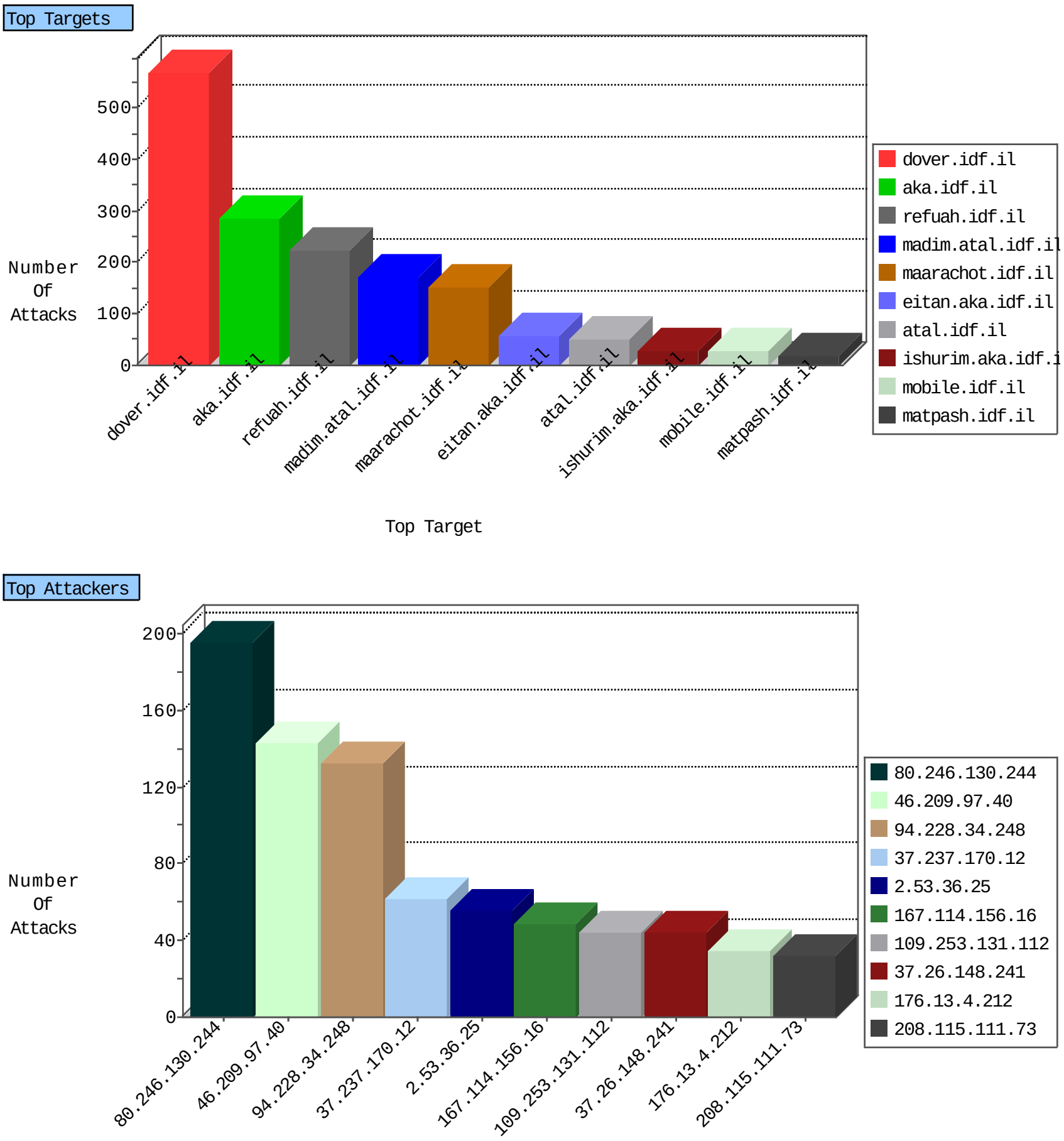
04-20-2016-14:04:05 to 04-20-2016-15:04:05

IDF Under Attack
Daily Report



04-20-2016-14:04:05 to 04-20-2016-15:04:05

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	TCP handshake violation, first packet not syn	drop	4953
46.19.86.143	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2698
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
81.218.88.234	Israel	147.237.76.42	refuah.idf.il	Anomaly-TCP-shortheader	dest-reset	5
81.218.88.234	Israel	147.237.76.42	refuah.idf.il	Anomaly-TCP-SYN-FIN	dest-reset	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	2
122.52.104.54	Philippines	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.i	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

04-20-2016-14:04:05 to 04-20-2016-15:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-20-2016-14:04:05 to 04-20-2016-15:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.64.96.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.183.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.128.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
60.254.110.210	147.237.77.216	India	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.158.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
27.25.248.94	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
176.13.7.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.48.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
173.65.154.27	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.253.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.72.93.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.149.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.74.127.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.232.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
27.25.248.94	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.55.143.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
173.65.154.27	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.39.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.65.154.27	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
149.50.14.83	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

04-20-2016-14:04:05 to 04-20-2016-15:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.244	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	195
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	133
46.209.97.40	Iran, Islamic Republic of	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	81
46.209.97.40	Iran, Islamic Republic of	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	51
37.26.148.241	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	44
203.133.171.33	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
37.237.170.12	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
62.90.122.236	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
107.167.97.215	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
37.237.170.12	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	23
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
69.31.51.51	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
207.241.229.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
109.253.225.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.22.135.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.136.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.14.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.22.131.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.179.224.23	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
149.50.118.151	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
85.65.4.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.116.226.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.209.97.40	Iran, Islamic Republic of	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.209.97.40	Iran, Islamic Republic of	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.176.19.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.176.19.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.250.86.135	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.105.204.106	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.124.116	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
79.180.13.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.124.116	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
157.55.39.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.121.156.160	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.130.238.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.147.56	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.44	Israel	147.237.76.31	nakchal.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

04-20-2016-14:04:05 to 04-20-2016-15:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.36.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
109.253.131.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
176.13.4.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
46.117.31.167	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	19
176.13.22.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
2.55.26.243	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	8
31.129.170.42	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
31.168.103.115	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.103.115	Block	5
31.129.170.42	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.129.170.42	Block	5
185.27.106.60	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 185.27.106.60	Block	4
79.183.26.75	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	4
79.183.26.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/	Block	3
46.19.86.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.148.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.0.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.225.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
85.65.4.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.17.251	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	2
46.19.86.192	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
177.228.140.156	Mexico	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	2
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew	Block	2
178.214.93.59	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	2
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.15.221	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;DocID in www.aka.idf.il/giyus/leshakot/	None	1
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
130.185.155.10	Sweden	147.237.77.74	law.idf.il	PHP Attempt	Block	1
37.237.170.12	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
69.58.178.59	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
106.186.113.132	Japan	147.237.0.34	tikshuv.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sviva	Block	1
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
159.220.74.5	United Kingdom	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
130.185.155.10	Sweden	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
40.77.167.65	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/navmenu/	Block	1
91.143.226.180	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in aka.idf.il/main/sachar/markiveysachar.aspx	None	1
77.126.196.240	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.schooly.co.il/benzvi/	Block	1
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.168.103.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/buttonback.png	Block	1
109.67.19.75	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
80.246.130.244	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
2.53.36.25	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Open Mode	None	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1

04-20-2016-14:04:05 to 04-20-2016-15:04:05