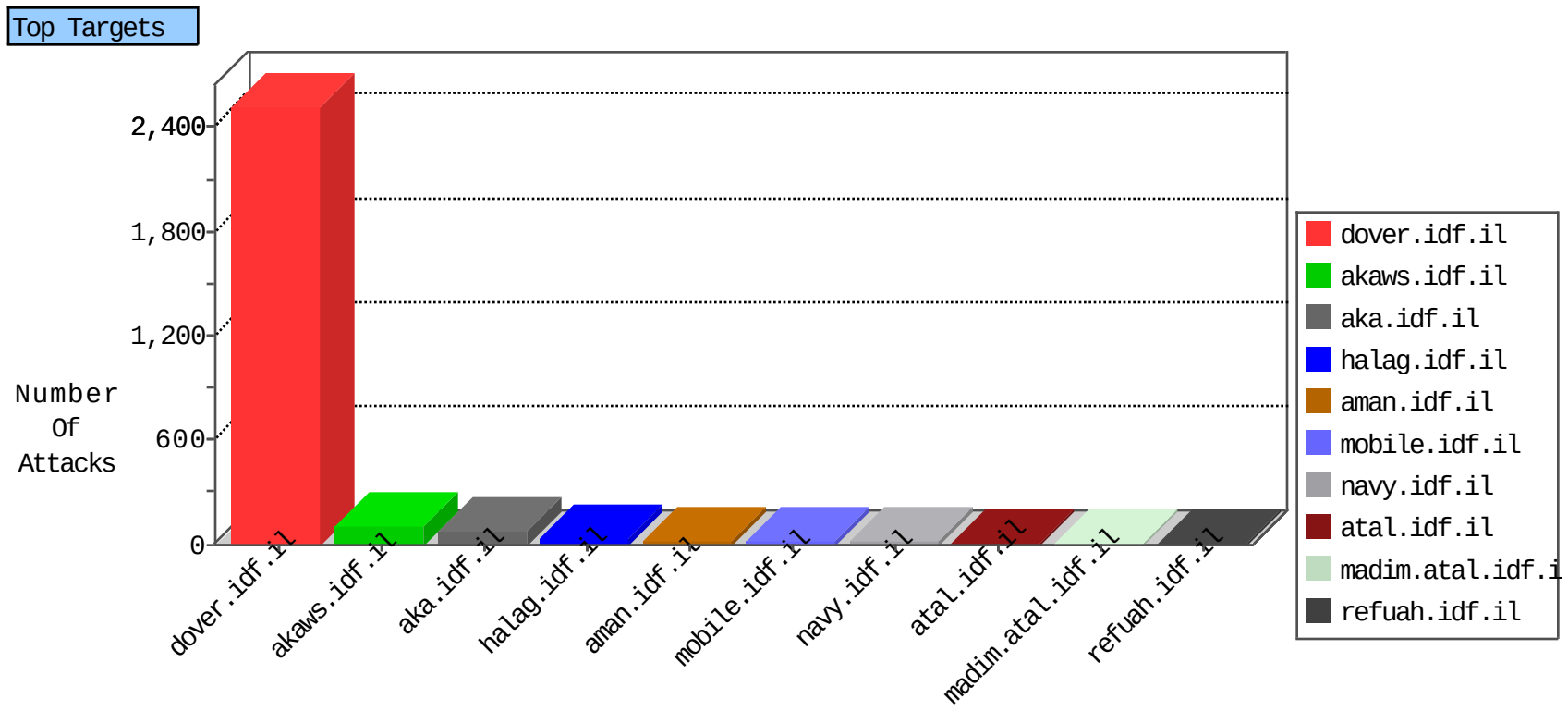
12-18-2015-23:04:08 to 12-19-2015-00:04:08

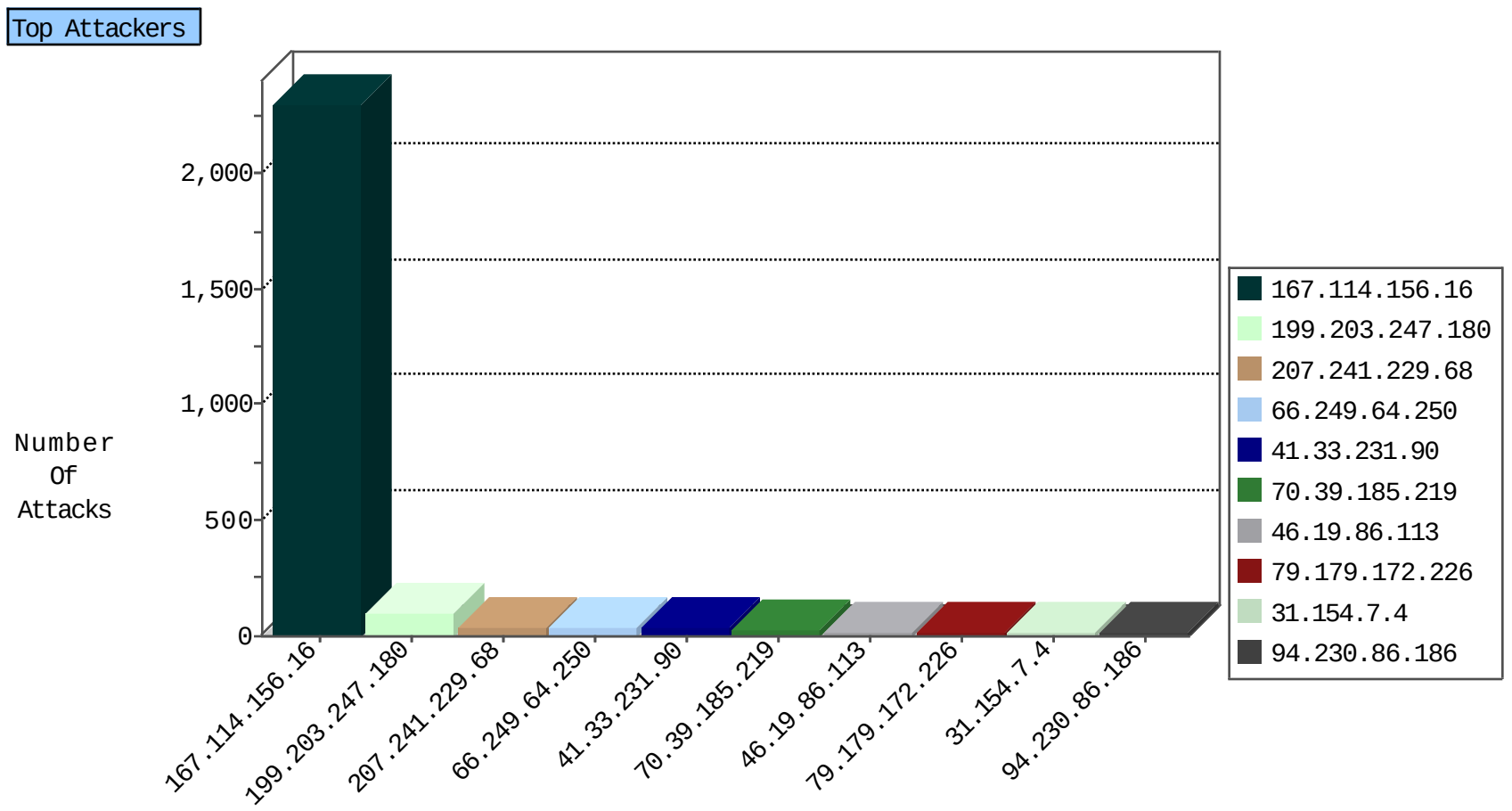
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-18-2015-23:04:08 to 12-19-2015-00:04:08

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	3453
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	891
70.39.185.219	Satellite Provider	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
70.39.185.219	Satellite Provider	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
70.39.185.219	Satellite Provider	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Htps	drop	1

12-18-2015-23:04:08 to 12-19-2015-00:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-18-2015-23:04:08 to 12-19-2015-00:04:08

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	3
84.245.15.57	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
180.97.221.22	147.237.77.216	China	dover.idf.il	SQL Injection - Select From	1
180.97.221.22	147.237.77.216	China	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	1
180.97.221.22	147.237.77.216	China	dover.idf.il	ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt	1
112.196.49.101	147.237.77.170	India	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
110.153.0.131	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.245.15.57	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.245.15.57	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
180.97.221.22	147.237.77.216	China	dover.idf.il	SQL generic sql with comments injection attempt - GET parameter	1
180.97.221.22	147.237.77.216	China	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	1
180.97.221.22	147.237.77.216	China	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	1
177.240.51.37	147.237.76.30	Mexico	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.196.49.101	147.237.77.170	India	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
84.245.15.57	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

12-18-2015-23:04:08 to 12-19-2015-00:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
199.203.247.180	Israel	147.237.0.35	akaws.idf.il	drop		drop	103
207.241.229.68	United States	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	38
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	31
66.249.73.228	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.113	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
70.39.185.219	Satellite Provide	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
94.230.86.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
40.77.167.41	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.7.4	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.179.172.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.186	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.18.112	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.33.82	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.113	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.18.112	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.179.172.226	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
87.69.49.202	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	4
79.182.106.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.113.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.7.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.22.134.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.158.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.7.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.180.60.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.135.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.199.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
90.59.10.144	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
70.39.185.219	Satellite Provide	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
149.78.32.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.97.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.72.178	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.43	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.246.50.213	Sweden	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
162.209.124.35	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
213.57.44.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
66.249.73.244	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
195.239.16.40	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.86.104	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.86.5	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
213.57.44.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
195.239.16.53	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
79.183.127.230	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
169.229.3.90	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
5.22.131.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

12-18-2015-23:04:08 to 12-19-2015-00:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.68.10	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	3
37.142.68.10	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	3
185.32.179.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 204.13.200.200	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	2
84.111.12.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.255.253.62	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	2
84.229.198.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.179.150.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	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	1
66.249.78.34	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/6/1706.pdf	Block	1
180.97.221.22	China	147.237.77.216	dover.idf.il	Multiple MSSQL Data Retrieval with Implicit Conversion Errors(+) from 180.97.221.22	None	1
51.254.39.246	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
93.172.43.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.172.226	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.179.172.226	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.111.73	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
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
84.108.136.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.175.25.171	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/shared/usercontrols/headerupper/	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
180.97.221.22	China	147.237.77.216	dover.idf.il	Multiple signatures from 180.97.221.22	Block	1
51.254.39.246	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-signup.php	Block	1
95.13.165.44	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/g	Block	1
79.179.172.226	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sip_storage/	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
54.154.238.9	United States	147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/../images/shared/home.png	Block	1
180.97.221.22	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/news/html/	Block	1
40.77.167.7	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
95.160.16.164	Poland	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
79.180.60.183	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20187-he/dover.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
37.26.148.198	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
79.176.123.153	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
54.209.60.63	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
40.77.167.105	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
95.160.16.164	Poland	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/administrator	Block	1
79.181.24.243	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1540-13036-he/dover.aspx target=	Block	1
66.249.78.20	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/4/1704.pdf	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/kkkkkkk=07595daakkkkkkk_07595daa	Block	1

12-18-2015-23:04:08 to 12-19-2015-00:04:08