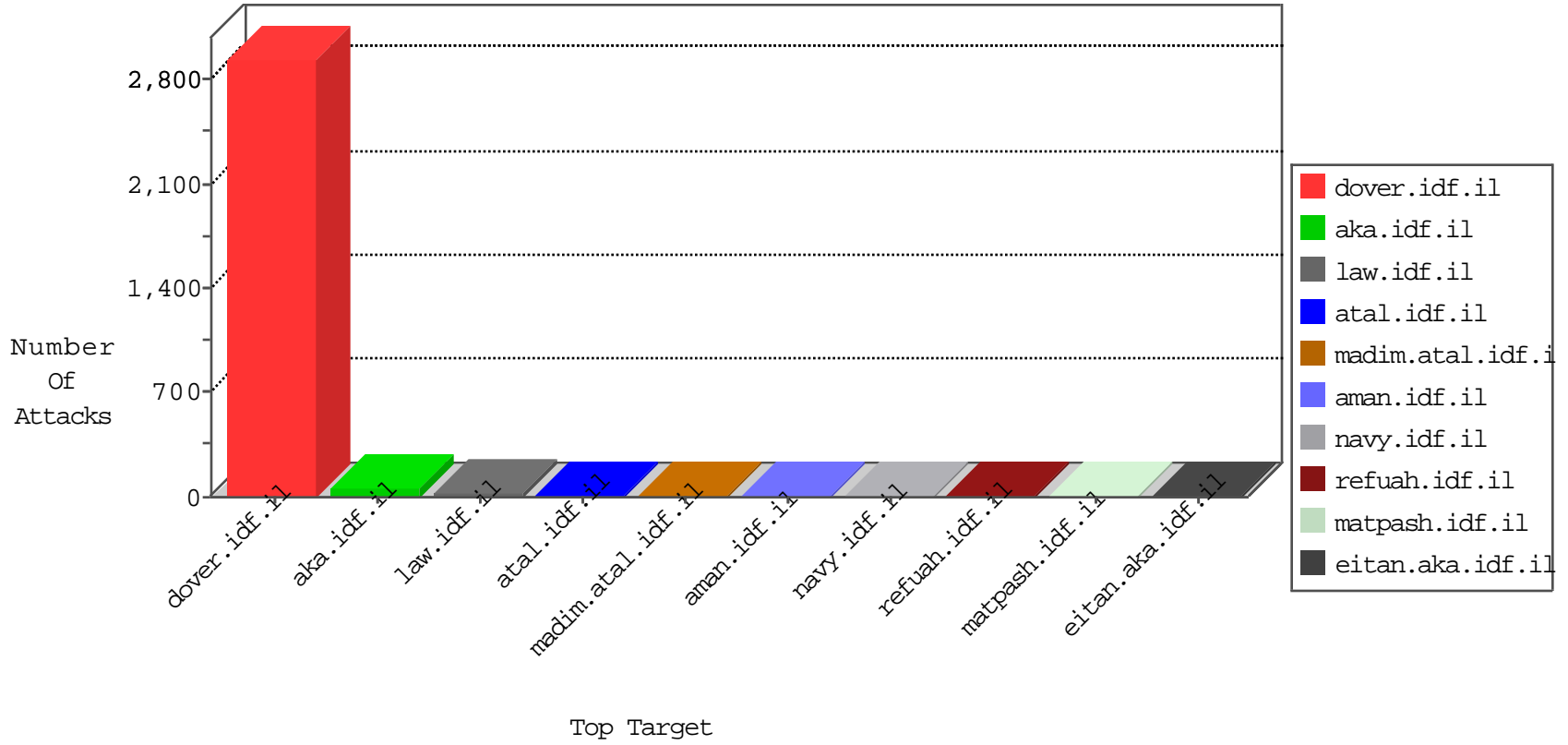


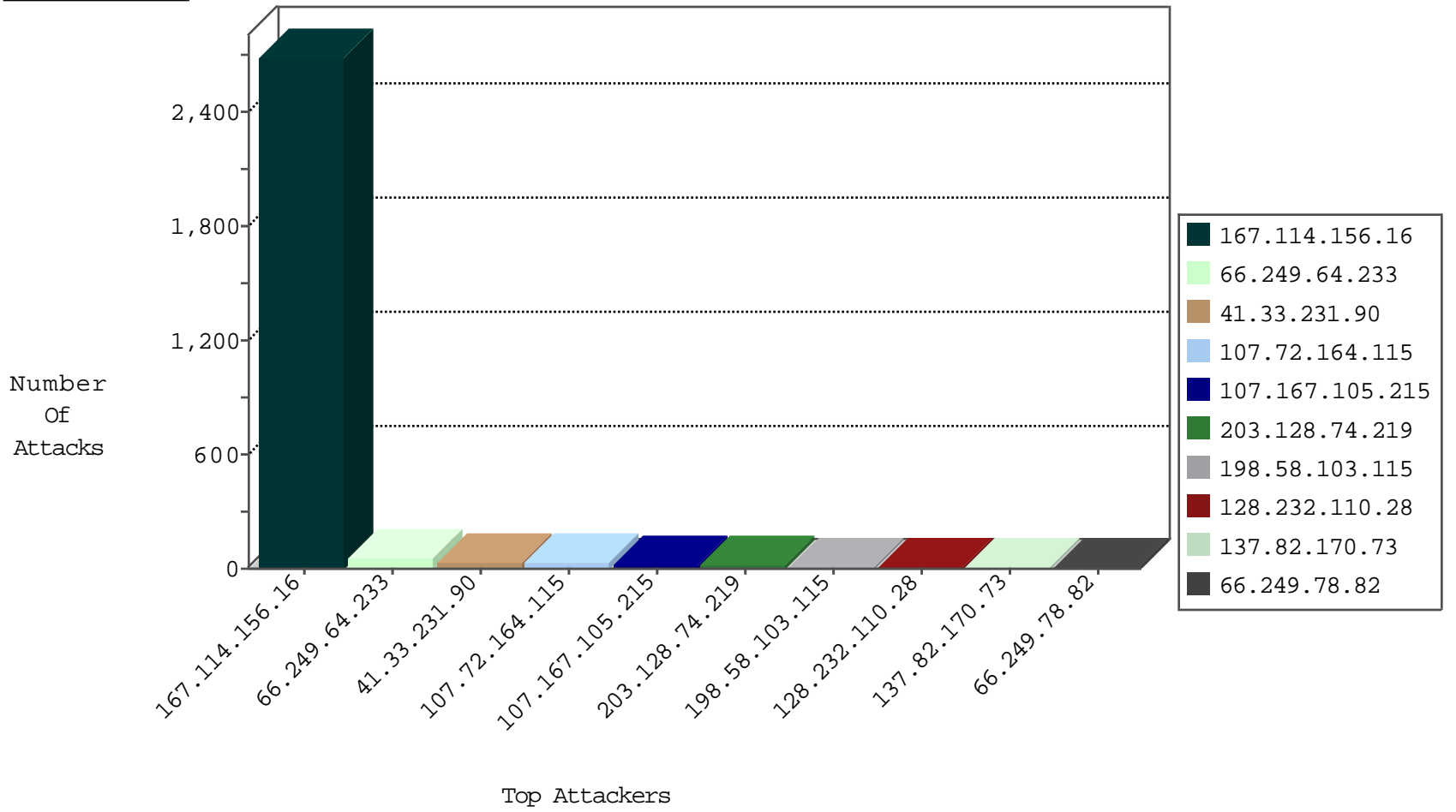
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.82	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3991
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3464
93.174.93.218	Netherlands	147.237.0.19	madim.atal.idf.il	block-sp-trafl	drop	2

11-25-2015-04:04:01 to 11-25-2015-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.79	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.130	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.95	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.117	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.232	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
220.245.240.26	147.237.72.14	Australia	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
166.149.26.62	147.237.72.217	United States	e.idf.il	ET SCAN Potential SSH Scan	1
134.191.232.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
118.75.39.3	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.228.207.18	147.237.72.217	Germany	e.idf.il	ET SCAN NMAP -sS window 1024	1
220.245.240.26	147.237.72.14	Australia	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
166.149.26.62	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
118.121.196.3	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
107.223.62.170	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	222
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
107.72.164.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
107.167.105.215	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.96.128.60	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
66.249.64.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
137.82.170.73	Canada	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.241.226.42	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
100.100.22.12		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
203.128.74.219	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.167.76	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	4
157.55.39.112	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
203.128.74.219	Indonesia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
62.219.116.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.165.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
124.158.17.98	Australia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
203.128.74.219	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
41.218.170.239	Egypt	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
199.30.25.67	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
112.74.67.109	China	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.124	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
66.249.66.96	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
137.82.170.73	Canada	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
119.57.35.94	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.64.230	Israel	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	2
128.232.110.28	United Kingdom	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
203.128.74.219	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.89.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
65.55.210.46	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
137.82.170.73	Canada	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
203.128.74.219	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
96.244.120.20	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.166	United States	147.237.0.19	medim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
112.74.67.109	China	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
193.105.134.220	Sweden	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
68.80.229.73	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
137.116.71.170	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.93.218	Netherlands	147.237.0.19	madim.atal.idf.il	Multiple NULL Character in Method from 93.174.93.218	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
93.174.93.218	Netherlands	147.237.0.19	madim.atal.idf.il	Multiple Illegal Byte Code Character in Method from 93.174.93.218	Block	2
66.249.66.112	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.112	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
176.12.143.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/2796.jpg	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
86.99.81.117	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.67.232	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
45.55.131.62		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/894-he/nakchal.aspxshared/usercontrols/headerupper/	Block	1
125.111.233.234	China	147.237.72.166	aka.idf.il	URL is Above Root Directory www.aka.idf.il/../../error/styles/error.css	Block	1
93.174.93.218	Netherlands	147.237.0.19	madim.atal.idf.il	NULL Character in Method	Block	1
70.211.10.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
185.25.151.159	Poland	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/25112010mas korot.aspx	Block	1
108.50.147.155	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20187-he/dover.aspx)	Block	1
91.196.50.33	Poland	147.237.77.233	atal.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	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
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1234-he/atal.aspx	Block	1
46.117.246.138	Israel	147.237.76.30	himush.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 46.117.246.138	Block	1
137.116.71.170	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/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/1133-22461-he/dover.aspx.	Block	1
77.12.5.7	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
197.41.17.248	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
112.74.67.109	China	147.237.77.235	sviva.idf.il	Unauthorized URL Access to www.wooyun.org/	Block	1
93.174.93.218	Netherlands	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.78.79	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	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
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/profs.asp	Block	1
141.212.122.160	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	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
79.183.142.205	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
197.41.17.248	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.66.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
41.65.151.90	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
114.98.248.224	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 114.98.248.224	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17516-he/dover.aspx	Block	1
141.212.122.160	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	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
86.99.81.117	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
199.30.25.125	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
41.65.151.90	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
114.98.248.224	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-he/idfg.aspx/trackback/	Block	1