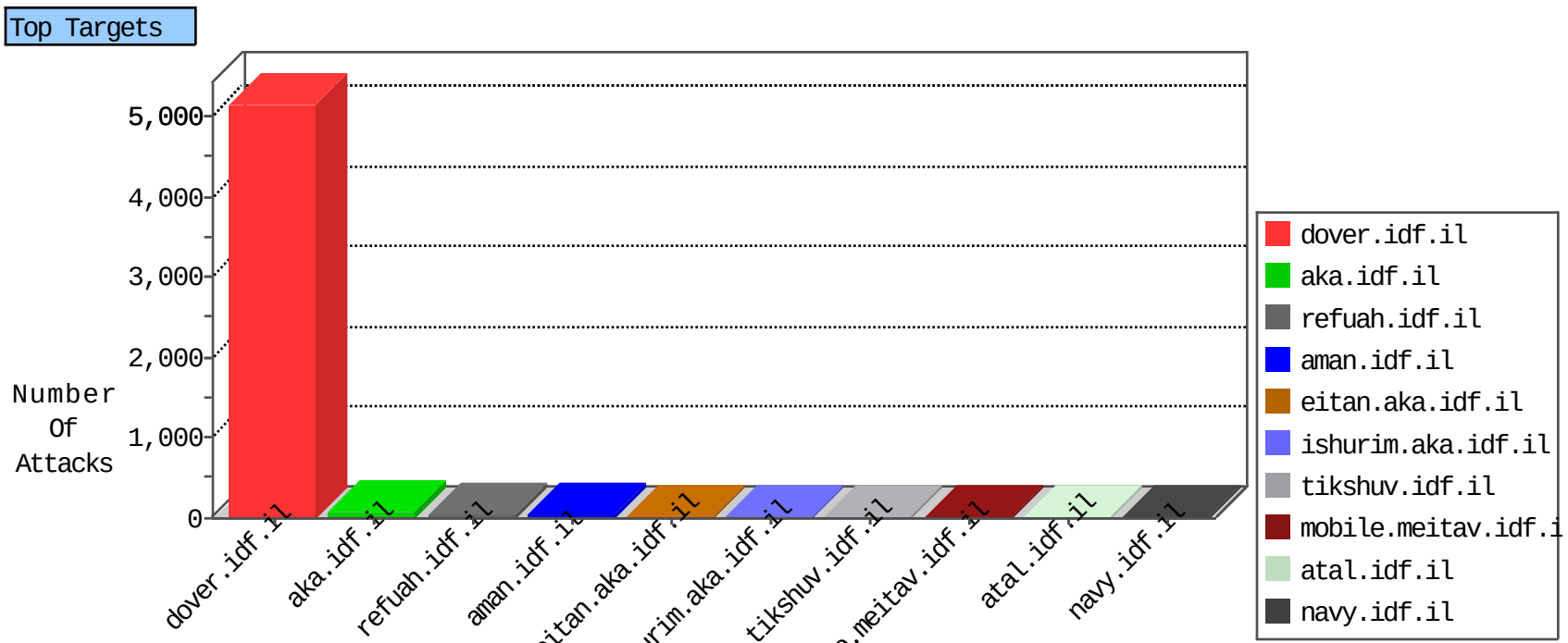
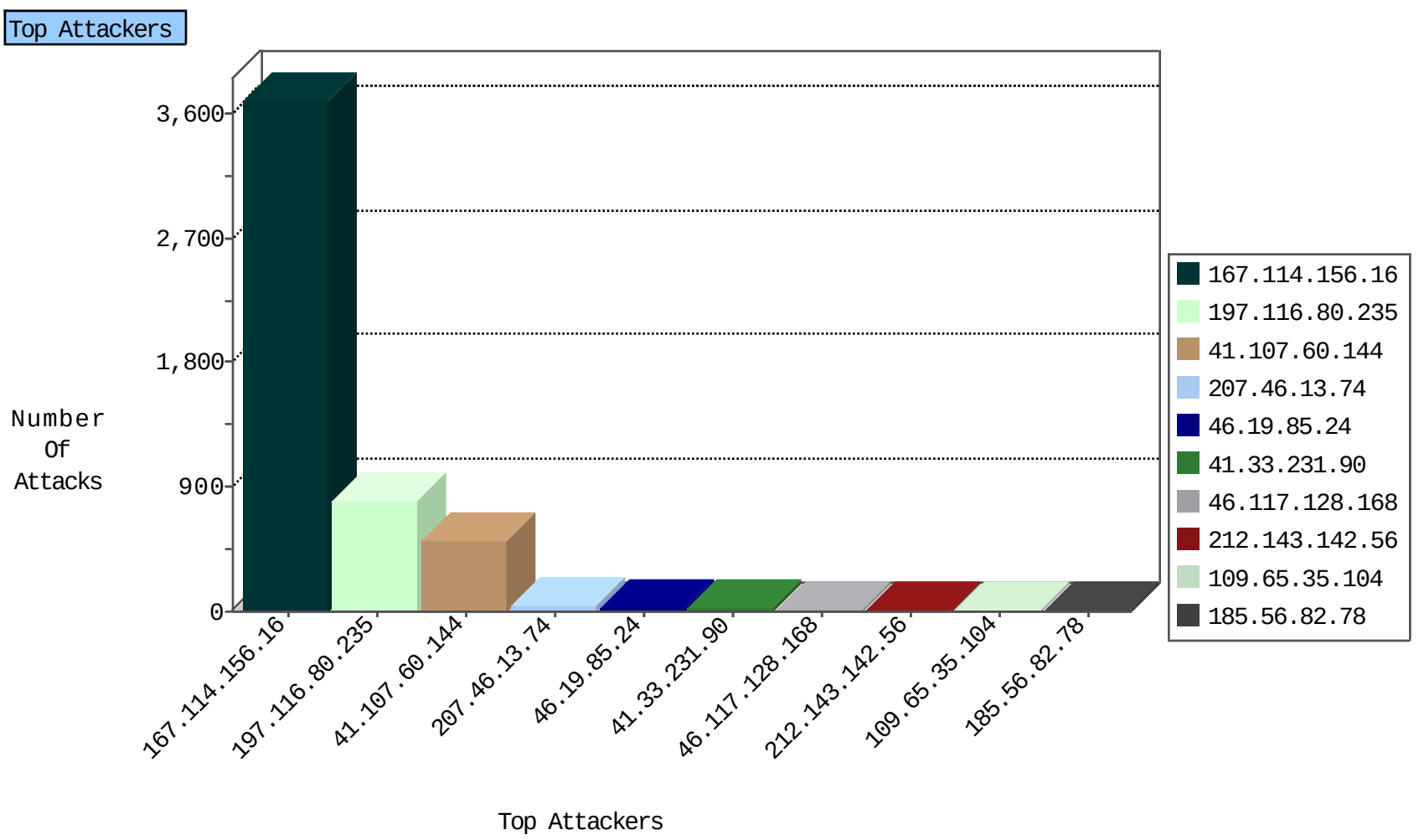
04-12-2016-00:04:00 to 04-12-2016-01:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-12-2016-00:04:00 to 04-12-2016-01:04:00

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	Block_Ip_Web_In	drop	3692
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	882
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	366
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	279
192.115.177.203	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	124
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	33
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
197.89.248.238	South Africa	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
82.145.220.213	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	2
10.0.0.1		147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	1
185.94.111.1	Russian Federation	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
64.233.172.163	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1

04-12-2016-00:04:00 to 04-12-2016-01:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.71.44.66	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.88.158.46	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.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

04-12-2016-00:04:00 to 04-12-2016-01:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
64.233.172.171	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
185.56.82.78	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
88.204.187.90	147.237.77.243	Kazakstan	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
185.56.82.78	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.78.38	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.82.78	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.56.82.78	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
24.37.17.226	147.237.8.14	Canada	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
151.11.201.3	147.237.77.178	Italy	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
151.11.201.3	147.237.77.178	Italy	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
107.158.255.194	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
185.56.82.78	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
107.158.255.194	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -f -sS	1
185.56.82.78	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.128.144.131	147.237.76.177	Canada	ncore.idf.il	ET SCAN NMAP -f -sS	1
185.56.82.78	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.94.36.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.56.82.78	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
185.56.82.78	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.56.82.78	147.237.0.15	Netherlands	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
24.37.17.226	147.237.8.14	Canada	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
151.11.201.3	147.237.77.178	Italy	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
108.21.79.196	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
107.158.255.194	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
185.56.82.78	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.128.144.131	147.237.76.177	Canada	ncore.idf.il	ET SCAN NMAP -sS window 2048	1

04-12-2016-00:04:00 to 04-12-2016-01:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	346
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	drop		drop	117
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	71
207.46.13.74	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	45
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	SYN Attack		reject	28
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
109.65.35.104	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
197.116.80.235	Algeria	147.237.77.216	dover.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	10
46.19.86.84	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.24	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.116.193.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
45.79.147.229	United States	147.237.76.39	mobile.meitav.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	6
46.19.85.24	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.224.149	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
62.219.137.5	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.74	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.121.211.156	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.121.211.156	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.65.1.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.83.144	United States	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
134.3.2.222	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
104.38.57.188	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.182.103.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.43.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.240.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.92.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.44.248.124	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.178.207.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.124.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.5.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.171.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.22.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.133.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.204.52	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.66.237.115	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.182.31.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.36.5	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
82.166.100.163	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
41.44.248.124	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
217.153.185.109	Poland	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.30.24.47	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.117.128.168	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	5
199.30.24.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.117.128.168	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/3/	Block	3
65.55.210.98	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.36	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.196	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	3
46.19.85.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.25.34	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.63	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.102	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
213.57.203.71	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/size220x0/sip_storage	Block	2
46.117.128.168	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 46.117.128.168	Block	2
157.55.39.65	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
84.228.224.149	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
213.8.204.14	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
64.79.85.205	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/shared/usercontrols/headerupper/	Block	1
45.79.147.229	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /	Block	1
198.58.103.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
109.64.124.40	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
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
157.55.39.194	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/mpm/neot_yuvalim.asp	Block	1
84.228.224.149	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
109.206.153.8	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
77.75.76.160	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn	Block	1
46.121.211.156	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1806.jpg	Block	1
173.208.46.155	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/brothers/skira/default.asp	None	1
85.64.71.154	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/71513	Block	1
109.226.44.156	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.182.216.51	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
47.18.37.40	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-en/dover.aspx application	Block	1
173.232.20.121	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
87.69.79.31	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1
157.55.39.13	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
82.231.209.52	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/marchandising	Block	1
207.46.13.72	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/faq/faq.aspx	Block	1
62.219.137.5	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
5.41.66.190	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/idf-admin	Block	1
185.120.125.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
109.64.52.97	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

04-12-2016-00:04:00 to 04-12-2016-01:04:00