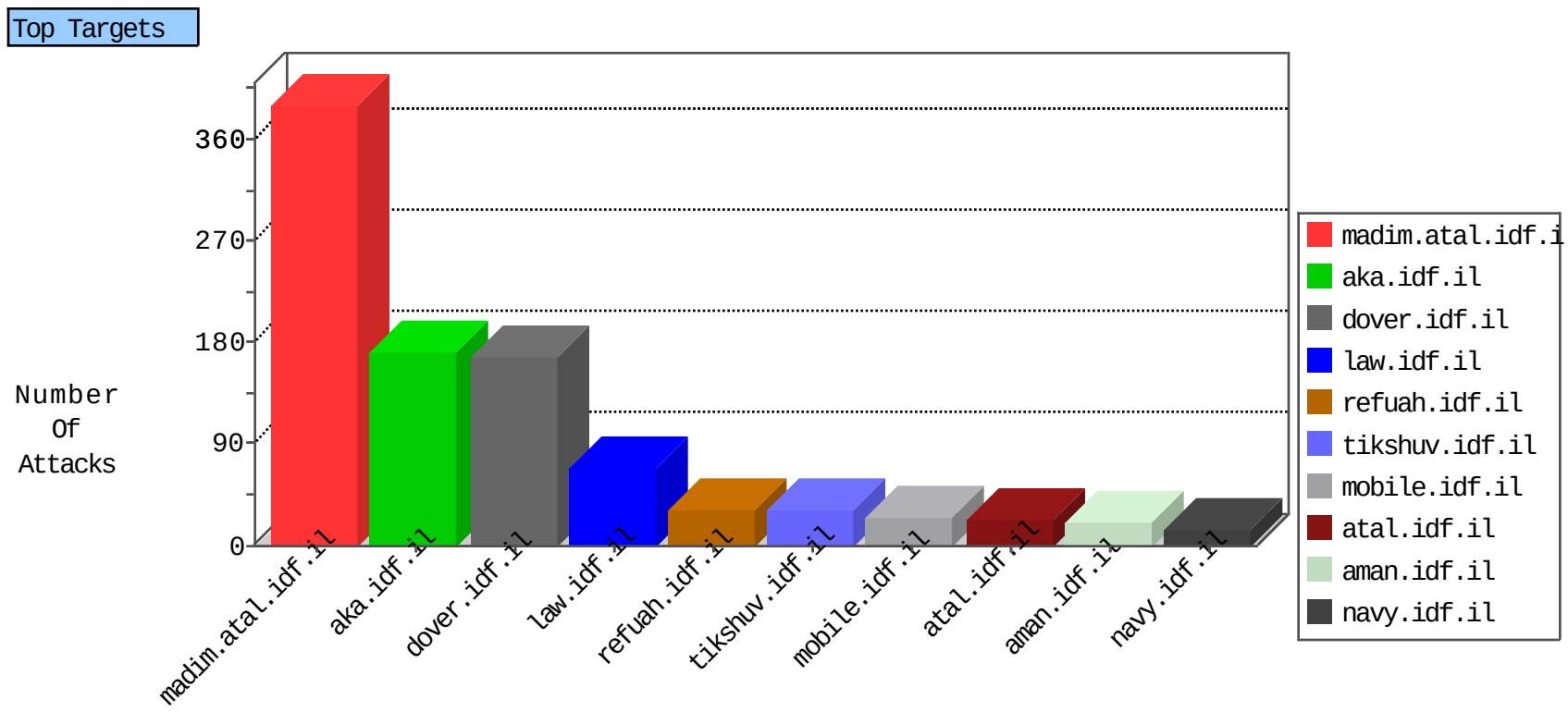
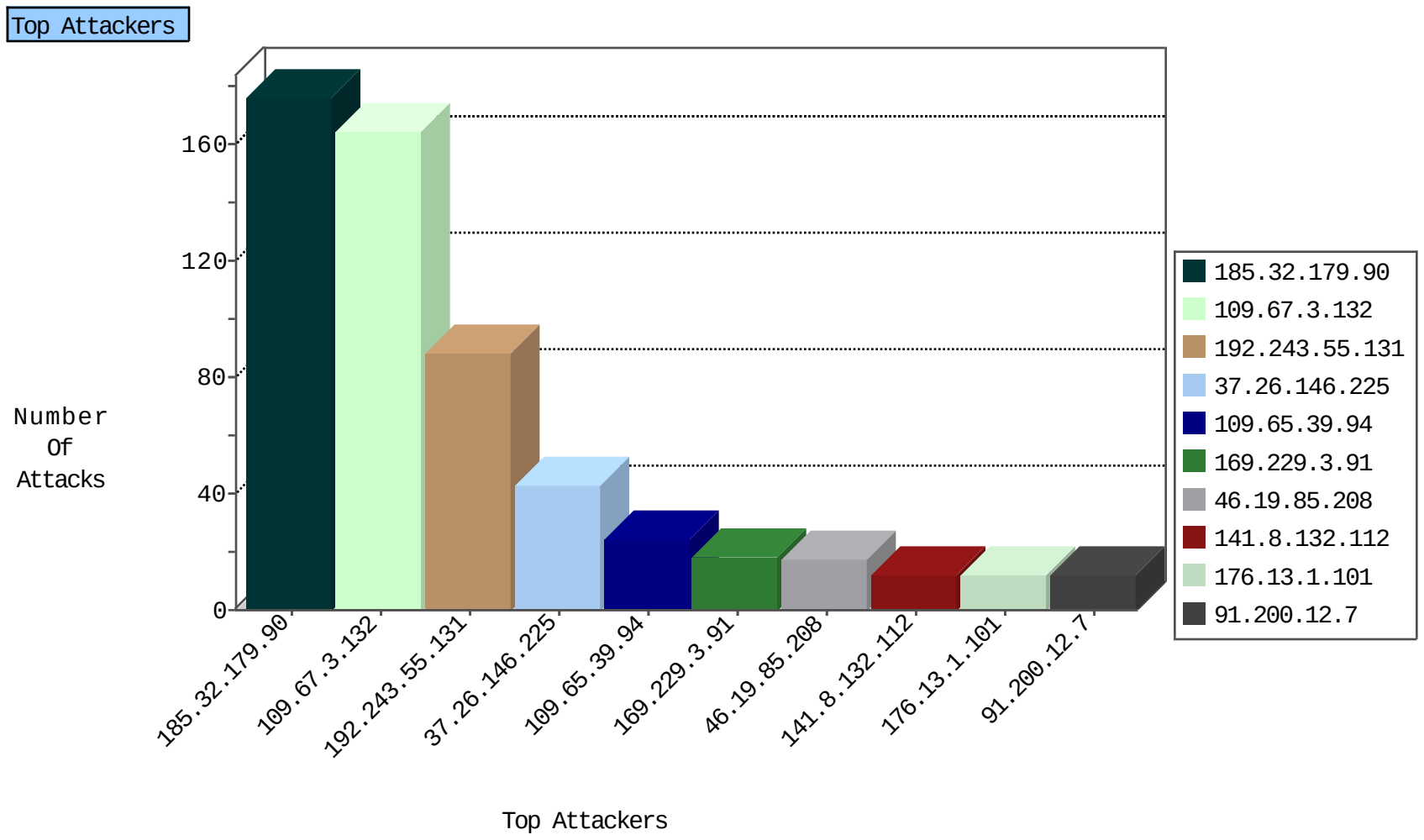
03-04-2016-11:04:04 to 03-04-2016-12:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



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

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	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
184.105.139.69	United States	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
85.10.203.133	Germany	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
45.210.181.48	Uruguay	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1		147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
85.10.203.133	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
85.10.203.133	Germany	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
74.208.153.47	United States	147.237.8.45	e.eitan.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
185.94.111.1		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
85.10.203.133	Germany	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
86.99.187.46	United Arab Emirates	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
74.208.153.47	United States	147.237.8.46	e.chinuch.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
85.10.203.133	Germany	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.233.109	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
213.57.220.233	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
79.178.149.181	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.86.116	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
213.57.75.70	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.254.32.6	United Kingdom	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.29.162	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
51.254.32.6	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
62.210.148.247	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
46.19.85.231	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
79.215.196.195	Germany	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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
185.106.92.164		147.237.76.200	eitan.aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
185.106.92.164		147.237.76.200	eitan.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1

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

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.32.179.90	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
199.203.35.237	147.237.77.176	Israel	matpash.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
185.106.92.164	147.237.76.200		eitan.aka.idf.il	ET WEB_SERVER Muieblackcat scanner	1
183.3.202.115	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
176.13.17.135	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
162.250.125.26	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
128.127.0.45	147.237.76.197	Italy	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.76.86	India	navy.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.77.179	United States	e.mazi.idf.il	ET DROP Dshield Block Listed Source	1
187.132.6.6	147.237.76.177	Mexico	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
183.3.202.115	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
162.250.125.26	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
128.127.0.45	147.237.76.197	Italy	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
115.28.218.77	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
46.19.85.208	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
176.13.1.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.180.53.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.131	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.131	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
89.139.137.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.67.3.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
46.19.85.138	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.135.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
88.253.1.211	Turkey	147.237.77.74	law.idf.il	drop	SAM rule	drop	5
176.13.17.135	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.139.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
91.200.12.7	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
91.200.12.136	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
37.26.146.225	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.136	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
91.200.12.7	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
91.200.12.136	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
91.200.12.7	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
91.200.12.141	Ukraine	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
5.102.195.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.200.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.228.177.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.110.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.60.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.88		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.225	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.80.154.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.210.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.228.179.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.186.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	170
109.67.3.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	158
109.65.39.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
109.253.136.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
213.57.200.23	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.57.200.23	Block	8
109.253.133.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
87.69.238.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.14.119	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.14.119	Block	3
2.54.14.119	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
87.68.78.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.57.180.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
131.253.25.179	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.146.225	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	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
85.64.222.252	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/registrationwizard/	Block	2
169.229.3.91	United States	147.237.72.156	aman.idf.il	Illegal Byte Code Character in URL	Block	1
46.19.86.44	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.i	Illegal Byte Code Character in URL	Block	1
108.30.243.178	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
207.46.13.98	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/contactus.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
5.28.156.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
119.63.142.14	Pakistan	147.237.77.74	law.idf.il	Parameter Type Violation pos in www.law.idf.il/163-6958-en/patzar.aspx	Block	1
50.19.40.148	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
173.252.114.116	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/sip_storage/files/5/1595.pdf&usg=afqjcnf7zcvav4-pkz0ll6iobdoy0tkjhw&sig2=7tfyww2e736-1dncb3zbca	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.i	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/klali	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
37.26.146.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.139.137.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
54.90.169.176	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/brothers/skira/default.asp	Block	1
173.252.122.119	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/sip_storage/files/5/1595.pdf&usg=afqjcnf7zcvav4-pkz0ll6iobdoy0tkjhw&sig2=7tfyww2e736-1dncb3zbca	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.i	NULL Character in URL	Block	1
2.52.51.60	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
213.57.200.23	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
82.166.148.177	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in Method	Block	1
157.55.39.40	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/unitfs.asp	Block	1
95.77.235.216	Romania	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
176.228.70.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/ ג'מלא'ם	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.i	Unknown HTTP Request Method â¿NÁ[[#29]]@±>••,Åç in URL	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Abnormally Long Request method	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
157.55.39.58	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	1
95.77.235.216	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.64.234	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1397-he/atal.aspx	Block	1

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