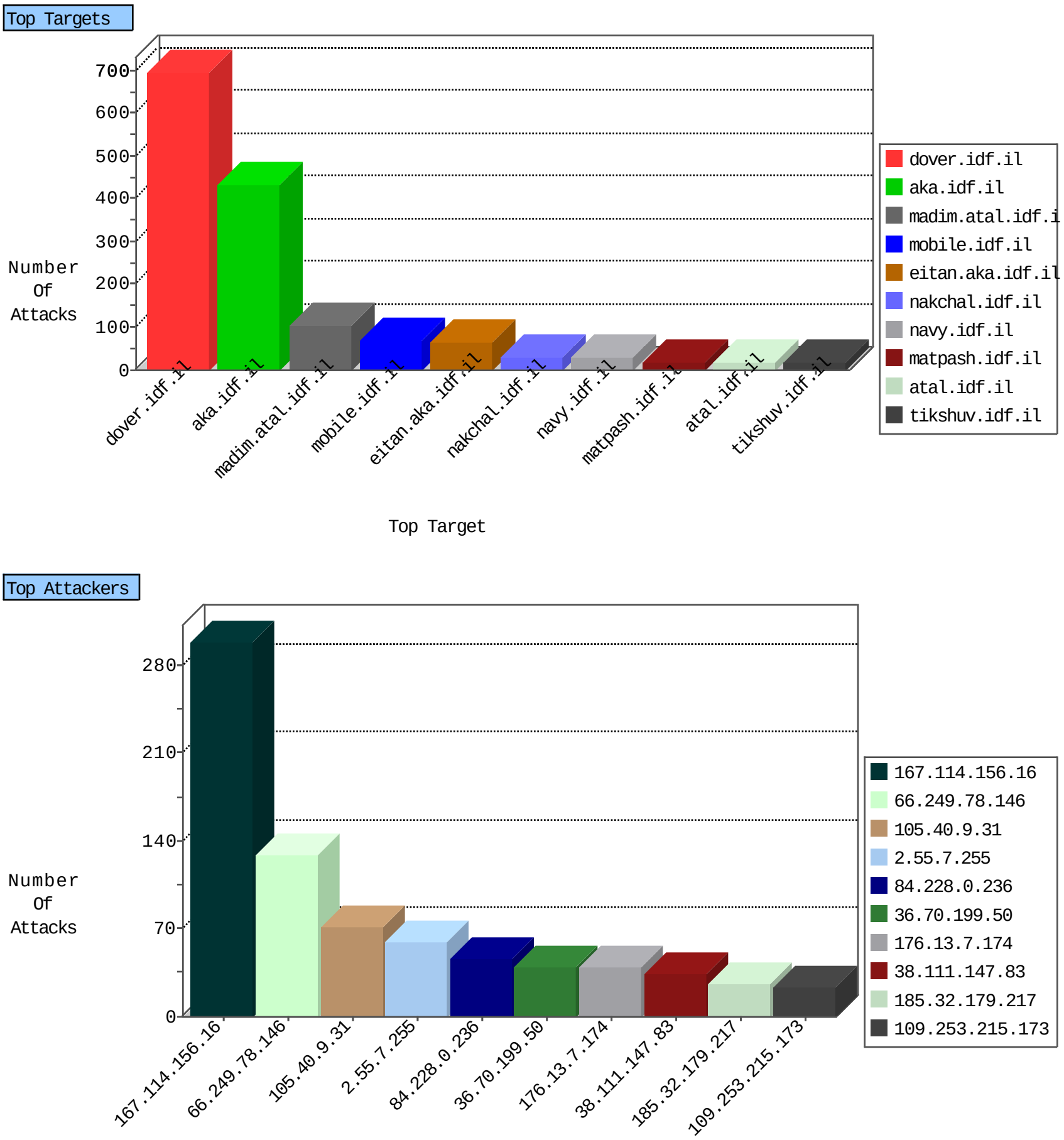
04-27-2016-13:04:08 to 04-27-2016-14:04:08

IDF Under Attack Daily Report



04-27-2016-13:04:08 to 04-27-2016-14:04:08

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	HTTP-POST-Segmented-DoS	dest-reset	11024
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1841
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
31.168.225.146	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
84.108.216.83	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	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
89.46.102.242	Romania	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
5.102.222.157	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
89.46.102.242	Romania	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
89.46.102.242	Romania	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1

04-27-2016-13:04:08 to 04-27-2016-14:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
103.21.58.191	India	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
94.245.88.135	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2

04-27-2016-13:04:08 to 04-27-2016-14:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
103.21.58.191	147.237.72.166	India	aka.idf.il	SQL Injection - Select From	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
94.245.88.135	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	4
66.249.81.218	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	2
106.186.113.132	147.237.77.235	Japan	sviva.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.66.17	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
89.248.167.131	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
200.195.135.82	147.237.77.226	Brazil	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
89.248.167.131	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.167.131	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.167.131	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
63.221.141.195	147.237.72.217	United States	e.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
13.92.245.177	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
89.248.167.131	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	1
13.92.245.177	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -f -sS	1
89.248.167.131	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
2.53.157.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.167.131	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
89.248.167.131	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.78.38	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
13.92.245.177	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
5.102.200.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-27-2016-13:04:08 to 04-27-2016-14:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	129
105.40.9.31	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
84.228.0.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
36.70.199.50	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
38.111.147.83	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
176.13.7.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.253.215.173	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.53.7.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
1.129.96.141	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
176.6.121.242	Germany	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.179.155.129	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
80.246.130.235	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
188.54.129.99	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.253.211.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.46.41.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.121.84.185	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
46.121.84.185	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	11
185.32.179.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.213.149.147	Syrian Arab Republic	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.196.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
207.46.13.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.32.179.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
109.65.188.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
149.78.109.209	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.177.62.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.177.62.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
109.253.135.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.202.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.177	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
176.13.7.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.108.14.80	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.147.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.180.22.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
149.78.109.209	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.32.179.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
80.246.139.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.177.103.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

04-27-2016-13:04:08 to 04-27-2016-14:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.7.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
176.13.18.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
2.53.137.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
85.65.62.30	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 85.65.62.30	Block	5
87.70.108.179	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	3
79.178.202.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.64.119.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.102.6.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
38.111.147.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.9.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.102.6.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.196.74	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.211.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.178.20.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
188.225.147.164	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1
106.186.113.132	Japan	147.237.77.235	sviva.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
5.29.193.128	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl59 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
82.80.134.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Malformed URL	Block	1
46.121.84.185	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
149.50.31.55	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
207.46.13.108	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112435.pdf).	Block	1
66.249.64.186	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
84.228.41.192	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Unknown HTTP Request Method ™,¯«[[#11]][[#20]][[#25]]Î[[#18]]7RUfÓPT¥waÎ[[#19]]Žm•K[[#17]]‘¸#012ó[[#14]]ÁY^W3õ›åIjé[[#17]]z in URL	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in Method	Block	1
105.40.9.31	Egypt	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
79.178.224.74	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.199.154.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/scrollpanebottom.gif	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Abnormally Long Request method	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
109.253.135.21	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
38.111.147.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
105.40.9.31	Egypt	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$txtSearch in www.idf.il/1283-en/dover.aspx	Block	1
80.246.130.235	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
46.19.86.96	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
85.65.62.30	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/homepage/mobile	Block	1
79.177.18.143	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl57 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
106.186.113.132	Japan	147.237.77.235	sviva.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1

04-27-2016-13:04:08 to 04-27-2016-14:04:08