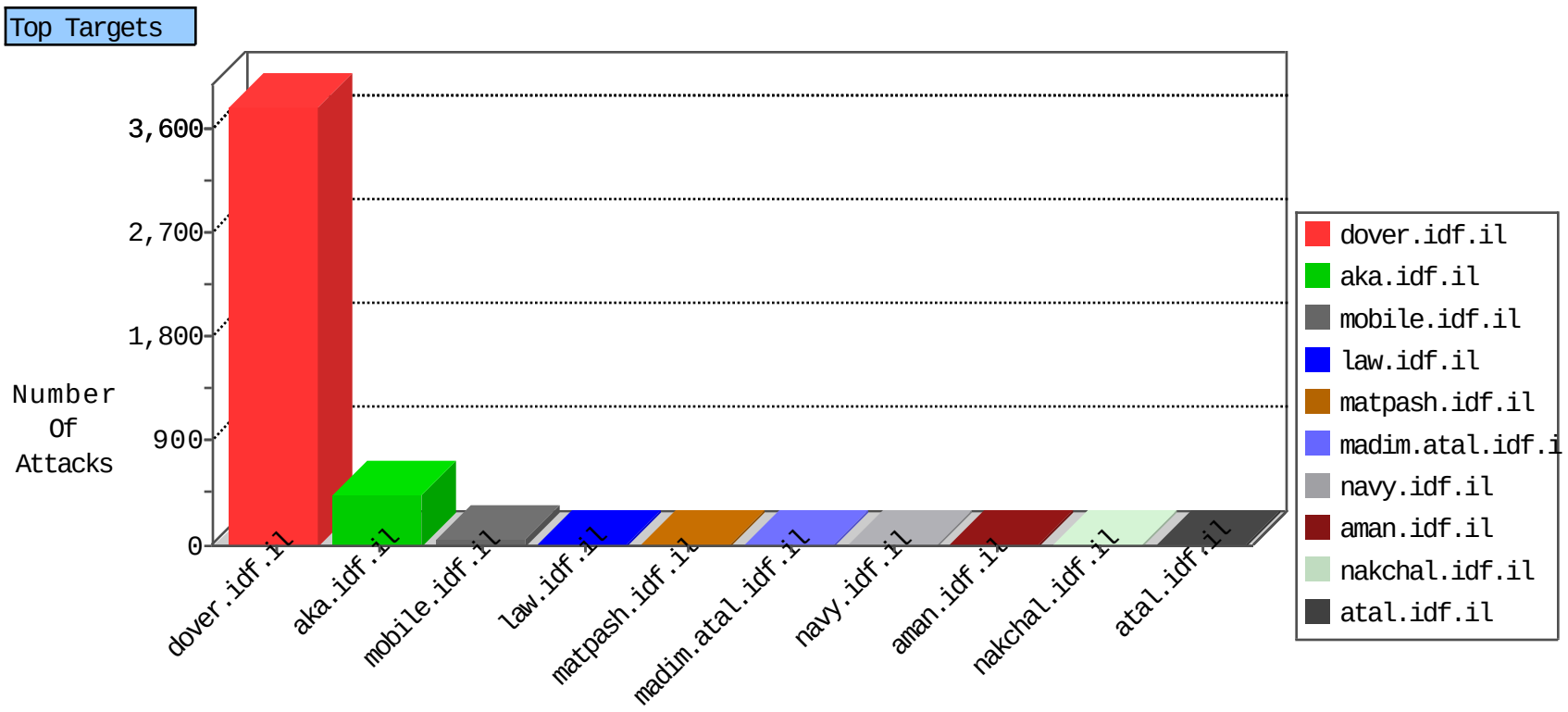
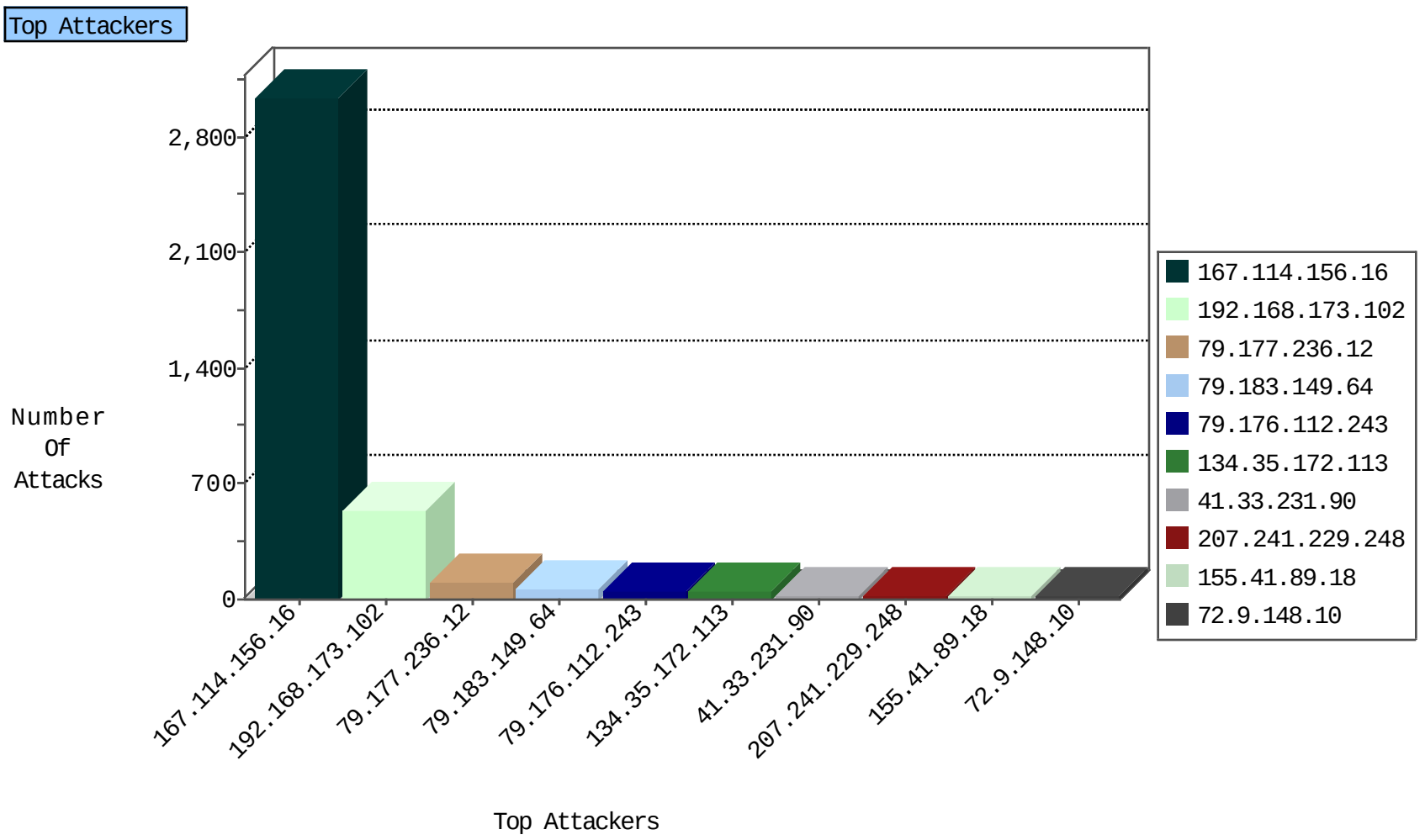
04-08-2016-22:04:05 to 04-08-2016-23:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-08-2016-22:04:05 to 04-08-2016-23:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.77.16.91	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4123
134.35.172.113	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3150
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3033
79.177.236.12	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	103
79.183.149.64	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	60
92.241.34.143	Jordan	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	21
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
185.94.111.1	Russian Federation	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
105.239.85.192	Sudan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
192.96.201.142	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
37.26.148.171	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1

04-08-2016-22:04:05 to 04-08-2016-23:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.36.93	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
123.126.113.109	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
37.187.137.225	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
37.187.137.225	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
36.110.147.67	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-08-2016-22:04:05 to 04-08-2016-23:04:05

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
174.37.194.144	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
174.37.194.144	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
117.34.70.143	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.0.15	Canada	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
211.149.156.87	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.76.86	Kazakstan	navy.idf.il	ET SCAN NMAP -sS window 4096	1
202.164.39.21	147.237.76.196	India	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.71.107.44	147.237.76.31	Israel	nakchal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
202.164.39.21	147.237.76.44	India	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.93.192.122	147.237.8.28	South Africa	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.76.170.207	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
174.37.194.144	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
117.34.70.143	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
115.124.40.9	147.237.0.33	India	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.33.246.86	147.237.76.198	Romania	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.76.86	Kazakstan	navy.idf.il	ET SCAN NMAP -sS window 3072	1
202.164.39.21	147.237.76.147	India	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.78.38	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
202.164.39.21	147.237.76.34	India	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

04-08-2016-22:04:05 to 04-08-2016-23:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	353
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	184
79.176.112.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
207.241.229.248	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	24
134.35.172.113	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
155.41.89.18	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
134.35.172.113	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
79.194.71.235	Germany	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.64.228.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	8
169.0.177.194	South Africa	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.200.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.231.102.118	Kuwait	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.231.102.118	Kuwait	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.250.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
106.38.241.150	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
2.54.176.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
173.77.16.91	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
62.56.255.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.64.228.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
155.41.89.18	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
65.55.210.241	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
154.70.157.1	Uganda	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.53.43.119	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
154.70.157.1	Uganda	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
87.70.59.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.210.246.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.159.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.81	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.71.72.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.26.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
92.241.34.143	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.179.117.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.69.34	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.113.109.195	Canada	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.83.57.49	Senegal	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.65.61.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.16.221	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.128.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
79.181.194.177	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

04-08-2016-22:04:05 to 04-08-2016-23:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.111.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.111.72	Block	6
46.120.23.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
17.138.56.13	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
151.25.105.145	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
5.29.110.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
17.138.56.13	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.13	Block	2
85.65.232.46	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
54.210.18.124	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
207.46.13.105	United States	147.237.72.166	aka.idf.il	Unknown Parameter sidescroll in aka.idf.il/giyus/leshakot/	None	1
131.253.25.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.187.114.171	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /irj/portal	Block	1
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1283-	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza/	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	1
41.222.198.122	Congo, The Democratic Republic of the	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
157.55.39.154	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 93.158.152.52	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/size100x0/2427.jpg	Block	1
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
76.31.170.233	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
190.53.54.119	Honduras	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15558-en/dover.aspx.	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/size100x0/3493.jpg	Block	1
213.57.44.13	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
141.212.122.209	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
79.183.23.90	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
190.53.54.119	Honduras	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
109.253.140.231	Israel	147.237.76.31	nakchal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/authenticationservice.asmx/getauthuser	Block	1
149.50.76.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1

04-08-2016-22:04:05 to 04-08-2016-23:04:05