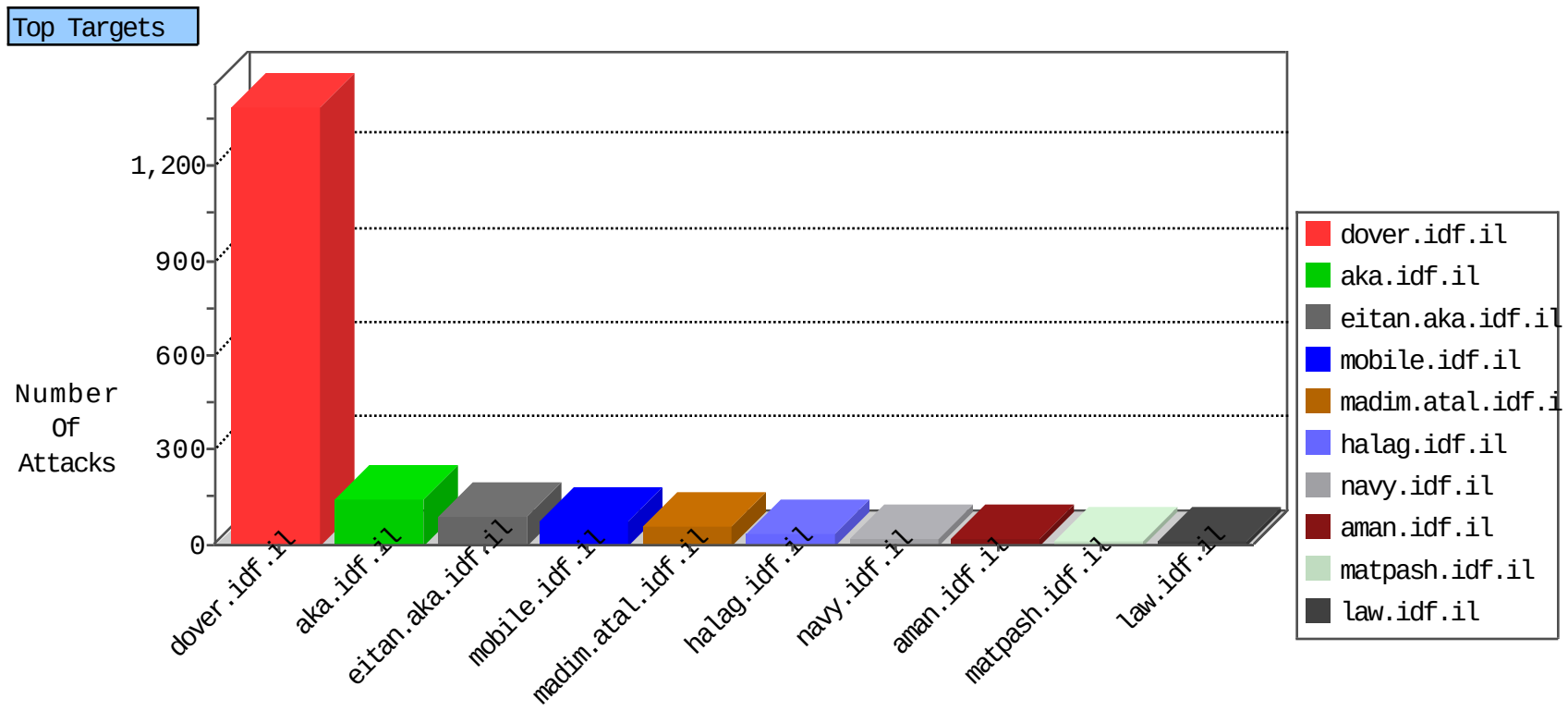
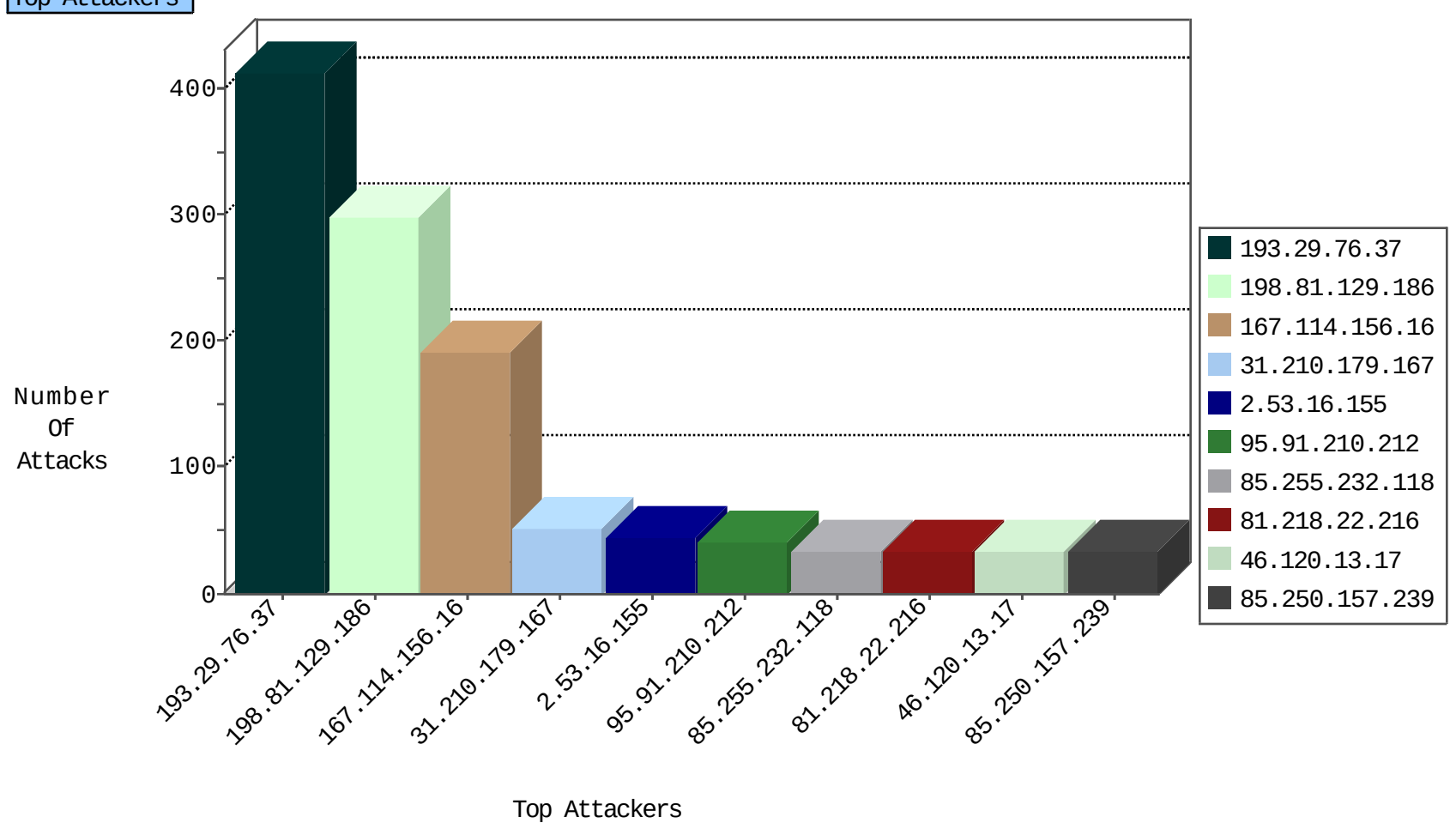
04-28-2016-16:04:07 to 04-28-2016-17:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-28-2016-16:04:07 to 04-28-2016-17:04:07

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	11504
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	6444
191.249.111.93	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	401
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	214
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
93.173.59.140	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
68.116.5.134	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	2
207.46.13.137	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.66.5	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.136.2	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

04-28-2016-16:04:07 to 04-28-2016-17:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.62.106	Israel	147.237.76.86	navy.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	4

04-28-2016-16:04:07 to 04-28-2016-17:04:07

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
66.249.81.218	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	2
107.158.255.194	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.158	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
185.110.132.55	147.237.77.74	Ukraine	law.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.72.217	Indonesia	e.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.55	147.237.76.86	Ukraine	navy.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.140.23	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
109.160.174.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.158.255.194	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
101.200.82.129	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.72.217	Indonesia	e.idf.il	ET SCAN NMAP -sS window 2048	1
185.110.132.55	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.72.217	Indonesia	e.idf.il	ET SCAN NMAP -f -sS	1
185.110.132.55	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
139.217.27.204	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 3072	1

04-28-2016-16:04:07 to 04-28-2016-17:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
193.29.76.37	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	413
198.81.129.186	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	288
31.210.179.167	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
95.91.210.212	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
85.255.232.118	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
85.250.157.239	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
81.218.22.216	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
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
93.169.133.52	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
45.55.58.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
50.158.169.180	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
1.39.39.72	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.120.13.17	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
162.243.104.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.120.13.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.184.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.222.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.18.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.81.129.193	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.120.13.17	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.147.247	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
37.26.147.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
37.26.147.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.147.247	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
46.19.85.46	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
88.254.109.108	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.8.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
188.66.85.218	United Kingdom	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
5.102.195.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.76.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.57.187.212	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.18.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.88.38.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.37.171.106	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
208.54.86.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.168.118.254	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
207.46.13.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
95.186.117.96	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

04-28-2016-16:04:07 to 04-28-2016-17:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.16.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
198.81.129.186	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
132.3.25.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
185.32.179.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
84.108.62.106	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/9/2199.jpg	Block	4
132.3.25.78	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
84.108.62.106	Israel	147.237.76.86	navy.idf.il	Unauthorized HTTP Method	Block	4
2.53.51.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
132.3.25.80	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.184.78	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
149.88.38.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
149.88.38.118	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	3
109.67.180.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.222.92	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
204.79.180.208	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.159	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/602-2265-he/patzar.aspx - paragraph_12	Block	1
176.13.8.125	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.67.117.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
77.75.77.62	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/32/	Block	1
46.19.85.46	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
198.81.129.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.250.157.239	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
207.46.13.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12535-he/dover.aspx×ž×ª×’×™×¡×•	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/smalim.aspx	Block	1
2.53.182.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
80.246.140.55	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
198.81.129.207	United States	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	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-8829-he/atal.aspx	Block	1
208.115.113.82	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/templatecontrols/generic/	Block	1
66.249.79.87	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
188.0.131.83	Kazakstan	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
84.94.21.217	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/contactus/mobile	Block	1
204.79.180.89	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
51.255.65.21	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/portalmiluim/templates/www.behazdaa.org	Block	1
109.64.138.59	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
213.57.187.212	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.22.135.176	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
188.225.130.127	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
204.79.180.94	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
62.1.114.100	Greece	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.117.232	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.67.117.232	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/home/def...78&catid=38978	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

04-28-2016-16:04:07 to 04-28-2016-17:04:07