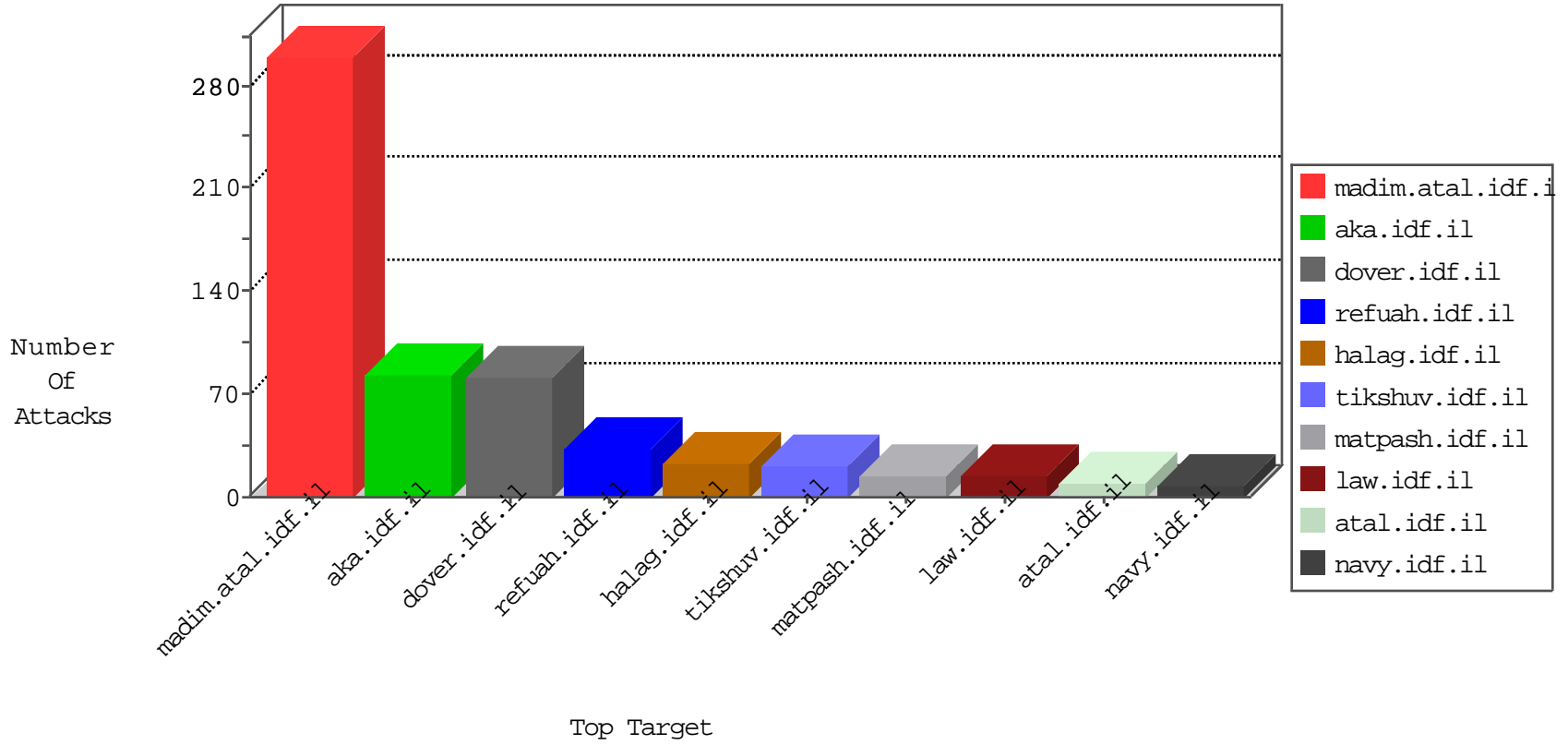


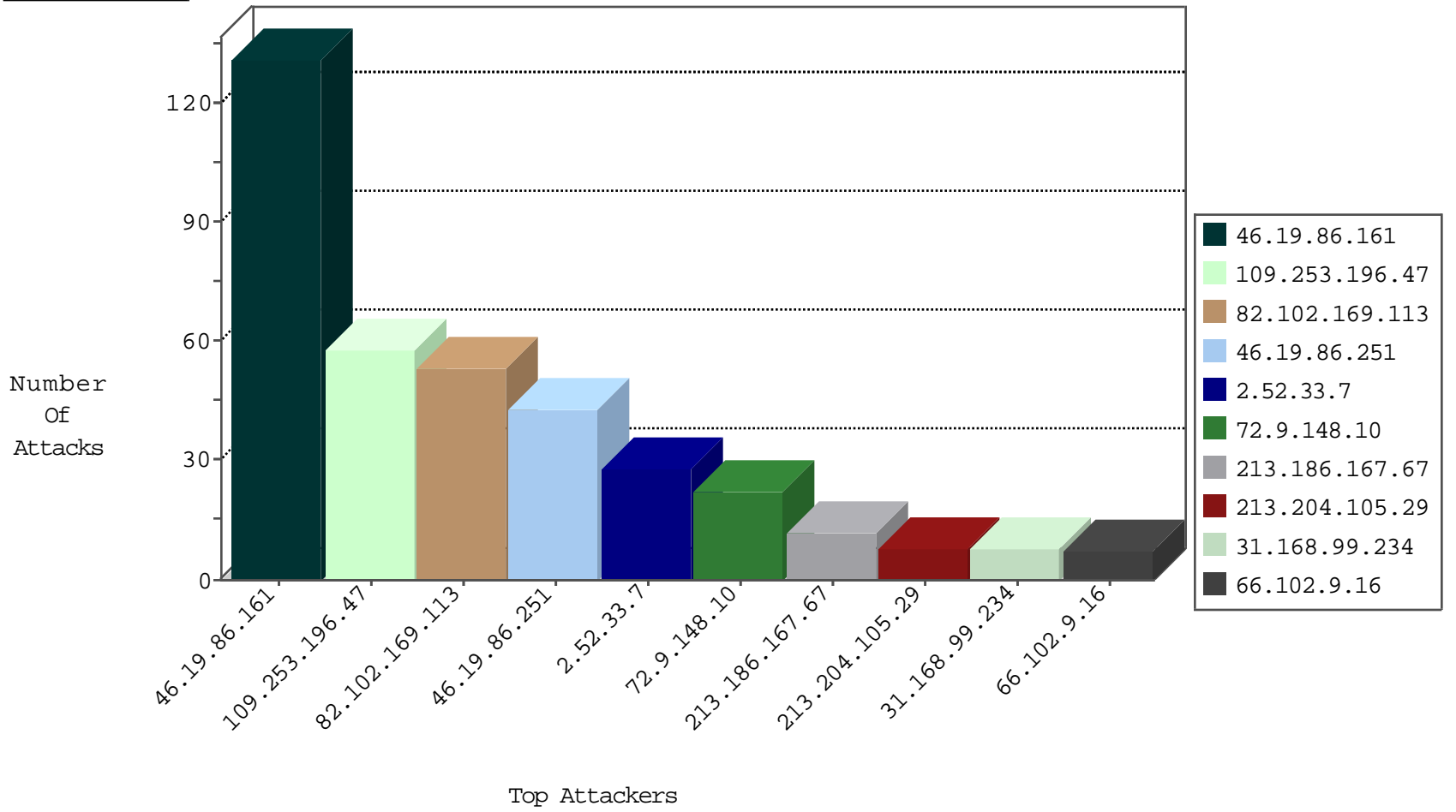
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.216.46	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.52	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.252	United States	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.99.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
107.150.56.254	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
176.13.22.140	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.119	Italy	147.237.0.34	tikshuv.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.69.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.128	Italy	147.237.0.34	tikshuv.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
69.64.36.190	United States	147.237.72.166	aka.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.129	Italy	147.237.77.234	halag.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
104.168.147.242	United States	147.237.77.74	law.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
104.168.147.242	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
123.126.113.80	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
66.249.64.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
213.204.105.29	147.237.76.86	Lebanon	navy.idf.il	ET SCAN NMAP -sA (2)	2
80.246.130.204	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
66.249.93.24	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	1
46.116.44.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.22	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
2.54.186.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.33.7	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
66.102.9.16	United States	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
213.186.167.67	Jordan	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
213.186.167.67	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
84.94.158.202	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
37.26.148.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.59.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.9.5	United States	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
185.3.146.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.32.179.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.149.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.148.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.148.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.64.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.2.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.229	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.149.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.20.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.102.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.52.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.215.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.169.20	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
81.218.205.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.204.105.29	Lebanon	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
199.30.25.60	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.102.195.127	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
8.37.228.77	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
2.54.161.144	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
209.140.32.7	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.54.16.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
82.102.169.113	Israel	147.237.0.19	medim.atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
70.39.186.218	Satellite Provider	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
149.78.26.56	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
213.204.105.29	Lebanon	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.28.131.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
70.39.186.222	Satellite Provider	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
212.199.169.20	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
157.55.2.163	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
2.52.30.94	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.108.185.15	Israel	147.237.77.216	dover.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
46.19.86.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
109.253.196.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
46.19.86.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
37.26.149.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
82.80.137.14	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
176.13.16.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.46.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.132.202	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
197.44.174.32	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
173.247.228.10	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
5.29.54.102	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
212.143.38.222	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
66.249.65.37	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
37.142.64.96	Israel	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	1
185.120.126.10		147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
46.71.221.15	Armenia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
203.106.159.163	Malaysia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
5.255.253.122	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
212.199.169.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.66.64	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1119-he/asp.	Block	1
37.142.64.96	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
185.120.126.10		147.237.76.147	chinuch.aka.idf.il	Distributed PHP Attempt	Block	1
110.92.98.1	Singapore	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.133.28	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.106.159.163	Malaysia	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
46.71.221.15	Armenia	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
184.105.139.67	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
31.168.31.178	Israel	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	1
85.65.185.40	Israel	147.237.77.234	halag.idf.il	Distributed PHP Attempt	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
185.120.126.10		147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
157.55.39.183	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
82.80.137.14	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.80.137.14	Block	1
207.46.13.70	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.64.143	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
185.112.248.32		147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
31.168.31.178	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	Block	1
85.65.185.40	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on www.logistics.atal.idf.il/xmlrpc.php	Block	1
68.180.229.62	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
197.44.174.32	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
173.247.228.10	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
82.80.137.14	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
212.143.38.222	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
185.120.126.10		147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1