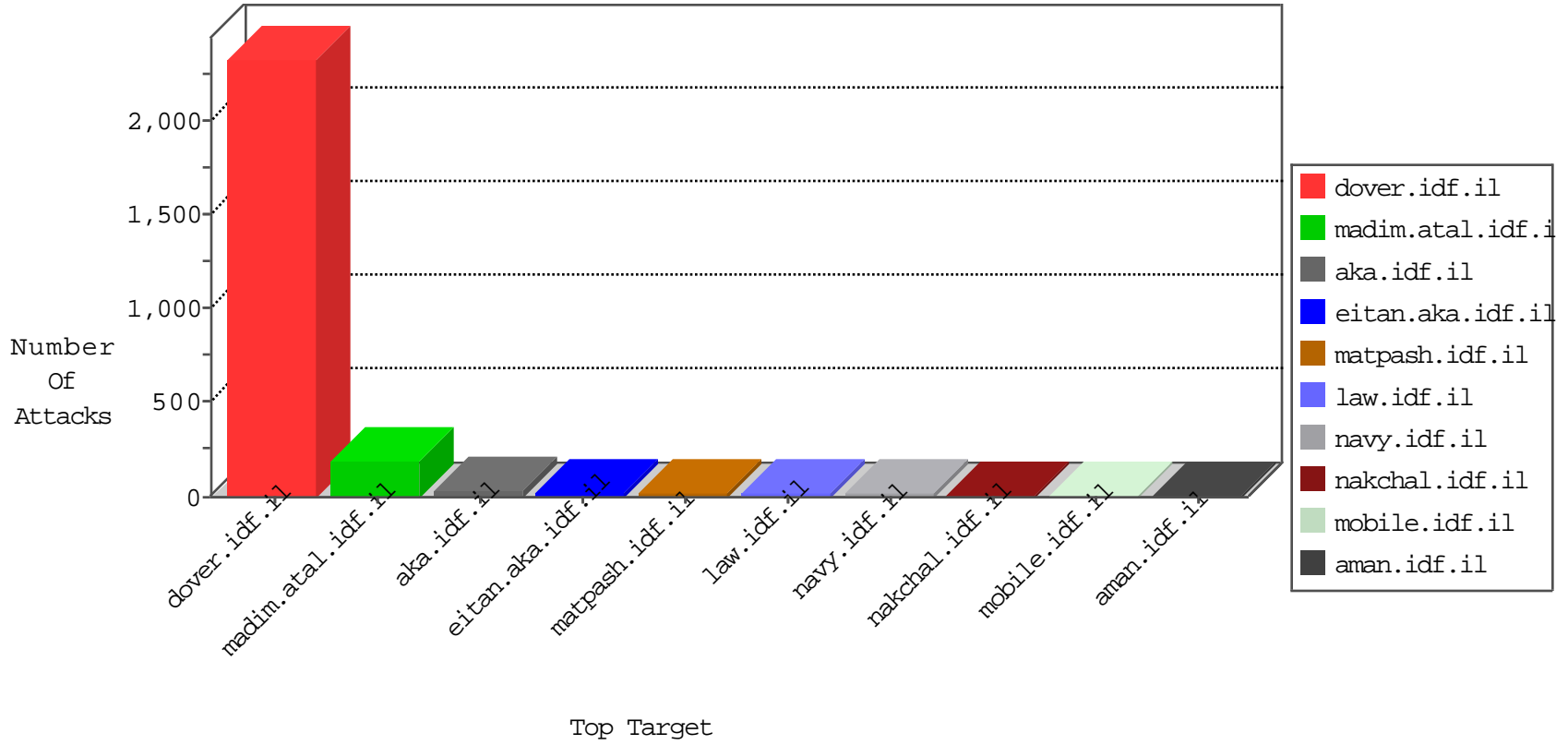


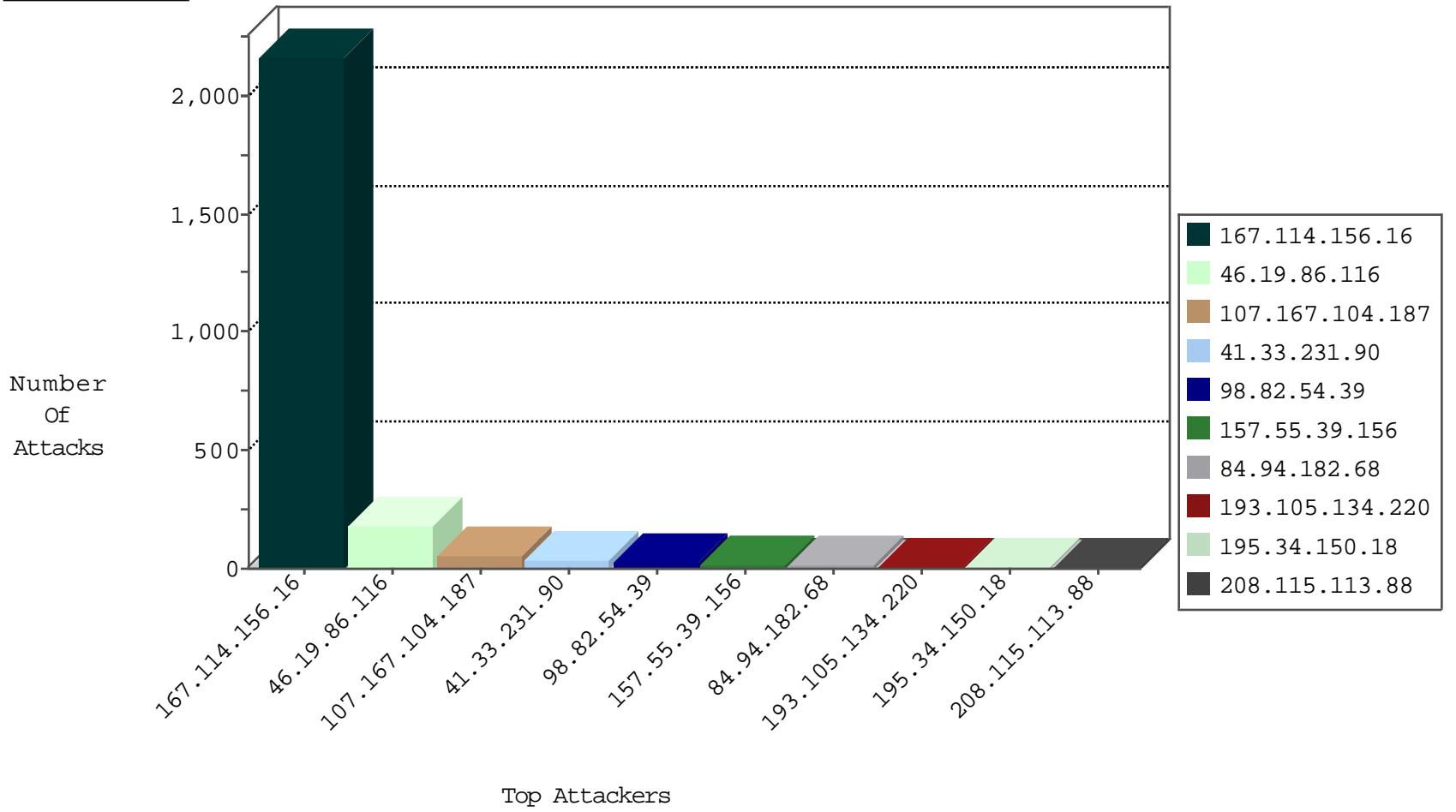
IDF Under Attack Daily Report



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	3296
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	583
66.249.69.93	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	52
115.239.228.10	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
124.161.142.10	China	147.237.8.45	e.eitan.idf.i	Invalid TCP Flags	drop	2

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
110.80.61.191	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
197.52.92.47	Egypt	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	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
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
193.201.227.84	147.237.0.15	Ukraine	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
172.98.200.238	147.237.77.121		e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
101.23.2.175	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
68.71.165.35	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.84	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.238	147.237.77.121		e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
168.62.238.153	147.237.76.148	United States	ggcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
79.174.70.237	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
107.167.104.187	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
157.55.39.156	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
98.82.54.39	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.99	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.52.11.236	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
98.82.54.39	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
98.82.54.39	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
98.82.54.39	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.52.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.174	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
130.193.50.1	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.47.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
50.18.94.121	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
109.253.158.144	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
50.87.144.178	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
195.154.184.104	France	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
157.55.39.198	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
131.253.24.158	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.82	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.64.68	Netherlands	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.212	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.120.57.180	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.119	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.109.113.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
193.105.134.220	Sweden	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
62.210.139.78	France	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.95	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.56	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
131.253.26.249	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.84	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.28.180.101	Israel	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
80.82.64.68	Netherlands	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
193.105.134.220	Sweden	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
155.133.82.40	Poland	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
94.23.217.180	France	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
193.105.134.220	Sweden	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
69.124.195.57	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.115	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	132
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.116	Block	47
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	6
84.94.182.68	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.94.182.68	Block	5
85.250.108.86	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	4
84.94.182.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
80.246.136.51	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
184.168.200.129	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	2
84.94.182.68	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.94.182.68	Block	2
198.71.228.68	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
84.94.182.68	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	2
176.10.104.243	Switzerland	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
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
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/drushim/misrot.aspx	Block	1
62.210.84.121	France	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/wp-login.php	Block	1
188.143.232.40	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/searchresults/searchresults.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
157.55.39.5	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
198.154.225.251	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	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
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
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
62.219.138.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
197.52.92.47	Egypt	147.237.77.216	dover.idf.il	Parameter Type Violation ID in www.idf.il/1294-ar/dover.aspx	Block	1
157.55.39.103	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
198.154.225.251	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/61998	Block	1
184.168.200.129	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
109.67.161.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
216.218.206.67	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.75.116	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
157.55.39.156	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in aka.idf.il/kamlar/	None	1
92.126.50.145	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	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
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1111-he/nakhal.aspx	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/blog/	Block	1
184.168.200.129	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
155.133.82.40	Poland	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
198.71.228.68	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
157.55.39.156	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/chamatz/kurs/default.asp	None	1
104.131.189.142	United States	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.118.163.95	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
62.210.84.121	France	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	1
188.143.232.14	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
155.133.82.40	Poland	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
198.71.228.68	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/xmlrpc.php	Block	1