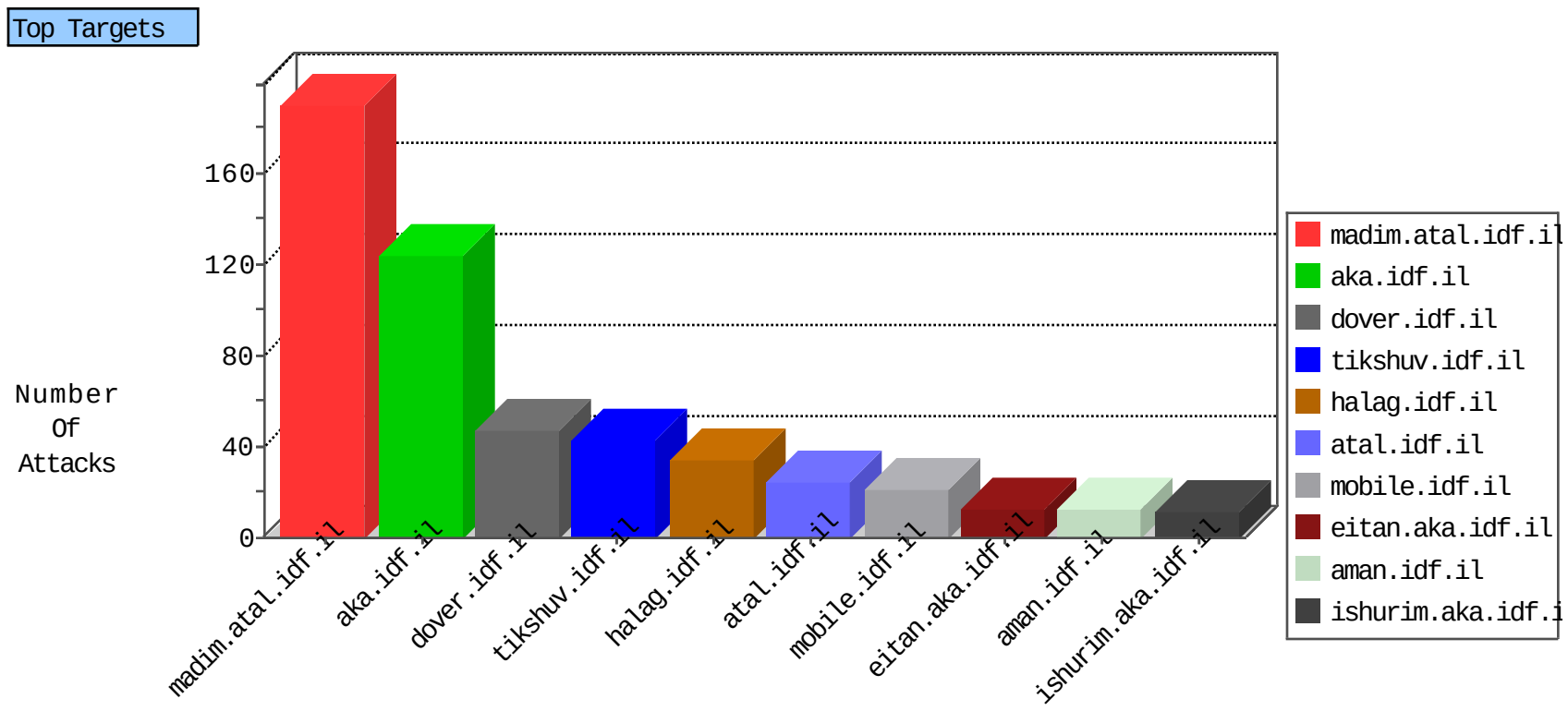
03-05-2016-11:04:07 to 03-05-2016-12:04:07

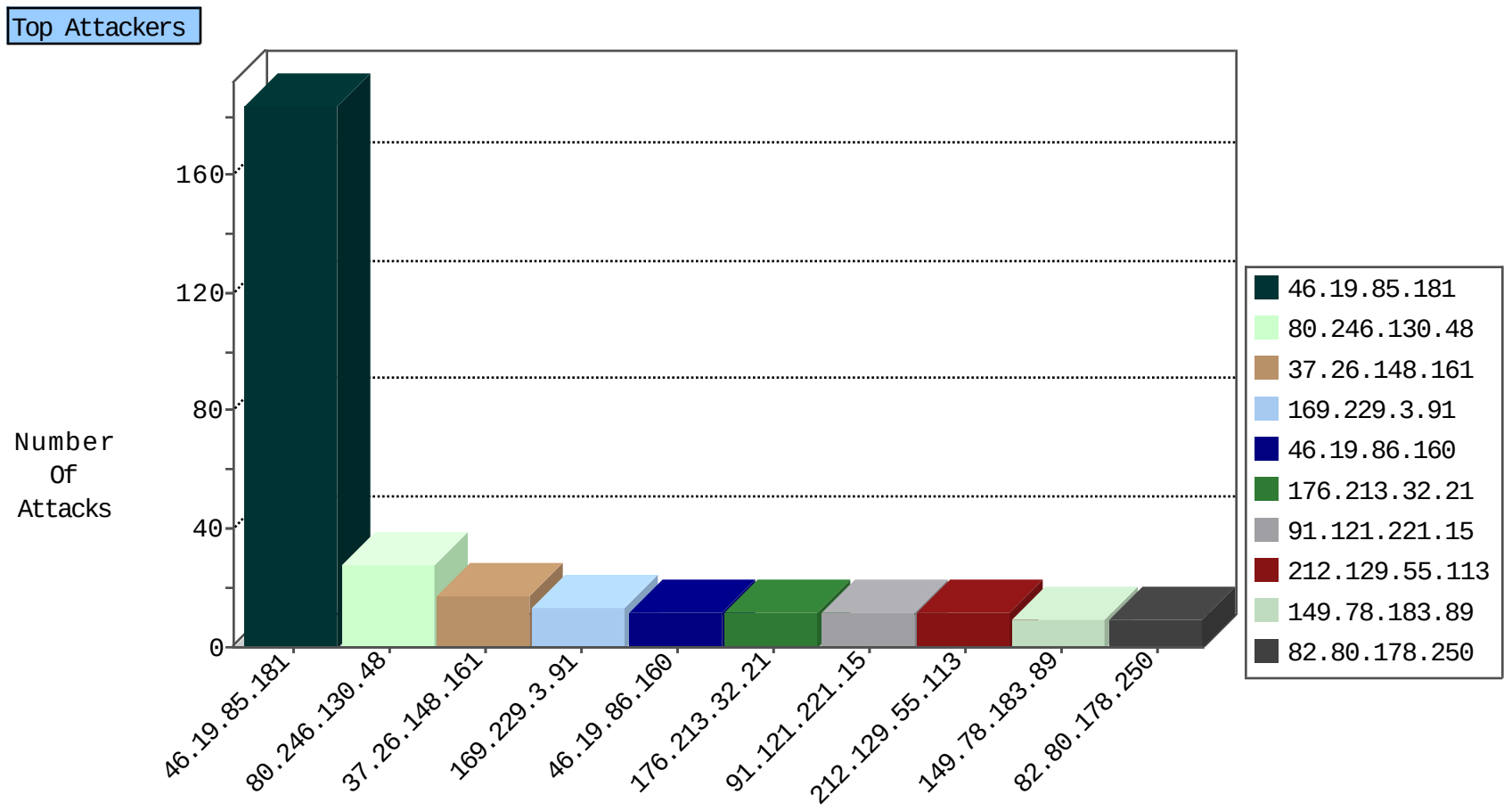
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-05-2016-11:04:07 to 03-05-2016-12:04:07

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
111.118.160.177	Australia	147.237.0.16	my-kosher-kravi.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
74.82.47.13	United States	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1
37.128.85.37	Poland	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1

03-05-2016-11:04:07 to 03-05-2016-12:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.125.89.0	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
31.154.163.198	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.182.151.228	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
84.228.86.248	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
91.121.221.15	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
91.121.221.15	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
151.80.44.115	Italy	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
91.121.221.15	France	147.237.77.170	maarachot.idf.il	C1000074: HTTP: majestic bot	Block	2
31.168.18.238	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.25.139	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
91.121.221.15	France	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2
91.121.221.15	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
91.121.221.15	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
2.54.140.149	Israel	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
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
31.154.249.157	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
39.47.176.165	Pakistan	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-05-2016-11:04:07 to 03-05-2016-12:04:07

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
212.129.55.113	147.237.76.31	France	nakchal.idf.il	ET SCAN Potential SSH Scan	1
111.118.160.177	147.237.0.200	Australia	m4u.idf.il	ET SCAN Potential SSH Scan	1
212.129.55.113	147.237.8.27	France	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
111.118.160.177	147.237.0.15	Australia	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
212.129.55.113	147.237.0.34	France	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
60.25.197.237	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
210.178.74.167	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.101.186.244	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
198.20.69.98	147.237.77.235	United States	sviva.idf.il	ET DROP Dshield Block Listed Source	1
212.129.55.113	147.237.77.170	France	maarachot.idf.il	ET SCAN Potential SSH Scan	1
189.196.247.184	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.129.55.113	147.237.76.196	France	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
179.43.141.234	147.237.77.243	Switzerland	mobile.idf.il	ET SCAN Potential SSH Scan	1
212.129.55.113	147.237.76.86	France	navy.idf.il	ET SCAN Potential SSH Scan	1
179.43.141.234	147.237.77.121	Switzerland	e.navy.idf.il	ET SCAN Potential SSH Scan	1
212.129.55.113	147.237.72.167	France	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
111.118.160.177	147.237.0.17	Australia	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
212.129.55.113	147.237.0.200	France	m4u.idf.il	ET SCAN Potential SSH Scan	1
95.130.13.220	147.237.76.31	France	nakchal.idf.il	ET SCAN Potential SSH Scan	1
212.129.55.113	147.237.0.19	France	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
37.139.27.231	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
210.178.74.167	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.101.186.244	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
212.129.55.113	147.237.77.235	France	sviva.idf.il	ET SCAN Potential SSH Scan	1
212.129.55.113	147.237.76.201	France	e.atal.idf.il	ET SCAN Potential SSH Scan	1
187.150.170.245	147.237.76.30	Mexico	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.129.55.113	147.237.76.176	France	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
179.43.141.234	147.237.77.216	Switzerland	dover.idf.il	ET SCAN Potential SSH Scan	1

03-05-2016-11:04:07 to 03-05-2016-12:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
80.246.130.48	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
37.26.148.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
85.250.229.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.160	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.46.39.174	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.117.56	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.177.154.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.178.250	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.108.71.49	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.131.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.117.206.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.148.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
82.80.178.250	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.148.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.120.126.178		147.237.72.156	aman.idf.il	drop	SAM rule	drop	4
79.183.13.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.213.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.239.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.228.140	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.73.173	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
87.71.45.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.97.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.130.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.50.14	Russian Federation	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.155.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.166.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.160	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
87.68.255.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.177.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.56.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.43.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.89.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.73.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.157.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.142.165.167	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
66.249.66.137	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.250.49.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.22.131.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.120.126.178		147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
37.46.38.141	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.78.183.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.129.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

03-05-2016-11:04:07 to 03-05-2016-12:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.117.130.98	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.88.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.84	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	184
176.213.32.21	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
176.213.32.21	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.213.32.21	Block	5
149.78.183.89	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
79.178.120.61	Israel	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	3
79.178.120.61	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	Block	3
46.117.206.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.183.89	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.183.89	Block	2
5.29.187.130	Israel	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	2
5.29.187.130	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on www.logistics.atal.idf.il/xmlrpc.php	Block	2
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
2.54.53.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
85.64.170.17	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.66.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	1
184.105.247.195	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
37.26.148.161	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Illegal Byte Code Character in Method	Block	1
109.67.126.128	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
79.178.120.61	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	NULL Character in Method	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.54.164.249	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1242-he/atal.aspx	Block	1
87.68.255.168	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site- øªø§ø±ùšø® ø§ù„ ø¯ø®ù^ù„ 2-12-2004	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	Illegal Byte Code Character in URL	Block	1
118.193.163.150	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
79.178.120.61	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.78.183.89	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
105.100.70.177	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il./ar	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
207.46.13.171	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.19.86.160	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	Unknown HTTP Request Method vJ›½[[#11]]d4Š{•-§‰µdBDK©0ÊÛö”aÌÀ# in URL	Block	1
139.195.23.189	Indonesia	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
80.246.130.48	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.64.209.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter _ in www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	None	1
213.8.204.47	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
46.117.104.187	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
139.195.23.189	Indonesia	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
2.52.160.84	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
80.246.130.172	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.213.32.21	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
14.149.126.230	China	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Abnormally Long Request	Block	1