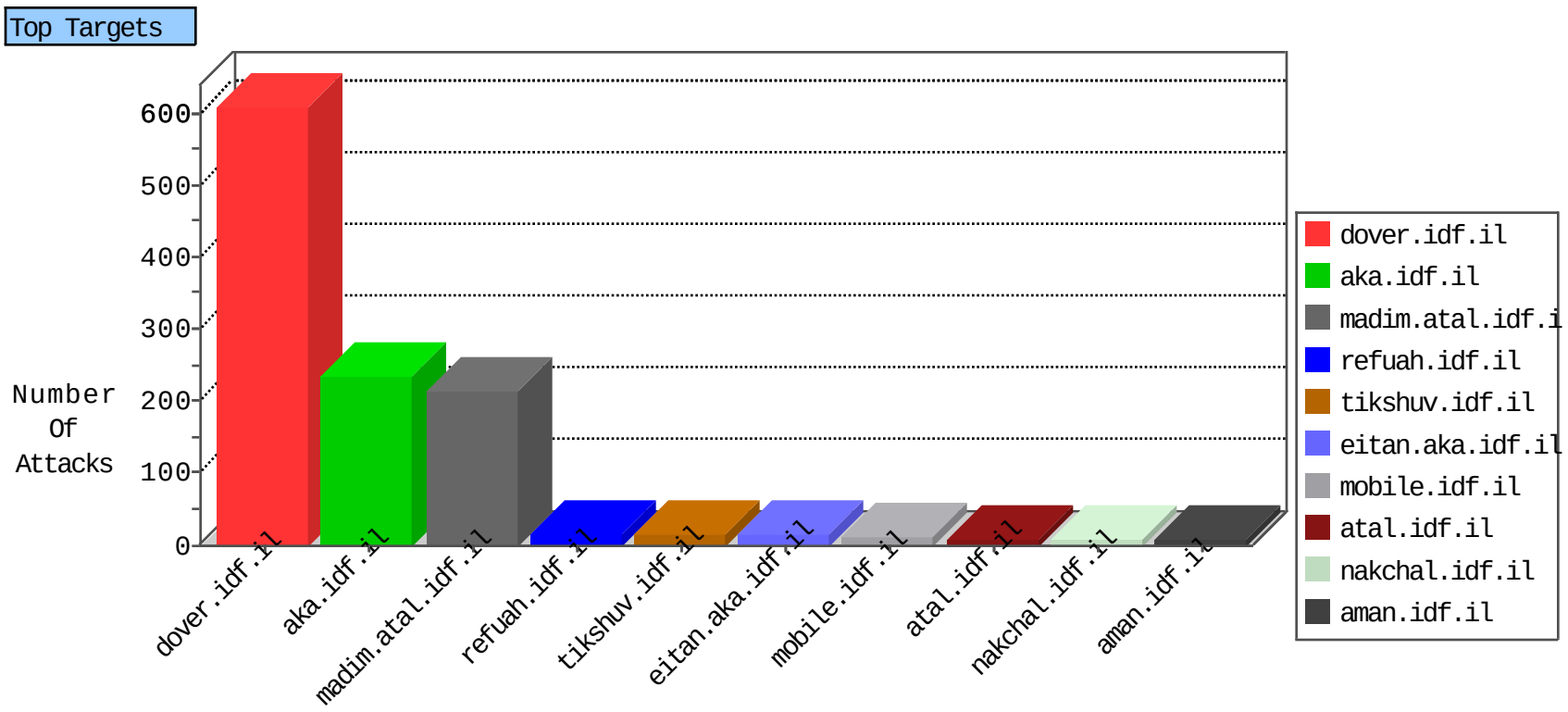
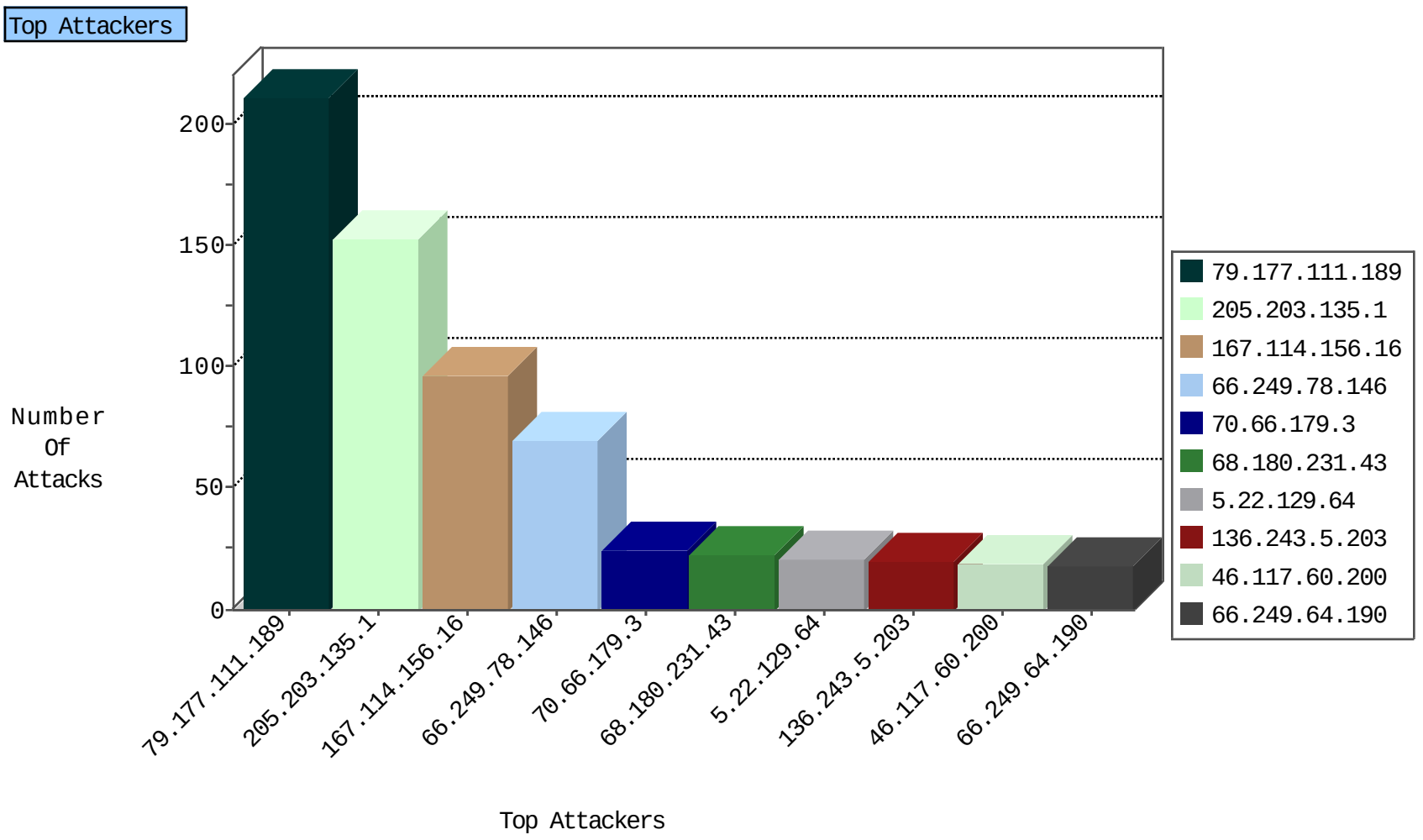
04-29-2016-09:04:03 to 04-29-2016-10:04:03

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-29-2016-09:04:03 to 04-29-2016-10:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4653
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1711
82.145.217.193	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
185.94.111.1	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

04-29-2016-09:04:03 to 04-29-2016-10:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-29-2016-09:04:03 to 04-29-2016-10:04:03

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
66.249.64.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.240.213.93	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.17.100.16	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
162.221.204.132	147.237.0.34	Canada	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
40.69.45.42	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
161.202.120.149	147.237.72.14	Japan	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.76.148	Turkey	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
104.219.238.10	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.193.74.175	147.237.0.19	Gibraltar	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
65.55.210.129	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.77.74	United Kingdom	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
40.69.45.42	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
162.221.204.132	147.237.0.34	Canada	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
114.215.150.44	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.76.148	Turkey	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
103.237.145.145	147.237.72.14	Vietnam	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
87.70.20.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.72.166	United States	aka.idf.il	ET DROP Dshield Block Listed Source	1

04-29-2016-09:04:03 to 04-29-2016-10:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
70.66.179.3	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
5.22.129.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.183.247.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
24.237.158.8	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.60.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.111.152.97	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
82.145.223.135	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.134.55.152	Finland	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
79.180.27.239	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
94.230.86.252	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
88.254.110.197	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.117.60.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.78	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.25.88	United States	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
89.119.251.40	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.7.230.13	Cyprus	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.8.142.34	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.60.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.66.70.104	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
77.126.168.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.206	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.214.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.60.200	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
66.249.64.170	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-29-2016-09:04:03 to 04-29-2016-10:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.111.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	211
199.30.24.222	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
65.55.210.255	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
199.30.24.7	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
185.5.223.73	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
65.55.210.129	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
125.212.193.90	Vietnam	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	2
199.30.24.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.97	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
31.223.176.30	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.183.247.101	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/size100x0/3395.jpg	Block	1
157.55.39.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19142-en/dover...the	Block	1
106.184.3.122	Japan	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Method	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/navmenu/	Block	1
217.66.237.223	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.14	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
182.50.142.89	Singapore	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 182.50.142.89	Block	1
125.212.193.90	Vietnam	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 125.212.193.90	Block	1
81.4.164.134	Cyprus	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.75.16	Block	1
5.29.150.207	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18907-en/dover.aspx <a href=	Block	1
106.184.3.122	Japan	147.237.76.200	eitan.aka.idf.il	NULL Character in Method	Block	1
74.82.47.3	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
182.50.142.89	Singapore	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
65.55.210.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
125.212.193.90	Vietnam	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/wp-login.php	Block	1
84.108.79.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.75.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/size100x0/2827.jpg	Block	1
31.192.254.110	Kyrgyzstan	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
164.132.161.34	Italy	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
109.64.185.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
144.76.90.230	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
85.65.244.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/shalishut/site/gallery.aspx	None	1
31.192.254.110	Kyrgyzstan	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
176.114.191.12	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/66846.ppt'a=0	Block	1
125.212.193.90	Vietnam	147.237.76.31	nakchal.idf.il	Admin Blocking	Block	1
79.180.9.149	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
195.234.4.207	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
149.78.84.162	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
94.230.86.12	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19667-he/idfgdover.aspx)	Block	1
182.50.142.89	Singapore	147.237.77.233	atal.idf.il	Admin Blocking	Block	1

04-29-2016-09:04:03 to 04-29-2016-10:04:03