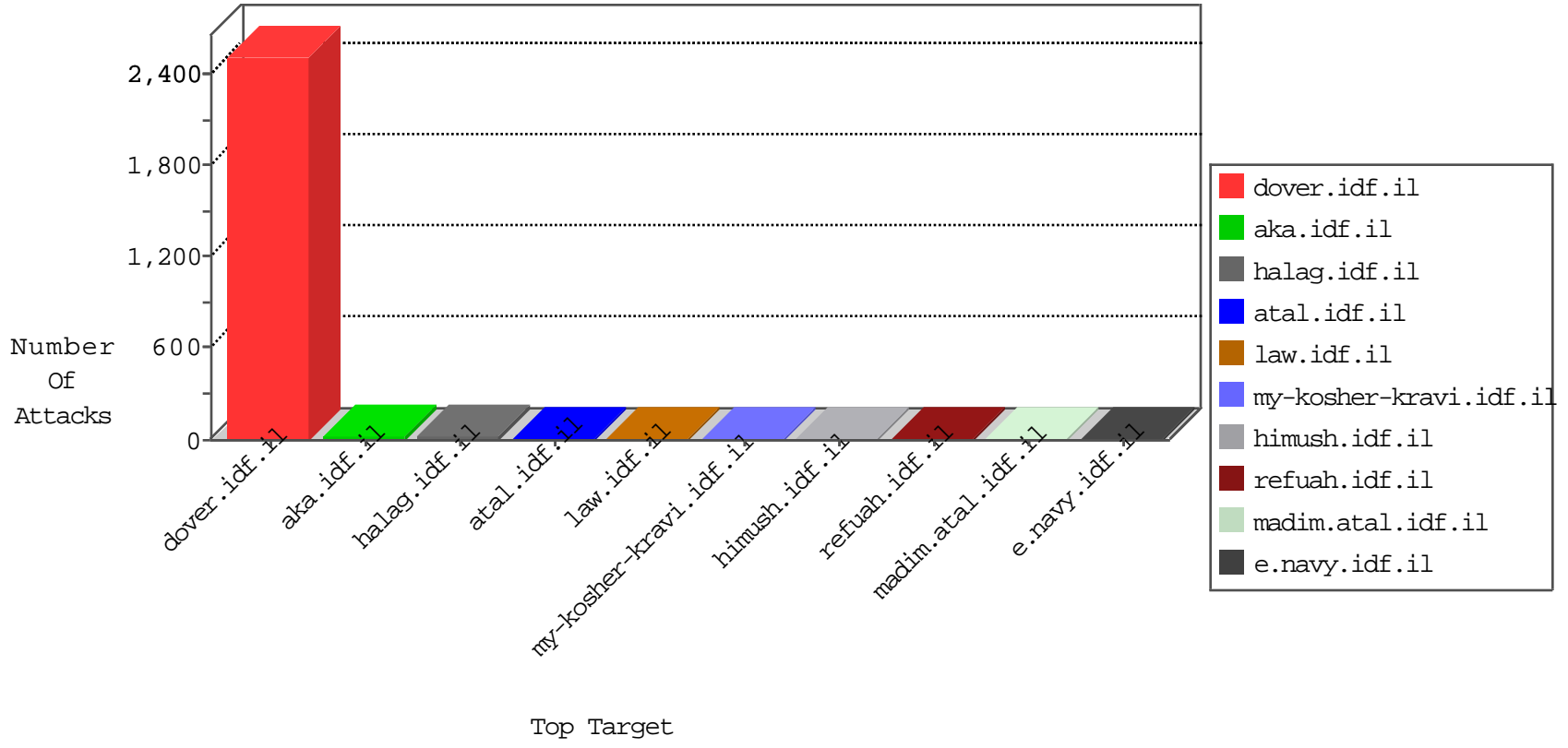


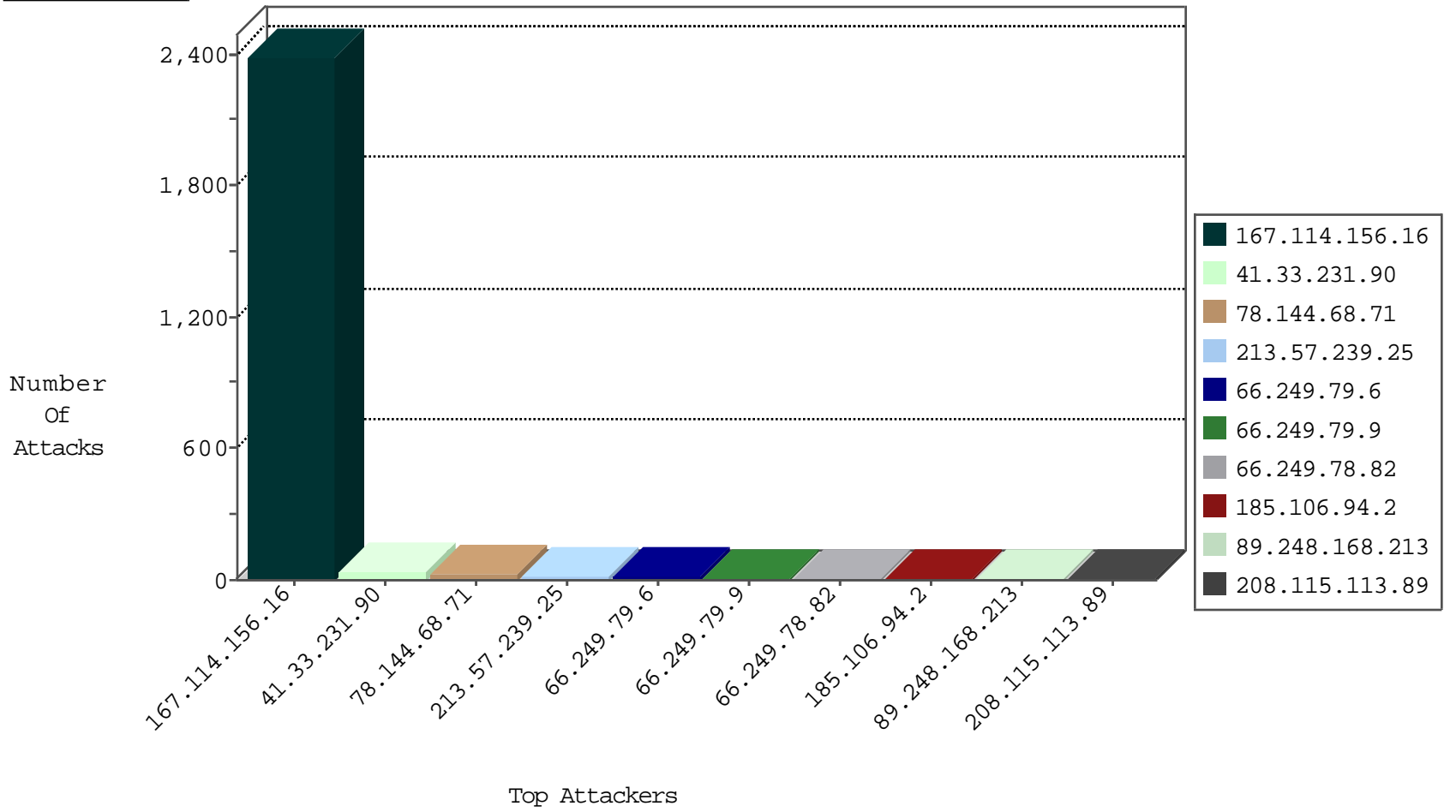
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6346
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3525

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.106.94.2		147.237.77.233	atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
185.106.94.2		147.237.77.233	atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
188.165.15.224	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
193.111.140.153	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
118.238.1.113	Japan	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	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
203.151.93.164	147.237.76.42	Thailand	refuah.idf.il	ET SCAN Potential SSH Scan	2
187.160.109.22	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.106.94.2	147.237.77.233		atal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
177.238.237.5	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.168.213	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.168.213	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.181	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
89.248.168.213	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.181	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
89.248.168.213	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
203.151.93.164	147.237.76.39	Thailand	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
185.112.102.222	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
177.238.237.5	147.237.77.235	Mexico	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
133.130.118.109	147.237.0.34	Japan	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.168.213	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.168.213	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.181	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
89.248.168.213	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
203.151.93.164	147.237.76.30	Thailand	himush.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
78.144.68.71	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
213.57.239.25	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.79.9	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.64.195	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
89.138.0.201	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.95.50	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
167.88.12.201	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
65.55.210.145	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.108.108.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
84.108.108.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.64.207.163	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
62.210.136.217	France	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
74.82.47.47	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.100	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
8.37.228.77	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
141.212.122.145	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.138.0.201	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.90.57.196	United States	147.237.77.170	maarachot.idf.il	Directory Traversal	directory traversal overflow	monitor	1
74.82.47.31	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
146.185.239.102	Russian Federation	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.141	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
218.22.211.69	China	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.146	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.31	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.78.149.185	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.144	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.8	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.96	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.147	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
120.36.226.3	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.34	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
149.78.149.185	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.144	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.19	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.211	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.154	United States	147.237.0.33	idf.il	drop		drop	1
132.3.65.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.43	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.76	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
157.55.39.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
141.212.122.145	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.1.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.150.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
109.66.185.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1134-he/dover.aspx	Block	1
37.26.149.164	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$LoginControl\$captcha\$captchaText in www.aka.idf.il/main/giyus/default.aspx	None	1
120.36.226.3	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/editor/assetmanager/assetmanager.asp	Block	1
85.250.227.151	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
208.90.57.196	United States	147.237.77.170	maarachot.idf.il	URL is Above Root Directory www.maarachot.idf.il/../../	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12801-he/dover.aspxx"x?"xe	Block	1
5.255.253.116	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
157.55.39.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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
77.75.79.32	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/25/	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1153-en/dover.aspx	Block	1
178.154.243.93	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
37.26.149.188	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1
130.193.50.20	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
92.96.74.124	United Arab Emirates	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1065-he/dover.aspx	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
5.255.253.151	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.218	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1402-he/atal.aspx	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
85.64.207.163	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation searchText in www.idf.il/1560-en/dover.aspx	Block	1
178.154.243.95	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
141.8.142.27	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
92.96.74.124	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3294.jpg	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1065-en/dover.aspx	Block	1
5.255.253.185	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
176.12.145.252	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	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
85.250.227.151	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 85.250.227.151	Block	1
188.143.232.21	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/homepage.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.64.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
2.54.153.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.129	United States	147.237.77.233	atal.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
95.108.158.158	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1664	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1133-he/dover.aspx	Block	1
37.26.149.164	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
176.12.145.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
85.250.227.151	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
207.46.13.49	United States	147.237.72.166	aka.idf.il	Unknown Parameter cd5b9038 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1