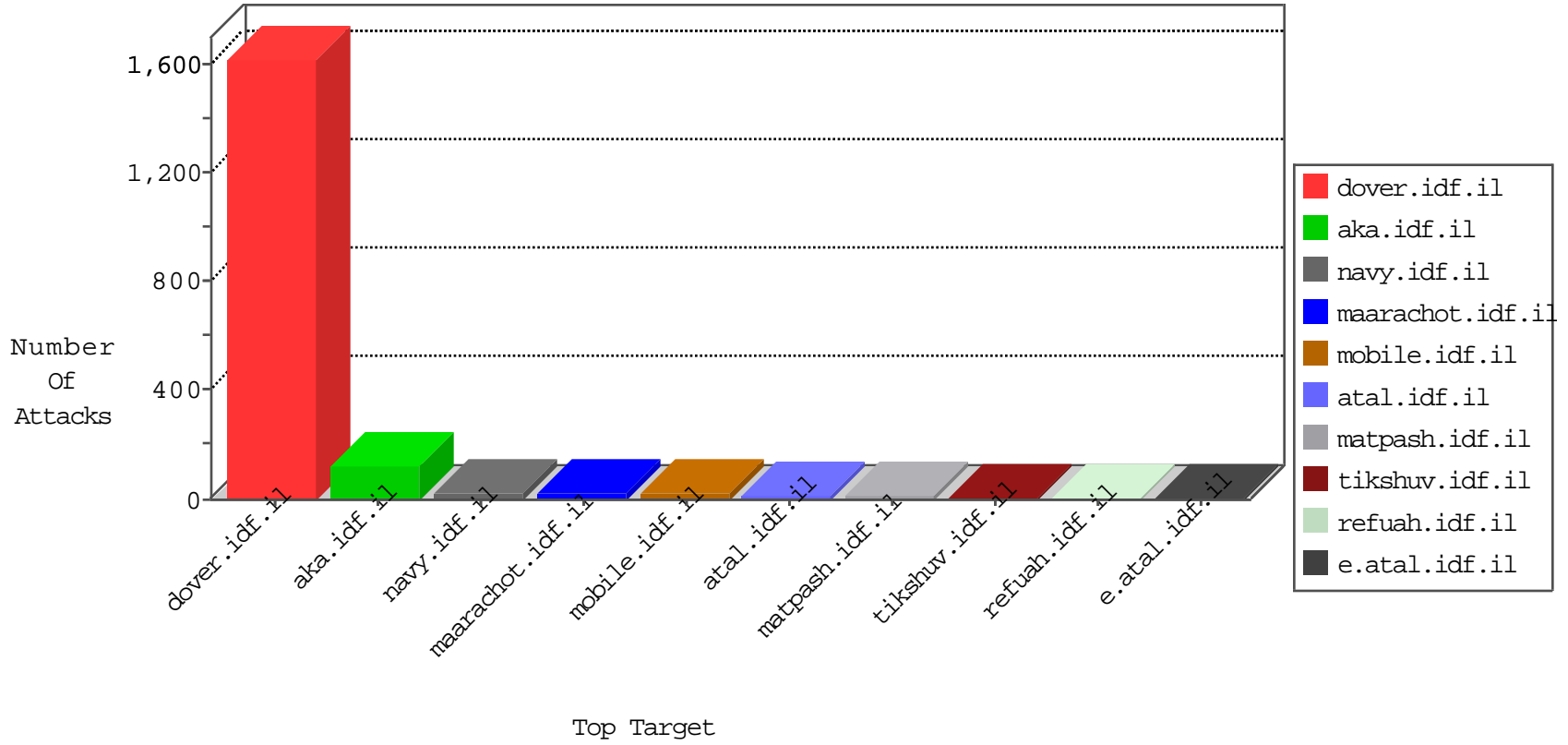


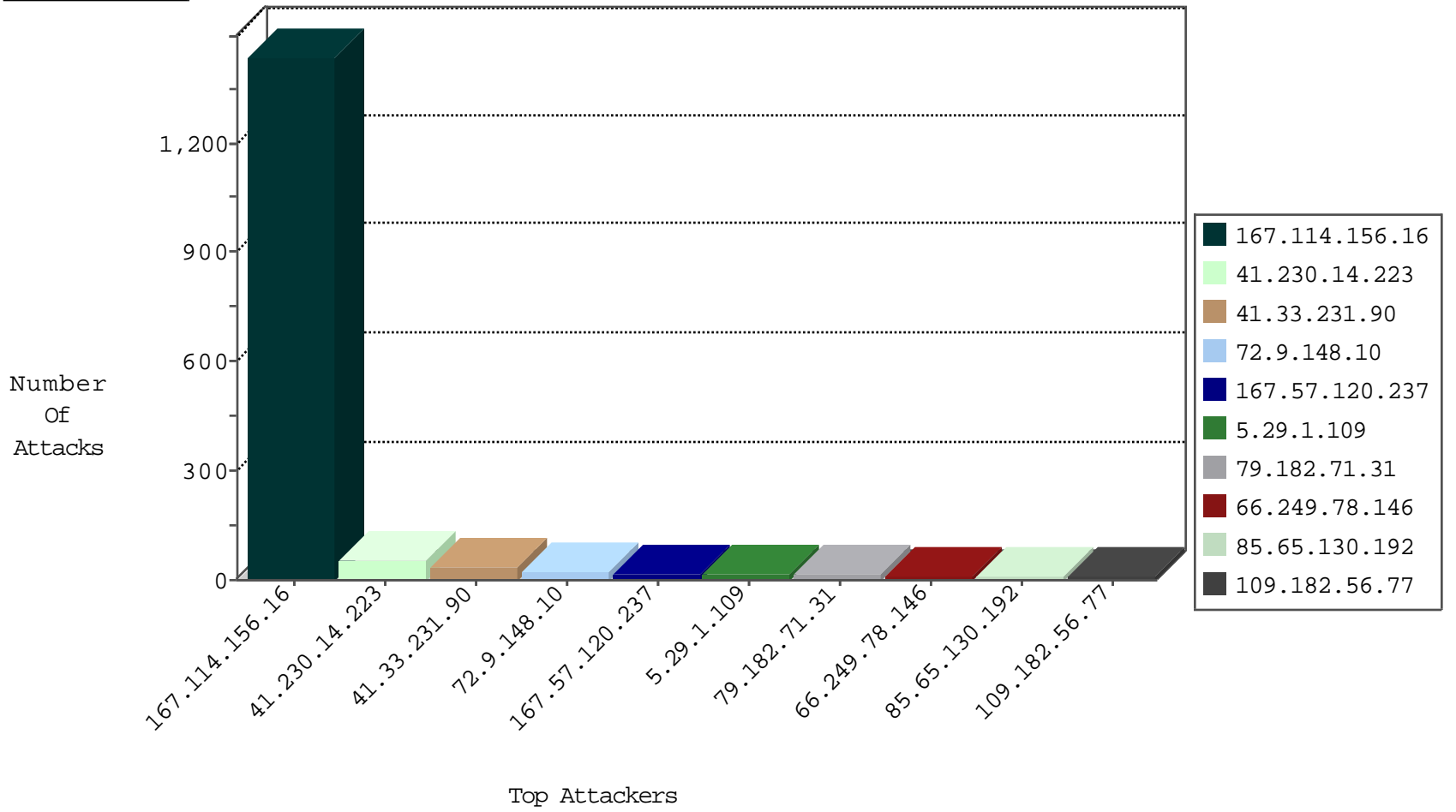
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	DOS-Tool-SwitchbladG	dest-reset	3552
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	69

01-02-2016-01:07:03 to 01-02-2016-02:07:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Block	1

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
125.65.165.215	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
218.199.48.57	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.146	147.237.72.166	United States	aka.idf.il	WEB-CGI redirect access	1
218.199.48.57	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
183.60.252.84	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 2048	1
181.25.11.117	147.237.76.31	Argentina	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
125.65.165.215	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
125.65.165.215	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
218.199.48.57	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
125.65.165.215	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
218.199.48.57	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
218.199.48.57	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.252.84	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 4096	1
183.60.252.84	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -f -sS	1
168.62.238.153	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.165.215	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
218.199.48.57	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	drop	SAM rule	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
79.182.71.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.182.56.77	Slovenia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
85.65.130.192	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
79.180.37.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
104.130.65.175	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
109.67.50.218	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
5.29.1.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
5.29.1.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
167.57.120.237	Uruguay	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
109.253.139.54	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.59	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.52.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
167.57.120.237	Uruguay	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.29	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
167.57.120.237	Uruguay	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.142.238.128	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.39.52	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.253.138.253	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
40.77.167.95	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
157.55.39.8	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.181.184.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.60.125	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.171.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.11.45.21	Palestinian Territory, Occupied	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
128.127.107.126	Netherlands	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.145.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.146.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
77.237.146.28	Czech Republic	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
85.65.145.144	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
84.111.38.159	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.183.202.248	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
85.65.145.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
46.120.72.186	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.177.132.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
54.183.217.178	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
91.200.12.137	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
109.253.138.253	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	4
41.131.97.114	Egypt	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	3
41.131.97.114	Egypt	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
109.67.51.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.182.71.31	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.182.71.31	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
5.29.1.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.121.65.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.8.204.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
109.253.209.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.65.49.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.73.227	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/dangotkenesesh.aspx	Block	1
166.62.116.223	United States	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/redirects/ssl-redirect.html	Block	1
128.127.107.126	Netherlands	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
52.90.147.70	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery.plugins/jquery.equalheights.js	Block	1
2.54.170.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.242.246.23	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/writetous/default.asp	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
166.62.116.223	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/xmlrpc.php	Block	1
46.19.86.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
141.212.122.160	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3142.jpg	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
166.62.116.223	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
109.253.139.54	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.182.71.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sip_storage/files/3/	Block	1
66.249.78.194	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
149.202.98.161	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
40.77.167.76	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8921-he/refuah.aspx	Block	1
166.62.116.223	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
109.253.194.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.166.137.204	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.228.180.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.206	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
164.138.120.166	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.73.227	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.73.227	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1