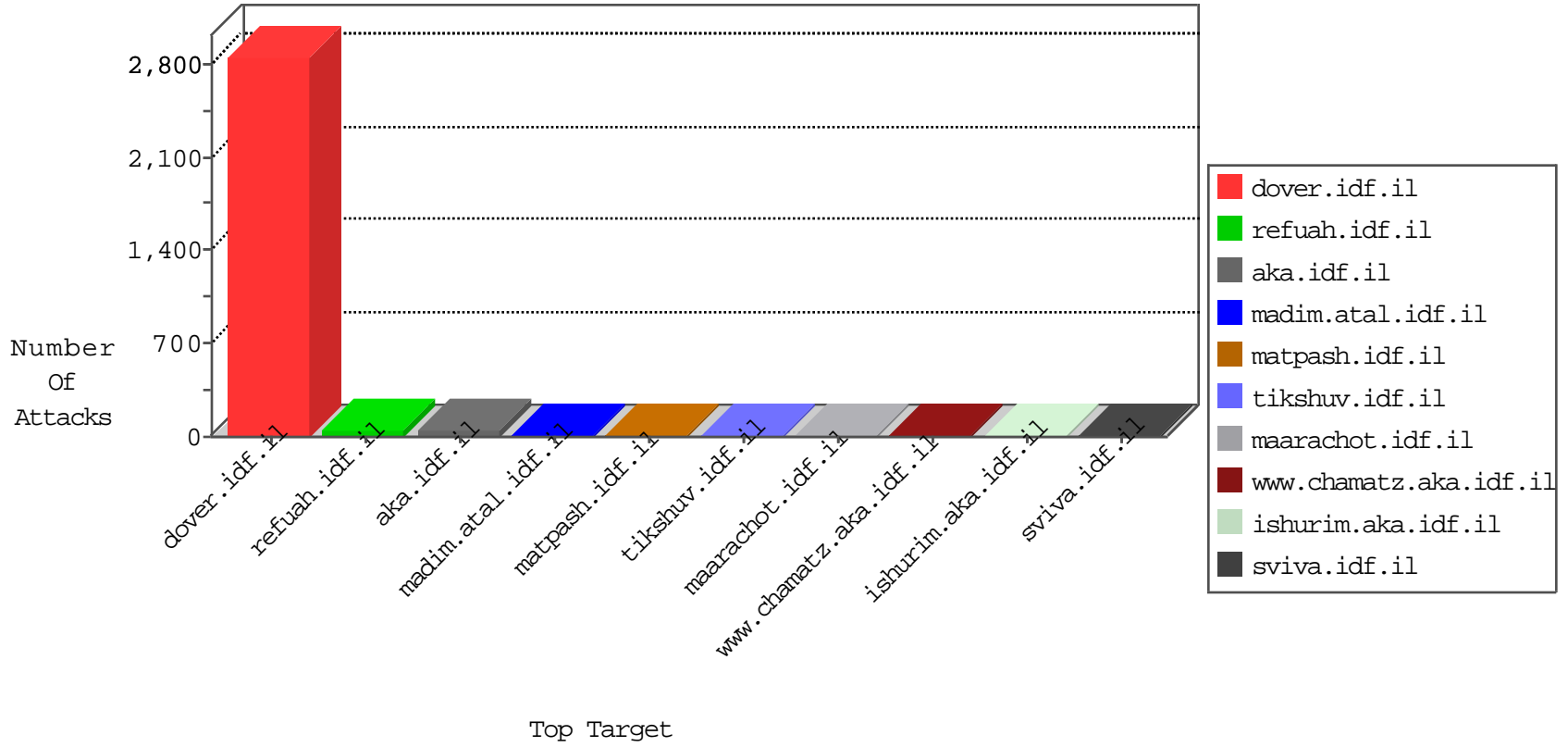


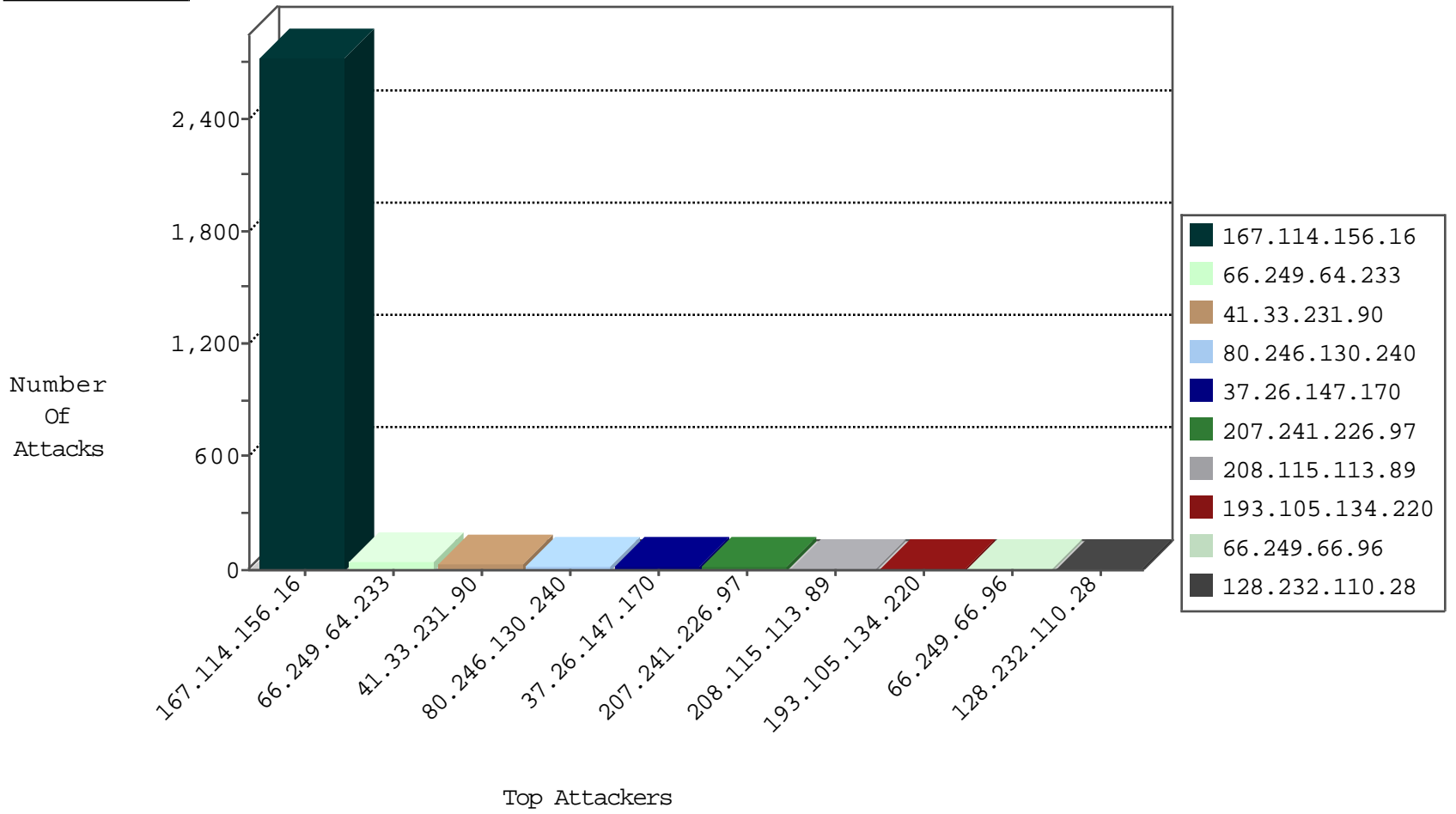
IDF Under Attack Daily Report



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	3553
173.242.125.211	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
197.157.244.240	Scmalia	147.237.76.30	himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
146.185.239.100	Russian Federation	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1

11-25-2015-05:04:07 to 11-25-2015-06:04:07

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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
208.67.1.145	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
208.67.1.145	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
112.245.114.160	147.237.0.19	China	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.117.208.243	147.237.77.227		e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.42.147	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
31.6.71.154	147.237.8.45	Poland	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
210.50.197.154	147.237.77.243	Australia	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
210.50.197.154	147.237.77.170	Australia	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
210.50.197.154	147.237.77.170	Australia	maarachot.idf.il	ET SCAN NMAP -f -sS	1
208.67.1.145	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
208.67.1.145	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.77.216	Sweden	dover.idf.il	ET SCAN NMAP -sS window 1024	1
110.77.216.146	147.237.8.28	Thailand	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.161.250.235	147.237.77.212	Turkey	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.42.147	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
210.50.197.154	147.237.77.243	Australia	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
210.50.197.154	147.237.77.170	Australia	maarachot.idf.il	ET SCAN NMAP -sS window 1024	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	80
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.26.147.170	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
80.246.130.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
207.241.226.97	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	14
66.249.66.96	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.18.51.183	Russian Federation	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
207.241.226.42	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	4
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop		drop	3
149.78.231.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.66.183.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.180.35	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
208.115.111.73	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
128.232.110.28	United Kingdom	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
104.131.199.242	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
146.185.239.102	Russian Federation	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.221	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.57.57.11	China	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
193.105.134.220	Sweden	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.92	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.174	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
137.116.71.170	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
202.112.51.96	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.26	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
193.105.134.220	Sweden	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.169	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
193.105.134.220	Sweden	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.119	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.174	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.208	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
204.79.180.181	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
193.105.134.220	Sweden	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
41.218.170.239	Egypt	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
141.212.122.170	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
193.105.134.220	Sweden	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
186.28.89.236	Colombia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.102.254.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.175	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.113.89	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
141.212.121.209	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
204.79.180.181	United States	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
193.105.134.220	Sweden	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.4	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
46.19.85.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
5.29.224.138	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
176.13.6.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
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	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
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	2
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
66.249.78.2	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
185.3.146.188	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/iturim/	Block	1
47.17.213.224	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
173.70.42.183	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
8.37.70.105	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/894-he/navy.aspx&usg=alkjrhg5psieitx80lqgnoa02xq03h0bjw	Block	1
80.246.130.240	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/21032011sufa.aspx	Block	1
41.130.233.25	Egypt	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
176.13.14.8	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding D4dJ({-ocBc 4%E*mJ9VC3l\$;J-38EXcbw7Utc6\$I6vF0n^6p-j@HuhP5T)qLnQ5hX}1:{B98p-Fa?7LJ*jN&DeqCYHW!/ in m.my-kosher-kravi.idf.il/ajax/createcaptchainage.aspx	None	1
114.98.248.224	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 114.98.248.224	Block	1
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/72199-he/maarachot.aspx	Block	1
185.25.148.240	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/size100x0/2392.jpg	Block	1
175.136.61.24	Malaysia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
8.37.70.140	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1345-he/navy.aspx&usg=alkjrhjtdxf2fwvbckhfm_zd3eb0zrf9q	Block	1
89.138.196.202	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
41.237.89.130	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
176.13.14.8	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.14.8	None	1
141.212.122.160	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/	Block	1
5.9.41.72	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.9.41.72	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
185.25.148.240	Poland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.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/0/size100x0/3120.jpg	Block	1
12.220.96.3	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtContent in www.idf.il/1038-en/dover.aspx	Block	1
175.136.61.24	Malaysia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	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
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
41.237.89.130	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
178.255.215.87	France	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
149.78.231.128	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
5.9.41.72	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9589-he/refuah.aspx	Block	1
185.25.151.159	Poland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/size100x0/2413.jpg	Block	1
31.13.102.103	Ireland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-he/tikshuv.aspx#vltisivr7k70	Block	1
176.12.139.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Unknown Parameter l in www.chinuch.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
149.78.231.128	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 149.78.231.128	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
207.46.13.97	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.72	Block	1