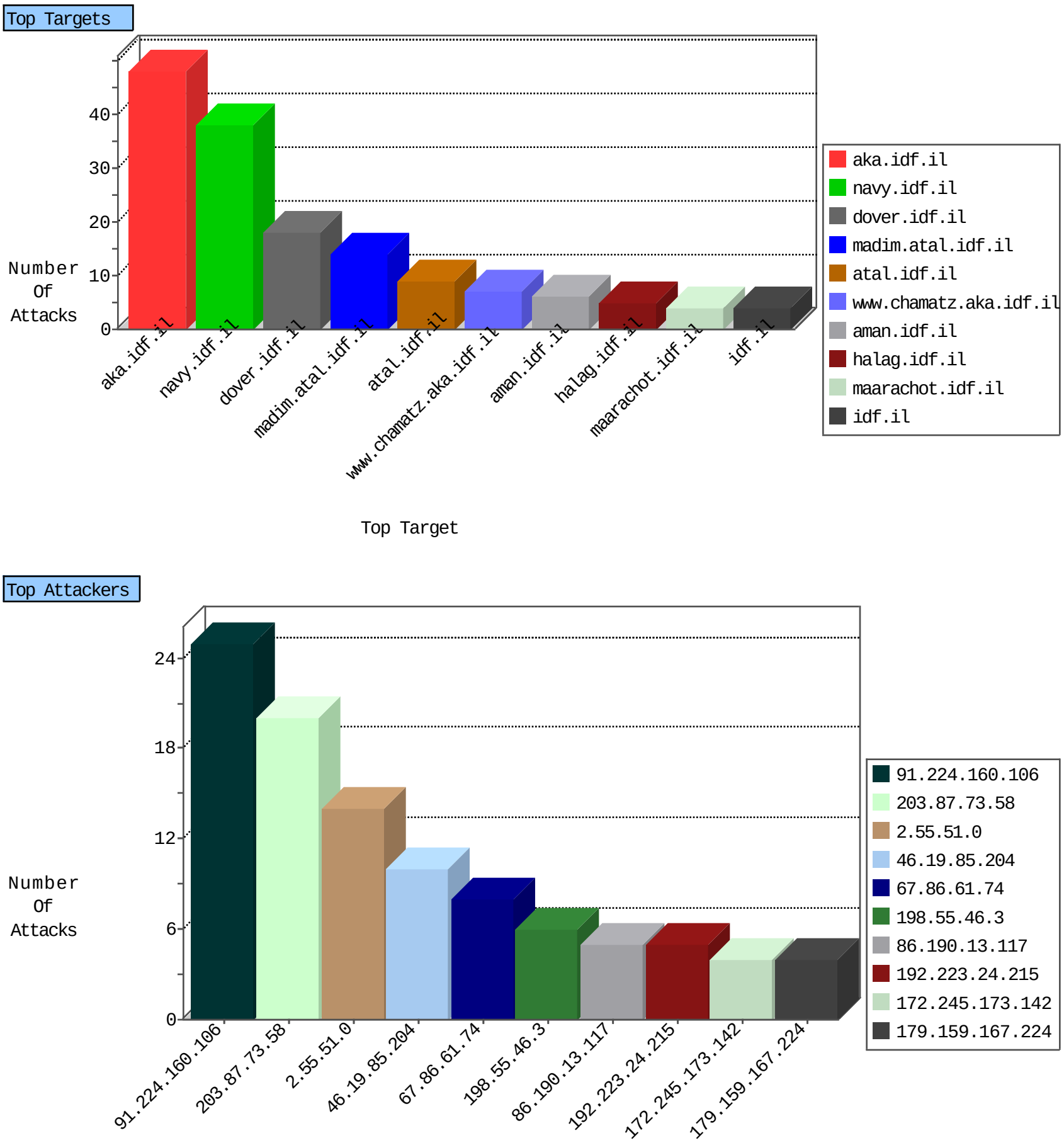
09-11-2016-04:04:00 to 09-11-2016-05:04:00

IDF Under Attack Daily Report



09-11-2016-04:04:00 to 09-11-2016-05:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
79.181.238.164	Israel	147.237.76.42	refuah.idf.il	Black List	drop	3
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
177.75.222.231	Brazil	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
66.249.75.46	Israel	147.237.77.226	www.chamatz.aka.idf.il	network flood IPv4 TCP-SYN	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
177.75.222.231	Brazil	147.237.77.235	sviva.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
128.223.8.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-11-2016-04:04:00 to 09-11-2016-05:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.32.75	Germany	147.237.77.216	dover.idf.i	C1000074: HTTP: majestic bot	Permit	2
199.87.254.195	United States	147.237.77.74	law.idf.il	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1

09-11-2016-04:04:00 to 09-11-2016-05:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	2
45.79.71.122	147.237.77.234	United States	halag.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
220.242.82.185	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
191.96.249.18	147.237.76.86	Chile	navy.idf.il	ET SCAN Potential SSH Scan	1
172.245.173.142	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1
139.162.13.205	147.237.77.226	Singapore	www.chamatz.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.222	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	1
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.158	147.237.72.156	Sweden	aman.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.71.122	147.237.77.170	United States	maarachot.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
91.224.160.106	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
191.96.249.18	147.237.77.170	Chile	maarachot.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
176.47.0.9	147.237.77.216	Saudi Arabia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.224.160.106	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
172.245.173.142	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
46.227.67.158	147.237.76.31	Sweden	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1

09-11-2016-04:04:00 to 09-11-2016-05:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
203.87.73.58	Australia	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
203.87.73.58	Australia	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
46.19.85.204	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
86.190.13.117	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
203.87.73.58	Australia	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
179.159.167.224	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
203.87.73.58	Australia	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.204	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.69.106	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.21	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	illegal header format detected: Illegal start line in request	monitor	2
67.86.61.74	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
67.86.61.74	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
46.19.85.204	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
64.246.178.34	United States	147.237.72.166	aka.idf.il	Header Rejection	header rejection pattern found in request	monitor	2
67.86.61.74	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
207.46.13.173	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
203.87.73.58	Australia	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
67.86.61.74	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.223.24.215	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
172.245.173.142	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
109.253.203.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.123	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.41	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.139.109.97	France	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
216.218.206.104	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.238.133.4	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
192.223.24.215	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
172.245.173.142	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.113	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.208	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
161.202.72.146	Japan	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.94.37.27	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
192.223.24.215	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
141.212.122.33	United States	147.237.0.33	idf.il	drop		drop	1
192.223.24.215	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
162.219.230.208	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
31.25.73.247	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.76.15.145	China	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.34	United States	147.237.0.33	idf.il	drop		drop	1
77.124.61.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.86.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
192.223.24.215	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
172.56.42.25	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.152.115.202	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.26.146.145	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.123	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.40	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.124.61.44	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

09-11-2016-04:04:00 to 09-11-2016-05:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.51.0	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	14
198.55.46.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/undefined	Block	6
66.249.66.107	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.107	Block	2
66.249.66.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/assetlinks.json	Block	1
207.46.13.178	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
79.178.5.224	Israel	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
139.162.13.205	Singapore	147.237.77.226	www.chamatz.aka.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
217.231.205.158	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
79.178.5.224	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/xmlrpc.php	Block	1
139.162.13.205	Singapore	147.237.77.226	www.chamatz.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.66.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
88.163.70.42	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/kadatz/	Block	1
68.180.229.181	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2065-he/cogat.aspx	Block	1
96.47.157.10	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
204.79.180.204	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
68.180.229.190	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
108.14.66.38	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1

09-11-2016-04:04:00 to 09-11-2016-05:04:00