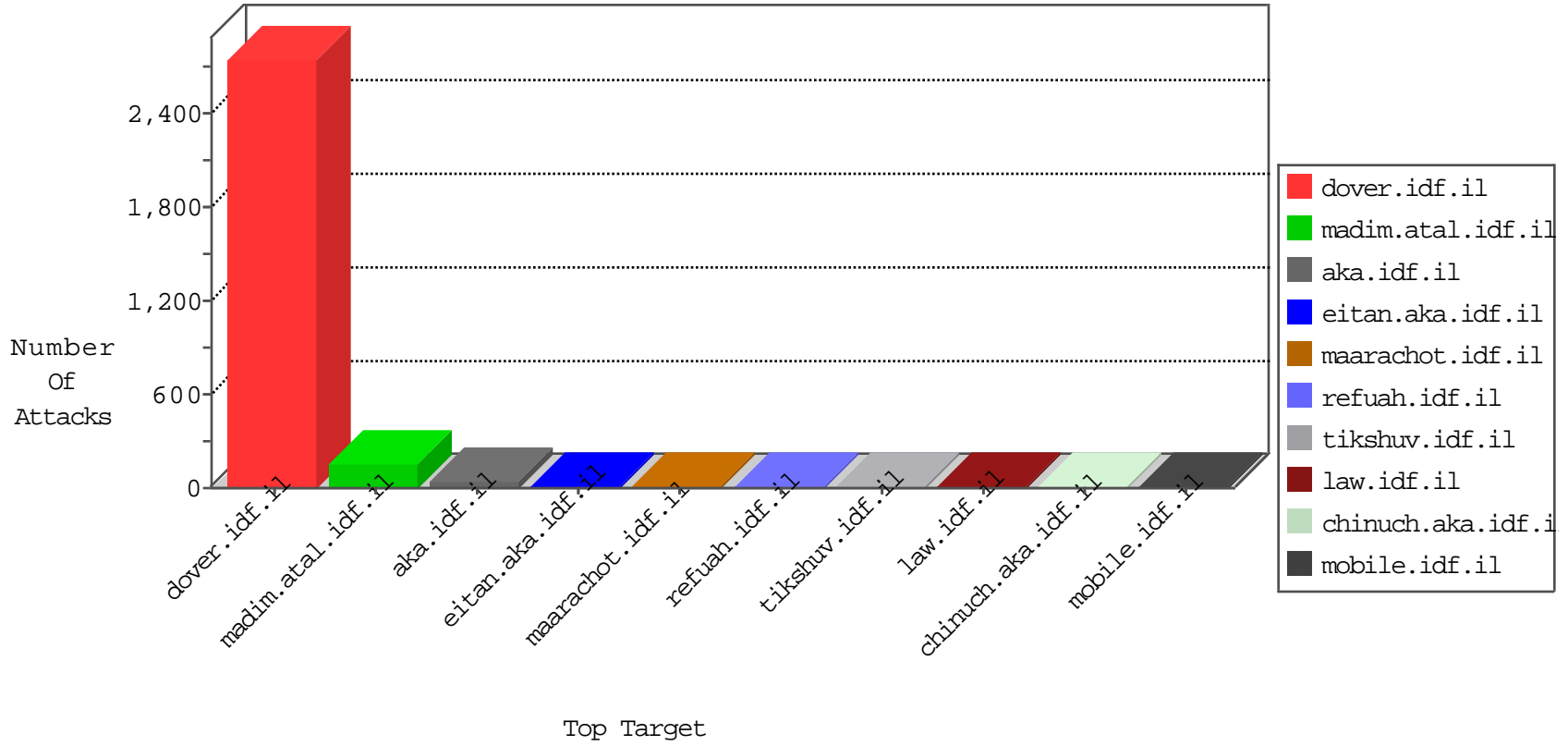


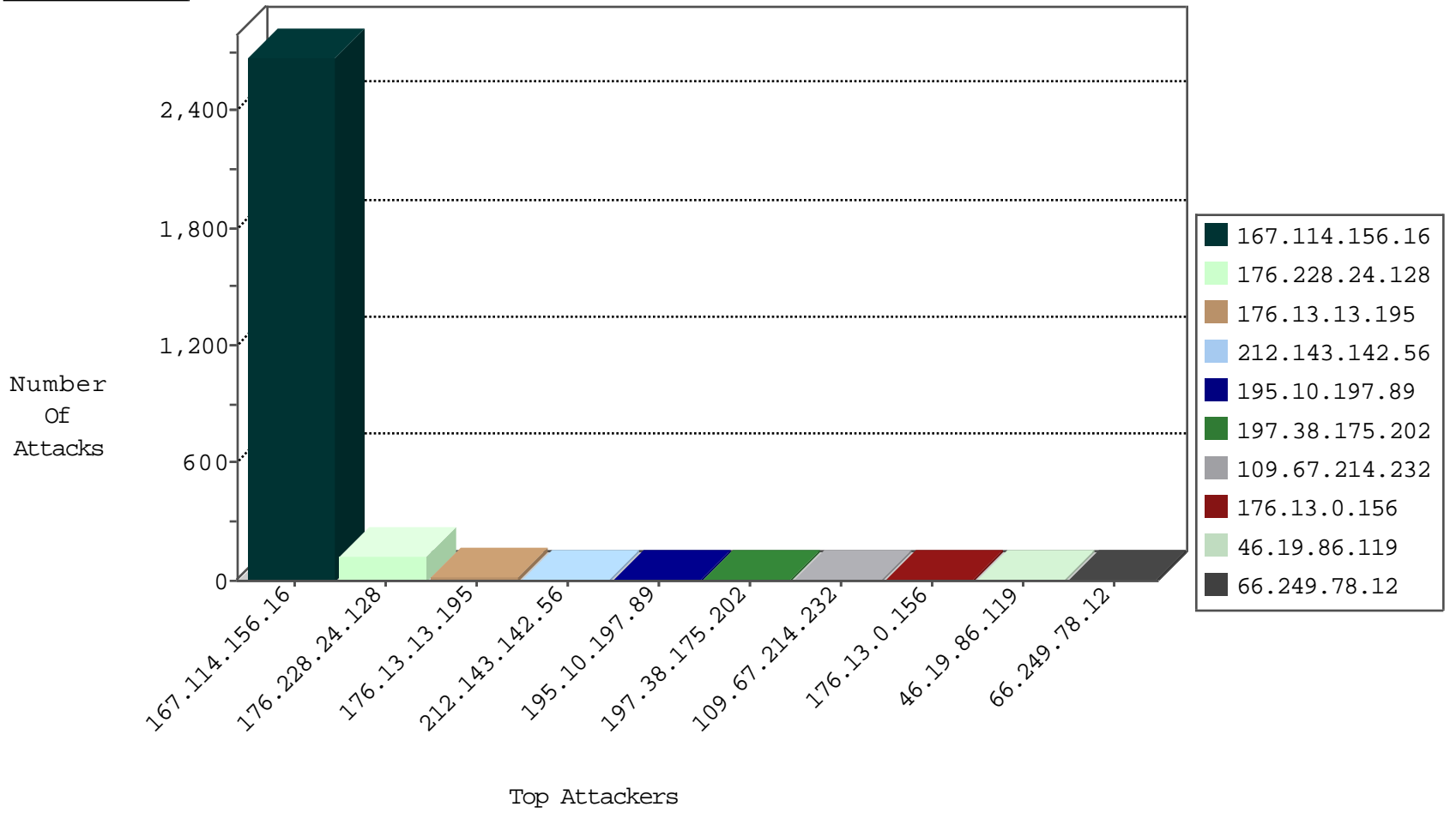
IDF Under Attack Daily Report



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	3445
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
184.105.139.108	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1

03-16-2016-06:04:00 to 03-16-2016-07:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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
193.105.134.220	147.237.0.200	Sweden	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
188.126.77.138	147.237.0.200	Sweden	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
41.78.73.30	147.237.0.35	Somalia	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
188.126.77.138	147.237.77.243	Sweden	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
93.113.125.12	147.237.0.34	Romania	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
49.123.3.24	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
23.96.109.87	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 3072	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	SYN Attack	SYN -> SYN-ACK -> RST	reject	33
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	6
66.249.78.12	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.0.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.214.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
197.38.175.202	Egypt	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	5
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.30.24.199	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.10.197.89	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
77.125.126.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.232.157.55	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.65.97.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.10.197.89	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.183.114.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.65.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.210.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.10.197.89	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.194.84.106	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
37.26.148.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
84.111.159.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
99.25.234.93	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
184.105.139.103	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.95.85.171	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.156	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.65.1.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP anomaly detected	Non-compliant TCP packets coming from multiple external sources were detected. This may result from potential network configuration problem.	drop	1
184.105.139.74	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.173	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.59.107	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.253.145.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.20.69.74	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.113.125.12	Romania	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
184.105.139.110	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.148.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.157	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
213.57.194.75	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

03-16-2016-06:04:00 to 03-16-2016-07:04:00

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
184.105.139.74	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
41.232.157.55	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.174	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.54.130.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
137.116.71.170	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
198.20.69.74	United States	147.237.0.33	idf.il	drop		drop	1
93.113.125.12	Romania	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
184.105.139.112	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.12	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.148.145	Israel	147.237.72.166	aka.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
176.228.24.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	119
176.13.13.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.86.119	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	6
66.249.83.84	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.13.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
80.246.130.219	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.246.130.234	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.83.78	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.181	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
40.77.167.24	United States	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on www.tikshuv.idf.il/site/contactus.aspx parameter catId	Block	1
157.55.39.130	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.aspx/getjs	Block	1
79.180.237.7	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/3394.jpg	Block	1
180.76.15.9	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9014-he/refuah.aspx	Block	1
52.58.29.145	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/faq.aspx	Block	1
83.110.110.98	United Arab Emirates	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
67.72.108.95	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19178-he/dover.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1153-he/dover.aspx	Block	1
79.181.250.4	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/2764.jpg	Block	1
184.105.139.70	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
62.219.139.32	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
83.110.110.98	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
68.180.230.51	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1283-en/dover.aspx	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/size100x0/3142.jpg	Block	1
207.46.13.5	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
62.219.139.32	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
83.110.110.98	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
68.180.230.164	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.127	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/shared/usercontrols/navmenu/	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1379-he/dover.aspx	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.64.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/yohalan/main/main.asp	Block	1
207.46.13.131	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/contactus.aspx	Block	1
141.212.122.145	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
68.180.230.189	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/homepage/asp	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19278-he/kkkkkkk=2aa22d8bkkkkkkk_2aa22d8b	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
83.110.110.98	United Arab Emirates	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1