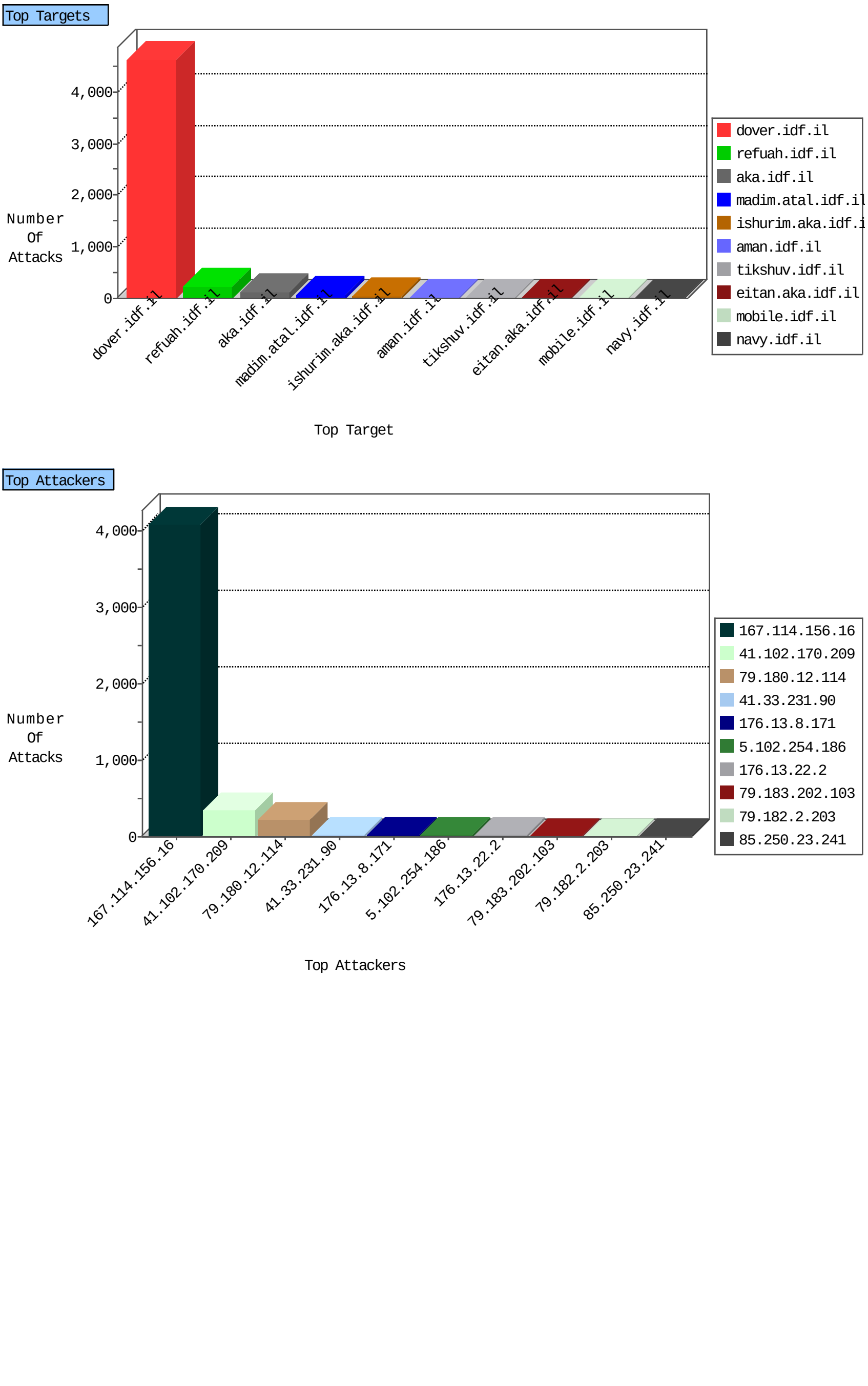
04-13-2016-21:04:08 to 04-13-2016-22:04:08

IDF Under Attack Daily Report



04-13-2016-21:04:08 to 04-13-2016-22:04:08

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	Block_Ip_Web_In	drop	4094
91.106.50.81	Iraq	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	1
185.94.111.1	Russian Federation	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

04-13-2016-21:04:08 to 04-13-2016-22:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.159.177.70	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
61.135.189.114	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
149.78.168.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.47	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
84.109.180.213	Israel	147.237.77.170	maarachot.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
111.202.102.65	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-13-2016-21:04:08 to 04-13-2016-22:04:08

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	3
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
91.106.50.81	147.237.77.216	Iraq	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	2
195.216.176.244	147.237.76.148	Latvia	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
116.202.34.89	147.237.77.216	India	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
95.110.228.55	147.237.72.166	Italy	aka.idf.il	Tehila - Perl LWP with fake user agent	1
91.106.50.81	147.237.77.216	Iraq	dover.idf.il	SQL 1 = 0 - possible sql injection attempt	1
88.204.187.90	147.237.8.24	Kazakstan	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
198.199.124.215	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.76.147	Latvia	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
189.199.172.21	147.237.0.33	Mexico	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.128.144.131	147.237.76.176	Canada	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
88.204.187.90	147.237.8.24	Kazakstan	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
87.69.197.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.65.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-13-2016-21:04:08 to 04-13-2016-22:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.102.170.209	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	347
79.180.12.114	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	223
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
176.13.8.171	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
80.246.138.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
185.32.179.233	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
46.120.22.123	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.41.94.147	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.253.222.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.8.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.149.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.86.122.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
149.88.55.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.78.50.61	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.120.230.191	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.129.255	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.186.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.158	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
85.65.212.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.29.209.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
149.78.234.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.30	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.102.254.63	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.134.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.184.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.144.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.130.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
5.22.135.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.185	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.2.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.27.187.130	Spain	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.120.126.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.152	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.237.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.53.186	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.177.94.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
24.173.91.18	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.22.130.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.182.2.203	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
66.102.8.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.182.2.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

04-13-2016-21:04:08 to 04-13-2016-22:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.22.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
79.183.202.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
5.102.254.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
85.250.23.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
207.46.13.72	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
91.106.50.81	Iraq	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.106.50.81	Block	4
80.246.136.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
188.163.78.47	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 188.163.78.47	Block	4
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.216	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
89.138.179.199	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
2.53.26.10	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.178.218.194	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Untraceable SSL Sessions from 79.178.218.194 (Protocol violation (SSL_CONN_CLIENT_FINISH_RESUMED_SESSION))	None	2
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.180.12.114	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.66.1	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/28032011masaiyot.aspx	Block	1
188.163.78.47	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
2.53.187.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
178.134.153.100	Georgia	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
95.86.125.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.177	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter PageNum in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
157.55.39.30	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam/main/procedure.asp	Block	1
79.178.218.194	Israel	147.237.72.167	ishurim.aka.idf.il	Abnormally Long Request method	Block	1
46.121.43.101	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.121.43.101	Block	1
178.134.153.100	Georgia	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
95.110.228.55	Italy	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il../wp-login.php	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
208.115.113.93	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.143	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
31.210.187.225	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
91.106.50.81	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/ and 1=1	Block	1
79.178.218.194	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Abnormally Long Request from 79.178.218.194	Block	1
46.121.43.101	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/kkkkkkk=40ee37adkkkkkkk_40ee37ad	Block	1
109.186.171.0	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.246.136.109	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
157.55.39.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
41.102.170.209	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.123.192.152	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
110.86.186.223	China	147.237.77.176	matpash.idf.il	Unauthorized HTTP Method	Block	1
2.53.34.168	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyuis	Block	1
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspxping	Block	1

04-13-2016-21:04:08 to 04-13-2016-22:04:08