-01-2016-07:04:01 to 05-01-2016-08:04:01

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	3
192.184.40.68	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
192.184.40.68	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
72.227.236.50	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
192.184.40.68	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
37.26.147.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.27.105.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
13.92.100.128	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
184.80.10.136	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
13.82.25.17	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
173.193.130.54	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
104.197.72.206	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
207.232.45.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.129.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.94.124.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.184.40.68	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
79.176.93.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.184.40.68	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.56	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.184.40.68	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
13.92.100.128	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
184.80.10.136	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
13.82.25.17	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
176.13.23.33	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
2.53.34.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.193.130.54	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
208.100.26.228	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
104.197.72.206	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.77.179	United States	e.mazi.idf.il	ET DROP Dshield Block Listed Source	1
84.228.152.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

05-01-2016-07:04:01 to 05-01-2016-08:04:01

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	51
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
37.26.149.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
80.246.136.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.55.137.53	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.55.144.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.93.97	Europe	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	11
37.26.148.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.221.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.93.101	Europe	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
2.53.24.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
196.140.87.216	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.55.49.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.55.49.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.53.34.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.49.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.248.82.141	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.55.49.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
37.26.149.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.49.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
2.55.49.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
197.41.146.63	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
68.180.231.43	United States	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
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.111.1.118	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.23.33	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.176.10.71	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.55.44.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
120.164.46.168	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.23.33	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.10.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.212.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.18	Israel	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
2.53.6.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

05-01-2016-07:04:01 to 05-01-2016-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	186
2.53.138.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
46.19.85.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
37.26.147.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
37.26.146.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.253.200.11	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.253.200.11	Block	7
37.26.149.180	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
185.32.179.191	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
109.253.221.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.122	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.53.188.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.141.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
91.200.12.49	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
91.200.12.49	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
31.154.19.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.250	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
212.150.163.132	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
176.13.15.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/57056.pdf&ved=0ahukewj88mpmt6fmahuc_iwkhwntar4qfggdmai&usg=afqjcnf1yolugsboijiblzxiye0gplabcg&sig2=sljt3vnb9hu32rwuqzye5w	Block	1
5.29.171.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
68.180.231.46	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.167.111.180	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
138.134.192.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
2.53.34.139	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
87.71.47.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/71556.pdf	Block	1
46.19.85.112	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
184.105.139.67	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
109.253.211.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.39.222.159	Netherlands	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for /	Block	1
207.46.13.55	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/kamlar/	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
46.19.85.213	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
184.105.139.70	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
109.253.212.179	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
17.142.152.239	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/apple-app-site-association	Block	1
79.180.187.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus.	Block	1
207.46.13.177	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
66.249.66.176	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
149.88.195.82	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
2.53.178.46	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1841-he/dover.aspx	Block	1
50.153.246.145	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/894-he/eitan.aspx	None	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/rights/asp/	Block	1
66.249.66.179	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/8/1558.jpg	Block	1
176.13.2.188	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1

05-01-2016-07:04:01 to 05-01-2016-08:04:01