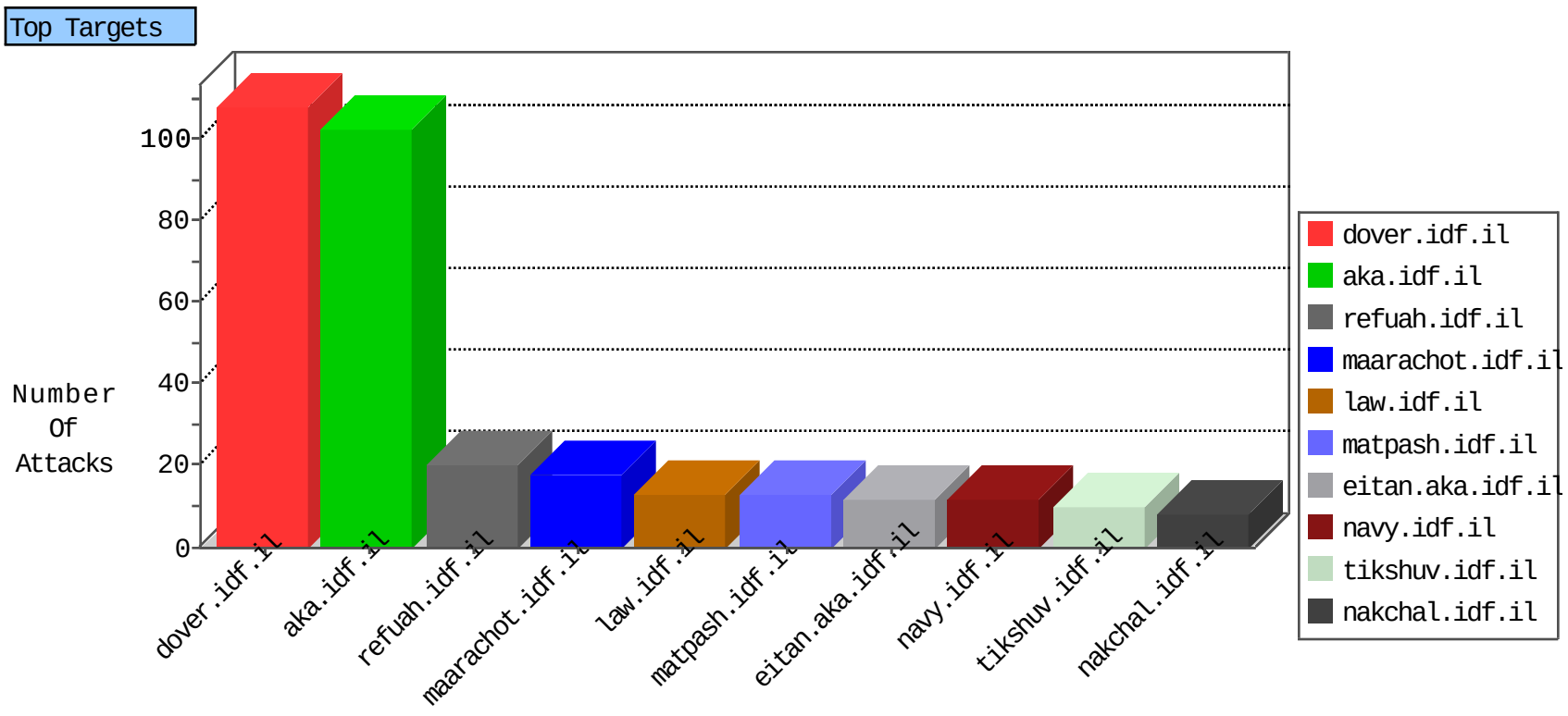
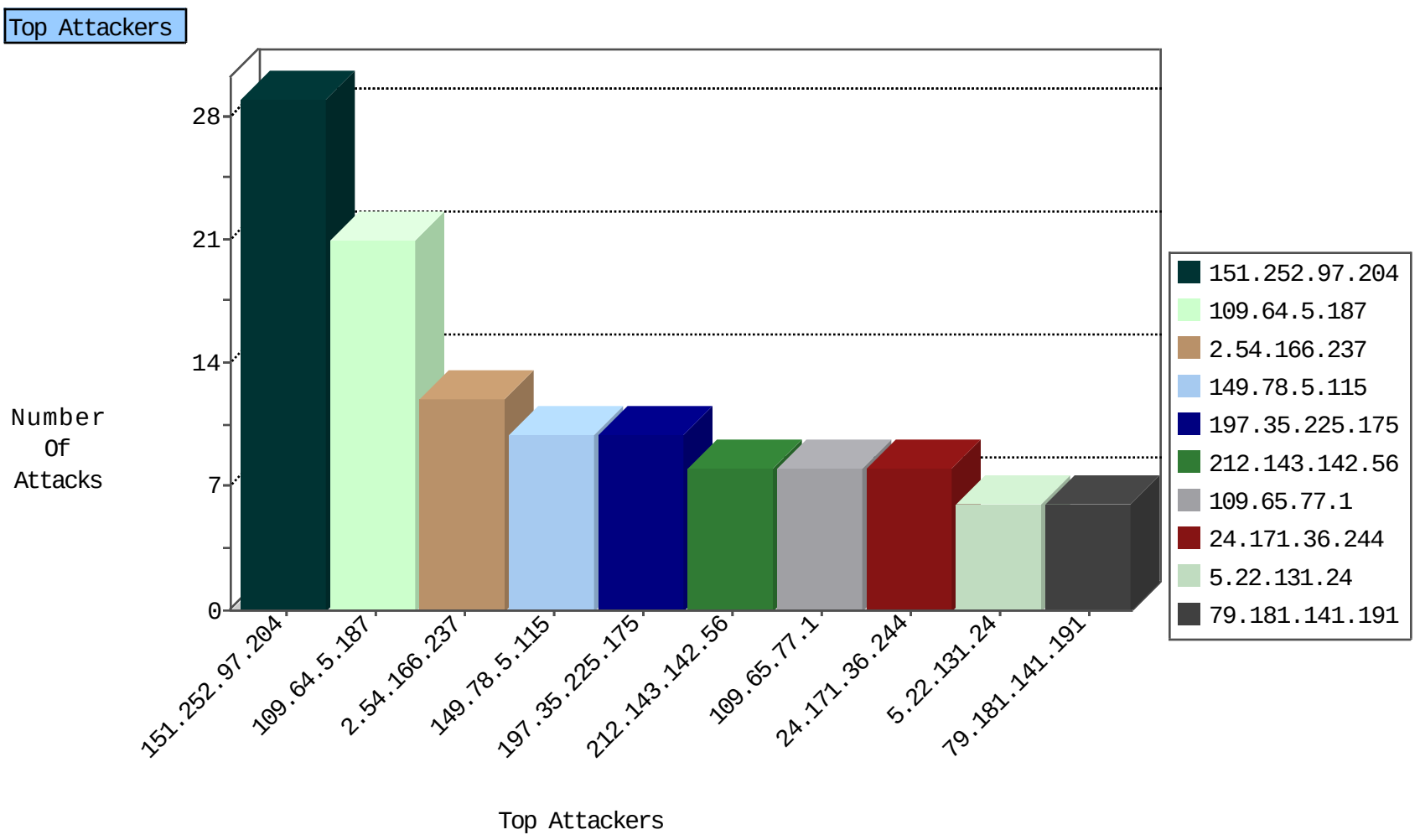
03-06-2016-00:04:06 to 03-06-2016-01:04:06

IDF Under Attack
Daily Report

Top Targets



Top Attackers



03-06-2016-00:04:06 to 03-06-2016-01:04:06

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
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
122.117.75.77	Taiwan	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
113.252.177.163	Hong Kong	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
113.255.188.131	Hong Kong	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1

03-06-2016-00:04:06 to 03-06-2016-01:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.127.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
199.30.25.83	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-06-2016-00:04:06 to 03-06-2016-01:04:06

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
61.240.144.67	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.187.18.143	147.237.77.243	Vietnam	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.140	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
61.240.144.67	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.187.18.143	147.237.77.243	Vietnam	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
41.41.29.238	147.237.77.121	Egypt	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
198.180.198.185	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
185.72.179.221	147.237.76.199		e.nakchal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
146.148.28.121	147.237.77.216	United States	dover.idf.il	ET WEB_SPECIFIC_APPS OS Commerce 2.2 RC2 Potential Anonymous Remote Code Execution	1

03-06-2016-00:04:06 to 03-06-2016-01:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.5.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
151.252.97.204	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
2.54.166.237	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
24.171.36.244	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
151.252.97.204	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.160.199.217	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	5
151.252.97.204	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
106.38.241.151	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
37.46.41.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.154.135.113	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.180.31.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.5.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.172.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.144.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.63.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.169.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.166.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.16.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
151.252.97.204	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.65.98.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.128	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.27.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.129.34	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.180.23.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.165.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.189.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.88.243.22	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
109.65.77.1	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
109.186.144.98	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.117.193.168	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.185	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.65.77.1	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
176.13.0.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
207.241.237.227	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
176.13.0.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.65.77.1	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
185.120.125.28		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.65.77.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
2.52.134.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
94.230.86.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.102.195.96	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.55	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
23.101.61.176	Ireland	147.237.72.166	aka.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1

03-06-2016-00:04:06 to 03-06-2016-01:04:06

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
92.22.149.30	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
196.215.148.187	South Africa	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

03-06-2016-00:04:06 to 03-06-2016-01:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.21.231	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	4
146.148.28.121	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
41.230.14.223	Tunisia	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	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
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
197.33.10.254	Egypt	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/r□l=	Block	2
203.192.196.154	India	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 203.192.196.154	Block	2
79.181.141.191	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	1
197.35.225.175	Egypt	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
109.177.149.206	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.51	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/clientscripts.js	Block	1
165.120.109.213	United Kingdom	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
94.230.86.46	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
89.138.106.196	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
213.151.47.114	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
5.29.74.167	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
149.78.5.115	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	1
5.22.131.24	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
149.50.85.120	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
87.69.155.9	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
197.35.225.175	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
109.64.33.196	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
66.249.75.202	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
197.35.225.175	Egypt	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
149.78.114.10	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	1
89.247.112.171	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
204.79.180.208	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.22.131.24	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
149.78.5.115	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
87.70.6.192	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
79.181.141.191	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed PHP Attempt	Block	1
197.35.225.175	Egypt	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/xmlrpc.php	Block	1
109.177.149.206	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
94.230.86.46	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.64.56	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
189.102.39.215	Brazil	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
89.138.106.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
213.151.51.225	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 213.151.51.225	Block	1
5.29.74.167	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
149.78.5.115	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/xmlrpc.php	Block	1
5.22.131.24	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on www.nakhal.idf.il/xmlrpc.php	Block	1
149.78.5.115	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
87.70.2.90	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
198.58.103.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
109.64.33.196	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.75.210	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/enlarge.asp	Block	1
197.35.225.175	Egypt	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on www.nakhal.idf.il/xmlrpc.php	Block	1
41.230.14.223	Tunisia	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	1
151.252.97.204	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1

03-06-2016-00:04:06 to 03-06-2016-01:04:06