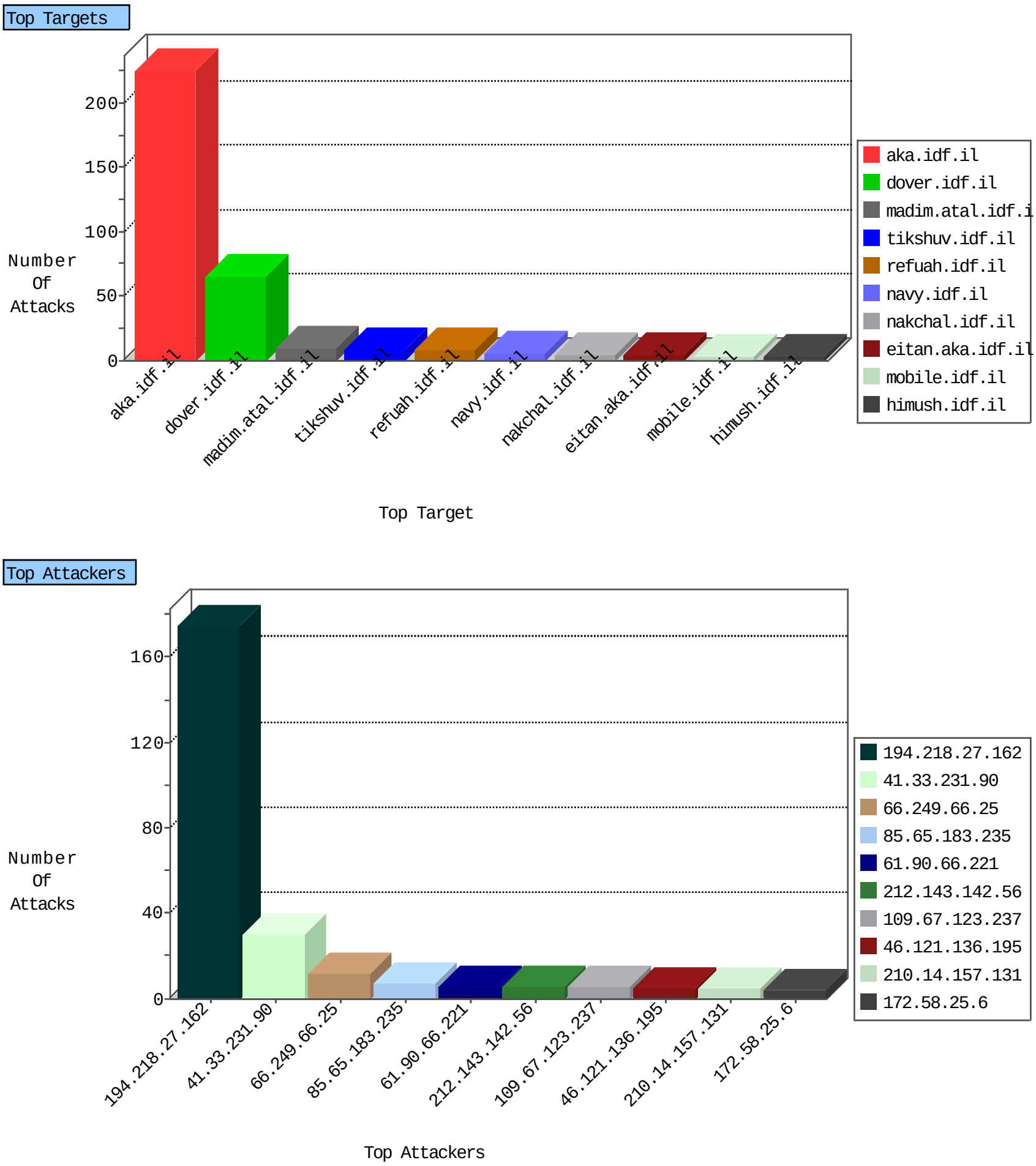
03-02-2016-05:04:06 to 03-02-2016-06:04:06

IDF Under Attack
Daily Report



03-02-2016-05:04:06 to 03-02-2016-06:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.94.111.1		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.96	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
164.132.54.194	Italy	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.112	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
59.126.151.156	Taiwan	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
216.60.132.15	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.100	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.120	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.88	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.54	United States	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.108	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.92	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
89.248.173.115	Netherlands	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.108	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
47.88.103.153	Canada	147.237.0.19	madim.atal.idf.il	block-sp-traf1	drop	1

03-02-2016-05:04:06 to 03-02-2016-06:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.150	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
151.80.31.151	Italy	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
151.80.31.153	Italy	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.154	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
188.165.15.209	France	147.237.77.176	matpash.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.152	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
207.46.13.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
151.80.31.152	Italy	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-02-2016-05:04:06 to 03-02-2016-06:04:06

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
189.254.90.133	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
113.76.90.199	147.237.76.30	China	himush.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
210.117.121.60	147.237.72.167	Korea, Republic of	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
98.119.105.221	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
210.14.157.131	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
210.14.157.131	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
210.14.157.131	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
189.254.90.133	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.221	147.237.76.42		refuah.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
210.117.121.60	147.237.72.167	Korea, Republic of	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.87.16.148	147.237.76.148		gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
210.14.157.131	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
210.14.157.131	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
189.254.90.133	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1

03-02-2016-05:04:06 to 03-02-2016-06:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	117
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	58
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
61.90.66.221	Thailand	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.123.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.102.6.143	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
172.58.25.6	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.12.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.124.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.12.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
120.59.175.36	India	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.180.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.225.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.90.246.233	United Kingdom	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
141.212.122.199	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.39	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.123	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.95	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
162.196.177.252	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
94.199.151.22	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.20.69.98	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.79.130.52	United Kingdom	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.200	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.43	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.123	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.200	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
171.16.0.120	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.8	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.98	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
183.60.149.203	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.205	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.90.244.30	United Kingdom	147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
218.22.211.69	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
47.88.103.153	Canada	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.228	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.8	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
184.105.139.74	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.206	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.90.244.30	United Kingdom	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
47.88.103.153	Canada	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.38	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.104	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.83	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

03-02-2016-05:04:06 to 03-02-2016-06:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	12
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.183.235	Block	6
46.121.136.195	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	5
31.154.94.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.140.125	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
176.9.61.55	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
46.120.182.240	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
184.105.139.70	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/m/modules/forums/forum.aspx	Block	1
184.105.247.196	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9186-he/refuah.aspx	Block	1
113.76.90.199	China	147.237.76.30	himush.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
54.213.177.200	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in Method	Block	1
184.168.46.66	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
17.138.56.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/templates/www.behazdaa.org.il	Block	1
54.213.177.200	United States	147.237.77.19	law-forum.idf.il	NULL Character in Method	Block	1
185.106.104.242		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1

03-02-2016-05:04:06 to 03-02-2016-06:04:06