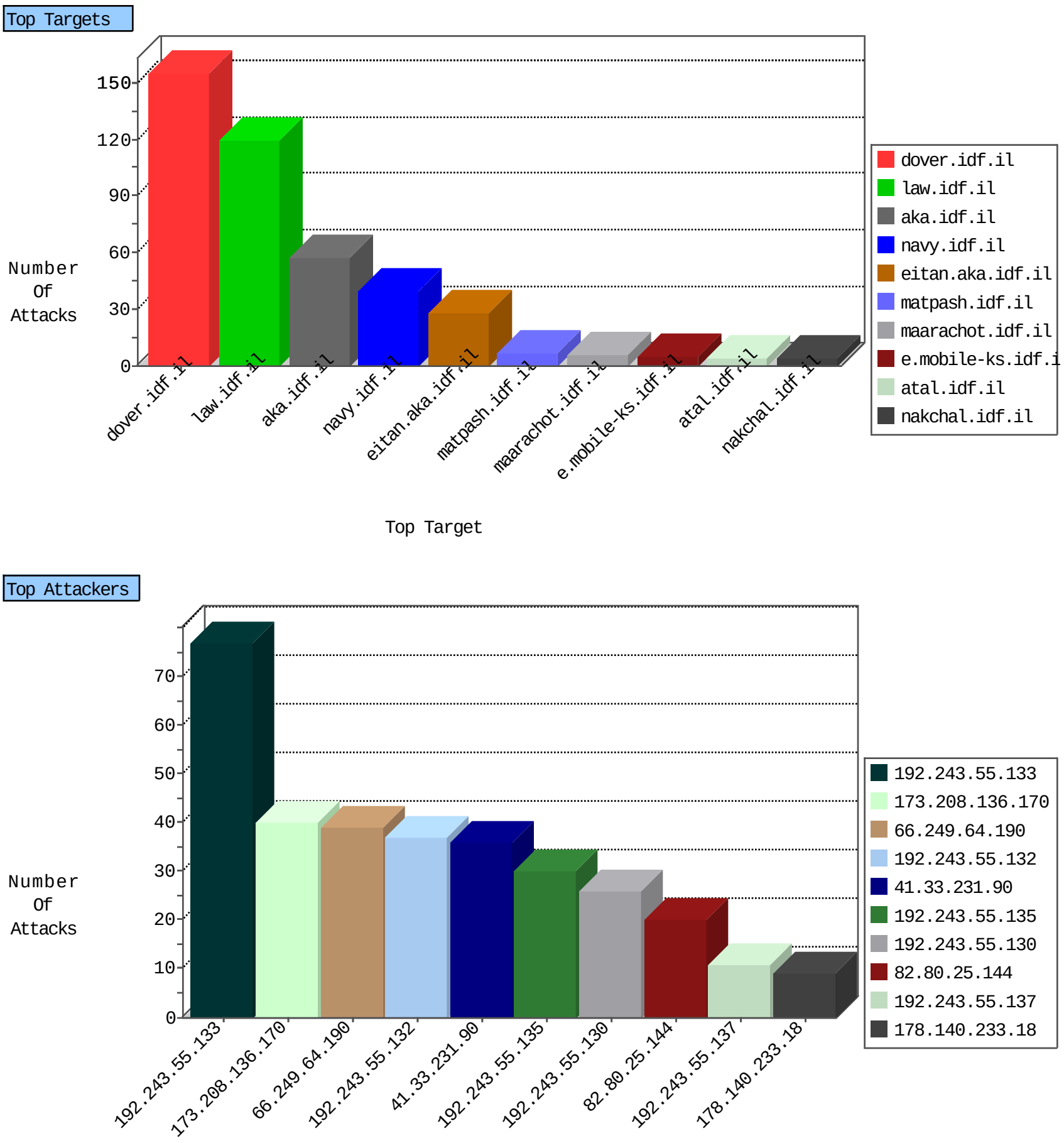
03-04-2016-05:04:03 to 03-04-2016-06:04:03

IDF Under Attack Daily Report



03-04-2016-05:04:03 to 03-04-2016-06:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	2
213.238.176.44	Turkey	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.33	Switzerland	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
207.141.11.146	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
213.238.176.44	Turkey	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.120	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
213.238.176.44	Turkey	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
213.238.176.44	Turkey	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.120	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
213.238.176.44	Turkey	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
161.202.165.6	Netherlands	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
213.238.176.44	Turkey	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1

03-04-2016-05:04:03 to 03-04-2016-06:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.162.167	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
94.23.19.178	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
27.251.94.30	India	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.160.195.5	China	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-04-2016-05:04:03 to 03-04-2016-06:04:03

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
82.80.25.144	147.237.77.227	Israel	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
82.80.25.144	147.237.76.31	Israel	nakchal.idf.il	ET SCAN Potential SSH Scan	2
82.80.25.144	147.237.0.200	Israel	m4u.idf.il	ET SCAN Potential SSH Scan	2
82.80.25.144	147.237.0.17	Israel	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
82.80.25.144	147.237.77.170	Israel	maarachot.idf.il	ET SCAN Potential SSH Scan	1
82.80.25.144	147.237.77.19	Israel	law-forum.idf.il	ET SCAN Potential SSH Scan	1
82.80.25.144	147.237.76.198	Israel	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
82.80.25.144	147.237.72.166	Israel	aka.idf.il	ET SCAN Potential SSH Scan	1
115.214.65.23	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
82.80.25.144	147.237.8.27	Israel	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.44	Canada	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
82.80.25.144	147.237.0.35	Israel	akaws.idf.il	ET SCAN Potential SSH Scan	1
82.80.25.144	147.237.77.234	Israel	halag.idf.il	ET SCAN Potential SSH Scan	1
82.80.25.144	147.237.77.178	Israel	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
82.80.25.144	147.237.77.74	Israel	law.idf.il	ET SCAN Potential SSH Scan	1
82.80.25.144	147.237.76.199	Israel	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
82.80.25.144	147.237.76.197	Israel	e.himush.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.25.144	147.237.72.167	Israel	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
116.110.166.159	147.237.76.30	Vietnam	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.80.25.144	147.237.72.156	Israel	aman.idf.il	ET SCAN Potential SSH Scan	1
115.214.65.23	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.193	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1

03-04-2016-05:04:03 to 03-04-2016-06:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
173.208.136.170	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.133	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
178.140.233.18	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
176.77.41.134	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.110.70.96	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.77.67.96	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.218	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.135	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.132	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.136	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
192.243.55.133	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.132	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.157.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.137	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.210.159.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.130	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.135	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2

03-04-2016-05:04:03 to 03-04-2016-06:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	11
177.38.192.3	Brazil	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
207.46.13.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
112.207.248.232	Philippines	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
198.20.69.74	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.66.72	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1039-he/cogat	Block	1
37.203.214.2	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter doc in www.aka.idf.il/kamlar/klali/default.asp	None	1
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/mobile/modules/forums/forum.aspx	Block	1
37.203.214.2	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
185.106.94.30		147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/xmlrpc.php	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/list.aspx	None	1
207.241.229.223	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1240-he/atal.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
66.249.64.171	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/894-he	Block	1
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/history/stm	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter itemid in www.aka.idf.il/kamlar/gallery/showpicture.asp	None	1
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.66.72	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.72	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/forgotpassword.aspx	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter a.. in www.aka.idf.il/giyus/general/	None	1

03-04-2016-05:04:03 to 03-04-2016-06:04:03