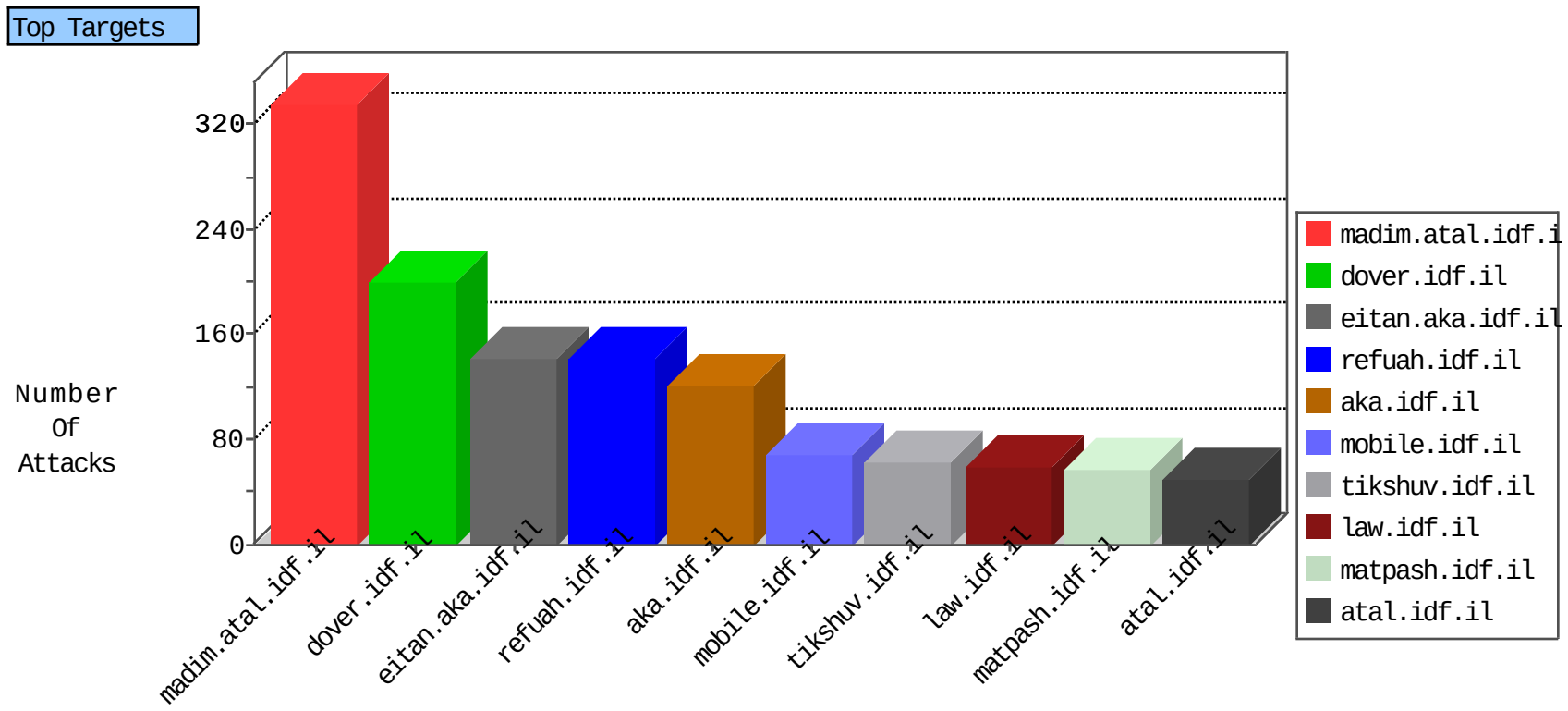
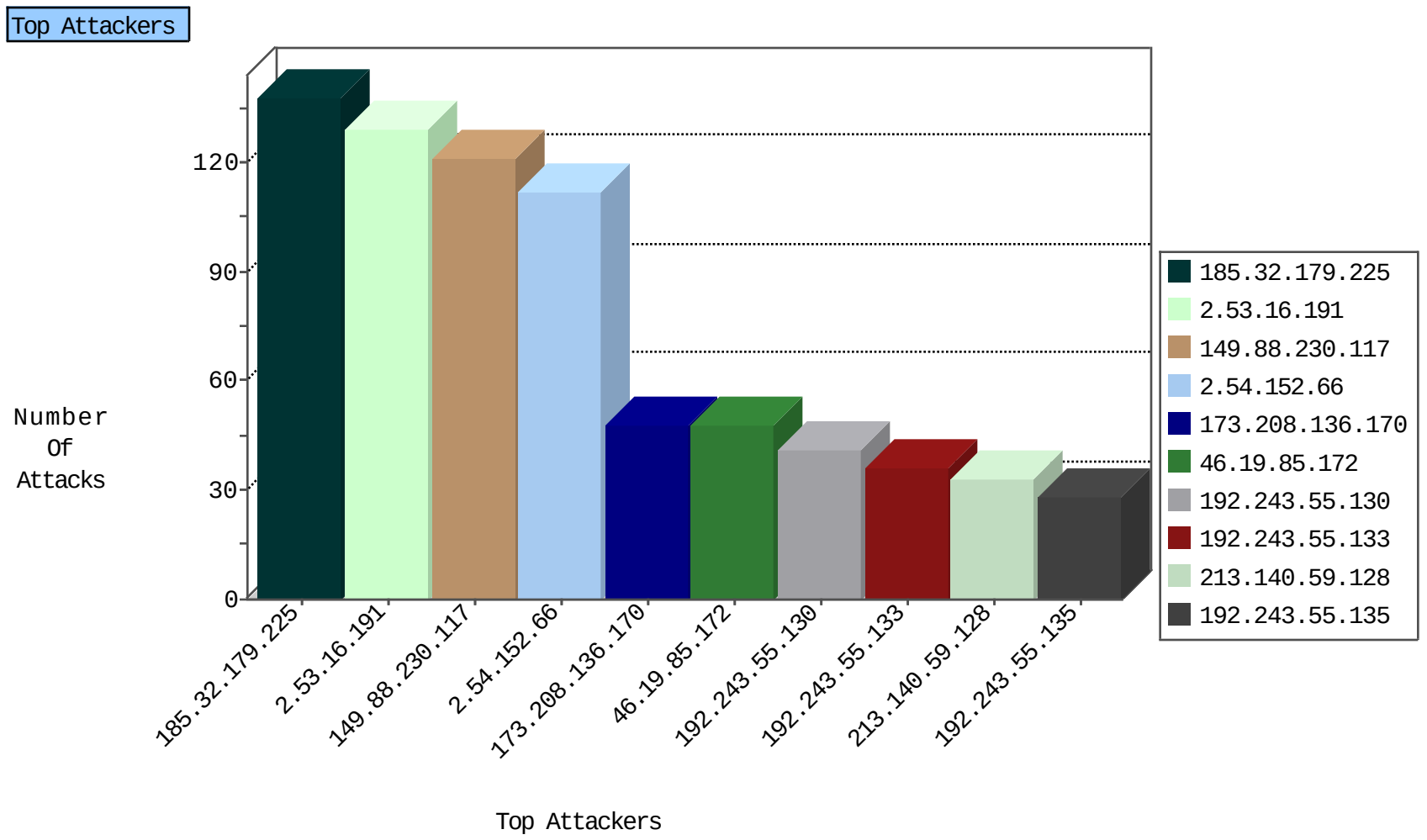
03-09-2016-23:04:03 to 03-10-2016-00:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-09-2016-23:04:03 to 03-10-2016-00:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
115.239.228.10	China	147.237.0.35	akaws.idf.il	JLM_Under_Attack_Con_Http	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
89.248.160.138	Netherlands	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
46.166.139.242	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
115.239.228.10	China	147.237.0.35	akaws.idf.il	JLM_Purple_Con_Limit_Http	drop	1
46.166.139.242	Netherlands	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

03-09-2016-23:04:03 to 03-10-2016-00:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.163	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.184	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	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-09-2016-23:04:03 to 03-10-2016-00:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.32.179.225	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
122.141.236.69	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
122.141.236.69	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	147.237.72.217	Turkey	e.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
218.246.0.97	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
209.198.1.250	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
202.117.3.104	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
122.141.236.69	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
122.141.236.69	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
209.198.1.250	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
202.117.3.104	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

03-09-2016-23:04:03 to 03-10-2016-00:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.16.191	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	129
149.88.230.117	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	120
46.19.85.120	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
141.0.14.18	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
66.249.93.121	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	21
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	18
2.52.141.242	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
176.13.4.102	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
213.140.59.128	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.19.85.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
141.0.15.44	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
66.249.93.125	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
85.104.183.230	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
94.159.167.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.140.59.128	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
203.13.128.104	Australia	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.140.59.128	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.176.24.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.140.59.128	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.39.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.176	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.130	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
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.176	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.136.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.130	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.159.101.251	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.135.110	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.208.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.189.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.151.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.132.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-09-2016-23:04:03 to 03-10-2016-00:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	132
2.54.152.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
46.19.85.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
173.208.136.170	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	Block	40
2.54.36.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
79.176.64.8	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.176.64.8	Block	12
46.19.86.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
173.208.136.170	United States	147.237.77.233	atal.idf.il	Multiple Admin Blocking from 173.208.136.170	Block	7
176.213.20.2	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
176.213.20.2	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.213.20.2	Block	5
37.142.68.1	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	4
37.142.68.1	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	4
2.54.151.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.1.172.206	Hungary	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
46.19.85.120	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	2
79.176.64.8	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
46.19.86.103	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
203.13.128.104	Australia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;t in www.eitan.aka.idf.il/scriptresource.axd	None	1
176.13.4.102	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/2/1682.doc	Block	1
24.217.39.157	United States	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	1
66.249.65.239	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
185.35.62.11	Switzerland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
149.88.230.117	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
203.13.128.104	Australia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;t in www.eitan.aka.idf.il/webresource.axd	None	1
24.217.39.157	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	Block	1
85.93.91.84	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.19.85.155	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/images/0108-	Block	1
173.208.136.170	United States	147.237.77.233	atal.idf.il	Admin Blocking	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69421.pdf	Block	1
92.80.242.3	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
203.13.128.104	Australia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;f in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
79.181.164.66	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
176.213.20.2	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
92.80.242.3	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9364-he/refuah.aspx	Block	1
203.13.128.104	Australia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;rnd in www.eitan.aka.idf.il/shared/ajax/createcaptchaimage.aspx	None	1
80.246.130.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.65.232	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
41.34.196.95	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/	Block	1
99.247.1.187	Canada	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
69.171.228.120	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-09-2016-23:04:03 to 03-10-2016-00:04:03