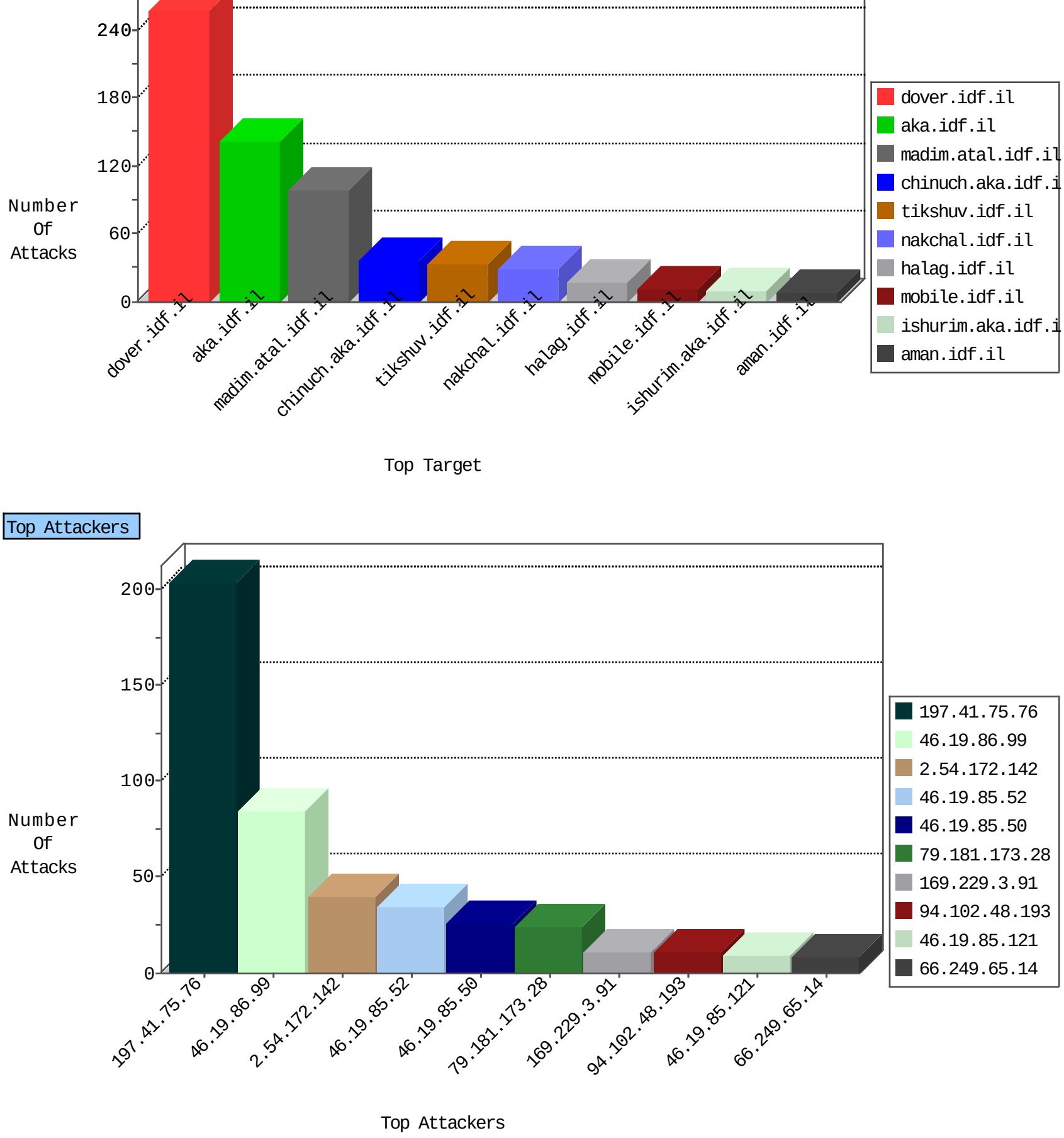
03-05-2016-10:04:04 to 03-05-2016-11:04:04

IDF Under Attack
Daily Report



03-05-2016-10:04:04 to 03-05-2016-11:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.41.75.76	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	204
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
134.147.203.115	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.132	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.102	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.74	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.122	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
179.43.141.238	Switzerland	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1
216.218.206.73	United States	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.110	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
184.105.139.74	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.82	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.110	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.78	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.90	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.118	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

03-05-2016-10:04:04 to 03-05-2016-11:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.107.7	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
37.26.149.188	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.67.43.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.67.151.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.253.212.132	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.119	Italy	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
157.55.39.145	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-05-2016-10:04:04 to 03-05-2016-11:04:04

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
66.249.65.14	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
104.128.144.131	147.237.76.197	Canada	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
95.130.13.220	147.237.76.34	France	yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
52.27.12.37	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
222.186.15.120	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
198.180.198.185	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
198.180.198.185	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -f -sS	1
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
95.130.13.220	147.237.76.38	France	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
95.130.13.220	147.237.76.34	France	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.15.120	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
41.41.29.238	147.237.72.167	Egypt	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
222.186.15.120	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
198.180.198.185	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 2048	1

03-05-2016-10:04:04 to 03-05-2016-11:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.172.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	39
46.19.85.52	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
46.19.85.50	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.181.173.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.186.172.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.121	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
83.130.127.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.65.14	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.41.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.32.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.79.68.161	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.120.126.4		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.129.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.28.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.138.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.156.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.218.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.189	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.161.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.160.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.147.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.219.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.17.33	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
172.56.6.79	United States	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.217.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.172.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
69.30.214.46	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
5.22.135.118	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
62.90.165.54	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.86.99	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.73.132	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
37.46.39.47	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.99	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
149.78.215.93	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
69.30.214.46	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	2
46.19.86.164	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.179.36.140	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
5.22.130.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.46.41.199	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.165.71	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
94.102.48.193	Netherlands	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.108	United States	147.237.76.34	yohalan.idf.il	drop		drop	1

03-05-2016-10:04:04 to 03-05-2016-11:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
46.19.86.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
79.177.2.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.119.122.177	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mazi/	Block	3
46.19.85.52	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
206.255.59.186	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
82.137.205.69	Syrian Arab Republic	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.165	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/faq/faq.aspx	Block	1
185.112.248.32		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
77.126.167.41	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1153-he/dover.aspx	Block	1
46.19.85.121	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Distributed NULL Character in Method	Block	1
84.108.186.33	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
66.249.66.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
192.115.130.253	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/112767.pdf	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
78.135.10.147	Turkey	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1380-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Abnormally Long Request method	Block	1
84.108.186.33	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
66.249.69.81	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1398-he/atal.aspx	Block	1
198.20.69.74	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in Method	Block	1
213.8.247.238	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Method	Block	1
94.64.80.199	Greece	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.125.76.16	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
206.255.59.186	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Abnormally Long Request	Block	1
79.179.36.140	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.23.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
77.125.76.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/xmlrpc.php	Block	1

03-05-2016-10:04:04 to 03-05-2016-11:04:04