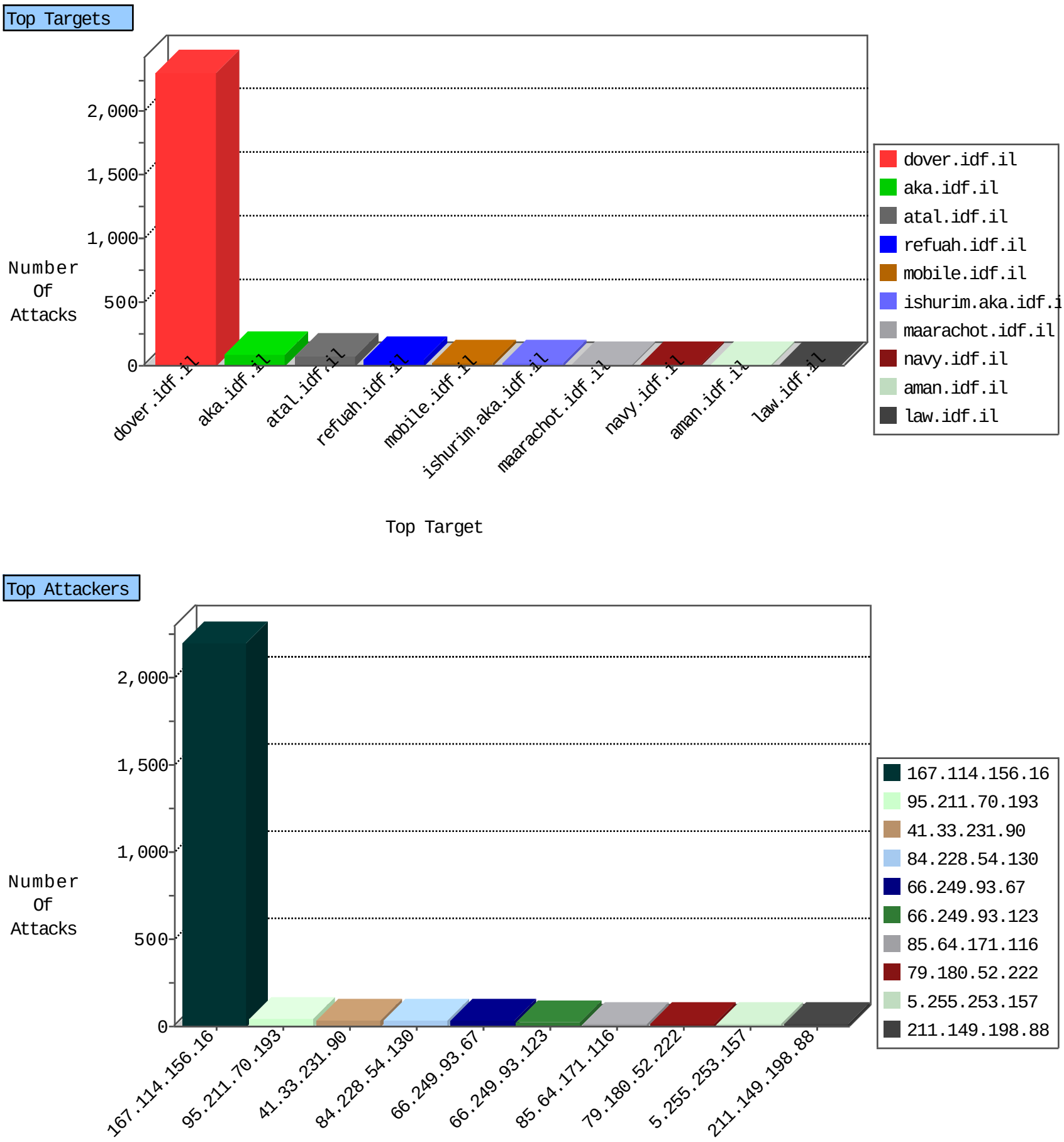
12-18-2015-07:04:09 to 12-18-2015-08:04:09

IDF Under Attack
Daily Report



12-18-2015-07:04:09 to 12-18-2015-08:04:09

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	3517
180.97.106.36	China	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.162	China	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1

12-18-2015-07:04:09 to 12-18-2015-08:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.207		147.237.76.42	refuah.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	6
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
185.130.5.207		147.237.76.42	refuah.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

12-18-2015-07:04:09 to 12-18-2015-08:04:09

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
94.102.48.195	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.56.37.47	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.39.222.253	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
192.162.100.148	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.207	147.237.76.42		refuah.idf.il	ET WEB_SERVER Muieblackcat scanner	1
180.250.66.131	147.237.0.16	Indonesia	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
123.220.251.190	147.237.72.166	Japan	aka.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
116.233.79.200	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
116.233.79.200	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
116.202.32.18	147.237.77.216	India	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
220.231.195.122	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
189.198.25.48	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.250.66.131	147.237.0.33	Indonesia	idf.il	ET SCAN Potential SSH Scan	1
123.220.251.190	147.237.76.31	Japan	nakchal.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
123.220.251.190	147.237.72.156	Japan	aman.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
116.233.79.200	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
116.233.79.200	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1

12-18-2015-07:04:09 to 12-18-2015-08:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
95.211.70.193	Netherlands	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
84.228.54.130	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	14
79.180.52.222	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.64.171.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop		drop	8
5.102.254.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
66.249.93.67	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.93.67	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.136.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.67.63.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop		drop	5
66.249.93.123	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.93.123	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
95.211.70.193	Netherlands	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
159.203.91.105	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
66.249.69.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.95.211.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop		drop	3
79.183.211.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
213.57.131.49	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.102.254.67	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.93.127	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
199.30.25.255	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
68.65.120.48		147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
68.65.120.48		147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.93.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
123.220.251.190	Japan	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
218.22.211.69	China	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
87.69.132.141	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
192.114.21.43	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
45.35.71.181		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
77.237.138.202	Czech Republic	147.237.77.19	law-forum.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
184.105.139.99	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
68.65.120.48		147.237.0.35	akaws.idf.il	drop		drop	1
149.50.87.164	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
185.130.5.207		147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

12-18-2015-07:04:09 to 12-18-2015-08:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
211.149.198.88	China	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	5
109.65.155.179	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.155.179	Block	3
211.149.198.88	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 211.149.198.88	Block	3
211.149.198.88	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/plus/download.php	Block	2
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
109.253.134.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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
77.237.138.202	Czech Republic	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	1
46.19.85.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
109.65.155.179	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	1
84.228.54.130	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
123.220.251.190	Japan	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/manager/html	Block	1
24.184.27.89	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
79.180.180.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.90.131.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.67.222.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
85.93.91.84	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
66.249.93.67	Israel	147.237.77.233	atal.idf.il	URL is Above Root Directory www.atal.idf.il/../../images/shared/menustrech.png	Block	1
141.212.122.112	United States	147.237.72.166	aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
37.142.64.119	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.182.123.178	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9364-he/refuah.aspx	Block	1
95.211.70.193	Netherlands	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1824-he/dover.aspx	Block	1
37.142.64.119	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
157.55.39.28	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
81.209.177.95	Europe	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9057-he/refuah.aspx	Block	1
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	1
123.220.251.190	Japan	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/manager/html	Block	1
95.211.70.193	Netherlands	147.237.72.166	aka.idf.il	Multiple signatures from 95.211.70.193	Block	1
68.180.231.40	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/	Block	1
45.35.71.181		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.226	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
81.209.177.189	Europe	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/contactform/contactform.aspx	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18562-he/dover.aspx	Block	1
123.220.251.190	Japan	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/manager/html	Block	1

12-18-2015-07:04:09 to 12-18-2015-08:04:09